



Technische details

- [Netwerkprotocollen, op pagina 1](#)
- [Netwerkprotocollen, op pagina 4](#)
- [Informatie over USB-poort \(alleen 8800\), op pagina 6](#)
- [SIP- en NAT-configuratie, op pagina 7](#)
- [Cisco Discovery Protocol, op pagina 13](#)
- [LLDP-MED, op pagina 14](#)
- [Definitieve netwerkbeleidsoplossing en QoS, op pagina 19](#)

Netwerkprotocollen

Cisco IP-telefoon 8800-serie ondersteunt diverse industriestandaard en Cisco-netwerkprotocollen die vereist zijn voor gesproken communicatie. In de volgende tabel ziet u een overzicht van de netwerkprotocollen die door de telefoons worden ondersteund.

Tabel 1: Ondersteunde netwerkprotocollen voor Cisco IP-telefoon 8800-serie

Netwerkprotocol	Doel	Opmerkingen
Bluetooth	Bluetooth is een draadloos persoonlijk netwerk-protocol (WPAN) dat aangeeft hoe apparaten over korte afstand communiceren.	Cisco IP-telefoon ondersteunen Bluetooth. Cisco IP-telefoon 8800-serie ondersteunt Bluetooth 4.0. Cisco IP Phone 8800-serie ondersteunt Bluetooth niet.
Bootstrap Protocol (BootP)	BootP schakelt een netwerkapparaat, zoals Cisco IP-telefoon, in om bepaalde opstartgegevens te detecteren, zoals het IP-adres.	—
Cisco Discovery Protocol (CDP)	CDP is een apparaatdetectieprotocol dat werkt op alle door Cisco gefabriceerde apparatuur. Een apparaat kan CDP gebruiken om zijn bestaan aan te geven voor andere apparaten en informatie over andere apparaten te ontvangen in het netwerk.	Cisco IP-telefoon geven informatie te gebruiken voor hulp-VLAN-id, poort en QoS-classificatie (Quality of Service) met de

Netwerkprotocol	Doel	Opmerkingen over
Dynamic Host Configuration Protocol (DHCP)	DHCP wijst een IP-adres dynamisch toe aan netwerkapparaten. Met DHCP kunt u een IP-telefoon aansluiten op het netwerk en de telefoon laten werken zonder dat u handmatig een IP-adres moet toewijzen of aanvullende netwerkparameters moet configureren.	DHCP is standaard uitgeschakeld, moet worden ingeschakeld, moet een subnetmasker en gateway worden geconfigureerd voor elke telefoon configuratie. Opmerking De parameter Use DHCP (gebruik DHCP) heeft de waarde Use DHCP als de waarde Use DHCP is waargenomen, waarin DHCP wordt gebruikt voor DHCP.
Hypertext Transfer Protocol (HTTP)	HTTP is de standaardmanier voor informatie-overdracht en het verplaatsen van documenten over internet en het web.	Cisco IP-telefoons gebruiken het HTTP-protocol voor het configureren van de telefoon en voor het downloaden van firmware.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is een combinatie van Hypertext Transfer Protocol met het SSL/TLS-protocol voor het leveren van codering en veilige identificatie van servers.	Sommige webtoepassingen gebruiken HTTP- als HTTPS-URL's voor Cisco IP-Phones die HTTPS-URL's gebruiken voor HTTPS-URL's.
IEEE 802.1X	Met de IEEE 802.1X-standaard wordt een protocol voor client-/servergebaseerd toegangsbeheer en verificatie gedefinieerd dat ervoor zorgt dat niet-geautoriseerde clients geen verbinding kunnen maken met een LAN via openbaar toegankelijke poorten. Totdat de client wordt geverifieerd, staat 802.1X-toegangsbeheer alleen EAPOL-verkeer (Extensible Authentication Protocol over LAN) toe via de poort waarmee de client is verbonden. Als de verificatie is gelukt, kan normaal verkeer de poort passeren.	Cisco IP-telefoon ondersteunt de IEEE 802.1X-standaard voor de volgende protocollen: EAP-FAST en EAP-TLS. Wanneer 802.1X-verbinding is ingeschakeld op de telefoon, wordt de pc-poort en spraakpoort beschermd door 802.1X.
IEEE 802.11n/802.11ac	De IEEE 802.11-standaard geeft aan hoe apparaten communiceren via een draadloos LAN-netwerk (WLAN). 802.11n werkt met de 2,4-GHz en 5-GHz band en 802.11ac werkt met de 5-GHz band.	De 802.11-interfaces van de telefoon zijn beschikbaar voor het geval de telefoon is ingeschakeld of ongeschakeld. Alleen Cisco IP-telefoons ondersteunen WLAN.
Internet Protocol (IP)	IP is een berichtprotocol dat pakketten adresseert en verzendt via het netwerk.	Als netwerkapparaten communiceren met IP, moeten ze een IP-adres, subnet en gateway hebben. IP-adressen, subnetmaskers en gateways worden automatisch toegevoerd aan de IP-telefoon gebruikende Dynamic Host Configuration Protocol. Als DHCP niet wordt gebruikt, moet de telefoon lokaal handmatig worden geconfigureerd.

Netwerkprotocol	Doel	Opmerkingen
Link Layer Discovery Protocol (LLDP)	LLDP is een gestandaardiseerd netwerkdetectieprotocol (vergelijkbaar met CDP) dat wordt ondersteund op een aantal apparaten van Cisco en derden.	Cisco IP-telefo pe-poort.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is een uitbreiding van de LLDP-standaard voor spraakproducten.	Cisco IP-telefo de SW-poort v informatie zoal <ul style="list-style-type: none"> • Configur • Apparaat • Voedings • Inventaris Voor meer info LLDP-MED ra LLDP-MED an http://www.cisco.com/US
Real-Time Transport Protocol (RTP)	RTP is een standaardprotocol voor het transporteren van real-time gegevens, zoals interactieve spraak via gegevensnetwerken.	Cisco IP-telefo voor het verzem spraakverkeer gateways.
Real-Time Control Protocol (RTCP)	RTCP werkt samen met RTP voor het leveren van QoS-gegevens (zoals jitter, latentie en retourvertraging) op RTP-stromen.	RTCP is standa
Session Description Protocol (SDP)	SDP is het gedeelte van het SIP-protocol dat bepaalt welke parameters tijdens een verbinding beschikbaar zijn tussen twee eindpunten. Conferenties worden opgezet met behulp van de SDP-voorzieningen die worden ondersteund door alle eindpunten van de conferentie.	SDP-voorzieni DTMF-detectie normaal gespro door een oproe de gebruikte M SIP-eindpunten toe van deze p
Session Initiation Protocol (SIP)	SIP is de IETF-standaard (Internet Engineering Task Force) voor multimediaconferentie via IP. SIP is een op ASCII gebaseerd controleprotocol op de applicatielaag (gedefinieerd in RFC 3261), dat kan worden gebruikt om gesprekken tussen twee of meer eindpunten tot stand te brengen, te onderhouden en te beëindigen.	Net als andere functies als sig een telefoniene signalering kun netwerkgrenze Sessiebeheer b kenmerken van beheren. Cisco IP-telefo SIP-protocol w alleen IPv6, all IPv6.
Transmission Control Protocol (TCP)	TCP is een verbindingsgericht transportprotocol.	Cisco IP-telefo verbinding te n oproepbeheers toegang tot XM

Netwerkprotocol	Doel	Opmerkingen over
Transport Layer Security (TLS)	TLS is een standaardprotocol voor het beveiligen en verifiëren van communicatie.	Nadat de beveiliging is ingesteld, kunnen Cisco IP-telefoons gebruikmaken van TLS voor veilige registratie en oproepbeheersystemen.
Trivial File Transfer Protocol (TFTP)	TFTP zorgt dat u bestanden over het netwerk kunt verzenden. Op de Cisco IP-telefoon kunt u met TFTP een configuratiebestand ophalen dat specifiek is voor het telefoontype.	TFTP vereist een TFTP-server die automatisch kan worden gevonden door de DHCP-server.
User Datagram Protocol (UDP)	UDP is een verbindingsloos berichtenprotocol voor het leveren van gegevenspakketten.	UDP wordt alleen gebruikt voor SIP-signalering op de telefoon en niet UDP.

Netwerkprotocollen

Cisco IP-telefoons ondersteunen diverse industriestandaard en Cisco-netwerkprotocollen die vereist zijn voor gesproken communicatie. In de volgende tabel ziet u een overzicht van de netwerkprotocollen die door de telefoons worden ondersteund.

Tabel 2: Ondersteunde netwerkprotocollen voor Cisco IP-telefoon

Netwerkprotocol	Doel
Bootstrap Protocol (BootP)	BootP schakelt een netwerkapparaat, zoals Cisco IP-telefoon, in om de noodzakelijke opstartgegevens te detecteren, zoals het IP-adres.
Cisco Discovery Protocol (CDP)	CDP is een apparaatdetectieprotocol dat werkt op alle door Cisco gefabriceerde apparatuur. Een apparaat kan CDP gebruiken om zijn bestaan aan te geven voor andere apparaten en informatie over andere apparaten te ontvangen in het netwerk.
Domeinnaamserver (DNS)	DNS zet domeinnamen om in IP-adressen.
Dynamic Host Configuration Protocol (DHCP)	DHCP wijst een IP-adres dynamisch toe aan netwerkapparaten. Met DHCP kunt u een IP-telefoon aansluiten op het netwerk en de telefoon laten werken zonder dat u handmatig een IP-adres moet toewijzen of aanvullende netwerkparameters moet configureren.
Hypertext Transfer Protocol (HTTP)	HTTP is het standaardprotocol voor informatie-overdracht en het verspreiden van documenten over internet en het web.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is een combinatie van Hypertext Transfer Protocol met het SSL/TLS-protocol voor het leveren van beveiligde en veilige identificatie van servers.

Netwerkprotocol	Doel
Internet Protocol (IP)	IP is een berichtprotocol dat pakketten adresseert en verzendt via het netwerk.
Link Layer Discovery Protocol (LLDP)	LLDP is een gestandaardiseerd netwerkdetectieprotocol (vergelijkbaar met CDP) dat wordt ondersteund op een aantal apparaten van Cisco en andere fabrikanten.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is een uitbreiding van de LLDP-standaard die is ontworpen voor spraakproducten.
Network Transport Protocol (NTP)	NTP is een netwerkprotocol voor kloksynchronisatie tussen computers op het netwerk via pakketgeschakelde gegevensnetwerken met variabele latencies.
Real-Time Transport Protocol (RTP)	RTP is een standaardprotocol voor het transporteren van real-time gegevens zoals interactieve spraak en video, via gegevensnetwerken.
Real-Time Control Protocol (RTCP)	RTCP werkt samen met RTP voor het leveren van QoS-gegevens (zoals latencies en retourvertraging) op RTP-stromen.
Session Description Protocol (SDP)	SDP is het gedeelte van het SIP-protocol dat bepaalt welke parameters voor een verbinding beschikbaar zijn tussen twee eindpunten. Conferenties worden opgezet met behulp van de SDP-voorzieningen die worden ondersteund door alle eindpunten van de conferentie.
Session Initiation Protocol (SIP)	SIP is de IETF-standaard (Internet Engineering Task Force) voor het opzetten van multimediaconferenties via IP. SIP is een op ASCII gebaseerd controlerend protocol op de applicatielaag (gedefinieerd in RFC 3261), dat kan worden gebruikt om gesprekken tussen twee of meer eindpunten tot stand te brengen, te onderhouden en te beëindigen.

Netwerkprotocol	Doel
Secure Real-Time Transfer protocol (SRTP)	SRTP is een uitbreiding van het RTP-audio-/videoprofiel (Real-Time Protocol) en garandeert de integriteit van RTP- en RTCP-pakketten (Real-Time Control Protocol) door het leveren van verificatie, integriteit en codering van mediapakketten tussen twee eindpunten.
Transmission Control Protocol (TCP)	TCP is een verbindingsgericht transportprotocol.
Transport Layer Security (TLS)	TLS is een standaardprotocol voor het beveiligen en verifiëren van communicatie.
Trivial File Transfer Protocol (TFTP)	TFTP zorgt dat u bestanden over het netwerk kunt verzenden. Op de Cisco IP-telefoon kunt u met TFTP een configuratiebestand op te laden dat specifiek is voor het telefoontype.
User Datagram Protocol (UDP)	UDP is een verbindingsloos berichtenprotocol voor het leveren van gegevenspakketten.

Verwante onderwerpen

- [De netwerkinstellingen controleren](#)
- [Controleren of de telefoon start](#)

Informatie over USB-poort (alleen 8800)

De Cisco IP Phones 8861, 8851 en 8865 ondersteunen maximaal vijf apparaten die verbinding met elke USB-poort maken. Elk apparaat dat is verbonden met de telefoon, wordt meegeteld. Uw telefoon kan bijvoorbeeld vijf USB-apparaten op de poort aan de zijkant en vijf extra standaard USB-apparaten op de poort aan de achterkant ondersteunen. Veel USB-producten van derden tellen als meerdere USB-apparaten: een apparaat dat bijvoorbeeld een USB-hub en -hoofdtelefoon bevat, kan worden geteld als twee USB-apparaten. Zie de documentatie over USB-apparaten voor meer informatie.



Opmerking

- Hubs zonder voeding worden niet ondersteund en hubs met voeding met meer dan vier poorten worden niet ondersteund.
- USB-hoofdtelefoons die verbinding maken met de telefoon via een USB-hub worden niet ondersteund.

Elke toetsuitbreidingsmodule die verbinding maakt met de telefoon, telt als een USB-apparaat. Als er drie toetsuitbreidingsmodules met de telefoon zijn verbonden, worden deze geteld als drie USB-apparaten.

De USB-poort uitschakelen

Als u niet wilt dat gebruikers een of alle USB-poorten voor bepaalde doeleinden gaan gebruiken, kunt u de USB-poort aan de achterkant en/of de USB-poort aan de zijkant van de telefoon uitschakelen. De uitgeschakelde USB-poort heeft dan geen enkele functie meer. De USB-hoofdtelefoon en de toetsuitbreidingsmodule (KEM) worden bijvoorbeeld niet herkend. Ook wordt er geen aangesloten apparaat opgeladen.

Als u niet wilt dat gebruikers de USB-poort voor bepaalde doeleinden gaan gebruiken, kunt u die poort uitschakelen op de webpagina van de telefoon. De enige USB-poort zit aan de achterkant van de telefoon. De uitgeschakelde USB-poort heeft dan geen enkele functie meer. De USB-hoofdtelefoon wordt bijvoorbeeld niet herkend. Ook wordt er geen aangesloten apparaat opgeladen.

De Cisco IP-telefoon 8851 heeft slechts één USB-poort en wel aan de zijkant. De Cisco IP-telefoon 8861 en 8865 hebben twee USB-poorten, één USB-poort aan de zijkant en één USB-poort aan de achterkant.

De Cisco IP-telefoon 6871 heeft één USB-poort en wel aan de achterkant.

Voordat u begint

Open de beheerwebpagina van de telefoon. Zie [De webinterface van de telefoon openen](#).

Procedure

- Stap 1** Selecteer **Spraak > Systeem**.
- Stap 2** Stel in de sectie **Energie-instellingen** de parameter **USB-poort achterkant uitschakelen** in op **Ja** om de USB-poort aan de achterkant uit te schakelen.
- U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:
- ```
<Disable_Back_USB_Port ua="na">No</Disable_Back_USB_Port>
```
- Opties: Ja en Nee
- Standaard: Nee
- Stap 3** Stel in de sectie **Energie-instellingen** de parameter **USB-poort zijkant uitschakelen** in op **Ja** om de USB-poort aan de zijkant uit te schakelen.
- U kunt deze parameter configureren in het XML-bestand met de telefoonconfiguratie (cfg.xml) door een tekenreeks met deze notatie in te voeren:
- ```
<Disable_Side_USB_Port ua="na">No</Disable_Side_USB_Port>
```
- Opties: Ja en Nee
- Standaard: Nee
- Stap 4** Klik op **Submit All Changes**.
-

SIP- en NAT-configuratie

SIP en Cisco IP-telefoon

De Cisco IP-telefoon gebruikt Session Initiation Protocol (SIP), dat interoperabiliteit toestaat met alle IT-serviceproviders die SIP ondersteunen. SIP is een met IETF gedefinieerd signaleringsprotocol waarmee spraakcommunicatiesessies in een IP-netwerk worden beheerd.

Met SIP wordt signalerings- en sessiebeheer binnen een telefonienetwerk met pakketten afgehandeld. Met *signalering* kan gespreksinformatie over netwerkgrenzen heen worden verzonden. Met *Sessiebeheer* worden de kenmerken van een end-to-end gesprek beheerd.

In typische commerciële IP-telefonie-implementaties, gaan alle gesprekken via een SIP-proxyserver. De ontvangende telefoon wordt de SIP-UAS (User Agent Server) genoemd terwijl de vragende telefoon de UAC (User Agent Client) wordt genoemd.

Routing van SIP-berichten is dynamisch. Als een SIP-proxy een aanvraag ontvangt van een UAS voor een verbinding, maar de UAC niet kan vinden, stuurt de proxy het bericht door naar een andere SIP-proxy in het netwerk. Wanneer de UAC wordt gevonden, wordt het antwoord teruggestuurd naar de UAS en worden de twee UA's met een directe peer-to-peer sessie verbonden. Spraakverkeer wordt tussen UA's via dynamisch toegewezen poorten verzonden met behulp van RTP (Real-time Protocol).

Met RTP worden real-time gegevens verzonden, zoals audio en video. Met RTP wordt geen real-time levering van gegevens gegarandeerd. RTP biedt mechanismen voor het verzenden en ontvangen van toepassingen ter ondersteuning van streaminggegevens. Doorgaans wordt RTP boven op UDP uitgevoerd.

SIP via TCP

Om statusgeoriënteerde communicatie te garanderen kan Cisco IP-telefoon TCP als het transportprotocol voor SIP gebruiken. Dit protocol verschaft *gegarandeerde levering* waarmee wordt gegarandeerd dat verloren pakketten opnieuw worden verzonden. Met het TCP wordt ook gegarandeerd dat de SIP-pakketten in dezelfde volgorde worden ontvangen als waarin ze zijn verzonden.

Met TCP wordt het probleem van UDP-poortblokkering opgelost door middel van bedrijfsfirewalls. Met TCP hoeven nieuwe poorten niet open te zijn of pakketten verwijderd, omdat TCP al wordt gebruikt voor basisactiviteiten, zoals browsen op internet of e-commerce.

Redundantie SIP-proxy

Een gemiddelde SIP-proxyserver kan tienduizenden abonnees verwerken. Met een back-upserver kan een actieve server tijdelijk worden uitgeschakeld voor onderhoud. De telefoons ondersteunt het gebruik van back-upservers om servicestoring te minimaliseren of te elimineren.

Een eenvoudige manier om proxyredundantie te ondersteunen, is door een SIP-proxyserver op te geven in het telefoonconfiguratieprofiel. De telefoon stuurt een DNS NAPTR- of SRV-query naar de DNS-server. Indien geconfigureerd, retourneert de DNS-server SRV-records die een lijst met servers voor het domein bevatten, met hun hostnamen, prioriteit, luisterpoorten, enzovoort. De telefoon probeert verbinding te maken met de servers in de volgorde van prioriteit. De server met een lager nummer heeft een latere prioriteit. In een query worden maximaal zes NAPTR-records en twaalf SRV-records ondersteund.

Wanneer de telefoon niet kan communiceren met de primaire server, kan de telefoon een failover uitvoeren naar een server met een lagere prioriteit. Indien geconfigureerd, kan de telefoon de verbinding met de primaire telefoon herstellen. Failover- en failback-ondersteuning schakelt tussen servers met verschillende SIP-transportprotocollen. De telefoon voert geen failback uit naar de primaire server tijdens een actief gesprek totdat het gesprek is beëindigd en aan de failback-voorwaarden is voldaan.

Voorbeeld van bronrecords van de 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

```

Het volgende voorbeeld toont de prioriteit van de servers vanuit het perspectief van de telefoon.

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

De telefoon stuurt altijd SIP-berichten naar het beschikbare adres met de hoogste prioriteit en met de status UP in de lijst. In het voorbeeld stuurt de telefoon alle SIP-berichten naar het adres 1.1.1.1. Als het adres 1.1.1.1 in de lijst is gemarkeerd met de status DOWN, communiceert de telefoon met 2.2.2.2. De telefoon kan de verbinding herstellen naar 1.1.1.1 wanneer aan de gespecificeerde failback-voorwaarden is voldaan. Voor meer informatie over failover en failback, zie [SIP-proxy failover, op pagina 9](#) en [SIP-proxy terugval, op pagina 10](#).

SIP-proxy failover

De telefoon voert een failover uit in een van de volgende gevallen:

- De telefoon verzendt SIP-berichten en ontvangt geen reacties van de server.
- De server beantwoordt met een code die overeenkomt met de opgegeven code in **RSC back-up proberen**.
- De telefoon krijgt een aanvraag voor een TCP-verbinding.

Het wordt nadrukkelijk aanbevolen om **Automatisch registreren bij failover** in te stellen op **Ja** wanneer **SIP-transport** is ingesteld op **Automatisch**.

U kunt deze parameters voor een specifiek toestel ook configureren in het configuratiebestand:

```

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

```

waarbij *n* het toestelnummer is.

Telefoongedrag

Wanneer de telefoon niet kan communiceren met de momenteel verbonden server, wordt de status van de serverlijst vernieuwd. De server die niet beschikbaar is, is gemarkeerd met de status DOWN in de lijst met servers. De telefoon probeert verbinding te maken met de server met topprioriteit met de status UP in de lijst.

In het volgende voorbeeld zijn de adressen 1.1.1.1 en 2.2.2.2 niet beschikbaar. De telefoon verzendt SIP-berichten naar 3.3.3.3, die de hoogste prioriteit heeft tussen de servers met de 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 het volgende voorbeeld zijn twee SRV-records van de DNS-NAPTR-reactie. Voor elke SRV-record zijn er drie A-records (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

We gaan ervan uit dat de telefoon geen verbinding kan maken met 1.1.1.1 en vervolgens wordt geregistreerd bij 1.1.1.2. Wanneer 1.1.1.2 uitvalt, hangt het telefoongedrag af van de instelling van **Proxy fallback-interval**.

- Wanneer **Proxy fallback-interval** is ingesteld op **0**, probeert de telefoon de adressen in deze volgorde: 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- Wanneer **Proxy fallback-interval** is ingesteld op een andere waarde dan nul, probeert de telefoon de adressen in deze volgorde: 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

SIP-proxy terugval

Voor de proxy-fallback moet een andere waarde dan nul zijn opgegeven in het veld **Proxy-fallbackinterval** op het tabblad **Ext (n)** in de webinterface van de telefoon. Als u dit veld instelt op 0, is de SIP-proxy failbackfunctie uitgeschakeld. U kunt deze parameter voor een specifiek toestel ook configureren in het configuratiebestand in deze indeling in te voeren:

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

waarbij *n* het toestelnummer is.

De tijd dat de telefoon een failback activeert, hangt af van de telefoonconfiguratie en de SIP-transportprotocollen die in gebruik zijn.

Om de telefoon in staat te stellen om failback uit te voeren tussen verschillende SIP-transportprotocollen, stelt u **SIP-transport** in op **Automatisch** op het tabblad **Ext (n)** in de telefoonwebinterface. U kunt deze parameter voor een specifiek toestel ook configureren in het configuratiebestand met de volgende XML-tekenreeks:

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

waarbij *n* het toestelnummer is.

Failback van een UDP-verbinding

De failback van een UDP-verbinding wordt geactiveerd door SIP-berichten. In het volgende voorbeeld kan de telefoon eerst niet worden geregistreerd bij 1.1.1.1 (TLS) op tijdstip T1 nadat er geen reactie is van de

server. Wanneer SIP-timer F verloopt, registreert de telefoon bij 2.2.2.2 (UDP) op het moment T2 ($T2=T1+SIP\text{-timer F}$). De huidige verbinding is op 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	

De telefoon heeft de volgende configuratie:

```
<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>
```

waarbij n het toestelnummer is.

De telefoon vernieuwt de registratie op tijdstip T2 ($T2=(3600-16)*78\%$). Op de telefoon wordt de adreslijst gecontroleerd op de beschikbaarheid van de IP-adressen en de uitvaltijd. Als $T2-T1 \geq 60$, wordt de mislukte server 1.1.1.1 weer hervat in UP en wordt de lijst als volgt bijgewerkt. De telefoon verzendt SIP-berichten naar 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 van een TCP-of TLS-verbinding

De failback van een TCP-of TLS-verbinding wordt gestart door de parameter **Proxy fallback-interval**. In het volgende voorbeeld kan de telefoon niet worden geregistreerd bij 1.1.1.1 (UDP) op het moment dat T1 is en dus is geregistreerd bij 2.2.2.2 (TCP). De huidige verbinding is op 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	

De telefoon heeft de volgende configuratie:

```
<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>
```

waarbij n het toestelnummer is.

De proxy fallback-interval (60 seconden) wordt geteld bij T1. De telefoon activeert proxy failback op het moment van $T1 + 60$. Als u het proxy fallback-interval instelt op 0 in dit voorbeeld, houdt de telefoon de verbinding op 2.2.2.2.

Dubbele registratie

De telefoon wordt altijd geregistreerd bij zowel primaire (of primaire uitgaande) als alternatieve (of alternatieve uitgaande) proxy's. Na de registratie stuurt de telefoon eerst Invite en Non-Invite SIP-berichten via de primaire proxy. Als er geen antwoord komt van de primaire proxy na time-out voor de nieuwe INVITE, probeert de telefoon verbinding te maken met de alternatieve proxy. Als de telefoon niet kan worden geregistreerd bij de primaire proxy, wordt een INVITE verzonden naar de alternatieve proxy zonder de primaire proxy te proberen.



Opmerking De MPP-telefoons ondersteunen dubbele registratie alleen via de UDP-verbinding.

Dubbele registratie wordt per lijn ondersteund. Drie toegevoegde parameters kunnen worden geconfigureerd via webgebruikersinterface en externe inrichting:

- Alternatieve proxy: standaardwaarde is leeg.
- Alternatieve uitgaande proxy: standaardwaarde is leeg.
- Dubbele registratie: standaardwaarde is NEE (uitgeschakeld).

Nadat u de parameters hebt geconfigureerd, start u de telefoon op zodat de functie van kracht wordt.



Opmerking Geef een waarde op voor de primaire proxy (of primaire uitgaande proxy) en alternatieve proxy (of alternatieve uitgaande proxy) om de functie goed te laten werken.

Dubbele registratie en beperkingen voor DNS-SRV

- Wanneer dubbele registratie is ingeschakeld, moet proxyterugval of herstel van DNS-SRV zijn uitgeschakeld.
- Gebruik dubbele registratie niet samen met terugval- of herstelmechanismen. Bijvoorbeeld: BroadSoft-mechanisme.
- Er is geen herstelmechanisme voor functieaanvraag. De beheerder kan echter de tijd voor nieuwe registratie aanpassen voor een directe update van de registratiestatus voor de primaire en alternatieve proxy.

Dubbele registratie en alternatieve proxy

Wanneer de parameter voor dubbele registratie is ingesteld op **Nee**, wordt alternatieve proxy genegeerd.

Failover en herstelregistratie

- Failover: op de telefoon wordt een failover uitgevoerd in geval van een time-out/fout in de transport of TCP-verbindingfouten, indien de waarden voor RSC back-up proberen en RSC reg. opnieuw proberen zijn ingevuld.
- Herstel: op de telefoon wordt geprobeerd een nieuwe registratiepoging te doen bij de primaire proxy terwijl er een registratie of een actieve verbinding is met de secundaire proxy.

De parameter Auto Register When Failover (Automatisch registreren bij failover) bepaalt het failover-gedrag wanneer zich een fout voordoet. Wanneer deze parameter is ingesteld op Ja, wordt de telefoon opnieuw geregistreerd bij failover of herstel.

Terugvalgedrag

Terugvallen vindt plaats wanneer de huidige registratie vervalt of Interval terugvallen proxy wordt geactiveerd. Als Interval terugvallen proxy wordt overschreden, gaan alle nieuwe SIP-berichten naar de primaire proxy.

Wanneer bijvoorbeeld de waarde voor Register vervalt 3600 seconden is en Interval terugvallen proxy 600 seconden is, wordt de terugval 600 seconden later geactiveerd.

Wanneer de waarde voor Register vervalt 800 seconden is en Interval terugvallen proxy 1000 seconden is, wordt de terugval geactiveerd bij 800 seconden.

Nadat weer bij de primaire server is geregistreerd, gaan alle SIP-berichten naar de primaire server.

RFC3311

Cisco IP-telefoon ondersteunt RFC-3311, de SIP UPDATE-methode.

SIP NOTIFY XML-service

Cisco IP-telefoon ondersteunt de gebeurtenis SIP NOTIFY XML-service. Bij ontvangst van een SIP NOTIFY-bericht met een XML-service-gebeurtenis, wordt een identiteitsvraag gesteld aan NOTIFY met een 401-antwoord als het bericht niet de juiste referenties bevat. De client moet de juiste referenties leveren met behulp van MD5-digest met het SIP-accountwachtwoord voor de corresponderende lijn van de IP-telefoon.

De hoofdtekst van het bericht kan het XML-gebeurtenisbericht bevatten. Bijvoorbeeld:

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

Verificatie:

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

NAT-toewijzing met Session Border Controller

Het is raadzaam een serviceprovider te kiezen die NAT-toewijzing ondersteunt via een Session Border Controller. Met door de serviceprovider geleverde NAT-toewijzing hebt u meer mogelijkheden bij de selectie van een router.

NAT-toewijzing met SIP-ALG-router

NAT-toewijzing kan worden bereikt met behulp van een router die een SIP-ALG (Application Layer Gateway) heeft. Met behulp van een SIP-ALG-router hebt u meer mogelijkheden bij de selectie van een serviceprovider.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is onderhandelingsgebaseerd en met dit protocol wordt bepaald in welk virtueel LAN (VLAN) Cisco IP-telefoon zich bevindt. Als u een Cisco-switch gebruikt, is het Cisco Discovery Protocol (CDP) beschikbaar en standaard ingeschakeld. CDP heeft de volgende kenmerken:

- Verkrijgt de protocoladressen van naburige apparaten en detecteert het platform van deze apparaten.
- Geeft informatie weer over de interfaces die uw router gebruikt.
- Is onafhankelijk van media en protocol.

Als u een VLAN zonder CDP gebruikt, moet u een VLAN-id voor Cisco IP-telefoon invoeren.

LLDP-MED

Cisco IP-telefoon ondersteunt Link Layer Discovery Protocol voor Media Endpoint Devices (LLDP-MED) voor implementatie met Cisco of andere netwerkverbindingapparaten van derden die een Laag 2-mechanisme voor automatische detectie gebruiken. Implementatie van LLDP-MED gebeurt in overeenstemming met de specificatie IEEE 802.1AB (LLDP) van mei 2005 en ANSI TIA-1057 van april 2006.

Cisco IP-telefoon werkt als een LLDP-MED Media End Point Class III-apparaat met directe LLDP-MED-koppelingen naar netwerkverbindingapparaten in overeenstemming met Media Endpoint Discovery Reference Model and Definition (ANSI TIA-1057 sectie 6).

Cisco IP-telefoon ondersteunt alleen de volgende beperkte set Type-Length-Values (TLV) als een LLDP-MED Media Endpoint-apparaat, klasse III:

- TLV chassis-id
- TLV poort-id
- TLV Time to Live
- TLV poortbeschrijving
- TLV systeemnaam
- TLV systeemmogelijkheden
- IEEE 802.3 MAC/PHY-configuratie/Status-TLV (alleen voor bekabeld netwerk)
- TLV LLDP-MED-mogelijkheden
- TLV LLDP-MED-netwerkbeleid (voor toepassingstype=Alleen spraak)
- TLV LLDP-MED Extended Power-Via-MDI (alleen voor bekabeld netwerk)
- TLV LLDP-MED-firmwareversie
- Einde van LLDPDU-TLV

De uitgaande LLDPDU bevat indien van toepassing alle voorafgaande TLV's. Voor de inkomende LLDPDU wordt de LLDPDU genegeerd als een van de volgende TLV's ontbreken. Alle andere TLV's worden niet gevalideerd en genegeerd.

- TLV chassis-id
- TLV poort-id
- TLV Time to Live
- TLV LLDP-MED-mogelijkheden
- TLV LLDP-MED-netwerkbeleid (voor toepassingstype=Alleen spraak)
- Einde van LLDPDU-TLV

Cisco IP-telefoon stuurt indien van toepassing de afsluitings-LLDPDU. Het LLDPDU-frame bevat de volgende TLV's:

- TLV chassis-id
- TLV poort-id
- TLV Time to Live
- Einde van LLDPDU-TLV

Er zijn enkele beperkingen in de implementatie van LLDP-MED op Cisco IP-telefoons:

- Informatie van burens kan niet worden opgeslagen en opgehaald.
- SNMP en corresponderende MIB's worden niet ondersteund.
- Statistische tellers kunnen niet worden opgenomen en opgehaald.
- Volledige validatie van alle TLV's vindt niet plaats. TLV's die niet van toepassing zijn op de telefoons, worden genegeerd.
- Protocolstatusmachines zoals vermeld in de standaarden, worden alleen ter naslag gebruikt.

TLV chassis-id

Voor de uitgaande LLDPDU ondersteunt de TLV subtype=5 (netwerkadres). Wanneer het IP-adres bekend is, is de waarde van de chassis-id een octet van het INAN-adresfilienummer gevolgd door de octetreeks voor het IPv4-adres dat voor spraakcommunicatie wordt gebruikt. Als het IP-adres onbekend is, is de waarde voor de chassis-id 0.0.0.0. De enige ondersteunde INAN-adresfamilie is IPv4. Momenteel wordt het IPv6-adres voor de chassis-id niet ondersteund.

Voor de inkomende LLDPDU wordt de chassis-id behandeld als een ondoorzichtige waarde om de MSAP-id te vormen. De waarde wordt niet gevalideerd met het bijbehorende subtype.

TLV chassis-id is verplicht als de eerste TLV. Slechts één TLV chassis-id is toegestaan voor de uitgaande en inkomende LLDPDU's.

TLV poort-id

Voor de uitgaande LLDPDU ondersteunt de TLV subtype=3 (MAC-adres). Het MAC-adres van 6 octet voor de Ethernet-poort wordt gebruikt voor de waarde van poort-id.

Voor de inkomende LLDPDU wordt TLV poort-id behandeld als een ondoorzichtige waarde om de MSAP-id te vormen. De waarde wordt niet gevalideerd met het bijbehorende subtype.

TLV poort-id is verplicht als de tweede TLV. Slechts één TLV poort-id is toegestaan voor de uitgaande en inkomende LLDPDU's.

TLV Time to Live

Voor de uitgaande LLDPDU is de waarde van TTL (Time to Live) 180 seconden. Dit verschilt van de waarde van 120 seconden die volgens de standaard wordt aanbevolen. Voor de afsluitings-LLDPDU is de TTL-waarde altijd 0.

De TLV Time to Live is verplicht als de derde TLV. Slechts één TLV Time to Live is toegestaan voor de uitgaande en inkomende LLDPDU's.

Einde van LLDPDU-TLV

De waarde is 2 octet, alle nul. Deze TLV is verplicht en er is er slechts één toegestaan voor de uitgaande en inkomende LLDPDU's.

TLV poortbeschrijving

Voor de uitgaande LLDPDU in TLV poortbeschrijving is de waarde voor de poortbeschrijving hetzelfde als "TLV poort-id" voor CDP. De inkomende LLDPDU, TLV poortbeschrijving, wordt genegeerd en niet gevalideerd. Slechts één TLV poortbeschrijving is toegestaan voor uitgaande en inkomende LLDPDU's.

TLV systeemnaam

Voor Cisco IP-telefoon is de waarde SEP+MAC-adres.

Voorbeeld: SEPAC44F211B1D0

De inkomende LLDPDU, de systeemnaam-TLV, wordt genegeerd en niet gevalideerd. Slechts één systeemnaam-TLV is toegestaan voor de uitgaande en inkomende LLDPDU's.

TLV systeemmogelijkheden

Voor de uitgaande LLDPDU in TLV systeemmogelijkheden moeten de bitwaarden voor de velden met systeemmogelijkheden van 2 octet worden ingesteld voor Bit 2 (bridge) en Bit 5 (telefoon) voor een telefoon met een pc-poort. Als de telefoon geen pc-poort heeft, moet alleen Bit 5 worden ingesteld. Dezelfde systeemmogelijkheidswaarde moet worden ingesteld voor het veld met ingeschakelde mogelijkheid.

Voor de inkomende LLDPDU wordt de TLV systeemmogelijkheden genegeerd. De TLV wordt semantisch niet gevalideerd met het MED-apparaatype.

TLV systeemmogelijkheden is verplicht voor uitgaande LLDPDU's. Er is slechts één TLV systeemmogelijkheden toegestaan.

TLV beheeradres

Met TLV wordt een adres geïdentificeerd dat is gekoppeld aan de lokale LLDP-agent (die kan worden gebruikt om hogere laagagentiteiten te bereiken) om te helpen bij detectie door netwerkbeheer. Met TLV kan zowel het systeeminterfacenummer als een OID (Object Identifier) worden opgenomen, die zijn gekoppeld aan dit beheeradres, als een van beide of beide bekend zijn.

- Tekenreekslengte TLV-informatie: dit veld bevat de lengte (in octets) van alle velden in de TLV-informatiereeks.
- Tekenreekslengte beheeradres: dit veld bevat de lengte (in octet) van de velden voor het subtype beheeradres en het beheeradres.

TLV systeembeschrijving

Met TLV kan het netwerkbeheer de systeembeschrijving doorgeven.

- TLV information string length (Tekensreekslengte TLV-informatie): met dit veld wordt de exacte lengte (in octet) van de systeembeschrijving aangegeven.
- System description (Systeembeschrijving): dit veld bevat een alfanumerieke tekensreeks die een tekstuele beschrijving van de netwerkentiteit vormt. De systeembeschrijving bevat de identificatie met volledige naam en versie van het type systeemhardware, softwarebesturingsysteem en netwerksoftware. Indien implementaties IETF RFC 3418 ondersteunen, moet het sysDescr-object voor dit veld worden gebruikt.

IEEE 802.3 MAC/PHY-configuratie/Status-TLV

De TLV is niet voor automatische onderhandeling, maar voor probleemoplossingsdoeleinden. Voor de inkomende LLDPDU wordt de TLV genegeerd en niet gevalideerd. Voor de uitgaande LLDPDU moet voor de TLV de octetwaarde voor ondersteuning/status automatische onderhandeling het volgende zijn:

- Bit 0: stel in op 1 om aan te geven dat de ondersteuningsfunctie voor automatische onderhandeling wordt ondersteund.
- Bit 1: stel in op 1 om aan te geven dat de status voor automatische onderhandeling is ingeschakeld.
- Bit 2-7: stel in op 0.

De bitwaarden van het veld voor de doorgegeven mogelijkheid van automatische PMD-onderhandeling van 2 octet moet worden ingesteld op:

- Bit 13: 10BASE-T half-duplex modus
- Bit 14: 10BASE-T full-duplex modus
- Bit 11: 100BASE-TX half-duplex modus
- Bit 10: 100BASE-TX full-duplex modus
- Bit 15: onbekend

Bit 10, 11, 13 en 14 moeten worden ingesteld.

De waarde voor het operationele MAU-type van 2 octet moet worden ingesteld om het werkelijke operationele MAU-type weer te geven:

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

Zo wordt bijvoorbeeld de telefoon meestal ingesteld op 100BASE-TX full-duplex. De waarde 16 moet dan worden ingesteld. De TLV is optioneel voor een bekabeld netwerk en niet van toepassing op een draadloos netwerk. De telefoon verzendt deze TLV alleen in bekabelde modus. Wanneer de telefoon niet is ingesteld voor automatische onderhandeling, maar specifieke snelheid/duplexiteit, moet voor de uitgaande LLDPDU TLV, bit 1 voor de octetwaarde voor ondersteuning/status automatische onderhandeling leeg (0) zijn om aan te geven dat automatische onderhandeling is uitgeschakeld. Het veld voor de doorgegeven mogelijkheid van automatische PMD-onderhandeling van 2 octet moet worden ingesteld op 0x8000 om onbekend aan te geven.

TLV LLDP-MED-mogelijkheden

Voor de uitgaande LLDPDU moet de TLV apparaattype 3 (End Point Class III) hebben met de volgende bits ingesteld voor het veld 2-octet Capability (Mogelijkheid 2 octet):

Bit Position (Bitpositie)	Functie
0	LLDP-MED-mogelijkheden
1	Netwerkbeleid
4	Extended Power via MDI-PD
5	Overzicht

Als de TLV LLDP-MED niet aanwezig is, wordt de LLDPDU genegeerd voor de inkomende TLV. TLV LLDP-MED-mogelijkheden is verplicht en er is er slechts één toegestaan voor de uitgaande en inkomende LLDPDU's. Alle andere TLV's LLDP-MED worden genegeerd als deze aanwezig zijn vóór de TLV LLDP-MED-mogelijkheden.

TLV netwerkbeleid

In de TLV voor de uitgaande LLDPDU wordt de onbekende beleidsvlag (U) ingesteld op 1 om het VLAN of de DSCP te bepalen. Als de VLAN-instelling of DSCP bekend is, wordt de waarde ingesteld op 0. Wanneer het beleid onbekend is, worden alle andere waarden ingesteld op 0. Voordat het VLAN wordt bepaald of gebruikt, wordt de getagde markering (T) ingesteld op 0. Als het gemarkeerde VLAN (VLAN-id > 1) wordt gebruikt voor de telefoon, wordt de getagde markering (T) ingesteld op 1. Gereserveerd (X) wordt altijd ingesteld op 0. Als het VLAN wordt gebruikt, worden de bijbehorende VLAN-id en L2-prioriteit dienovereenkomstig ingesteld. Geldige waarde voor VLAN-id ligt in het bereik 1-4094. VLAN-id=1 wordt echter nooit gebruikt (beperking). Als DSCP wordt gebruikt, wordt het waardebereik van 0-63 dienovereenkomstig ingesteld.

In de TLV voor de inkomende LLDPDU zijn TLV's voor meerdere netwerkbeleidsregels toegestaan voor verschillende toepassingstypen.

LLDP-MED Extended Power-Via-MDI TLV

In de TLV voor de uitgaande LLDPDU is de binaire waarde voor voedingstype ingesteld op "0 1" om aan te geven dat het voedingstype voor de telefoon PD Device (PD-apparaat) is. De voedingsbron voor de telefoon wordt ingesteld op "PSE and local" (PSE en lokaal) met binaire waarde "1 1". De voedingsprioriteit wordt ingesteld op binair "0 0 0 0" om onbekende prioriteit aan te geven terwijl de voedingswaarde is ingesteld op maximale voedingswaarde. De voedingswaarde voor Cisco IP-telefoon is 12900mW.

Voor de inkomende LLDPDU wordt de TLV genegeerd en niet gevalideerd. Slechts één TLV is toegestaan in de uitgaande en inkomende LLDPDU's. De telefoon verzendt de TLV alleen voor het bekabelde netwerk.

De LLDP-MED-standaard is oorspronkelijk ontwikkeld in de context van Ethernet. De discussie over LLDP-MED voor draadloze netwerken is nog niet afgerond. Raadpleeg ANSI-TIA 1057, bijlage C, C.3 Toepasbare TLV voor VoWLAN, tabel 24. Het wordt aan geraden TLV niet van toepassing te laten zijn binnen de context van het draadloze netwerk. Deze TLV is bedoeld voor gebruik in de context van PoE en Ethernet. Indien de TLV wordt toegevoegd, wordt er geen waarde mee verschaft voor netwerkbeheer of voedingsbeleidaanpassing voor de switch.

LLDP-MED Inventory Management TLV (TLV LLDP-MED-inventarisbeheer)

Deze TLV is optioneel voor apparaatklasse III. Voor de uitgaande LLDPDU wordt alleen firmwarevisie TLV ondersteund. De waarde voor de firmwarevisie is de versie van firmware op de telefoon. Voor de inkomende LLDPDU worden de TLV's genegeerd en niet gevalideerd. Slechts één firmwarerevisie TLV is toegestaan voor de uitgaande en inkomende LLDPDU's.

Definitieve netwerkbeleidsoplossing en QoS

Speciale VLAN's

VLAN=0, VLAN=1 en VLAN=4095 worden op dezelfde manier behandeld als een niet-getagd VLAN. Omdat het VLAN niet-getagd is, is CoS (Class of Service) niet van toepassing.

Standaard-QoS voor SIP-modus

Als er geen netwerkbeleid van CDP of LLDP-MED is, wordt het standaardnetwerkbeleid gebruikt. CoS wordt gebaseerd op de configuratie voor het specifieke toestel. Deze optie is alleen van toepassing als het handmatige VLAN is ingeschakeld en het handmatige VLAN-id niet gelijk is aan 0, 1 of 4095. ToS (type of service) is gebaseerd op de configuratie voor het specifieke toestel.

QoS-oplossing voor CDP

Als er een geldig netwerkbeleid van CDP is:

- Als het VLAN=0, 1 of 4095, wordt het VLAN niet ingesteld of wordt het VLAN niet-getagd. CoS is niet van toepassing, maar DSCP is van toepassing. ToS is gebaseerd op de standaardwaarde, zoals eerder is beschreven.
- Als $VLAN > 1$ en $VLAN < 4095$, wordt VLAN dienovereenkomstig ingesteld. CoS en ToS worden gebaseerd op de standaardwaarde, zoals eerder is beschreven. DSCP is van toepassing.
- De telefoon wordt opnieuw opgestart en de snelle startreeks wordt opnieuw gestart.

QoS-oplossing voor LLDP-MED

Als CoS van toepassing is en $CoS = 0$, wordt de standaardwaarde voor het specifieke toestel gebruikt, zoals eerder is beschreven. Maar de waarde die wordt weergegeven op L2-prioriteit voor TLV voor uitgaande LLDPDU, is gebaseerd op de waarde die wordt gebruikt voor toestel 1. Als CoS van toepassing is en $CoS! = 0$, wordt CoS gebruikt voor alle toestelnummers.

Als DSCP (toegewezen aan ToS) van toepassing is en $DSCP = 0$, wordt de standaardwaarde voor het specifieke toestel gebruikt, zoals eerder is beschreven. Maar de waarde die wordt weergegeven op DSCP voor TLV voor uitgaande LLDPDU, is gebaseerd op de waarde die wordt gebruikt voor het toestel 1. Als DSCP van toepassing is en als $DSCP! = 0$ is, wordt DSCP gebruikt voor alle toestelnummers.

Als $VLAN > 1$ en $VLAN < 4095$, wordt VLAN dienovereenkomstig ingesteld. CoS en ToS worden gebaseerd op de standaardwaarde, zoals eerder is beschreven. DSCP is van toepassing.

Als er een geldig netwerkbeleid voor de spraaktoepassing van LLDP-MED PDU is en als de getagde markering is ingesteld, zijn VLAN, L2-prioriteit (CoS) en DSCP (toegewezen aan ToS) allemaal van toepassing.

Als er een geldig netwerkbeleid voor de spraaktoepassing van LLDP-MED PDU is en als de getagde markering niet is ingesteld, is alleen DSCP (toegewezen aan ToS) van toepassing.

Cisco IP-telefoon wordt opnieuw gestart en de snelle startreeks wordt opnieuw gestart.

Coëxistentie met CDP

Als zowel CDP als LLDP-MED zijn ingeschakeld, wordt met het netwerkbeleid voor het VLAN het laatste beleid ingesteld of gewijzigd met een van de twee volgende detectiemodi. Als zowel LLDP-MED als CDP zijn ingeschakeld, verzendt de telefoon tijdens het opstarten CDP- en LLDP-MED-PDU's.

Inconsistente configuratie en gedragingen voor netwerkverbindingssapparaten voor CDP- en LLDP-MED-modi kunnen resulteren in een trillend rebootend gedrag op de telefoon vanwege het overschakelen naar verschillende VLAN's.

Als het VLAN niet is ingesteld door CDP en LLDP-MED, wordt de VLAN-id gebruikt die handmatig is geconfigureerd. Als de VLAN-id niet handmatig is geconfigureerd, wordt geen VLAN ondersteund. DSCP wordt gebruikt en met het netwerkbeleid wordt indien van toepassing LLDP-MED bepaald.

LLDP-MED en meerdere netwerkapparaten

U kunt hetzelfde toepassingstype voor netwerkbeleid gebruiken. Telefoons ontvangen echter verschillende Laag 2 of Laag 3 QoS-netwerkbeleidsregels van meerdere netwerkverbindingssapparaten. In een dergelijk geval wordt het laatste geldige netwerkbeleid geaccepteerd.

LLDP-MED en IEEE 802.X

Cisco IP-telefoon ondersteunt IEEE 802.X niet en werkt niet in een 802.1X bekabelde omgeving. IEEE 802.1X of Spanning Tree Protocols in netwerkapparaten kunnen echter resulteren in vertraging van snelle start-antwoord van switches.

Over de vertaling

Cisco biedt voor sommige gebieden lokalisatie aan voor deze content. De vertalingen worden echter alleen aangeboden ter informatie. Als er sprake is van inconsistentie, heeft de Engelse versie van de content de voorkeur.