Technische details

Ondersteunde netwerkprotocollen

Cisco IP-conferentietelefoons 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 1: Ondersteunde netwerkprotocollen op de Cisco IP-conferentietelefoon

Netwerkprotocol	Doel	Opmerkingen over gebruik
Bootstrap Protocol (BootP)	BootP schakelt een netwerkapparaat, zoals de 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.	De telefoon gebruikt CDP om informatie te communiceren als de hulp-VLAN-id, voedingsbeheerdetails per poort en QoS-configuratiegegeven (Quality of Service) met de Cisco Catalyst-switch.

Netwerkprotocol	Doel	Opmerkingen over gebruik
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 ingeschakeld. Als DHCP is uitgeschakeld, moet u het IP-adres, subnetmasker, gateway en TFTP-server lokaal handmatig op elke telefoon configureren. We raden u aan de aangepaste DHCP-optie 150 te gebruiken. Met deze methode kunt u het IP-adres van de TFTP-server configureren als de optiewaarde. **Opmerking** Als u optie 150 niet kunt gebruiken, kiest u DHCP-optie 66.
Hypertext Transfer Protocol (HTTP)	HTTP is het standaardprotocol voor informatie-overdracht en het verplaatsen van documenten over internet en het web.	Telefoons gebruiken HTTP voor XML-services, configuratie, upgrade en probleemoplossing.
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.	Voor webtoepassingen met ondersteuning voor zowel HTTP als HTTPS zijn twee URL's geconfigureerd. Telefoons die ondersteuning bieden voor HTTPS, kiezen de HTTPS-URL. Er wordt een hangslotpictogram weergegeven voor de gebruiker als de verbinding met de service via HTTPS verloopt.
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.	De telefoon implementeert de IEEE 802.1X-standaard via ondersteuning voor de volgende verificatiemethoden: EAP-FAST en EAP-TLS. Wanneer 802.1X-verificatie wordt ingeschakeld op de telefoon, moet u de spraak-VLAN uitschakelen.
Internet Protocol (IP)	IP is een berichtprotocol dat pakketten adresseert en verzendt via het netwerk.	Als netwerkapparaten willen communiceren met IP, moeten ze een toegewezen IP-adres, subnet en gateway hebben. IP-adressen, subnetten en gateway-id's worden automatisch toegewezen als u de telefoon gebruikt met Dynamic Host Configuration Protocol (DHCP). Als u DHCP niet gebruikt, moet u deze eigenschappen lokaal handmatig aan elke telefoon toewijzen. De telefoons ondersteunen het IPv6-adres.

Netwerkprotocol	Doel	Opmerkingen over gebruik
Link Layer Discovery Protocol (LLDP)	LLDP is een gestandaardiseerd netwerkdetectieprotocol (vergelijkbaar met CDP) dat wordt ondersteund op een aantal apparaten van Cisco en derden.	
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is een uitbreiding van de LLDP-standaard die is ontwikkeld voor spraakproducten.	De telefoon ondersteunt LLDP-MED op de SW-poort voor het communiceren van informatie zoals: • Configuratie spraak-VLAN • Apparaatdetectie • Voedingsbeheer • Inventarisbeheer Voor meer informatie over ondersteuning voor LLDP-MED raadpleegt u de whitepaper *LLDP-MED and Cisco Discovery Protocol* via deze URL: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cdd46.shtml
Real-Time Transport Protocol (RTP)	RTP is een standaardprotocol voor het transporteren van real-time gegevens, zoals interactieve spraak en video, via gegevensnetwerken.	De telefoons gebruiken het RTP-protocol voor het verzenden en ontvangen van real-time spraakverkeer van andere telefoons en 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 standaard ingeschakeld.
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 VoIP-protocollen is SIP ontworpen om functies als signalering en sessiebeheer te leveren binnen een telefonienetwerk met pakketten. Met signalering kunnen gespreksgegevens over netwerkgrenzen heen worden verzonden. Sessiebeheer biedt de mogelijkheid om de kenmerken van een end-to-end gesprek te beheren. Cisco IP-telefoons ondersteunen het SIP-protocol wanneer de telefoons werken met alleen IPv6, alleen IPv4, of met zowel IPv4 als IPv6.
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.	De telefoons gebruiken SRTP voor mediacodering.

Netwerkprotocol	Doel	Opmerkingen over gebruik
Transmission Control Protocol (TCP)	TCP is een verbindingsgericht transportprotocol.	Telefoons gebruiken TCP om verbinding te maken met een gespreksserver van derden en voor toegang tot XML-services.
Transport Layer Security (TLS)	TLS is een standaardprotocol voor het beveiligen en verifiëren van communicatie.	Als beveiliging wordt geïmplementeerd, gebruiken telefoons het TLS-protocol voor veilige registratie bij de gespreksserver van derden.
Trivial File Transfer Protocol (TFTP)	TFTP zorgt dat u bestanden over het netwerk kunt verzenden. Voor de telefoon kunt u met TFTP een configuratiebestand ophalen dat specifiek is voor het telefoontype.	TFTP vereist een TFTP-server in uw netwerk, die automatisch kan worden aangegeven vanaf de DHCP-server. Als u wilt dat een telefoon een TFTP-server gebruikt die afwijkt van de telefoon die wordt opgegeven door de DHCP-server, kunt u handmatig het IP-adres van de TFTP-server toewijzen via het menu Netwerkinstellingen op de telefoon.
User Datagram Protocol (UDP)	UDP is een verbindingsloos berichtenprotocol voor het leveren van gegevenspakketten.	De telefoons verzenden en ontvangen RTP-stromen die gebruikmaken van UDP.

Telefoongedrag tijdens netwerkcongestie

Alle factoren die de netwerkprestaties verslechteren, kunnen invloed hebben op de audiokwaliteit van de telefoon. In sommige gevallen kan een gesprek zelfs wegvallen. Bronnen van netwerkverslechtering zijn onder andere de volgende activiteiten:

- Beheertaken, zoals een interne poortscan of een beveiligingsscan.
- Aanvallen die zich voordoen op uw netwerk, zoals een Denial of Service-aanval.

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.

Routering 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

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

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

srv1     3600    IN    A   1.1.1.1
srv2     3600    IN    A   2.2.2.2
srv3     3600    IN    A   3.3.3.3
```

```
srv4     3600    IN    A   4.4.4.4
srv5     3600    IN    A   5.5.5.5
srv6     3600    IN    A   6.6.6.6
```

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 6en SIP-proxy terugval, op pagina 7.

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 voor beeld 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-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 > = 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.

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.

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 Transversal met telefoons

Met NAT (Network Address Translation) kunnen meerdere apparaten één, openbaar, routeerbaar IP-adres delen om verbindingen via internet tot stand te brengen. NAT is aanwezig in veel breedbandtoegangsapparaten om openbare en persoonlijke IP-adressen te vertalen. VoIP kan alleen samengaan met NAT als NAT-traversal aanwezig is.

Niet alle serviceproviders verschaffen NAT-traversal. Als uw serviceprovider geen NAT-traversal verschaft, hebt u verschillende mogelijkheden:

- **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.
- **NAT-koppeling met een statisch IP**-adres: NAT-koppeling met een extern (openbaar) statisch IP-adres kan worden bereikt om samen werking met de service provider te garanderen. Het in de router gebruikte NAT-mechanisme moet symmetrisch zijn. Zie Symmetrische of asymmetrische NAT bepalen voor meer informatie.

  Gebruik NAT-toewijzing alleen als het serviceprovidernetwerk geen Session Border Controller-functionaliteit verschaft. Meer informatie over het configureren van NAT-koppeling met een statisch IP-adres vindt u in NAT-toewijzing configureren met het statische IP-adres.
- **NAT-toewijzing met STUN**: als het serviceprovidernetwerk geen SBC-functionaliteit (Session Border Controller) verschaft en als aan de andere vereisten wordt voldaan, is het mogelijk STUN (Session Traversal Utilities voor NAT) te gebruiken om de NAT-toewijzing te detecteren. Zie voor meer informatie over het configureren van de NAT-toewijzing met STUN NAT-toewijzing met STUN configureren.

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 netwerkverbindingsapparaten 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 netwerkverbindingsapparaten 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 buren 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-adresfamilienummer 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-apparaattype.

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 laagentiteiten 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 (Tekenreekslengte TLV-informatie): met dit veld wordt de exacte lengte (in octet) van de systeembeschrijving aangegeven.
- System description (Systeembeschrijving): dit veld bevat een alfanumerieke tekenreeks die een tekstuele beschrijving van de netwerkentiteit vormt. De systeembeschrijving bevat de identificatie met volledige naam en versie van het type systeemhardware, softwarebesturingssysteem 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

Bit Position (Bitpositie)	Functie
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 netwerkverbindingsapparaten 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

Als hetzelfde toepassingstype wordt gebruikt voor het netwerkbeleid, maar verschillende Laag 2 of Laag 3 QoS-netwerkbeleidsregels worden ontvangen door de telefoons van meerdere netwerkverbindingsapparaten, wordt het laatste geldige netwerkbeleid gevolgd. Om een deterministisch en consistent netwerkbeleid te garanderen, moeten meerdere netwerkverbindingsapparaten geen conflicterende netwerkbeleidsregels versturen voor hetzelfde toepassingstype.