Technische Details

Spezifikationen zur Basisstation

Die folgende Tabelle zeigt die physischen Spezifikationen und Umgebungsspezifikationen für die Basisstation an.

Tabelle 1: Physische und Umgebungsspezifikationen

Spezifikation	Wert oder Bereich
Betriebstemperatur	0 bis 45 °C (32 °F bis 113 °F)
Relative Luftfeuchtigkeit beim Betrieb	10 % bis 90 % (nicht kondensierend)
Lagertemperatur	-10 °C bis 60 °C (14 °F bis 140 °F)
Relative Luftfeuchtigkeit bei Lagerung	10 % bis 95% (nicht kondensierend)
Höhe	120 mm (4,75 Zoll)
Breite	120 mm (4,75 Zoll)
Tiefe	30 mm (1,25 Zoll)
Gewicht	167 g (6 oz)
Kabel	• Kategorie 3/5/5e/6 für 10-Mbit/s-Kabel mit 4 Paaren • Kategorie 5/5e/6 für 100-Mbit/s-Kabel mit 4 Paaren

Spezifikation	Wert oder Bereich
Abstandsanforderungen	Wie von der Ethernet-Spezifikation unterstützt, wird vorausgesetzt, dass die maximale Kabellänge zwischen jeder Basisstation und dem Switch 100 Meter beträgt.
Netzanschluss	Netzteil für lokale Stromversorgung Ethernet-PoE (Ethernet-Adapter für normale Stromversorgung); IEEE 802.3: Power Class 2 (3,84 bis 6,49 W)
Hochfrequenz-(HF-)Bänder	Bänder werden im Werk festgelegt und können nicht vom Kunden geändert werden. • 1880 – 1895 (Taiwan) • • 1880 – 1900 MHz (Australien und Neuseeland – geringere Leistung 22 dBM) • 1880 – 1900 MHz (EU und APAC) • 1910 – 1930 MHz (LATAM und Argentinien) • 1910 – 1920 MHz (Brasilien und Uruguay) • 1910 – 1920 MHz (Uruguay – geringere Leistung 140 mW) • 1910 – 1930 MHz (Chile – geringere Leistung 22 dBM) • 1920 – 1930 MHz (USA und Canada)

Ausführliche technische Informationen über die Basisstation finden Sie auf dem Datenblatt unter:

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

Konfigurationsänderungen der Basisstation protokollieren

Sie können Konfigurationsänderungen, die Benutzer an der Basisstation vornehmen, mithilfe der Protokollierungsfunktion für Konfigurationsänderungen aufzeichnen. Auf ähnliche Weise können Sie Konfigurationsänderungen eines Mobilteils nachverfolgen. Im Änderungsprotokoll speichert der Basisspeicher die Informationen dazu, welche Parameter geändert werden. Diese Informationen enthalten jedoch nicht die tatsächlichen Details der Änderungen. Stattdessen werden nur bestimmte Änderungen gespeichert, die an der Konfiguration vorgenommen wurden. Das Änderungsprotokoll wird gelöscht, nachdem die Änderungen erfolgreich gemeldet wurden.

Konfigurationsänderungen melden

Wenn Konfigurationsänderungen an der Basisstation gemeldet werden, fordert die Basisstation DECT-gesperrte Mobilteile für Änderungsprotokolle an. Die Basisstation sendet für jedes gesperrte Mobilteil drei Anfragen (eine alle fünf Sekunden). Sobald die Anfragen für alle Mobilteile abgeschlossen sind, werden die Änderungsprotokolle der Basis und der Mobilteile gesammelt, verarbeitet und in die richtigen XML-Tags umgewandelt. Anschließend werden diese Tags an den Konfigurationsserver gesendet. Wenn ein Mobilteil

nicht reagiert, zeichnet das Syslog dieses Verhalten auf. Die Änderungsprotokolle der Mobilteile werden erst nach erfolgreicher Übermittlung an eine Basisstation gelöscht.

Spezifikationen zum Mobilteil

Die folgende Tabelle zeigt die physischen Spezifikationen und Umgebungsspezifikationen für die Mobilteile an.

Tabelle 2: Physische und Umgebungsspezifikationen

Spezifikation	Wert oder Bereich
Betriebstemperatur	0 bis 45 °C (32 °F bis 113 °F)
Relative Luftfeuchtigkeit beim Betrieb	10 % bis 90 % (nicht kondensierend)
Lagertemperatur	-10 °C bis 60 °C (14 °F bis 140 °F)
Relative Luftfeuchtigkeit bei Lagerung	10 % bis 95% (nicht kondensierend)
Höhe	6825-Mobilteil: 117 mm (4,6 Zoll) 6825 - Robustes Mobilteil: 117 mm (4,6 Zoll) 6823-Mobilteil: 122 mm (4,82 Zoll)
Breite	6825-Mobilteil: 46 mm (1,8 Zoll) 6825 - Robustes Mobilteil: 46 mm (1,8 Zoll) 6823-Mobilteil: 51 mm (1,99 Zoll)
Tiefe	6825-Mobilteil: 20 mm (0,78 Zoll) 6825 - Robustes Mobilteil: 20 mm (0,78 Zoll) 6823-Mobilteil: 23 mm (0,91 Zoll)
Gewicht	6825-Mobilteil: 86 g (3 oz) 6825 - Robustes Mobilteil: 86 g (3 oz) 6823-Mobilteil: 90 g (3.17 oz)
Netzanschluss	Wiederaufladbarer Lithium-Ionen-Akku.

Ausführliche technische Informationen über die Mobilteile finden Sie auf dem Datenblatt unter:

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

Netzwerkprotokolle

Cisco Mobilteile und Basisstationen unterstützen mehrere Industriestandard- und Cisco Netzwerkprotokolle, die für die Sprachkommunikation erforderlich sind. Die folgende Tabelle enthält eine Übersicht der Netzwerkprotokolle, die von den Mobilteilen und Basisstationen unterstützt werden.

Tabelle 3: Unterstützte Netzwerkprotokolle

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Bootstrap Protocol (BootP)	BootP ermöglicht einem Netzwerkgerät, wie dem Mobilteil, bestimmte Startinformationen zu erkennen, wie z. B. die IP-Adresse.	—
Cisco Discovery Protocol (CDP)	CDP ist ein Protokoll für die Geräteerkennung, das auf allen Geräten von Cisco ausgeführt wird. Ein Gerät kann CDP verwenden, um sich für andere Geräte anzukündigen und Informationen über diese Geräte im Netzwerk zu empfangen. Zum Abrufen der VLAN-Netzwerkinformationen kann der systemeigene VLAN-Typ des CDP verwendet werden.	Das Gerät verwendet CDP, um Informationen, beispielsweise eine zusätzliche VLAN-ID, Details zur Energieverwaltung pro Port und QoS-Konfigurationsinformationen mit dem Cisco Catalyst-Switch zu übertragen.
DNS (Domain Name Server) (Domänennamenserver)	DNS übersetzt Domänennamen in IP-Adressen.	Die Basisstation besitzt einen DNS-Client zum Übersetzen von Domänennamen in IP-Adressen.
Dynamic Host Configuration Protocol (DHCP)	DHCP reserviert und weist IP-Adressen zu Netzwerkgeräten zu. DHCP ermöglicht, eine Basisstation im Netzwerk zu verbinden und zu aktivieren, ohne manuell eine IP-Adresse zuordnen oder zusätzliche Netzwerkparameter konfigurieren zu müssen.	DHCP ist standardmäßig aktiviert. Wenn DHCP deaktiviert ist, muss das Konfigurieren von IP-Adresse, Subnetzmaske und Gateway manuell und direkt auf jeder einzelnen Basisstation vorgenommen werden. Wir empfehlen, die angepasste DHCP-Option 160 oder 159 zu verwenden.
Hypertext Transfer Protocol (HTTP)	HTTP ist das Standardprotokoll zum Übertragen von Informationen und Dokumenten im Internet.	Die Basisstation nutzt HTTP für XML-Dienste, Bereitstellungen, Upgrades und zur Fehlerbehebung.

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Hypertext Transfer Protocol Secure (HTTPS)	HTTPS ist eine Kombination des Hypertext Transfer-Protokolls und des SSL/TLS-Protokolls für die Verschlüsselung und sichere Identifikation von Servern.	Webanwendungen, die sowohl HTTP als auch HTTPS unterstützen, verfügen zu diesem Zweck über zwei konfigurierte URLs. Basisstationen, die HTTPS unterstützen, wählen die HTTPS-URL aus. Ein Schloss-Symbol zeigt an, ob die Verbindung mit dem Service über HTTPS hergestellt wird.
Internet Protocol (IP)	IP ist ein Messaging-Protokoll, das Pakete im Netzwerk verarbeitet und sendet.	Um mit IP zu kommunizieren, muss Geräten eine IP-Adresse, ein Subnetz und ein Gateway zugewiesen sein. IP-Adressen-, Subnetz- und Gateway-IDs werden automatisch zugewiesen, wenn Sie für die Basisstation DHCP (Dynamic Host Configuration Protocol) nutzen. Wenn Sie DHCP nicht verwenden, müssen Sie diese Eigenschaften jeder Basisstation manuell zuweisen.
Link Layer Discovery Protocol (LLDP)	VLAN-Netzwerkinformationen können aus dem LLDP zahlreicher Subtypen des Typs 127 gesammelt werden. In dieser Implementierung werden die Informationen aus einem von zwei Untertypen entnommen, die wie folgt priorisiert werden: **1.** IEEE – PORT-VLAN-ID **2.** Netzwerkrichtlinie	
Network Time Protocol (NTP)	NTP ist ein Netzwerkprotokoll für die Uhrzeit-Synchronisierung zwischen den Computersystemen über paketvermittelte Datennetzwerke mit variabler Latenz.	Die Basisstation verwendet NTP zur Kommunikation mit dem Zeitserver.
Real-Time Transport Protocol (RTP)	RTP ist ein Standardprotokoll für die Übermittlung von Echtzeit-Daten, beispielsweise interaktive Sprache und Videos, über Datennetzwerke.	Die Basisstation verwendet das RTP-Protokoll zum Senden und Empfangen von Echtzeit-Sprachverkehr an bzw. von anderen Geräten und Gateways.
Real-Time Control Protocol (RTCP)	RTCP stellt zusammen mit RTP die QoS-Daten (beispielsweise Jitter, Latenz und Roundtrip-Verzögerung) auf RTP-Streams bereit.	RTCP ist standardmäßig deaktiviert.

Netzwerkprotokoll	Zweck	Hinweis zur Verwendung
Session Description Protocol (SDP)	Bei SDP handelt es sich um den Teil des SIP-Protokolls, der festlegt, welche Parameter während einer Verbindung zwischen zwei Endgeräten verfügbar sind. Beim Erstellen von Konferenzen werden nur die SDP-Funktionen verwendet, die von allen an der Konferenz teilnehmenden Endgeräten unterstützt werden.	Normalerweise werden SDP-Funktionen wie Codec-Typen, DTMF-Erkennung oder Komfortrauschen vom Drittanbieter-Anrufsteuerungssystem oder dem Medien-Gateway im laufenden Betrieb global konfiguriert. Bei manchen SIP-Endgeräten können diese Parameter jedoch direkt auf dem Endgerät konfiguriert werden.
Session Initiation Protocol (SIP)	SIP ist der IETF-Standard (Internet Engineering Task Force) für Multimedia-Konferenzen über IP. SIP ist ein ASCII-basiertes Steuerungsprotokoll auf Anwendungsebene (definiert in RFC 3261), das verwendet werden kann, um Anrufe zwischen zwei oder mehr Endpunkten zu initiieren, aufrechtzuerhalten und abzubrechen.	Wie andere VoIP-Protokolle ist SIP ausgelegt, um die Signalisierungsfunktionen und Sitzungsverwaltung in einem Telefonienetzwerk zu verarbeiten. Die Signalisierung ermöglicht, dass Anrufinformationen netzwerkübergreifend übermittelt werden. während das Sitzungsmanagement die Steuerung der Attribute eines End-to-End-Anrufs ermöglicht.
Secure Real-Time Transfer Protocol (SRTP)	SRTP ist eine Erweiterung des RTP Audio-/Videoprofils und stellt die Integrität von RTP- und RTCP-Paketen über Authentifizierung, Integrität und Verschlüsselung der Medienpakete zwischen zwei Endpunkten sicher.	Mobilteile und Basisstationen verwenden SRTP für die Medienverschlüsselung.
Transmission Control Protocol (TCP)	TCP ist ein verbindungsorientiertes Transportprotokoll.	—
Transport Layer Security (TLS)	TLS ist ein Standardprotokoll zum Schützen und Authentifizieren der Kommunikation.	Wenn die Sicherheit implementiert ist, verwendet die Basisstation das TLS-Protokoll für die sichere Registrierung mit dem Drittanbieter-Anrufsteuerungssystem.
Trivial File Transfer Protocol (TFTP)	TFTP ermöglicht die Dateiübertragung über das Netzwerk. Auf der Basisstation ermöglicht TFTP das Abrufen einer für den Telefontyp spezifischen Konfigurationsdatei.	TFTP erfordert einen TFTP-Server im Netzwerk, der vom DHCP-Server automatisch erkannt werden kann.
User Datagram Protocol (UDP)	UDP ist ein verbindungsloses Protokoll für die Übertragung von Datenpaketen.	Dieses Protokoll wird ausschließlich für RTP-Datenströme verwendet. SIP verwendet UDP, TCP und TLS.

Netzwerk-VLAN zurücksetzen

Wenn die Advertisement Discovery-Pakete eintreffen, werden sie überwacht und analysiert, und die darin enthaltenen Netzwerkinformationen werden mit früheren Paketen verglichen. Wenn sich das VLAN ändert, muss die DECT-Basiseinheit neu gestartet und erneut verbunden werden, um eine neue Netzwerkinitialisierung durchzuführen.

SIP-Konfiguration

SIP und das Cisco IP DECT-Telefon

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

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

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

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

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

SIP über TCP

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

SIP-Proxy-Redundanz

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

Eine einfache Methode, um die Proxyredundanz zu unterstützen, ist das Festlegen eines SIP-Proxyservers im Konfigurationsprofil der Basisstation. Die Basisstation sendet eine DNS-NAPTR- oder SRV-Abfrage an den DNS-Server. Wenn konfiguriert, gibt der DNS-Server SRV-Einträge zurück, in denen die Server in der Domäne mit Hostnamen, Priorität, Listening-Ports usw. aufgelistet sind. Die Basisstation versucht, die Server

in der Reihenfolge ihrer Priorität zu kontaktieren. Server mit einer niedrigeren Nummer haben eine höhere Priorität. In einer Abfrage werden bis zu sechs NAPTR-Einträge und zwölf SRV-Einträge unterstützt.

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

Beispiel für Ressourceneinträge vom DNS-Server

```
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
```

Das folgende Beispiel zeigt die Priorität der Server aus der Perspektive der 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
```

Die Basisstation sendet immer SIP-Nachrichten an die in der Liste verfügbare Adresse mit der höchsten Priorität und mit dem Status „UP“. Im Beispiel sendet die Basisstation alle SIP-Nachrichten an die Adresse 1.1.1.1. Wenn die Adresse 1.1.1.1 in der Liste mit dem Status „DOWN“ gekennzeichnet ist, kommuniziert die Basisstation stattdessen mit 2.2.2.2. Die Basisstation kann die Verbindung zu 1.1.1.1 wiederherstellen, wenn die angegebenen Failback-Bedingungen erfüllt sind. Weitere Informationen zu Failover und Failback finden Sie unter SIP-Proxy-Failover, auf Seite 8 und SIP-Proxy-Fallback, auf Seite 10.

SIP-Proxy-Failover

Die Basisstation führt in jedem der folgenden Fälle einen Failover durch:

- **Fast Response Timer expiry** (Ablauf des Timers für schnelle Antwort):In RFC3261 definieren die beiden Transaktions-Timer TIMER B und TIMER F, wann eine INVITE-Transaktion und eine Nicht-INVITE-Transaktion jeweils abgelaufen sind. Diese sind mit einem Standardwert von 5 Sek. konfigurierbar. Wenn einer dieser Zeitgeber abläuft und die entsprechende SIP-Transaktion fehlschlägt, wird das Failover ausgelöst. Anforderungen in einem Dialog lösen kein Failover aus.

- **SIP 5xx Response Codes** (SIP 5xx-Antwort Codes): Wenn der Server mit einer 5xx-Antwort auf eine SIP-Anforderung antwortet, wird ein Failover ausgelöst.
- **TCP disconnect:** (TCP-Verbindungstrennung): Wenn der Remote-Server die TCP-Verbindung trennt (z. B. TCP RST oder TCP FIN), wird ein Failover ausgelöst.

Es wird dringend empfohlen, **Failback before Failover** (Failback vor Failover) auf **Enabled** (Aktiviert) festzulegen, falls **SIP Transport** (SIP-Transport) auf **Auto** (Automatisch) festgelegt ist.

Sie können diese durchwahlspezifischen Parameter auch in der Konfigurationsdatei (`.xml`) konfigurieren:

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

Hierbei ist `n` die Durchwahl.

Failover-Verhalten der Basisstation

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

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

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	DOWN
2nd	2.2.2.2	TLS	DOWN
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

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

Priority	IP Address	SIP Protocol	Server	Status
1st	1.1.1.1	UDP	SRV1	DOWN
2nd	1.1.1.2	UDP	SRV1	UP
3rd	1.1.1.3	UDP	SRV1	UP
4th	2.2.2.1	TLS	SRV2	UP
5th	2.2.2.2	TLS	SRV2	UP
6th	2.2.2.3	TLS	SRV2	UP

Angenommen, dass die Basisstation keine Verbindung zu 1.1.1.1 herstellen konnte und dann eine Registrierung für 1.1.1.2 vorgenommen hat. Wenn 1.1.1.2 ausfällt, hängt das Verhalten der Basisstation von der Einstellung des **Proxy Fallback Intvl** (Intervall für Proxy-Fallback) ab.

- Wenn **Failover SIP Timer B** auf **0** eingestellt ist, versucht es die Basisstation mit den Adressen in dieser Reihenfolge: 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- Wenn **Failover SIP Timer B** auf einen anderen Wert als null (0) eingestellt ist, versucht es die Basisstation mit den Adressen in dieser Reihenfolge: 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

SIP-Proxy-Fallback

Das Proxy-Fallback erfordert, dass das Feld **Failback before Failover** (Failback vor Failover) auf der Webseite **Server** auf **Enabled** (Aktiviert) festgelegt ist. Wenn Sie dieses Feld auf **Disabled** (Deaktiviert) festlegen, wird die SIP-Proxy-Failback-Funktion deaktiviert. Sie können diese durchwahlspezifischen Parameter auch in der Konfigurationsdatei (`.xml`) im folgenden Format konfigurieren:

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

Hierbei ist `n` die Durchwahlnummer.

Die Zeit, zu der die Basisstation ein Failback auslöst, hängt von der Konfiguration und den verwendeten SIP-Transportprotokollen ab.

Damit die Basisstation ein Failback zwischen verschiedenen SIP-Transportprotokollen durchführen kann, legen Sie **SIP Transport** (SIP-Transport) auf der Webseite **Servers** (Server) auf **Auto** (Automatisch) fest. Sie können diese durchwahlspezifischen Parameter auch in der Konfigurationsdatei (`.xml`) mit der folgenden XML-Zeichenfolge konfigurieren:

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

Hierbei ist `n` der Server-Index.

Failback von einer UDP-Verbindung

Das Failback von einer UDP-Verbindung wird durch SIP-Nachrichten ausgelöst. Im folgenden Beispiel konnte die Basisstation zum Zeitpunkt T1 nicht auf „1.1.1.1 (TLS)“ registriert werden, da der Server keine Antwort gesendet hat. Wenn der SIP-Timer „F“ abläuft, wird die Basisstation zum Zeitpunkt T2 (T2 = T1 + SIP-Timer F) auf „2.2.2.2 (UDP)“ registriert. Die aktuelle Verbindung erfolgt über UDP auf 2.2.2.2.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS          DOWN        T1 (Down time)
2nd            2.2.2.2            UDP          UP
3rd            3.3.3.3            TCP          UP
```

Die Basisstation hat folgende Konfiguration:

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

Hierbei ist *n* die Durchwahlnummer.

Die Basisstation aktualisiert die Registrierung zum Zeitpunkt T2 (T2 = (3600–16) * 78 %). Die Basisstation überprüft die Adressliste auf die Verfügbarkeit der IP-Adressen und die Ausfallzeit. Bei T2-T1 > = 60 wird der fehlgeschlagene Server 1.1.1.1 wieder auf „UP“ gesetzt und die Liste wird wie folgt aktualisiert. Die Basisstation sendet SIP-Nachrichten an 1.1.1.1.

```
Priority       IP Address     SIP Protocol    Status
1st            1.1.1.1            TLS           UP
2nd            2.2.2.2            UDP           UP
3rd            3.3.3.3            TCP           UP
```

Registrierung für Failover und Wiederherstellung

- Failover: Die Basisstation führt einen Failover durch, wenn Transport-Timeout/-Fehler oder TCP-Verbindungsfehler auftreten. Voraussetzung ist, dass **Failover SIP Timer B** und **Failover SIP Timer F** Daten enthalten.

- Wiederherstellung: Die Basisstation versucht, sich erneut mit dem primären Proxy zu registrieren, wenn es mit dem sekundären Proxy registriert oder verbunden ist.

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

Fallback-Verhalten

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

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

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

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

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

Externe Geräte

Wir empfehlen die Verwendung von qualitativ hochwertigen, externen Geräten, die gegen unerwünschte RF-Signale (Radiofrequenz) und AF-Signale (Audiofrequenz) geschirmt sind. Externe Geräte sind beispielsweise Headsets, Kabel und Steckverbinder.

Je nach der Qualität dieser Geräte und deren Abstand zu anderen Geräten wie Mobiltelefonen oder Funkgeräten, kann trotzdem ein geringes Rauschen auftreten. In diesen Fällen empfehlen wir eine oder mehrere der folgenden Maßnahmen:

- Vergrößern Sie den Abstand zwischen dem externen Gerät und der RF- oder AF-Signalquelle.
- Verlegen Sie die Anschlusskabel des externen Geräts in einem möglichst großen Abstand zur RF- oder AF-Signalquelle.
- Verwenden Sie für das externe Gerät abgeschirmte Kabel oder Kabel mit hochwertiger Abschirmung und hochwertigen Anschlusssteckern.
- Kürzen Sie das Anschlusskabel des externen Geräts.
- Führen Sie die Kabel des externen Geräts durch einen Ferritkern oder eine ähnliche Vorrichtung.

Cisco kann keine Garantie für die Leistung von externen Geräten, Kabeln und Steckern übernehmen.

Vorsicht Verwenden Sie in EU-Ländern ausschließlich externe Lautsprecher, Mikrofone und Headsets, die mit der EU-Richtlinie 89/336/EWG konform sind.

Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.