



Technische Details

- [Netzwerkprotokolle](#), auf Seite 1
- [VLAN-Interaktion](#), auf Seite 5
- [Informationen zum USB-Port](#), auf Seite 6
- [SIP- und NAT-Konfiguration](#), auf Seite 7
- [CDP \(Cisco Discovery Protocol\)](#), on page 13
- [LLDP-MED](#), on page 14
- [Auflösung der Netzwerkrichlinie und QoS](#), auf Seite 19

Netzwerkprotokolle

Die Cisco IP-Telefon 8800-Serie unterstützt verschiedene eigene und Industriestandard-konforme Netzwerkprotokolle, die für die Sprachkommunikation benötigt werden. Die folgende Tabelle enthält eine Übersicht der von den Telefonen unterstützten Netzwerkprotokolle.

Tabelle 1: Von der Cisco IP-Telefon 8800-Serie unterstützte Netzwerkprotokolle

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Bluetooth	Bluetooth ist ein Kurzstrecken-Funkprotokoll (WPAN-Protokoll), das die Kommunikation zwischen Geräten über kurze Distanzen regelt.	Telefone des Typs Cisco IP-Telefon 8845, 8865 und 8851 unterstützen Bluetooth 4.1. Cisco IP-Telefon 8861 unterstützt Bluetooth 4.0. Cisco IP-Telefon 8811 und 8841 unterstützen kein Bluetooth.
Bootstrap Protocol (BootP)	Mit BootP kann ein Netzwerkgerät, beispielsweise Cisco IP-Telefon, bestimmte Startinformationen (z. B. die IP-Adresse) abfragen.	—

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Cisco Discovery Protocol (CDP)	<p>CDP ist ein Protokoll für die Geräteerkennung, das auf allen Geräten von Cisco ausgeführt wird.</p> <p>Mithilfe von CDP kann sich ein Gerät innerhalb des Netzwerks für andere Geräte erkennbar machen und Informationen über andere Geräte empfangen.</p>	Cisco IP-Telefons nutzen CDP für die Übertragung von Informationen, wie beispielsweise Zusatz-VLAN-ID, Energiemanagementdaten einzelner Ports oder Konfigurationsinformationen zur Quality of Service (QoS), an den Cisco Catalyst-Switch.
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP reserviert und weist IP-Adressen zu Netzwerkgeräten zu.</p> <p>DHCP ermöglicht das Einbinden eines IP-Telefons in ein Netzwerk, wobei das Telefon anschließend betriebsbereit ist, ohne dass manuell eine IP-Adresse zugewiesen oder zusätzliche Netzwerkparameter konfiguriert werden müssen.</p>	<p>DHCP ist standardmäßig aktiviert. Wenn DHCP deaktiviert ist, muss das Konfigurieren von IP-Adresse, Subnetzmaske und Gateway manuell und direkt auf jedem einzelnen Telefon vorgenommen werden.</p> <p>Hinweis Der Parameter Zu verwendende DHCP-Option hat 66,160,159,150,60,43,125 als Standardwert. Dieser Wert gibt die Reihenfolge an, in der das Telefon die vom DHCP-Server bereitgestellte IP-Adresse verwendet.</p>
Hypertext Transfer Protocol (HTTP)	HTTP ist das Standardprotokoll zum Übertragen von Informationen und Dokumenten im Internet und dem Web.	Cisco IP-Telefone verwenden das HTTP-Protokoll für XML-Dienste, zur Bereitstellung und Aktualisierung des Telefons sowie zu Fehlerbehebungszwecken.
Hypertext Transfer Protocol Secure (HTTPS)	HTTPS ist eine Kombination der Übertragungsprotokolle HTTP und SSL/TLS, die eine Verschlüsselung und sichere Identifizierung von Servern ermöglicht.	Einige Webanwendungen unterstützen HTTP- und HTTPS-Protokolle. Cisco IP-Telefone, die HTTPS unterstützen, verwenden die HTTPS-URL.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
IEEE 802.1X	<p>Der Standard IEEE 802.1X definiert ein Protokoll zur Client-Server-basierten Zugriffskontrolle und Authentifizierung, das dafür sorgt, dass sich ausschließlich autorisierte Clients über öffentlich zugängliche Ports mit einem LAN verbinden können.</p> <p>Bis der Client authentifiziert ist, erlaubt die 802.1X-Zugriffssteuerung nur den EAPOL-Verkehr (Extensible Authentication Protocol over LAN) über den Port, mit dem der Client verbunden ist. Nach der erfolgreichen Authentifizierung kann der normale Verkehr über den Port weitergeleitet werden.</p>	<p>Die Implementierung des Standards IEEE 802.1X erfolgt auf dem Cisco IP-Telefon durch Unterstützung der Authentifizierungsmethoden EAP-FAST und EAP-TLS.</p> <p>Wenn auf dem Telefon die 802.1X-Authentifizierung aktiviert ist, sollten Sie das PC-Port- und Sprach-VLAN deaktivieren.</p>
IEEE 802.11n/802.11ac	<p>Der Standard IEEE 802.11 regelt die Kommunikation von Geräten in einem lokalen Funknetzwerk (WLAN).</p> <p>Teilstandard 802.11n arbeitet sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzbereich, während 802.11ac nur für den 5-GHz-Frequenzbereich zuständig ist.</p>	<p>Die 802.11-Schnittstelle ist insbesondere in Situationen, in denen keine Ethernet-Verkabelung zur Verfügung steht bzw. eingesetzt werden soll, eine geeignete Bereitstellungsalternative.</p> <p>Nur Cisco IP-Telefon 8861 und 8865 unterstützen WLAN.</p>
Internet Protocol (IP)	<p>IP ist ein Messaging-Protokoll, das Pakete im Netzwerk verarbeitet und sendet.</p>	<p>Damit Netzwerkgeräte mittels IP kommunizieren können, müssen ihnen eine IP-Adresse, ein Subnetz und ein Gateway zugewiesen sein.</p> <p>Wenn Sie für Cisco IP-Telefon DHCP (Dynamic Host Configuration Protocol) nutzen, erfolgt die Zuweisung von IP-Adresse, Subnetz und Gateway automatisch. Wenn Sie DHCP nicht verwenden, müssen Sie diese Eigenschaften jedem Telefon manuell zuweisen.</p>
Link Layer Discovery Protocol (LLDP)	<p>LLDP ist ein standardisiertes Netzwerkerkennungsprotokoll (ähnlich wie CDP), das auf einigen Geräten von Cisco und Drittanbietern unterstützt wird.</p>	<p>Das Cisco IP-Telefon unterstützt LLDP auf dem PC-Port.</p>

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED ist eine Erweiterung des LLDP-Standards speziell für Produkte zur Sprachübertragung.	Das Cisco IP-Telefon unterstützt LLDP-MED auf dem SW-Port, um folgende Informationen weiterzugeben: <ul style="list-style-type: none"> • Sprach-VLAN-Konfiguration • Geräteerkennung • Energieverwaltung • Bestandsverwaltung Weitere Informationen zur Unterstützung von LLDP-MED können Sie dem „Whitepaper LLDP-MED and Cisco Discovery Protocol“ (LLDP-MED und das Cisco Discovery Protocol) entnehmen, das unter folgender Adresse abrufbar ist: http://www.cisco.com/1/153/0/15304/whp/00_00_04_01.html
Real-Time Transport Protocol (RTP)	RTP ist ein Protokoll zur Übertragung von Echtzeitdaten (z. B. interaktive Sprachübertragung) in Datennetzwerken.	Cisco IP-Telefons verwenden das RTP-Protokoll, um Echtzeit-Sprachverkehr zu senden und von anderen Telefonen und Gateways zu empfangen.
Real-Time Control Protocol (RTCP)	RTCP wird gemeinsam mit RTP genutzt und liefert QoS-Daten (z. B. Jitter-Werte, Latenz, Round-Trip-Verzögerung) von RTP-Datenströmen.	RTCP ist standardmäßig deaktiviert.
Session Description Protocol (SDP)	Bei SDP handelt es sich um den Teil des SIP-Protokolls, der festlegt, welche Parameter während einer Verbindung zwischen zwei Endgeräten verfügbar sind. Beim Erstellen von Konferenzen werden nur die SDP-Funktionen verwendet, die von allen an der Konferenz teilnehmenden Endgeräten unterstützt werden.	Normalerweise werden SDP-Funktionen wie Codec-Typen, DTMF-Erkennung oder Komfortauschen von der Drittanbieter-Anrufsteuerung oder dem Medien-Gateway im laufenden Betrieb global konfiguriert. Bei manchen SIP-Endgeräten können diese Parameter jedoch direkt auf dem Endgerät konfiguriert werden.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Session Initiation Protocol (SIP)	SIP ist der IETF-Standard (Internet Engineering Task Force) für Multimedia-Konferenzen über IP. SIP ist ein ASCII-basiertes Steuerungsprotokoll auf Anwendungsebene (definiert in RFC 3261), das verwendet werden kann, um Anrufe zwischen zwei oder mehr Endpunkten zu initiieren, aufrechtzuerhalten und abbrechen.	SIP ist wie andere VoIP-Protokolle für die Funktionen des Signalübertragungs- und Sitzungsmanagements innerhalb eines Netzwerks für paketbasierte Telefonie zuständig. Mittels Signalübertragung können Anrufinformationen über Netzwerkgrenzen hinweg transportiert werden, während das Sitzungsmanagement die Steuerung der Attribute eines End-to-End-Anrufs ermöglicht. Cisco IP-Telefons unterstützen das SIP-Protokoll sowohl beim Betrieb im reinen IPv6-Modus und im reinen IPv4-Modus wie auch im kombinierten IPv4/IPv6-Modus.
Transmission Control Protocol (TCP)	TCP ist ein verbindungsorientiertes Transportprotokoll.	Cisco IP-Telefons nutzen TCP für die Verbindung mit der Drittanbieter-Anrufsteuerung sowie für den Zugriff auf XML-Dienste.
Transport Layer Security (TLS)	TLS ist ein Standardprotokoll zum Schützen und Authentifizieren der Kommunikation.	Wenn entsprechende Sicherheitseinstellungen konfiguriert sind, verwenden Cisco IP-Telefons das TLS-Protokoll zum sicheren Registrieren bei der Drittanbieter-Anrufsteuerung.
Trivial File Transfer Protocol (TFTP)	TFTP ermöglicht die Dateiübertragung über das Netzwerk. Auf dem Cisco IP-Telefon ermöglicht TFTP das Abrufen einer für den Telefentyp spezifischen Konfigurationsdatei.	Für TFTP muss im Netzwerk ein TFTP-Server vorhanden sein, den der DHCP-Server automatisch identifizieren kann.
User Datagram Protocol (UDP)	UDP ist ein verbindungsloses Protokoll für die Übertragung von Datenpaketen.	Dieses Protokoll wird ausschließlich für RTP-Datenströme verwendet. Von der SIP-Signalübertragung der Telefone wird UDP nicht unterstützt.

VLAN-Interaktion

Das Cisco IP-Telefon enthält einen internen Ethernet-Switch, über den Pakete an das Telefon, an den Computerport und an den Netzwerkport auf der Rückseite des Telefons weitergeleitet werden können.

Wenn ein Computer an den Computerport angeschlossen ist, verwenden der Computer und das Telefon dieselbe physische Verbindung mit dem Switch und denselben Port am Switch. Dies wirkt sich folgendermaßen auf die VLAN-Konfiguration im Netzwerk aus:

- Die derzeit vorhandenen VLANs können auf IP-Subnetz-Basis konfiguriert werden. Möglicherweise sind jedoch keine zusätzlichen IP-Adressen verfügbar, die dem Telefon im gleichen Subnetz wie andere Geräte, die sich mit dem gleichen Port verbinden, zugewiesen werden können.
- Durch den bei Telefonen mit VLAN-Unterstützung vorhandenen Datenverkehr wird möglicherweise die Qualität des VoIP-Datenverkehrs verringert.
- Die Netzwerksicherheit meldet möglicherweise einen Bedarf zur Trennung des VLAN-Sprachdatenverkehrs vom VLAN-Datenverkehr.

Diese Probleme können Sie lösen, indem Sie den Sprachdatenverkehr in ein separates VLAN verlegen. Der Switch-Port, an den das Telefon angeschlossen ist, wird für separate VLANs für Folgendes konfiguriert:

- Weiterleitung des Sprachdatenverkehrs zum und vom IP-Telefon (zusätzliches VLAN z. B. in der Cisco Catalyst 6000-Serie)
- Datenverkehr zum und vom PC, der über den Computerport des IP-Telefons an den Switch angeschlossen ist (systemeigenes VLAN)

Durch die Verlegung der Telefone in ein separates, zusätzliches VLAN wird die Qualität des Sprachdatenverkehrs verbessert, und Sie können eine große Anzahl von Telefonen zu einem bestehenden Netzwerk hinzufügen, das eigentlich nicht genügend IP-Adressen für alle Telefone besitzt.

Weitere Informationen finden Sie in der Dokumentation für den Cisco Switch. Außerdem finden Sie Informationen zu Switches unter folgender URL:

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

Informationen zum USB-Port

Cisco IP-Telefone 8851, 8861 und 8865 unterstützen maximal fünf Geräte, die an den einzelnen USB-Ports angeschlossen sind. Jedes an das Telefon angeschlossene Gerät wird bei der Anzahl der maximal zulässigen Geräte berücksichtigt. Ihr Telefon kann beispielsweise am seitlichen Anschluss fünf USB-Geräte und am hinteren Anschluss fünf zusätzliche USB-Standardgeräte unterstützen. Viele USB-Produkte von Drittherstellern zählen jedoch als mehrere USB-Geräte, beispielsweise kann ein Gerät, das einen USB-Hub und ein Headset enthält, als zwei USB-Geräte zählen. Weitere Informationen hierzu finden Sie in der Dokumentation für das jeweilige USB-Gerät.



Hinweis

- Hubs ohne Stromversorgung werden nicht unterstützt; Hubs mit Stromversorgung mit mehr als vier Ports werden ebenfalls nicht unterstützt.
- USB-Headsets, die über einen USB-Hub an das Telefon angeschlossen sind, werden nicht unterstützt.

Jedes an das Telefon angeschlossene Erweiterungsmodul wird als USB-Gerät gezählt. Wenn drei Tastenerweiterungsmodule an das Telefon angeschlossen sind, zählen diese als drei USB-Geräte.

USB-Port deaktivieren

Wenn Sie nicht zulassen, dass Benutzer einen oder alle USB-Ports für bestimmte Zwecke verwenden dürfen, können Sie die Rückseite oder die Seite oder beide USB-Ports des Telefons deaktivieren. Der deaktivierte

USB-Port bietet keine Funktion. Zum Beispiel werden das USB-Headset und das Tastenerweiterungsmodul (Key Expansion Module, KEM) nicht erkannt. Außerdem wird kein verbundenes Gerät geladen.

Das Cisco IP-Telefon 8851 enthält nur einen USB-Port, den seitlichen USB-Port. Die Cisco IP-Telefone 8861 und 8865 enthalten zwei USB-Ports, einen seitlichen USB-Port und einen hinteren USB-Port.

Vorbereitungen

Greifen Sie auf die Webseite zur Telefonverwaltung zu. Siehe [Auf Weboberfläche des Telefons zugreifen](#).

Prozedur

-
- Schritt 1** Wählen Sie **Sprache > System** aus.
- Schritt 2** Legen Sie unter dem Abschnitt **Energieeinstellungen** den Parameter **Hinteren USB-Port deaktivieren** auf **Ja** fest, um den hinteren USB-Port zu deaktivieren.
- Sie können diesen Parameter in der XML-Konfigurationsdatei (cfg.xml) des Telefons konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:
- ```
<Disable_Back_USB_Port ua="na">No</Disable_Back_USB_Port>
```
- Optionen: Ja und Nein
- Standard: Nein
- Schritt 3** Legen Sie unter dem Abschnitt **Energieeinstellungen** den Parameter **Seitlichen USB-Port deaktivieren** auf **Ja** fest, um den seitlichen USB-Port zu deaktivieren.
- Sie können diesen Parameter in der XML-Konfigurationsdatei (cfg.xml) des Telefons konfigurieren, indem Sie eine Zeichenfolge in folgendem Format eingeben:
- ```
<Disable_Side_USB_Port ua="na">No</Disable_Side_USB_Port>
```
- Optionen: Ja und Nein
- Standard: Nein
- Schritt 4** Klicken Sie auf **Submit All Changes**.
-

SIP- und NAT-Konfiguration

SIP und das Cisco IP-Telefon

Das Cisco IP-Telefon verwendet SIP (Session Initiation Protocol), um die Interoperabilität mit allen IT-Serviceanbietern, die SIP unterstützen, zu ermöglichen. SIP ist ein IETF-definiertes Signalisierungsprotokoll, das die Sprachkommunikation in einem IP-Netzwerk steuert.

SIP verarbeitet die Signalisierung und Sitzungsverwaltung in einem Pakettelefonienetzwerk. Die *Signalisierung* ermöglicht, dass Anrufinformationen netzwerkübergreifend übermittelt werden. Die *Sitzungsverwaltung* steuert die Attribute eines durchgehenden Anrufs.

In einer typischen kommerziellen IP-Telefoniebereitstellung werden alle Anrufe über einen SIP-Proxyserver geleitet. Das empfangende Telefon wird als SIP UAS (User Agent Server) bezeichnet und das anfordernde Telefon als UAC (User Agent Client).

Das SIP-Nachrichtenrouting ist dynamisch. Wenn ein SIP-Proxy eine Verbindungsanforderung von einem UAS empfängt, aber den UAC nicht ermitteln kann, leitet der Proxy die Nachricht an einen anderen SIP-Proxy im Netzwerk weiter. Wenn der UAC gefunden wird, wird die Antwort zurück an den UAS geleitet und die beiden UAs werden über eine direkte Peer-zu-Peer-Sitzung verbunden. Der Sprachverkehr wird über dynamisch zugeordnete Ports mit RTP (Real-time Protocol) zwischen den UAs übertragen.

RTP überträgt Echtzeit-Daten, beispielsweise Audio und Video, aber garantiert die Echtzeit-Zustellung der Daten nicht. RTP stellt Methoden für sendende und empfangende Anwendungen bereit, um Streaming-Daten zu unterstützen. RTP wird normalerweise über UDP ausgeführt.

SIP über TCP

Um die statusorientierte Kommunikation zu garantieren, kann das Cisco IP-Telefon TCP als Transportprotokoll für SIP verwenden. Dieses Protokoll *garantiert die Zustellung*, um sicherzustellen, dass verlorene Pakete erneut übertragen werden. Zudem entspricht bei TCP die Reihenfolge, in der die SIP-Pakete empfangen werden, immer der Sendereihenfolge.

TCP behebt das Problem durch Firmen-Firewalls blockierter UDP-Ports. Mit TCP müssen keine neuen Ports geöffnet oder Pakete verworfen werden, da TCP bereits für Standardaktivitäten wie Internet-Browsing oder E-Commerce verwendet wird.

SIP-Proxy-Redundanz

Ein durchschnittlicher SIP-Proxyserver kann Zehntausende von Teilnehmern verarbeiten. Eine Reserveserver ermöglicht, dass ein aktiver Server für Wartungszwecke vorübergehend außer Betrieb genommen wird. Das Telefon unterstützt die Verwendung von Backup-Servern, um die Serviceunterbrechung zu minimieren oder zu verhindern.

Eine einfache Methode, um die Proxyredundanz zu unterstützen, ist das Festlegen eines SIP-Proxyservers im Telefonkonfigurationsprofil. Das Telefon sendet eine DNS-NAPTR- oder SRV-Abfrage an den DNS-Server. Wenn konfiguriert, gibt der DNS-Server SRV-Einträge zurück, in denen die Server in der Domäne mit Hostnamen, Priorität, Listening-Ports usw. aufgelistet sind. Das Telefon versucht, die Server in der Reihenfolge ihrer Priorität zu kontaktieren. Server mit einer niedrigeren Nummer haben eine höhere Priorität. In einer Abfrage werden bis zu sechs NAPTR-Einträge und zwölf SRV-Einträge unterstützt.

Wenn die Kommunikation des Telefons mit dem primären Server scheitert, kann das Telefon einen Failover auf einen Server mit niedrigerer Priorität durchführen. Wenn konfiguriert, kann das Telefon die Verbindung mit dem primären Server wiederherstellen. Die Failover- und Failback-Unterstützung wechselt zwischen Servern mit unterschiedlichen SIP-Transportprotokollen. Das Telefon führt während eines aktiven Anrufs keinen Failback auf den primären Server durch, sondern wartet, bis der Anruf beendet ist und die Failback-Bedingungen erfüllt sind.

Beispiel für Ressourceneinträge vom DNS-Server

```
aslbsoft      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

```

Das folgende Beispiel zeigt die Priorität der Server aus der Perspektive des Telefons.

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

Das Telefon sendet immer SIP-Nachrichten an die in der Liste verfügbare Adresse mit der höchsten Priorität und mit dem Status „UP“. Im Beispiel sendet das Telefon alle SIP-Nachrichten an die Adresse 1.1.1.1. Wenn die Adresse 1.1.1.1 in der Liste mit dem Status „DOWN“ gekennzeichnet ist, kommuniziert das Telefon stattdessen mit 2.2.2.2. Das Telefon kann die Verbindung zu 1.1.1.1 wiederherstellen, wenn die angegebenen Failback-Bedingungen erfüllt sind. Weitere Informationen zu Failover und Failback finden Sie unter [SIP-Proxy-Failover, auf Seite 9](#) und [SIP-Proxy-Fallback, auf Seite 10](#).

SIP-Proxy-Failover

Das Telefon führt in jedem der folgenden Fälle einen Failover durch:

- Das Telefon sendet SIP-Nachrichten und erhält keine Antwort vom Server.
- Der Server antwortet mit einem Code, der mit dem in **Try Backup RSC** angegebenen Code übereinstimmt.
- Das Telefon erhält eine Aufforderung zur TCP-Trennung.

Es wird dringend empfohlen, **Automatische Registrierung bei Failover** auf **Ja** festzulegen, falls **SIP-Transport** auf **Automatisch** festgelegt ist.

Sie können diese durchwahlspezifischen Parameter auch in der Konfigurationsdatei konfigurieren:

```

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

```

wobei *n* die Durchwahlnummer ist.

Failover-Verhalten des Telefons

Wenn das Telefon nicht mit dem aktuell verbundenen Server kommuniziert, wird der Serverlistenstatus aktualisiert. Der nicht verfügbare Server ist in der Serverliste mit dem Status „DOWN“ gekennzeichnet. Das Telefon versucht, eine Verbindung mit dem Server mit der höchsten Priorität in der Liste herzustellen, dessen Status „UP“ lautet.

Im folgenden Beispiel sind die Adressen 1.1.1.1 und 2.2.2.2 nicht verfügbar. Das Telefon sendet SIP-Nachrichten an die Adresse 3.3.3.3, die die oberste Priorität unter den Servern mit dem Status „UP“ hat.

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

Im folgenden Beispiel werden zwei SRV-Einträge aus der DNS-NAPTR-Antwort angezeigt. Für jeden SRV-Eintrag gibt es drei A-Einträge (IP-Adressen).

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

Nehmen wir an, dass das Telefon keine Verbindung zu 1.1.1.1 herstellen konnte und denn eine Registrierung für 1.1.1.2 vorgenommen hat. Wenn 1.1.1.2 ausfällt, hängt das Verhalten des Telefons von der Einstellung des **Proxy Fallback Intvl (Intervall für Proxy-Fallback)** ab.

- Wenn **Proxy Fallback Intvl (Intervall für Proxy-Fallback)** auf **0** festgelegt ist, versucht es das Telefon mit den folgenden Adressen in der angegebenen Reihenfolge: 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- Wenn **Proxy Fallback Intvl (Intervall für Proxy-Fallback)** auf einen anderen Wert als Null festgelegt ist, versucht es das Telefon mit den folgenden Adressen in der angegebenen Reihenfolge: 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

SIP-Proxy-Fallback

Der Proxy-Fallback erfordert, dass im Feld **Proxy Fallback Intvl (Intervall für Proxy-Fallback)** auf der Registerkarte **Ext (n)** der Telefon-Weboberfläche ein anderer Wert als Null angegeben ist. Wenn Sie dieses Feld auf 0 festlegen, wird die SIP-Proxy-Failback-Funktion deaktiviert. Sie können diese durchwahlspezifischen Parameter in der Konfigurationsdatei auch im folgenden Format konfigurieren:

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

wobei *n* die Durchwahlnummer ist.

Die Zeit, zu der das Telefon ein Failback auslöst, hängt von der Telefonkonfiguration und den verwendeten SIP-Transportprotokollen ab.

Damit das Telefon ein Failback zwischen verschiedenen SIP-Transportprotokollen durchführen kann, legen Sie **SIP-Transport** auf **Automatisch** auf der Weboberfläche des Telefons auf der Registerkarte **Durchwahl(n)** fest. Sie können diese durchwahlspezifischen Parameter in der Konfigurationsdatei auch mit der folgenden XML-Zeichenfolge konfigurieren:

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

wobei *n* die Durchwahlnummer ist.

Failback von einer UDP-Verbindung

Das Failback von einer UDP-Verbindung wird durch SIP-Nachrichten ausgelöst. Im folgenden Beispiel konnte das Telefon zum Zeitpunkt T1 nicht auf 1.1.1.1 (TLS) registriert werden, da es vom Server keine Antwort erhielt. Wenn der SIP-Timer F abläuft, wird das Telefon zum Zeitpunkt T2 ($T2 = T1 + \text{SIP-Timer F}$) auf 2.2.2.2 (UDP) registriert. Die aktuelle Verbindung erfolgt über UDP auf 2.2.2.2.

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	

Das Telefon hat die folgende Konfiguration:

```
<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>
```

wobei n die Durchwahlnummer ist.

Das Telefon aktualisiert die Registrierung zum Zeitpunkt T2 ($T2 = (3600-16) * 78\%$). Das Telefon überprüft die Adressliste auf die Verfügbarkeit der IP-Adressen und die Ausfallzeit. Wenn $T2 - T1 \geq 60$, der fehlgeschlagene Server 1.1.1.1 wird wieder auf „UP“ gesetzt, und die Liste wird wie folgt aktualisiert. Das Telefon sendet SIP-Nachrichten an 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 von einer TCP- oder TLS-Verbindung

Das Failback von einer TCP- oder TLS-Verbindung wird durch den Parameter **Proxy Fallback Intvl (Intervall für Proxy-Fallback)** ausgelöst. Im folgenden Beispiel konnte das Telefon zum Zeitpunkt T1 nicht unter 1.1.1.1 (UDP) registriert werden und wurde daher unter 2.2.2.2 (TCP) registriert. Die aktuelle Verbindung erfolgt über TCP auf 2.2.2.2.

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	

Das Telefon hat die folgende Konfiguration:

```
<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>
```

wobei n die Durchwahlnummer ist.

Das Proxy-Fallback-Intervall (60 Sekunden) zählt von T1 herunter. Das Telefon löst den Proxy-Failback zum Zeitpunkt $T1+60$ aus. Wenn Sie in diesem Beispiel das Proxy-Fallback-Intervall auf 0 festlegen, behält das Telefon die Verbindung auf 2.2.2.2 bei.

Doppelte Registrierung

Das Telefon registriert sich immer mit dem primären und alternativen Proxy. Nach der Registrierung sendet das Telefon eine Invite- und Non-Invite-SIP-Nachricht zuerst über den primären Proxy. Wenn nach dem Timeout keine Antwort für die neue INVITE vom primären Proxy erhalten wird, versucht das Telefon, sich

mit dem alternativen Proxy zu verbinden. Wenn sich das Telefon nicht mit dem primären Proxy registrieren kann, sendet es eine INVITE an den alternativen Proxy, ohne den primären Proxy zu kontaktieren.

Die duale Registrierung wird pro Leitung unterstützt. Über die Webbenutzeroberfläche und Remotebereitstellung können drei hinzugefügte Parameter konfiguriert werden:

- Alternativer Proxy: Der Standard ist leer.
- Alternativer ausgehender Proxy: Der Standard ist leer.
- Doppelte Registrierung: Der Standard ist NEIN (deaktiviert).

Starten Sie das Telefon neu, nachdem Sie die Parameter konfiguriert haben, um die Funktion zu übernehmen.



Note Geben Sie einen Wert für den primären Proxy (oder ausgehenden primären Proxy) und den alternativen Proxy (oder ausgehenden alternativen Proxy) für die Funktion ein, damit diese richtig funktioniert.

Doppelte Registrierung und DNS SRV-Einschränkungen

- Wenn die duale Registrierung aktiviert ist, müssen der DNS SRV Proxy-Fallback oder die Wiederherstellung deaktiviert werden.
- Verwenden Sie die duale Registrierung nicht mit anderen Fallback- oder Wiederherstellungsmethoden. Beispiel: BroadSoft-Methode.
- Für Funktionsanforderungen ist keine Wiederherstellungsmethode verfügbar. Der Administrator kann die Zeitdauer für die erneute Registrierung jedoch anpassen, um den Registrierungsstatus für den primären und alternativen Proxy schnell zu aktualisieren.

Doppelte Registrierung und alternativer Proxy

Wenn der Parameter für die duale Registrierung auf **Nein** festgelegt ist, wird der alternative Proxy ignoriert.

Registrierung für Failover und Wiederherstellung

- Failover: Das Telefon führt einen Failover bei einer Zeitüberschreitung/Fehler während des Transports oder bei einem TCP-Verbindungsfehler aus, wenn die Werte Backup-RSC versuchen und Reg-RSC wiederholen angegeben sind.
- Wiederherstellung: Das Telefon versucht, sich erneut mit dem primären Proxy zu registrieren, wenn es mit dem sekundären Proxy registriert oder verbunden ist.

Der Parameter „Automatische Registrierung bei Failover“ steuert das Failover-Verhalten, wenn ein Fehler vorliegt. Wenn dieser Parameter auf „Ja“ festgelegt ist, wird das Telefon bei einem Failover oder einer Wiederherstellung erneut registriert.

Fallback-Verhalten

Ein Fallback tritt auf, wenn die aktuelle Registrierung abläuft oder das Intervall für den Proxy-Fallback ausgelöst wird.

Wenn das Intervall für den Proxy-Fallback überschritten wird, gehen alle neuen SIP-Nachrichten an den primären Proxy.

Wenn der Wert für den Ablauf der Registrierung beispielsweise 3.600 Sekunden und das Intervall für den Proxy-Fallback 600 Sekunden beträgt, wird der Fallback 600 Sekunden später ausgelöst.

Wenn der Wert für den Ablauf der Registrierung beispielsweise 800 Sekunden und das Intervall für den Proxy-Fallback 1.000 Sekunden beträgt, wird der Fallback 800 Sekunden ausgelöst.

Nach der erfolgreichen Registrierung auf dem primären Server, gehen alle SIP-Nachrichten an den primären Server.

RFC3311

Das Cisco IP-Telefon unterstützt RFC-3311, die SIP UPDATE-Methode.

SIP NOTIFY XML-Service

Das Cisco IP-Telefon unterstützt das SIP NOTIFY XML-Serviceereignis. Bei Empfang einer SIP NOTIFY-Nachricht mit einem XML-Serviceereignis ruft das Telefon die NOTIFY mit einer 401-Antwort ab, wenn die Nachricht nicht die korrekten Anmeldeinformationen enthält. Der Client muss die korrekten Anmeldeinformationen unter Verwendung von MD5-Digest mit dem SIP-Kontokennwort für die entsprechende Leitung des IP-Telefons bereitstellen.

Der Nachrichtentext kann die XML-Ereignismeldung enthalten. Zum Beispiel:

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

Authentifizierung:

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

NAT-Zuordnung mit SBC (Session Border Controller)

Wir empfehlen einen Serviceanbieter, der die NAT-Zuordnung über SBC unterstützt. Wenn der Serviceanbieter die NAT-Zuordnung bereitstellt, haben Sie eine größere Routerauswahl.

NAT-Zuordnung mit einem SIP-ALG-Router

Die NAT-Zuordnung kann mit einem Router vorgenommen werden, der ein SIP-ALG (Application Layer Gateway) hat. Mit einem SIP-ALG-Router haben Sie eine größere Auswahl an Serviceanbietern.

CDP (Cisco Discovery Protocol)

Das Cisco Discovery Protocol (CDP) basiert auf der Aushandlung und bestimmt, in welchem virtuellen LAN (VLAN) sich das Cisco IP-Telefon befindet. Wenn Sie einen Cisco Switch verwenden, ist das Cisco Discovery Protocol verfügbar und standardmäßig aktiviert. Das CDP hat die folgenden Attribute:

- Das CDP ruft die Protokolladressen von Nachbargeräten ab und ermittelt die Plattform dieser Geräte.
- Das CDP zeigt die Informationen zu den Schnittstellen an, die der Router verwendet.

- Das CDP ist unabhängig von Medien und Protokollen.

Wenn Sie ein VLAN ohne CDP verwenden, müssen Sie eine VLAN-ID für das Cisco IP-Telefon eingeben.

LLDP-MED

Das Cisco IP-Telefon unterstützt LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) für die Bereitstellung mit Netzwerkverbindungsgeräten von Cisco oder Drittanbietern, die eine Methode für die automatische Ermittlung auf Schicht 2 verwenden. Die Implementierung von LLDP-MED erfolgt in Übereinstimmung mit der IEEE 802.1AB (LLDP) Spezifikation von Mai 2005 und ANSI TIA-1057 von April 2006.

Das Cisco IP-Telefon wird als ein Gerät der LLDP-MED-Medienendpunkt Klasse III mit direkten LLDP-MED-Verbindungen mit Netzwerkverbindungsgeräten betrieben (Media Endpoint Discovery Reference Model and Definition, ANSI TIA-1057 Section 6).

Das Cisco IP-Telefon unterstützt nur die folgenden begrenzten TLVs (Type-Length-Value) als ein LLDP-MED-Medienendpunktgerät Klasse III:

- Gehäuse-ID TLV
- Port-ID TLV
- Gültigkeitsdauer TLV
- Portbeschreibung TLV
- Systemname TLV
- Systemfunktionen TLV
- IEEE 802.3 MAC/PHY Konfiguration/Status TLV (nur für kabelgebundenes Netzwerk)
- LLDP-MED-Funktionen TLV
- LLDP-MED Netzwerkrichtlinie TLV (nur für Anwendungstyp=Sprache)
- LLDP-MED externe Leistung über MDI TLV (nur für kabelgebundenes Netzwerk)
- LLDP-MED Firmware-Revision TLV
- Ende von LLDPDU TLV

Die ausgehende LLDPDU enthält gegebenenfalls alle vorangestellten TLVs. Für die eingehende LLDPDU wird die LLDPDU verworfen, wenn eine der folgenden TLVs fehlt. Alle anderen TLVs werden nicht validiert und ignoriert.

- Gehäuse-ID TLV
- Port-ID TLV
- Gültigkeitsdauer TLV
- LLDP-MED-Funktionen TLV
- LLDP-MED Netzwerkrichtlinie TLV (nur für Anwendungstyp=Sprache)
- Ende von LLDPDU TLV

Das Cisco IP-Telefon sendet gegebenenfalls die LLDPDU zum Herunterfahren. Der LLDPDU-Rahmen enthält die folgenden TLVs:

- Gehäuse-ID TLV
- Port-ID TLV
- Gültigkeitsdauer TLV
- Ende von LLDPDU TLV

Für die Implementierung von LLDP-MED auf Cisco IP-Telefonen gelten einige Einschränkungen:

- Das Speichern und Abrufen von Nachbarinformationen wird nicht unterstützt.
- SNMP und die entsprechenden MIBs werden nicht unterstützt.
- Das Aufzeichnen und Abrufen von statistischen Zählern wird nicht unterstützt.
- Nicht alle TLVs werden vollständig validiert. TLVs, die für die Telefone nicht angewendet werden, werden ignoriert.
- Protokollstatusgeräte werden, wie in den Standards angegeben, nur für Referenzzwecke verwendet.

Gehäuse-ID TLV

Für die ausgehende LLDPDU unterstützt die TLV den Untertyp=5 (Netzwerkadresse). Wenn die IP-Adresse bekannt ist, ist der Wert der Gehäuse-ID ein Oktett der INAN-Adressenfamiliennummer gefolgt von der Oktett-Zeichenfolge für die IPv4-Adresse, die für die Sprachkommunikation verwendet wird. Wenn die IP-Adresse unbekannt ist, hat die Gehäuse-ID den Wert 0.0.0.0. Die einzige INAN-Adressenfamilie, die unterstützt wird, ist IPv4. Die IPv6-Adresse für die Gehäuse-ID wird derzeit nicht unterstützt.

Für die eingehende LLDPDU wird die Gehäuse-ID als ein Wert behandelt, um die MSAP-ID zu erstellen. Der Wert wird nicht mit dem Untertyp validiert.

Der Gehäuse-ID-TLV ist als erster TLV erforderlich. Für die ausgehenden und eingehenden LLDPDUs ist nur ein Gehäuse-ID-TLV zulässig.

Port-ID TLV

Für die ausgehende LLDPDU unterstützt die TLV den Untertyp=3 (MAC-Adresse). Die aus 6 Oktetten bestehende MAC-Adresse für den Ethernet-Port wird für den Wert der Port-ID verwendet.

Für die eingehende LLDPDU wird die Port-ID TLV als ein Wert behandelt, um die MSAP-ID zu erstellen. Der Wert wird nicht mit dem Untertyp validiert.

Der Port-ID-TLV ist als zweiter TLV erforderlich. Für die ausgehenden und eingehenden LLDPDUs ist nur ein Port-ID-TLV zulässig.

Gültigkeitsdauer TLV

Für die ausgehende LLDPDU beträgt der Gültigkeitsdauer TTL-Wert 180 Sekunden. Dieser Wert unterscheidet sich vom empfohlenen Standard von 120 Sekunden. Für die LLDPDU zum Herunterfahren ist der TTL-Wert immer 0.

Der Gültigkeitsdauer-TLV ist als dritter TLV erforderlich. Für die ausgehenden und eingehenden LLDPDUs ist nur ein GültigkeitsdauerTLV zulässig.

Ende von LLDPDU TLV

Der Wert ist 2 Oktette (alle Null). Diese TLV ist erforderlich. Für ausgehende und eingehende LLDPDUs ist nur eine TLV erlaubt.

Portbeschreibung TLV

Für die ausgehende LLDPDU in der Portbeschreibung TLV ist der Wert für die Portbeschreibung mit der Port-ID TLV für CDP identisch. Die eingehende LLDPDU, die Portbeschreibung TLV, wird ignoriert und nicht validiert. Für die ausgehenden und eingehenden LLDPDUs ist nur ein Portbeschreibungs-TLV zulässig.

Systemname TLV

Für das Cisco IP-Telefon ist der Wert die SEP+MAC-Adresse.

Beispiel: SEPAC44F211B1D0

Die eingehende LLDPDU, die Systemname TLV, wird ignoriert und nicht validiert. Für die ausgehenden und eingehenden LLDPDUs ist nur ein Systemname-TLV zulässig.

Systemfunktionen TLV

Für die ausgehende LLDPDU in der Systemfunktionen TLV sollten die Bit-Werte für die Systemfunktionsfelder mit 2 Oktetten für Bit 2 (Bridge) und Bit 5 (Telefon) für ein Telefon mit einem PC-Port festgelegt werden. Wenn das Telefon keinen PC-Port hat, sollte nur Bit 5 festgelegt werden. Der gleiche Systemfunktionswert sollte für das Feld Funktion aktivieren festgelegt werden.

Für die eingehende LLDPDU wird die Systemfunktionen TLV ignoriert. Die TLV wird nicht semantisch mit dem MED-Gerätetyp validiert.

Die Systemfunktionen TLV ist für ausgehende LLDPDUs erforderlich. Nur eine Systemfunktionen TLV ist zulässig.

Verwaltungsadresse TLV

Die TLV identifiziert eine Adresse, die dem lokalen LLDP-Agenten zugewiesen ist (kann verwendet werden, um Entitäten auf einer höheren Stufe zu erreichen), um die Ermittlung durch die Netzwerkverwaltung zu unterstützen. Die TLV ermöglicht, dass die Systemschnittstellenummer und eine Objekt-ID (OID) einbezogen werden, die dieser Verwaltungsadresse zugewiesen sind, wenn diese bekannt sind.

- Länge der TLV-Informationszeichenfolge: Dieses Feld enthält die Länge (in Oktetten) aller Felder in der TLV-Informationszeichenfolge.
- Zeichenfolgenlänge der Verwaltungsadresse: Dieses Feld enthält die Länge (in Oktetten) der Felder Verwaltungsadresse-Untertyp und Verwaltungsadresse.

Systembeschreibung TLV

Die TLV erlaubt der Netzwerkverwaltung die Systembeschreibung anzukündigen.

- Länge der TLV-Informationszeichenfolge: Dieses Feld zeigt die genaue Länge (in Oktetten) der Systembeschreibung an.
- Systembeschreibung: Dieses Feld enthält eine alphanumerische Zeichenfolge, die die Netzwerkentität beschreibt. Die Systembeschreibung umfasst den vollen Namen und die Versionsidentifizierung des Systemhardwaretyps, des Betriebssystems und der Netzwerksoftware. Wenn IETF RFC 3418 von der Implementierung unterstützt wird, sollte das sysDescr-Objekt für dieses Feld verwendet werden.

IEEE 802.3 MAC/PHY Konfiguration/Status TLV

Die TLV ist nicht für die automatische Aushandlung, sondern für die Fehlerbehebung bestimmt. Für die eingehende LLDPDU wird die TLV ignoriert und nicht validiert. Für die ausgehende LLDPDU für die TLV sollte der Oktett-Wert für die Unterstützung/den Status der automatischen Aushandlung wie folgt lauten:

- Bit 0: Legen Sie 1 fest, um anzugeben, dass die automatische Aushandlung unterstützt wird.
- Bit 1: Legen Sie 1 fest, um anzugeben, dass der Status der automatischen Aushandlung aktiviert ist.
- Bit 2-7: Legen Sie 0 fest.

Die Bit-Werte für die 2 Oktette PMD für die automatische Aushandlung sollten wie folgt festgelegt werden:

- Bit 13: 10BASE-T-Halbduplex-Modus
- Bit 14: 10BASE-T-Vollduplex-Modus
- Bit 11: 100BASE-TX-Halbduplex-Modus
- Bit 10: 100BASE-TX-Vollduplex-Modus
- Bit 15: Unbekannt

Bit 10, 11, 13 und 14 sollten festgelegt werden.

Der Wert für den funktionsfähigen MAU-Typ mit 2 Oktetten sollte festgelegt werden, um den tatsächlichen funktionsfähigen MAU-Typ zu reflektieren:

- 16: 100BASE-TX-Vollduplex
- 15: 100BASE-TX-Halbduplex
- 11: 10BASE-T-Vollduplex
- 10: 10BASE-T-Halbduplex

Das Telefon ist normalerweise auf 100BASE-TX-Vollduplex festgelegt. In diesem Fall sollte der Wert 16 festgelegt werden. Die TLV ist optional für ein kabelgebundenes Netzwerk und auf ein Drahtlosnetzwerk nicht anwendbar. Das Telefon sendet diese TLV nur im verkabelten Modus. Wenn das Telefon nicht für die automatische Aushandlung konfiguriert ist, aber für Geschwindigkeit/Duplizität, sollte für die ausgehende LLDPDU TLV Bit 1 für den Oktett-Wert der Unterstützung/des Status der automatischen Aushandlung auf 0 festgelegt sein, um anzuzeigen, dass die automatische Aushandlung deaktiviert ist. Die 2 Oktette PMD für die automatische Aushandlung sollten auf 0x8000 festgelegt werden, um einen unbekanntes Wert anzugeben.

LLDP-MED-Funktionen TLV

Für die ausgehende LLDPDU sollte die TLV den Gerätetyp 3 (Endpunktklasse III) mit den folgenden Bits im Feld 2-Oktett-Funktion haben:

Bit-Position	Funktion
0	LLDP-MED-Funktionen
1	Netzwerkrichtlinie
4	Erweiterte Leistung über MDI-PD
5	Inventar

Für die eingehende TLV wird die LLDPDU verworfen, wenn die LLDP-MED TLV nicht vorhanden ist. Diese LLDP-MED-Funktionen TLV ist erforderlich. Für ausgehende und eingehende LLDPDUs ist nur eine TLV erlaubt. Alle anderen LLDP-MED TLVs vor der LLDP-MED-Funktionen TLV werden ignoriert.

Netzwerkrichtlinien TLV

In der TLV für die ausgehende LLDPDU wird das unbekannte Richtlinienflag (U) auf 1 festgelegt, bevor das VLAN oder DSCP bestimmt wird. Wenn die VLAN-Einstellung oder DSCP bekannt ist, wird der Wert auf 0 festgelegt. Wenn die Richtlinie unbekannt ist, werden alle anderen Werte auf 0 festgelegt. Bevor das VLAN bestimmt oder verwendet wird, wird das markierte Flag (T) auf 0 festgelegt. Wenn das markierte VLAN (VLAN-ID > 1) für das Telefon verwendet wird, wird das markierte Flag (T) auf 1 festgelegt. Reserviert (X) ist immer auf 0 festgelegt. Wenn das VLAN verwendet wird, werden die entsprechende VLAN-ID und L2-Priorität entsprechend festgelegt. Der gültige Wertebereich für die VLAN-ID ist 1 bis 4094. Die VLAN-ID=1 wird jedoch nie verwendet (Einschränkung). Wenn DSCP verwendet wird, wird der Wertebereich von 0 bis 63 entsprechend festgelegt.

In der TLV für die eingehende LLDPDU sind mehrere Netzwerkrichtlinien TLVs für verschiedene Anwendungstypen zugelassen.

LLDP-MED erweiterte Leistung über MDI TLV

In der TLV für die ausgehende LLDPDU ist der binäre Wert für den Leistungstyp auf „0 1“ festgelegt, um anzugeben, dass der Leistungstyp für das Telefon das PD-Gerät ist. Die Leistungsquelle für das Telefon wird mit dem binären Wert „1 1“ auf „PSE und lokal“ festgelegt. Die Leistungspriorität ist auf den binären Wert „0 0 0 0“ festgelegt, um eine unbekannte Priorität anzugeben, während der Leistungswert auf den maximalen Wert gesetzt ist. Der Leistungswert für das Cisco IP-Telefon ist 12.900 mW.

Für die eingehende LLDPDU wird die TLV ignoriert und nicht validiert. Für die ausgehenden und eingehenden LLDPDUs ist nur ein TLV zulässig. Das Telefon sendet die TLV nur für ein kabelgebundenes Netzwerk.

Der LLDP-MED-Standard wurde ursprünglich im Zusammenhang mit dem Ethernet entworfen. LLDP-MED für Drahtlosnetzwerke steht weiterhin zur Diskussion. Siehe ANSI-TIA 1057, Anhang C, C.3 Zutreffende TLV für VoWLAN, Tabelle 24. Es wird empfohlen, dass die TLV für drahtlose Netzwerke nicht zutreffend ist. Diese TLV ist für die Verwendung mit PoE und Ethernet bestimmt. Die TLV unterstützt die Netzwerkverwaltung oder Anpassung der Leistungsrichtlinie auf dem Switch nicht.

LLDP-MED Bestandsverwaltung TLV

Diese TLV ist für die Geräteklasse III optional. Für die ausgehende LLDPDU wird nur der Firmware-Revision-TLV unterstützt. Der Wert für die Firmware-Revision ist die Version der Firmware auf dem Telefon. Für die eingehende LLDPDU, werden die TLVs ignoriert und nicht validiert. Für die ausgehenden und eingehenden LLDPDUs ist nur ein Firmware-Revision-TLV zulässig.

Auflösung der Netzwerkrichtlinie und QoS

Besondere VLANs

VLAN=0, VLAN=1 und VLAN=4095 werden genauso wie ein nicht markiertes VLAN behandelt. Da das VLAN nicht markiert ist, trifft die CoS (Class of Service) nicht zu.

Standard-QoS für SIP-Modus

Wenn keine Netzwerkrichtlinie von CDP oder LLDP-MED vorhanden ist, wird die Standardnetzwerkrichtlinie verwendet. CoS basiert auf der Konfiguration für einen bestimmten Anschluss. Sie ist nur zutreffend, wenn das manuelle VLAN aktiviert ist und die manuelle VLAN-ID nicht gleich 0, 1 oder 4095 ist. Der Dienstyp (Type of Service, ToS) basiert auf der Konfiguration für die bestimmte Durchwahl.

QoS-Auflösung für CDP

Wenn eine gültige Netzwerkrichtlinie von CDP vorhanden ist:

- Wenn das VLAN=0, 1 oder 4095 ist, wird das VLAN nicht festgelegt oder seine Markierung wird aufgehoben. CoS ist nicht anwendbar, aber DSCP ist anwendbar. ToS basiert, wie bereits beschrieben, auf dem Standard.
- Wenn das VLAN > 1 und das VLAN < 4095 ist, wird das VLAN entsprechend festgelegt. CoS und ToS basieren, wie bereits beschrieben, auf dem Standard. DSCP ist anwendbar.
- Das Telefon und die erste Startsequenz werden neu gestartet.

QoS-Auflösung für LLDP-MED

Wenn CoS anwendbar und CoS=0 ist, wird der Standard für die angegebene Durchwahl verwendet. Der für die L2-Priorität für TLV für die ausgehende LLDPDU angezeigte Wert basiert jedoch auf dem Wert, der für Durchwahl 1 verwendet wird. Wenn CoS zutreffend und CoS != 0 ist, wird CoS für alle Durchwahlen verwendet.

Wenn DSCP (zu ToS zugeordnet) anwendbar und DSCP = 0 ist, wird der Standard für den angegebenen Anschluss verwendet. Der für DSCP für TLV für die ausgehende LLDPDU angezeigte Wert basiert jedoch auf dem Wert, der für Durchwahl 1 verwendet wird. Wenn DSCP zutreffend und DSCP != 0 ist, wird DSCP für alle Durchwahlen verwendet.

Wenn das VLAN > 1 und das VLAN < 4095 ist, wird das VLAN entsprechend festgelegt. CoS und ToS basieren, wie bereits beschrieben, auf dem Standard. DSCP ist anwendbar.

Wenn eine gültige Netzwerkrichtlinie für die Sprachanwendung von LLDP-MED PDU vorhanden und das markierte Flag festgelegt ist, sind das VLAN, die L2-Priorität (CoS) und DSCP (zu ToS zugeordnet) anwendbar.

Wenn eine gültige Netzwerkrichtlinie für die Sprachanwendung von LLDP-MED PDU vorhanden und das markierte Flag nicht festgelegt ist, ist nur DSCP (zu ToS zugeordnet) anwendbar.

Das Cisco IP-Telefon und die erste Startsequenz werden neu gestartet.

Koexistenz mit CDP

Wenn CDP und LLDP-MED aktiviert sind, bestimmt die Netzwerkrichtlinie für das VLAN die letzte Richtlinie, die mit einem Erkennungsmodus festgelegt oder geändert wurde. Wenn LLDP-MED und CDP aktiviert sind, sendet das Telefon während des Starts CDP und LLDP-MED PDUs.

Die inkonsistente Konfiguration und das inkonsistente Verhalten von Netzwerkverbindungsgeräten für den CDP- und LLDP-MED-Modus können in einem schwingenden Neustartverhalten des Telefons resultieren, da zu verschiedenen VLANs gewechselt wird.

Wenn das VLAN von CDP und LLDP-MED festgelegt wird, wird die VLAN-ID verwendet, die manuell konfiguriert wurde. Wenn die VLAN-ID nicht manuell konfiguriert wurde, wird kein VLAN unterstützt. DSCP wird verwendet und die Netzwerkrichtlinie bestimmt LLDP-MED (falls zutreffend).

LLDP-MED und mehrere Netzwerkgeräte

Wenn für die Netzwerkrichtlinie der gleiche Anwendungstyp verwendet wird, aber unterschiedliche QoS-Netzwerkrichtlinien auf Schicht 2 und 3 auf den Telefonen von mehreren Netzwerkgeräten empfangen werden, wird die letzte gültige Netzwerkrichtlinie verwendet. Um eine deterministische und konsistente Netzwerkrichtlinie sicherzustellen, sollten mehrere Netzwerkgeräte keine widersprüchlichen Netzwerkrichtlinien für den gleichen Anwendungstyp senden.

LLDP-MED und IEEE 802.X

Das Cisco IP-Telefon unterstützt IEEE 802.X nicht und funktioniert nicht in einer verkabelten 802.1X-Umgebung. IEEE 802.1X oder STPs (Spanning Tree Protocols) können jedoch zu einer Verzögerung der schnellen Startantwort von Switches führen.