Technische details

Specificaties basisstation

De volgende tabel beschrijft de fysieke en operationele omgevingsspecificaties voor het basisstation.

Tabel 1: Fysieke en operationele omgevingsspecificaties

Specificatie	Waarde of bereik
Bedrijfstemperatuur	0° tot 45°C (32° tot 113°F)
Relatieve vochtigheid bij in bedrijf	10% tot 90% (niet-condenserend)
Opslagtemperatuur	–10° tot 60°C (14° tot 140°F)
Relatieve vochtigheid opslag	10% tot 95% (niet-condenserend)
Hoogte	120 mm (4,75 inch)
Breedte	120 mm (4,75 inch)
Diepte	30 mm (1,25 inch)
Gewicht	167 g (6 oz.)
Snoeren	• Categorie 3/5/5e/6 voor 10-Mbps snoeren met 4 paar • Categorie 5/5e/6 voor 100-Mbps snoeren met 4 paar
Afstandsvereisten	Conform de Ethernet-specificatie wordt een maximale kabellengte ondersteund tussen een basisstation en de switch van 100 meter.

Specificatie	Waarde of bereik
Voeding	Voedingsadapter voor lokale stroom PoE Ethernet (Ethernet-adapter voor normale voeding); IEEE 802.3: voedingsklasse 2 (3,84 - 6,49 W)
RF-banden (radiofrequentie)	Banden worden ingesteld in de fabriek en kunnen niet worden gewijzigd door klanten. • 1880 - 1895 (Taiwan) • • 1880 – 1900 MHz (Australië en Nieuw-Zeeland – minder stroom 22 dBM) • 1880 – 1900 MHz (E.U. en APAC) • 1910 – 1930 MHz (LATAM en Argentinië) • 1910 – 1920 MHz (Brazilië en Uruguay) • 1910 – 1920 MHz (Uruguay – minder stroom 140 mW) • 1910 – 1930 MHz (Chili – minder stroom 22 dBM) • 1920 – 1930 MHz (VS en Canada)

Meer technische informatie over het basisstation vindt u in het gegevensblad op:

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-dect-6800-series-multiplatform-firmware/datasheet-listing.html

Configuratiewijzigingen van basisstation vastleggen in logboeken

U kunt de configuratiewijzigingen van gebruikers in het basisstation vastleggen met de functie voor het vastleggen van configuratiewijzigingen. Op dezelfde manier kunt u de configuratiewijzigingen van de handset bijhouden. In de wijzigingslogboeken wordt in het basisgeheugen de informatie opgeslagen over de parameters die zijn gewijzigd. Deze informatie bevat echter geen details van de wijzigingen. Er worden alleen specifieke wijzigingen in de configuratie opgeslagen. Het wijzigingslogboek wordt gewist nadat de wijzigingen zijn gerapporteerd.

Rapportage van configuratiewijzigingen

Wanneer er wijzigingen in de configuratie van het basisstation worden gerapporteerd, vraagt het basisstation met DECT vergrendelde handsets om wijzigingenlogboeken. Het basisstation verzendt drie verzoeken, om de vijf seconden één, voor elke vergrendelde handset. Zodra de aanvragen voor alle handsets zijn voltooid, worden de wijzigingslogboeken van de basis en de handsets verzameld, verwerkt en omgezet in de juiste XML-tags. Vervolgens worden deze tags naar de configuratieserver verzonden. Als de handset niet reageert, let de syslog dit gedrag vast. De wijzigingslogboeken van de handset van het apparaat worden alleen gewist nadat deze op een basisstation zijn afgeleverd.

Specificaties handset

De volgende tabel beschrijft de fysieke en operationele omgevingsspecificaties voor de handsets.

Tabel 2: Fysieke en operationele omgevingsspecificaties

Specificatie	Waarde of bereik
Bedrijfstemperatuur	0° tot 45°C (32° tot 113°F)
Relatieve vochtigheid bij in bedrijf	10% tot 90% (niet-condenserend)
Opslagtemperatuur	–10° tot 60°C (14° tot 140°F)
Relatieve vochtigheid opslag	10% tot 95% (niet-condenserend)
Hoogte	6825 handset: 4.6 in. (117 mm) 6825 robuuste handset: 4.6 in. (117 mm) 6823 handset: 4.82 in. (122 mm)
Breedte	6825 handset: 1.8 in. (46 mm) 6825 robuuste handset: 1.8 in. (46 mm) 6823 handset: 1.99 in. (51mm)
Diepte	6825 handset: 0.78 in. (20 mm) 6825 robuuste handset: 0.78 in. (20 mm) 6823 handset: 0.91 in. (23 mm)
Gewicht	6825 handset: 3 g. (86 g) 6825 robuuste handset: 3 g. (86 g) 6823 handset: 3.17 g. (90 g)
Voeding	Oplaadbare Lithium Ion-batterij.

Meer technische informatie over de handsets vindt u in het gegevensblad op:

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-dect-6800-series-multiplatform-firmware/datasheet-listing.html

Netwerkprotocollen

Handsets en basisstations van Cisco 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 handsets en basisstations worden ondersteund.

Tabel 3: Ondersteunde netwerkprotocollen

Netwerkprotocol	Doel	Opmerkingen over gebruik
Bootstrap Protocol (BootP)	BootP schakelt een netwerkapparaat, zoals de handset, 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. Het systeemeigen VLAN-type van de CDP kan worden gebruikt om de VLAN-netwerkgegevens te verkrijgen.	Dit apparaat 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.
Domeinnaamserver (DNS)	DNS zet domeinnamen om in IP-adressen.	Het basisstation heeft een DNS-client om domeinnamen te vertalen in IP-adressen.
Dynamic Host Configuration Protocol (DHCP)	DHCP wijst een IP-adres dynamisch toe aan netwerkapparaten. Met DHCP kunt u een basisstation aansluiten op het netwerk en het basisstation laten werken zonder dat u handmatig een IP-adres moet toewijzen of aanvullende netwerkparameters moet configureren.	DHCP is standaard ingeschakeld. Indien uitgeschakeld, moet u het IP-adres, subnetmasker en gateway lokaal handmatig op elk basisstation configureren. We raden u aan dat u de aangepaste DHCP-optie 160, 159 gebruikt.
Hypertext Transfer Protocol (HTTP)	HTTP is het standaardprotocol voor informatie-overdracht en het verplaatsen van documenten over internet en het web.	Het basisstation gebruikt HTTP voor XML-services, configuratie, upgrade en probleemoplossing.
Hypertext Transfer Protocol Secure (HTTPS)	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 worden twee URL's geconfigureerd. Basisstations die HTTPS ondersteunen, kiezen de HTTPS-URL. Er wordt een hangslotpictogram weergegeven voor de gebruiker als de verbinding met de service via HTTPS verloopt.

Netwerkprotocol	Doel	Opmerkingen over gebruik
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 het basisstation gebruikt met Dynamic Host Configuration Protocol (DHCP). Als u DHCP niet gebruikt, moet u deze eigenschappen lokaal handmatig aan elk basisstation toewijzen.
Link Layer Discovery Protocol (LLDP)	Informatie over het VLAN-netwerk kunnen worden van de LLDP van vele subtypes van het type 127 worden opgehaald. In deze uitvoering wordt de informatie uit één van twee subtypes verkregen, met de volgende prioriteit: **1.** IEEE – POORT VLAN-ID **2.** Netwerkbeleid	
Network Transport Protocol (NTP)	NTP is een netwerkprotocol voor kloksynchronisatie tussen computersystemen via pakketgeschakelde gegevensnetwerken met variabele latentie.	Het basisstation gebruikt NTP om te communiceren met de tijdserver.
Real-Time Transport Protocol (RTP)	RTP is een standaardprotocol voor het transporteren van real-time gegevens, zoals interactieve spraak en video, via gegevensnetwerken.	Het basisstation gebruikt het RTP-protocol voor het verzenden en ontvangen van real-time spraakverkeer van andere apparaten 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 uitgeschakeld.
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-voorzieningen, zoals codectypen, DTMF-detectie en comfortabel geluid, worden normaal gesproken wereldwijd geconfigureerd door een oproepbeheersysteem van derden of een gebruikte mediagateway. Sommige SIP-eindpunten staan mogelijk configuratie toe van deze parameters op het eindpunt zelf.

Netwerkprotocol	Doel	Opmerkingen over gebruik
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.
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.	Handsets en basisstations gebruiken SRTP voor mediacodering.
Transmission Control Protocol (TCP)	TCP is een verbindingsgericht transportprotocol.	—
Transport Layer Security (TLS)	TLS is een standaardprotocol voor het beveiligen en verifiëren van communicatie.	Als beveiliging wordt geïmplementeerd, gebruikt het basisstation het TLS-protocol voor veilige registratie bij het gespreksbeheersysteem van derden.
Trivial File Transfer Protocol (TFTP)	TFTP zorgt dat u bestanden over het netwerk kunt verzenden. Voor het basisstation 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.
User Datagram Protocol (UDP)	UDP is een verbindingsloos berichtenprotocol voor het leveren van gegevenspakketten.	UDP wordt alleen gebruikt voor RTP-stromen. SIP maakt gebruik van UDP, TCP en TLS.

De netwerk-VLAN herstellen

Wanneer de ontdekkingspakketten voor advertenties arriveren, worden ze gecontroleerd en geanalyseerd en de daarin opgenomen netwerkinformatie wordt vergeleken met vorige pakketten. Als de VLAN verandert, moet de DECT-basis opnieuw worden opgestart en opnieuw worden verbonden om een nieuwe netwerkinitialisatie te voltooien.

SIP-configuratie

SIP en Cisco IP DECT-telefoon

De Cisco IP DECT-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 handset wordt de SIP-UAS (User Agent Server) genoemd terwijl de vragende handset 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 gebruikersagenten en worden de twee gebruikersagenten met een directe peer-to-peer sessie verbonden. Spraakverkeer wordt tussen gebruikersagenten 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 over TCP

Om statusgeoriënteerde communicatie te garanderen kan Cisco IP DECT-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.

Redundantie SIP-proxy

Een gemiddelde SIP-proxyserver kan tienduizenden abonnees verwerken. Met een back-upserver kan een actieve server tijdelijk worden uitgeschakeld voor onderhoud. Het basisstation 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 configuratieprofiel van het basisstation. Het basisstation 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. Het basisstation 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 het basisstation niet kan communiceren met de primaire server, kan het basisstation een failover uitvoeren naar een server met een lagere prioriteit. Indien geconfigureerd, kan het basisstation de verbinding met de primaire telefoon herstellen. Failover- en failback-ondersteuning schakelt tussen servers met verschillende SIP-transportprotocollen. Het basisstation 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

```
sipurash     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 het basisstation.

```
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
```

Het basisstation stuurt altijd SIP-berichten naar het beschikbare adres met de hoogste prioriteit en met de status UP in de lijst. In het voorbeeld stuurt het basisstation 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 het basisstation met 2.2.2.2. Het basisstation 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 8en SIP-proxy terugval, op pagina 9.

SIP-proxy failover

Het basisstation voert een failover uit in een van de volgende gevallen:

- **Timer snel antwoord verloopt**: in RFC3261 worden de twee transactietimers, TIMER B en TIMER F, gedefinieerd wanneer een INVITE-transactie en een Non-INVITE-transactie respectievelijk zijn verlopen. Deze kunnen met een standaardwaarde van 5 sec worden geconfigureerd. Wanneer een van deze timers afloopt en de bijbehorende SIP-transactie mislukt, wordt een failover geactiveerd. Failover wordt niet geactiveerd door aanvragen in een dialoogvenster.
- **SIP 5xx-reactiecodes:** als de server reageert met een 5xx-reactie op een SIP-verzoek, wordt een failover geactiveerd.
- **TCP-verbinding verbreken:** als de externe server de verbinding met TCP verbreekt (bijvoorbeeld TCP RST of TCP FIN), wordt een failover geactiveerd.

Het wordt nadrukkelijk aanbevolen om **Failback voor failover** in te stellen op **Ingeschakeld** wanneer **SIP-transport** is ingesteld op **Automatisch**.

U kunt deze parameters voor een specifiek toestel ook configureren in het configuratiebestand (`.xml`):

```
<SIP_Transport_n_>Auto</SIP_Transport_n_>
<Srv_Failback_Before_Failover_n_>Yes</Srv_Failback_Before_Failover_n_>
```

Waarbij `n` het toestelnummer is.

Werking van een failover in het basisstation

Wanneer het basisstation 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. Het basisstation 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. Het basisstation 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 het basisstation 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 gedrag van het basisstation af van de instelling van **Proxy fallback-interval**.

- Wanneer **SIP-Timer B voor failover** is ingesteld op **0**, probeert het basisstation de adressen in deze volg orde te wijzigen: 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- Wanneer **SIP-Timer B voor failover** is ingesteld op een andere waarde dan nul, probeert het basis station de adressen in deze volg orde te wijzigen: 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

SIP-proxy terugval

Voor de proxy fallback moet het veld **Failback voor failover** op de webpagina **Server** is ingesteld op **Ingeschakeld**. Als u dit veld instelt op **Uitgeschakeld**, is de failbackfunctie van SIP proxy uitgeschakeld. U kunt deze parameter voor een specifiek toestel ook configureren in het configuratiebestand (`.xml`) in deze indeling in te voeren:

```
<Srv_Failback_Before_Failover_n_>yes</Srv_Failback_Before_Failover_n_
```

Waarbij `n` het toestelnummer is.

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

Als u het basisstation wilt inschakelen om failback uit te voeren tussen verschillende SIP-transportprotocollen, stelt u **SIP-Transport** in op **Automatisch** op de webpagina **Servers**. U kunt deze parameter voor een specifiek toestel ook configureren in het configuratiebestand (`.xml`) met de volgende XML-tekenreeks:

```
<SIP_Transport_@SRVIDX_>AUTO</SIP_Transport_@SRVIDX_>
```

Waarbij `n` het serverindex aangeeft.

Failback van een UDP-verbinding

De failback van een UDP-verbinding wordt geactiveerd door SIP-berichten. In het volgende voorbeeld kan het basisstation 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 het basisstation 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
```

Het basisstation 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.

Het basisstation vernieuwt de registratie op tijdstip T2 (T2=(3600-16)*78%). Op het basisstation 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. Ingeschakeld: het basisstation 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
```

Failover en herstelregistratie

- Failover: op het basisstation wordt een failover uitgevoerd in geval van een time-out/fout in de transport of TCP-verbindingsfouten, indien de waarden voor **Failover-SIP-timer B** en **Failover-SIP-timer F** zijn ingevuld.
- Herstel: op het basisstation 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 het basisstation 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.

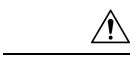
Externe apparaten

We bevelen u aan externe apparaten van goede kwaliteit te gebruiken, die zijn afgeschermd tegen ongewenste radiofrequentie- en audiofrequentiesignalen. Externe apparaten zijn bijvoorbeeld headsets, kabels en connectors.

Niettemin kan, bijvoorbeeld als gevolg van de nabijheid van andere apparaten zoals mobiele telefoons en radio's met zender en ontvanger, een bepaalde mate van ruis hoorbaar zijn. In deze gevallen raden we u aan een of meer van de volgende stappen te ondernemen:

- Plaats het externe apparaat uit de buurt van de bron van de radio- of audiofrequentiesignalen.
- Leid de kabels van het externe apparaat weg van de bron van de radio- of audiofrequentiesignalen.
- Gebruik afgeschermde kabels voor het externe apparaat of gebruik kabels met een betere afscherming en connector.
- Maak de kabel van het externe apparaat korter.
- Plaats ferrieten of vergelijkbare oplossingen op de kabels van het externe apparaat.

Cisco kan geen garantie bieden voor de prestaties van externe apparaten, kabels en connectors.



Voorzichtig In landen van de Europese Unie dient u alleen externe luidsprekers, microfoons en headsets te gebruiken die volledig voldoen aan de EMC-richtlijn [89/336/EEG].

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.