Erläuterung der Cisco IOS- und IOS XE-Anrufweiterleitung

Inhalt

Einleitung

Dieses Dokument enthält eine Erklärung der Anrufverteilung von Cisco IOS® und Cisco IOS XE.

Voraussetzungen

Anforderungen

Obwohl keine formalen Voraussetzungen für die Lektüre dieses Dokuments erforderlich sind, wird davon ausgegangen, dass der Leser bereits über Kenntnisse der zugrunde liegenden Sprachsignalisierungsprotokolle verfügt, die für die Herstellung und Verbindung von Telefongesprächen verwendet werden. Diese Protokolle werden im gesamten Netzwerk mehrfach referenziert.

Signalisierungsprotokolle: Session Initiation Protocol (SIP), H323 (h225/h245), Media Gateway Control Protocol (MGCP), Skinny Client Control Protocol (SCCP), ISDN Q931, E1 R2.

Medienprotokolle: Real Time Protocol (RTP), Sprachcodecs, Videocodecs.

Analoge Technologien: Ear and Mouth (E&M), Foreign Exchange Subscriber (FXS) und Foreign

Exchange Office (FXO).

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IOS und IOS XE Gateways
- 2800/3800/2900/3900/4300/4400/CSR1000v/CAT8000v/ASR100X/C8200/C8300 / ISR 1100

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

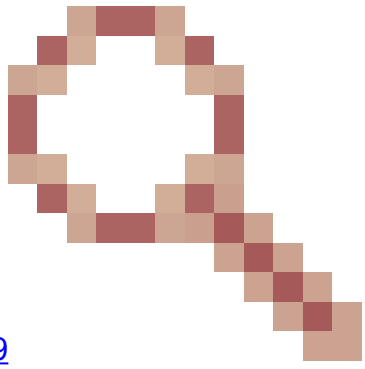
In diesem Dokument werden die Mechanismen für den Dial-Peer-Abgleich von ein- und ausgehenden Anrufen mit Plain Old Telefone Service (POTS) und Voice over IP (VoIP) Network beschrieben.

Neben den DFÜ-Peer-Informationen behandelt dieses Dokument wichtige Themen, die die Anrufweiterleitung betreffen. Dazu gehören die Nummernänderung, eine Kurzübersicht über die Bearbeitung von SIP-Nachrichten, einige Methoden zur Einschränkung der Anruffunktionen, eine Kurzübersicht zur Medien- und Signalisierungsbindung und schließlich eine kleine Fehlerbehebung.

In diesem Dokument werden Konfigurationsbeispiele sowie das Debuggen und Anzeigen von Befehlsausgaben als Bezugspunkte verwendet. Die zahlreichen Funktionen in diesem Dokument sind klar mit der Version gekennzeichnet, in der die Funktion sowohl in Cisco IOS als auch in Cisco IOS XE eingeführt wurde. Auf diese Informationen kann auch schnell im Abschnitt "Command and Feature Roadmap" (Befehls- und Funktions-Roadmap) verwiesen werden. Wenn es einen sehr bemerkenswerten Fehler gibt, ist es innerhalb des Textes verknüpft, sodass die Leser sich dessen bewusst sind.

Gemeinsame Definitionen

Attribut	Beschreibung
Ziffernfolge	Wird auch als Ziffernfolge, Telefonnummer, Nummer oder E164-Nummer bezeichnet.Besteht vollständig aus den Ziffern 0 bis 9 mit einem optionalen führenden Pluszeichen (+). Beispiel:

Attribut	Beschreibung
	8675309 123456789 +1972525222 +442084445555 +85225353333
Dialed Number Identification Service (DNIS)	Dies ist die angerufene Nummer oder die Zielnummer für einen Anruf.
Automatische Rufnummernerkennung	Dies ist die anrufende Nummer oder die Nummer des ursprünglichen Anrufers. Dies kann auch als Calling Line Identifier (CLID) bezeichnet werden, der auch als Anrufer-ID bezeichnet werden kann.
URI (Uniform Resource Identifier)	Ein URI ist entweder sip: oder tel: eine Zeichenfolge, die am häufigsten mit den VoIP-Protokollen SIP und H323 verwendet wird. URL-Beispiele: SIP:user@host.com SIP:user@sub.host.com SIP:user@10.10.10.10 sip:user@2001:4860:4860:8888 Tel.: 8675309 SIP:host.com
Carrier-ID	CID-Beispiele: cid:orange@host.com cid:orange@sub.host.com cid:orange@10.10.10.10 cid:orange@2001:4860:4860:8888   Hinweis: Cisco Bug-ID CSCua14749

Attribut	Beschreibung
	Carrier-ID funktioniert nicht auf IOS XE-Plattformen.
Route-String	Ein proprietärer Header von Cisco für ILS-Routenzeichenfolgen, die mit SIP verwendet werden. Beispiel: X-cisco-dest-route-string: <sip:configured-value>
ENDE	ENUM ist ein Protokoll, das mithilfe von Domain Name Service (DNS) E164-Telefonnummern in URIs übersetzt. Dies wird in diesem Dokument nicht behandelt.
PSTN	Öffentliches Telefonnetz
ITSP	Internet-Telefonie-Service Provider
SBC	Session Border Controller Dies ist das Gerät, das als Berührungspunkt zwischen dem Kunden-LAN und einem ITSP-/PSTN-Netzwerk dient.

Roadmap für Befehle und Funktionen

Funktion	IOS-Version	IOS XE-Version
Nummernerweiterung (Num-Exp) DFÜ-Peers (POTS und VOIP) Antwortadresse Zielmuster eingehende angerufene	11.3(1)T	Alle

Nummer Sitzungsziel (IPv4 und DNS) Max. Verbindungen (max. Verbindung) Durchwahl Vorwärtsziffern (POTS) Präfix (POTS) Timeouts Interdigit (Sprach-Port)		
Dial-Peer-Terminator	12.0	Alle
Jagdaufenthalt	12.0(5)T	Alle
ISDN-Karten	12,0(6)T	Alle
Dial-Peer-Sammelanschlussschemata	12,0(7)XK	Alle
Sprachübersetzungsregel und Profil ausgehende Übersetzung Nummerierungstyp Ziffernleiste (POTS)	12.0(7)XR1	Alle
session target (sip-server)	12.1(1)T	Alle
POTS-Trunk-Gruppe	12.1(3)T	Alle
DNIS-Map (ausgehend)	12.2(2)XB	Alle
Trunk-Gruppen-Label	12,2(11)T	Alle

DFÜ-Peer (Daten)	12,2(13)T	Alle
Sprachklassen-URI (ausgehend)	Artikel 12 Absatz 3 Buchstabe T	Alle
ausgehender Proxy	12,4(15)T	Alle
Sitzungsziel (IPv6)	12,4(22)T	Alle
SIP-Profile (ausgehend)	15,0(1)M	Alle
Sprachklassen-URI (eingehend) Sprachquellengruppe	15.1(2)T	3,8 s
SIP-Copylist Sitzungsziel (Registrar)	15.1(3)T	3,6 S
Anrufweiterleitung (url)	15.2(1)T	3,3 s
maximale Bandbreite	15.2(2)T	3,7 S
E164-Pattern-Maps (ausgehend)	15,2(4)M	3,7 S
Sprachklasse Route-String Anrufroute (Destest-Route-String)	15,3(3)M	3,10 S
Dial-Peer-Gruppen (VOIP) E164-Pattern-Maps (eingehend) Zielservergruppe	15.4(1)T	3,11 s

Anforderungsdurchlauf Session-Ziel (SIP-URI)		
Richtlinie für Dial-Peer-Bereitstellung SIP-Profile (eingehend)	15,4(2)T	3,12 S
DFÜ-Peer-Gruppe (POTS)	15.5(1)T	3,14 S
Sprachklassen-Tenants	15,6(2)T	16.3.1
VRF-Filterung für Dial-Peers	15,6(3)M	16.3.1
e164-Übersetzung	–	16.8.1
SIP-DSAPP	–	16.12.1
Huntstop für Servergruppen	–	17.4.1
SIP-Überwachungsport für Tenant-Filterung für Dial-Peers	–	17.8.1
Keepalive für auf DNS SRV basierende Optionen	–	17.9.1

Grundlagen von Cisco IOS/Cisco IOS XE Call Routing

Die Cisco IOS- und Cisco IOS XE-Gateways nutzen ein Dial-Peer-Konzept zur Steuerung der Anrufweiterleitung und zur Aushandlung von Funktionen für jeden Abschnitt eines Anrufs. Ein Anrufabschnitt ist die bidirektionale Kommunikation zwischen zwei Anrufagenten. Ein Anruf-Agent ist ein Gerät, das Telefonanrufe initiiert, verarbeitet oder weiterleitet. Dies kann und ist nicht auf Geräte von Telefonieanbietern, ein Cisco Gateway, ein IP-Telefon, einen Cisco Unified Communication Manager (CUCM), Cisco Unity Connection (CUC) usw. beschränkt. Es sind viel zu viele Anruf-Agenten in der Liste.

Szenario: Ein Anruf erreicht ein Cisco Gateway von einem anderen Anrufagenten und ist der

eingehende Anrufabschnitt (In-Leg). Das Gateway verarbeitet den Anruf und sendet ihn basierend auf der Verarbeitung an den nächsten Anruf-Agenten. Dies ist der ausgehende Anrufabschnitt (out-leg).

Abbildung 1 zeigt einen Anruf vom PSTN zum CUCM, der über ein Cisco Voice Gateway weitergeleitet wird, sowie die entsprechenden Informationen zum ein- und ausgehenden Anrufabschnitt.

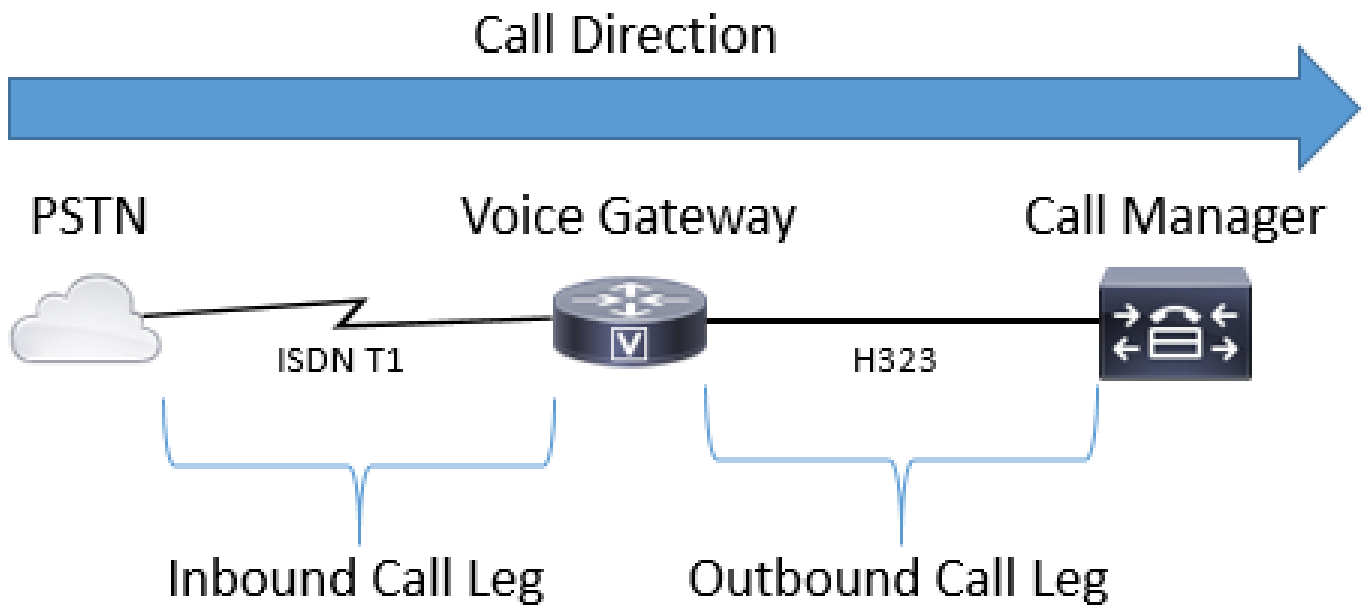


Abbildung 1: Legende für ein- und ausgehende Anrufe

Ein erfolgreicher Anruf über ein Cisco Gateway stimmt IMMER (siehe Hinweis) mit einem eingehenden oder ausgehenden DFÜ-Peer überein, um eine ordnungsgemäße Route festzulegen. Eingehende und ausgehende DFÜ-Peers ähneln den zuvor erwähnten Anrufabschnitten. In Bild 1 geht der Anruf vom PSTN am Cisco Gateway ein und muss einem eingehenden Dial-Peer entsprechen. Anschließend verwendet das Gateway einen Dial-Peer für ausgehende Anrufe, um den Anruf an den nächsten Anruf-Agenten weiterzuleiten. Beachten Sie, dass diese Begriffe aus der Perspektive des Cisco Gateways definiert werden.

Durch die Zuordnung eines Dial-Peers für jede Seite des Anrufs kann ein Administrator viele Aspekte der einzelnen Anrufabschnitte steuern. Beispiele hierfür sind Sprach-Codecs, DTMF-Einstellungen, Nummernänderung, Weiterleitung des Anrufs sowie eine Vielzahl weiterer Einstellungen. Dial-Peers können mit Match-Anweisungen für ein- und ausgehende Anrufe konfiguriert werden, sodass ein und derselbe Dial-Peer sowohl für den ein- als auch für den ausgehenden Zweig verwendet werden kann, wenn eine gültige Konfiguration für eingehende und ausgehende Anrufe auf diesen Dial-Peer angewendet wird.

Hinweis: Eine Ausnahme bilden MGCP- und SCCP-Sprach-Ports. Diese Signalisierungsprotokolle folgen bei der Anrufweiterleitung nicht dem normalen Dial-Peer-Zuordnungsmechanismus. Weitere Informationen finden Sie im Abschnitt zu SCCP und

---

MGCP.

Abbildung 2 zeigt die gleichen ein- und ausgehenden Anrufabschnitte wie Abbildung 1, jedoch mit den entsprechenden DFÜ-Peers für einen Anruf vom PSTN zum CUCM, der über ein Cisco Voice Gateway weitergeleitet wird.

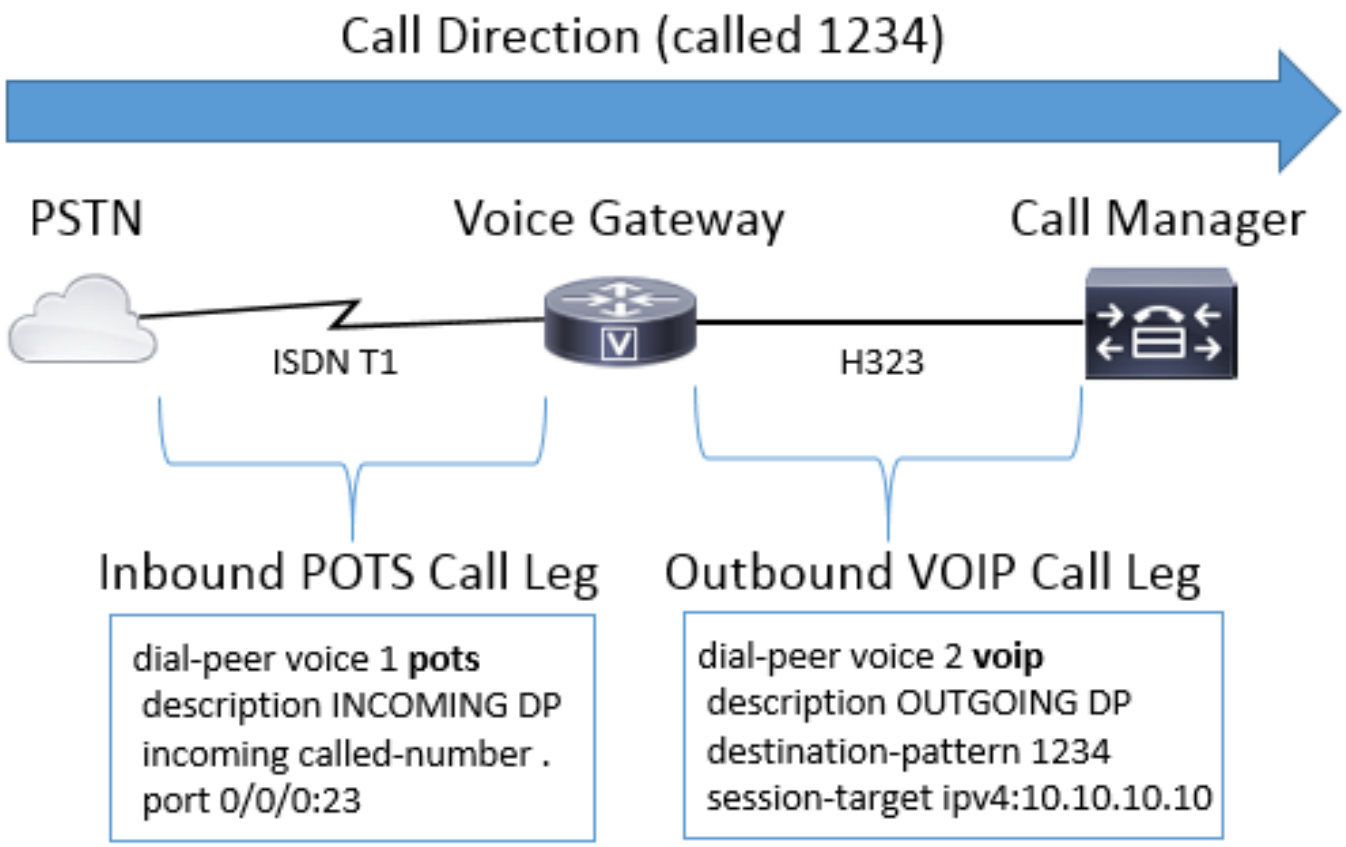


Abbildung 2: Darstellung von eingehenden und ausgehenden DFÜ-Peers

Cisco Voice Gateways können viele verschiedene Arten von Sprachanrufen und Protokollen miteinander verbinden, einschließlich IP-zu-IP, POTS-zu-POTS und IP-zu-POTS oder umgekehrt.

Abbildung 3 zeigt einen Anruf von VoIP zu VoIP über das Cisco Unified Border Element (CUBE).

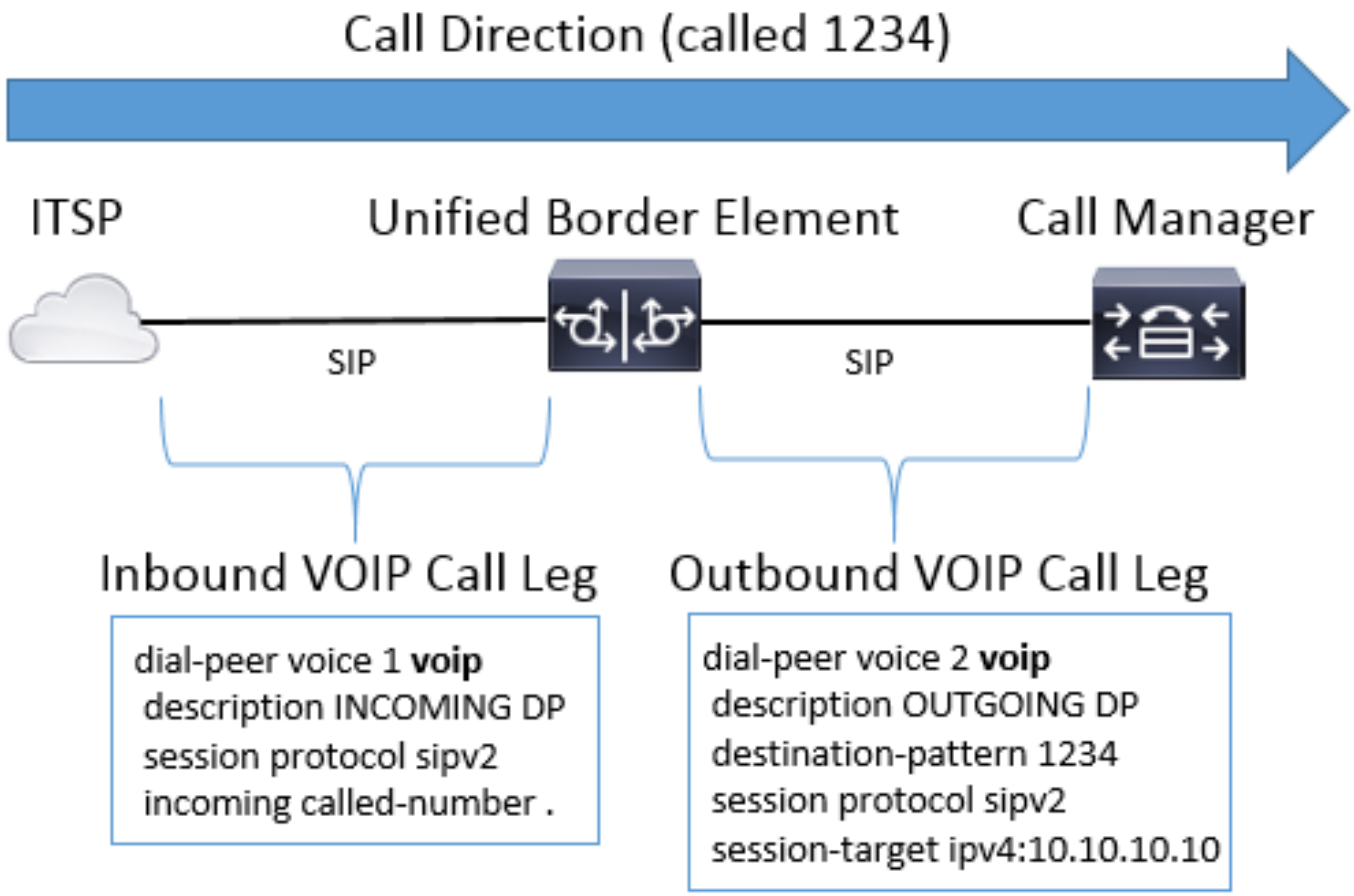


Abbildung 3: Eingehende und ausgehende DFÜ-Peers für einen VoIP-Anruf

Abbildung 4 zeigt einen POTS-zu-POTS-Anruf über ein Cisco Gateway.

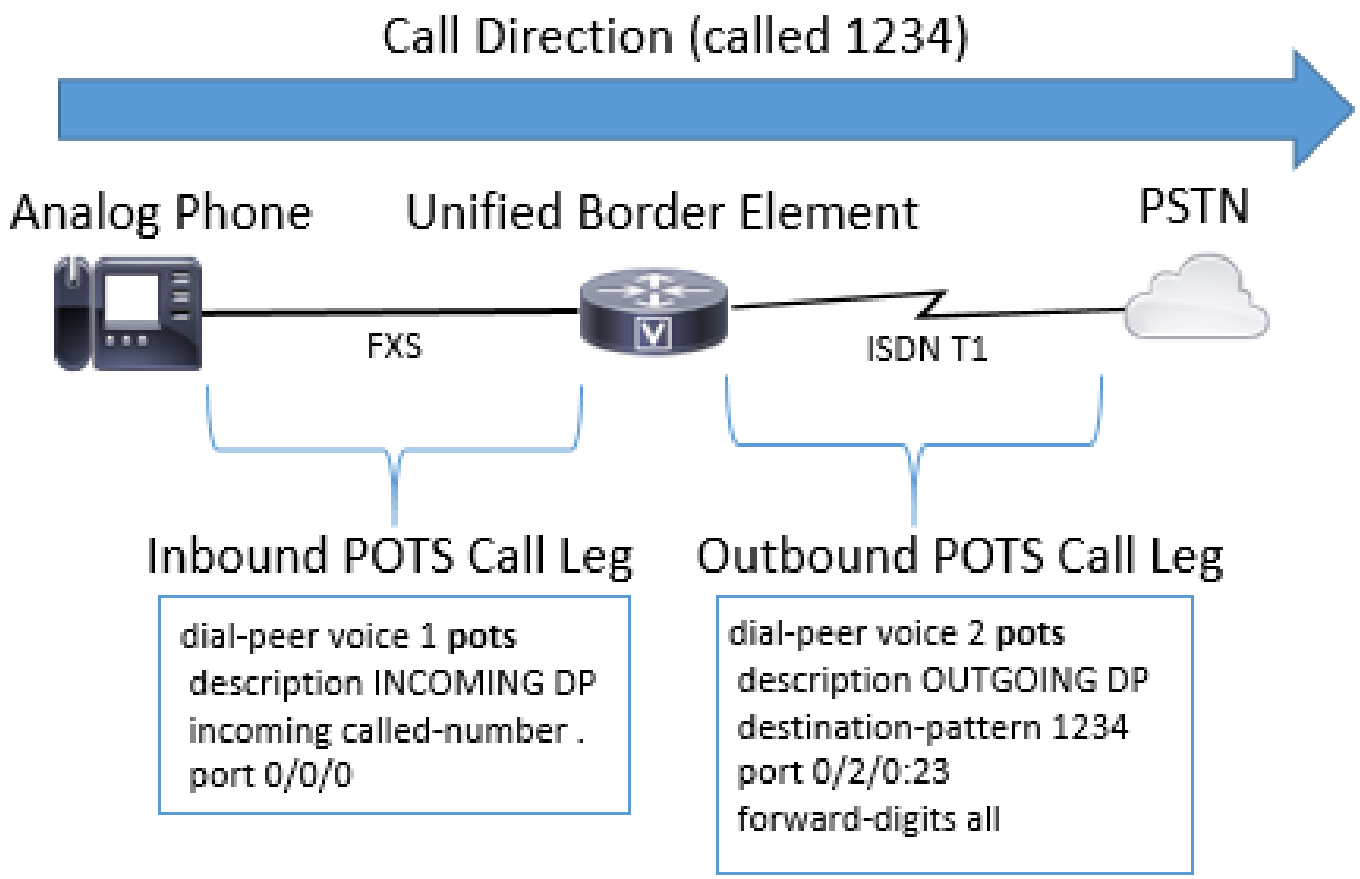


Abbildung 4: Eingehende und ausgehende DFÜ-Peers für einen POTS-zu-POTS-Anruf

Sprach-DFÜ-Peer-Typen

TÖPFE	Normale DFÜ-Peers des alten Telefoniedienstes werden für analoge Verbindungen wie analoge FXS-, FXO-, ISDN T1/E1s-, E1 R2- und E&M-Verbindungen (Ear and Mouth) verwendet. Diese senden oder empfangen einen Anruf an/von einem physischen Sprach-Port am Gateway.
VOIP	Voice Over IP-Dial-Peers werden hauptsächlich zur Steuerung von H323- und SIP-Verbindungen zum und vom Gateway verwendet. Diese Dial-Peers senden und empfangen Signalisierung von IPv4- und IPv6-Adressen sowie vollqualifizierten Domänennamen (Fully Qualified Domain Names, FQDN) über das Domain Name System (DNS). — VoIP-Dial-Peers können auch für Voice over Frame Relay (VoFR), Voice over ATM (VoATM), Voice over High-Level Data Link Control (VoHDLC) und Registration,

	Admission, and Status (RAS)-Signalisierungs- und Sitzungsziele für diese Dial-Peers verwendet werden und umfassen auch Einstellungen und ENUM-Werte. Hinweis: Einige dieser Konfigurationen sind ältere Technologien, die in neueren Netzwerken nicht verwendet werden, und mit IOS XE werden einige nicht mehr unterstützt. Daher werden sie in diesem Dokument nicht behandelt.
MMOIP	Multimedia-DFÜ-Peers für Mail über IP werden zum Senden von E-Mails an Exchange-Server verwendet. Diese werden hauptsächlich für das On-Ramp/Off-Ramp-Faxen von t37 verwendet. Diese Dial-Peer-Typen werden in diesem Dokument nicht behandelt.

Hinweis: Die maximale Anzahl der Dial-Peers, die auf einem Cisco Gateway konfiguriert werden können, hängt vom verfügbaren Speicher (DRAM) ab. Jeder Dial-Peer benötigt ca. 6 KB Speicher. Stellen Sie daher sicher, dass mindestens 20 % des gesamten Speichers des Gateways für andere CPU-Prozesse reserviert sind. Eine große Anzahl konfigurierter Dial-Peers kann die Verzögerung für die Weiterleitung eines Anrufs erhöhen. Dies kann wichtig sein, da die Cisco Sprachanwendung Dial-Peers von oben nach unten durchsucht, ähnlich wie eine Zugriffskontrollliste (ACL). Bei neueren Cisco Gateways ist dies in der Regel kein Problem.

Beispielfehler:

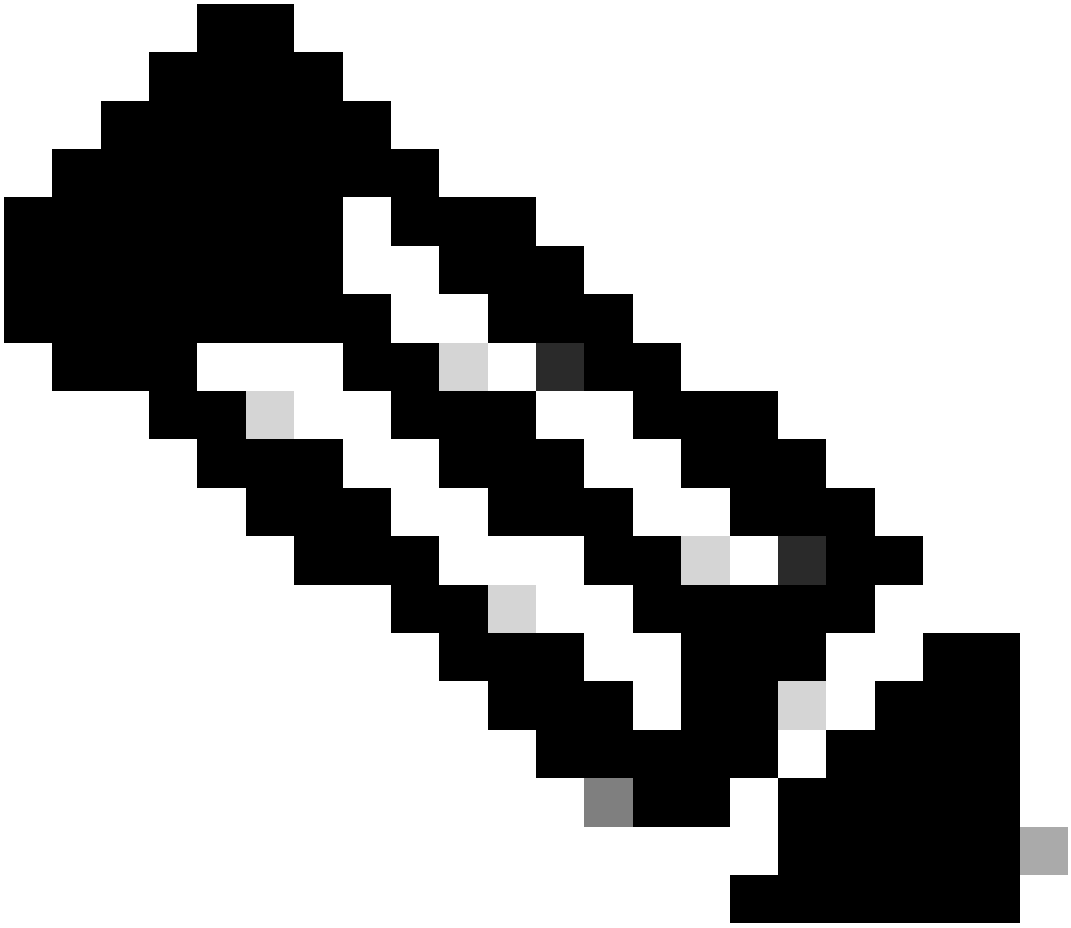
```
May 26 12:59:46.406: %DIALPEER_DB-3-ADDPEER_MEM_THRESHOLD: Addition of dial-peers limited by available m
```

Eingehende Dial-Peer-Zuordnung

Wenn ein Cisco Gateway eine Anforderung zur Einrichtung von Anrufen empfängt, beginnt es mit der Suche nach einem geeigneten DFÜ-Peer für diesen Anruf. Dabei handelt es sich nicht um eine Ziffernanalyse. Stattdessen wird die vollständige Nachricht verwendet, um zu bestimmen, welcher eingehende Dial-Peer ausgewählt wird. Die Reihenfolge der Elemente in der überprüften Nachricht hängt weitgehend vom Protokoll für den Anruf ab, das in den in Tabelle 1, Tabelle 2 und Tabelle 3 definierten Präferenzlisten angegeben ist. Ein Dial-Peer muss nur eine der Bedingungen für die Übereinstimmung erfüllen. Es müssen nicht alle Attribute im Dial-Peer konfiguriert werden, oder jedes Attribut muss mit den Informationen für die Anrufeinrichtung übereinstimmen. Alle DFÜ-Peers werden anhand des ersten Suchkriteriums durchsucht. Das Gateway geht nur dann zum nächsten Kriterium über, wenn keine Übereinstimmung gefunden wurde.

Tabelle 1. Bevorzugte eingehende SIP-DFÜ-Peers

Bevorzugung	Zuordnungskriterien	DFÜ-Peer-Befehle
1	URI	eingehender URI über <uri-tag>
2	URI	Eingehende URI-Anforderung <uri-tag>
3	URI	eingehender URI an <uri-tag>
4	URI	eingehender URI von <uri-tag>
5	Angerufene Nummer	incoming called-number <Nummer-Zeichenfolge> incoming called e164-pattern-map <pattern-map-number>
6	Anrufernummer	eingehender Anruf e164-pattern-map <pattern-map-number> answer-address <Nummer-Zeichenfolge>
7	Zielmuster (Destination-Pattern, ANI)	destination-pattern <Nummer-Zeichenfolge>
8	Carrier-ID	carrier-id source <Zeichenfolge>



Hinweis: Qualifizierte Dial-Peers für eingehende Anrufe können nach VRF oder Tenant gefiltert werden, wenn die entsprechende Funktion konfiguriert ist. Weitere Informationen finden Sie in den Abschnitten Virtual Routing and Forwarding (VRF) und Dial-Peer Hunting und Voice Class Tenants.

Tabelle 2. Eingehende H323-DFÜ-Peer-Auswahl - Voreinstellung

Bevorzugung	Zuordnungskriterien	DFÜ-Peer-Befehle
1	URI	Eingehender URI mit dem Namen <uri-tag> eingehender URI-Anruf <uri-tag>
2	Angerufene Nummer	incoming called-number <Nummer-Zeichenfolge>

		incoming called e164-pattern-map <pattern-map-number>
3	Anrufernummer	eingehender Anruf e164-pattern-map <pattern-map-number> answer-address <Nummer-Zeichenfolge>
4	Zielmuster (Destination-Pattern, ANI)	destination-pattern <Nummer-Zeichenfolge>
5	Carrier-ID	carrier-id source <Zeichenfolge>

Tabelle 3. Eingehende blockbasierte POTS-DFÜ-Peer-Auswahl-Voreinstellungen

Bevorzugung	Zuordnungskriterien	DFÜ-Peer-Befehle
1	Angerufene Nummer	incoming called-number <Nummer-Zeichenfolge>
2	Anrufernummer	answer-address <Nummer-Zeichenfolge>
3	Zielmuster (Destination-Pattern, ANI)	destination-pattern <Nummernfolge>
4	Sprach-Port	port <Sprach-Port-Nummer>

Wenn keine Übereinstimmungen vorhanden sind/Standardeinstellung Dial-Peer 0 peer_tag=0, pid:0

Wenn für einen eingehenden Dial-Peer für POTS- oder VoIP-Anrufe keine qualifizierten Übereinstimmungen vorliegen, weist das Gateway den Dial-Peer 0 zu. Dies ist nicht ideal, da Dial-Peer 0 nur über eingeschränkte Funktionen verfügt und Probleme mit Anrufen verursachen kann. Der Ausreißer hierfür sind die SCCP- und MGCP-Protokolle, die keine Dial-Peers zum Weiterleiten von Anrufen verwenden. Weitere Informationen finden Sie im Abschnitt zu MGCP und SCCP.

Dial-Peer-0-Funktionen

- Keine DTM-Relay-Mechanismen.
- Alle Sprachcodecs für VoIP-Anrufe angekündigt.
- Sprache mit Fax-Rate.
- Die Sprachpausenerkennung (Voice Activity Detection, VAD) ist aktiviert.
- Keine RSVP-Unterstützung.
- Keine IVR-Anwendungsunterstützung für POTS-Anrufe.
- Direct-Inward-Dial ist aktiviert.
- Keine Unterstützung für VRF

Abgleich ausgehender DFÜ-Peers

Ausgehende DFÜ-Peers werden verwendet, um POTS- oder VoIP-Anrufe vom Gateway an den nächsten Anruf-Agenten weiterzuleiten. Wie beim Vergleich eingehender Dial-Peers gibt es eine Liste von Elementen, die das Gateway zum Abgleich von Dial-Peers anhand der Präferenzreihenfolge für das jeweilige Protokoll verwenden kann. Anders als bei Dial-Peers für eingehende Anrufe schlägt der Anruf jedoch fehl, wenn kein qualifizierter Dial-Peer für die Weiterleitung des Anrufs vorhanden ist. Wie beim Dial-Peer-Matching für eingehende Anrufe werden alle Dial-Peers anhand der ersten Match-Kriterien durchsucht. Das Gateway geht nur dann zum nächsten Kriterium über, wenn keine Übereinstimmung gefunden wurde.

Tabelle 4. Bevorzugte ausgehende SIP-DFÜ-Peer-Auswahl

Bevorzugung	Zuordnungskriterien	DFÜ-Peer-Befehle
1	DFÜ-Peer-Gruppe DFÜ-Peer	destination dpg <dpg-tag> (DPG für eingehenden Dial-Peer konfiguriert)
2	URI der DFÜ-Peer-Bereitstellungsrichtlinie	Ziel-URI-von <uri-tag> Ziel-URI-zu <uri-tag> Ziel-URI-über <uri-tag> destination uri-diversion <uri-tag> Ziel-URI-referenziert von <uri-tag> (DPP für eingehenden Dial-Peer konfiguriert)
3	ILS-Routenzeichenfolge	destination route-string <route-string-tag>
4	URI und Carrier-ID	destination uri <uri-tag> AND carrier-id target <string>
5	Angerufene Nummer und Carrier-ID	destination-pattern <Nummer-Zeichenfolge> UND carrier-id target <Zeichenfolge>

6	URI	Ziel-URI <uri-tag>
7	Angerufene Nummer	destination-pattern <DNIS-Nummer> destination e164-pattern-map <pattern-map-number> dnis-map <dnis-map-Nummer>
8	Anrufernummer	destination calls e164-pattern-map <pattern-map-number>

Tabelle 5. Auswahl ausgehender H323-DFÜ-Peers - Voreinstellung

Bevorzugung	Zuordnungskriterien	DFÜ-Peer-Befehle
1	DFÜ-Peer-Gruppe DFÜ-Peer	destination dpg <dpg-tag> (konfiguriert auf eingehenden Dial-Peer)
2	URI und Carrier-ID	destination uri <uri-tag> AND carrier-id target <string>
3	Angerufene Nummer und Carrier-ID	destination-pattern <Nummer-Zeichenfolge> UND carrier-id target <Zeichenfolge>
4	URI	Ziel-URI <uri-tag>
5	Angerufene Nummer	destination-pattern <Nummer-Zeichenfolge> destination e164-pattern-map <pattern-map-number> dnis-map <dnis-map-Nummer>
6	Anrufernummer	destination calls e164-pattern-map <pattern-map-number>

Tabelle 6. Ausgehende POTS-DFÜ-Peer-Auswahlpräferenz

Bevorzugung	Zuordnungskriterien	DFÜ-Peer-Befehle*

1	DFÜ-Peer-Gruppe DFÜ-Peer	destination dpg <dpg-tag>(konfiguriert für eingehenden Dial-Peer)
2	URI und Carrier-ID	destination uri <uri-tag> AND carrier-id target <string>
3	Angerufene Nummer und Carrier-ID	destination-pattern <Nummer-Zeichenfolge> UND carrier-id target <Zeichenfolge>
4	URI	Ziel-URI <uri-tag>
5	Angerufene Nummer	destination-pattern <DNIS-Nummer>dnis-map <Kartennummer>

Hinweis: Im Abschnitt Nummernzeichenfolgen-DFÜ-Peer-Hunting und URI-DFÜ-Peer-Hunting wird beschrieben, wie das Gateway eine Liste potenzieller Befehle für jede Zeile mit Übereinstimmungskriterien auswertet, bevor zum nächsten Übereinstimmungskriterium übergegangen wird. Beispielsweise werden alle potenziellen Ziel-Musterübereinstimmungen und e164-Ziel-Musterzuordnungsbefehle ausgewertet, bevor die Anrufernummernbefehle überprüft werden.

Nummernzeichenfolgen-DFÜ-Peer-Verfolgung

Bevorzugte Nummernzeichenfolge:

Ähnlich wie URIs eine bestimmte Reihenfolge von Operationen zum Auswerten von Übereinstimmungen haben, gibt es auch einen Satz von Regeln, die beim Auswerten einer numerischen Ziffernfolge verwendet werden. Das standardmäßige Dial-Peer-Sammelanschlussschema für ein Cisco Gateway ist auf 0 festgelegt. Das bedeutet, dass das Gateway nach einem Muster mit der längsten Übereinstimmung (dem spezifischsten) sucht. Wenn zwei DFÜ-Peers mit derselben Länge für die Übereinstimmung vorhanden sind, prüft das Gateway die explizit definierte DFÜ-Peer-Präferenz. Wenn beide identisch sind, wählt das System eine Zufallsfolge aus.

Für die Konfiguration stehen andere Dial-Peer-Sammelanschlussschemata zur Verfügung. Bei den meisten Bereitstellungen wird jedoch der Standardwert 0 beibehalten.

Tipp: Wenn Dial-Peers außerhalb der Standardreihenfolge zugeordnet werden, kann ein Administrator die aktuelle Konfiguration auf ein nicht standardmäßiges Dial-Peer-Sammelanschlussschema überprüfen.

```
Gateway(config)# dial-peer hunt ?
  <0-7>  Dial-peer hunting choices, listed in hunting order within each choice:
  0 - Longest match in phone number, explicit preference, random selection.
  1 - Longest match in phone number, explicit preference, least recent use.
  2 - Explicit preference, longest match in phone number, random selection.
  3 - Explicit preference, longest match in phone number, least recent use.
  4 - Least recent use, longest match in phone number, explicit preference.
  5 - Least recent use, explicit preference, longest match in phone number.
  6 - Random selection.
  7 - Least recent use.
```

Der Dial-Peer-Algorithmus ermittelt den Dial-Peer mit der längsten Übereinstimmung und den meisten Nummern in einer Ziffernfolge, die genau mit einer Ziffernfolge in einer Ziffernfolge übereinstimmen. Dieses Konzept wird im nachfolgenden Szenario verdeutlicht.

Szenario: Berechtigte DFÜ-Peers wurden mit diesen möglichen Übereinstimmungen konfiguriert, und das Gateway wertet eine Ziffernfolge von 2001 aus. DFÜ-Peer 1 kann mit einer beliebigen Nummer von 2000 bis 2999 übereinstimmen, während DFÜ-Peer 2 mit 2000 bis 2009 übereinstimmen kann. Dial-Peer 2 würde für diesen Anruf zugeordnet, da es sich um die längste Übereinstimmung (genauer gesagt, die längste Übereinstimmung) für die Ziffernfolge 2001 handelt, wenn die Standardmethode für die DFÜ-Peer-Suche verwendet wird (Dial-Peer-Hunt 0). Mit anderen Worten, die Ziffernfolge 200 ist die größte Ziffernfolge, die genau mit einer Ziffernfolge in der Ziffernfolge 2001 übereinstimmt.

```
!
dial-peer voice 1 voip
 destination-pattern 2...
!
dial-peer voice 2 voip
 destination-pattern 200.
!
```

Die Voreinstellungen werden als vom Administrator definierte Gewichtung für jeden Dial-Peer definiert. Administratoren können eine Voreinstellung konfigurieren, sodass für den Anruf stets ein bestimmter Dial-Peer als erster verwendet wird. Standardmäßig sind alle DFÜ-Peers mit der Präferenz 0 verbunden. Ein Dial-Peer mit der Präferenz 0 wird vor einem anderen Dial-Peer mit der Präferenz 1 bis 10 abgeglichen. Die meisten Administratoren richten mehrere Dial-Peers ein, um einen Anruf an einen bestimmten CUCM-Subscriber zu senden, wobei ein Backup-Subscriber oder ein anderer Call Agent mithilfe eines anderen Dial-Peers mit einer niedrigeren Präferenz (der mit einer höheren Nummer konfiguriert ist) konfiguriert wird.

Szenario: Zwei DFÜ-Peers werden für die Ziffernfolge 2001 mit derselben Länge konfiguriert. Der Administrator definiert eine explizite Voreinstellung. Das Gateway wertet beide DFÜ-Peers gleich aus, da deren Übereinstimmungslänge identisch ist. Der Administrator legt den DFÜ-Peer 1 jedoch mit einer höheren Präferenz fest, sodass der DFÜ-Peer als erster Dial-Peer für die Anrufweiterleitung ausgewählt wird. Dial-Peer 2 bliebe als sekundäre Option erhalten, wenn beim ersten Dial-Peer ein Fehler auftritt.

```
!
dial-peer voice 1 voip
 destination-pattern 2...
 preference 1
!
dial-peer voice 2 voip
 destination-pattern 2...
 preference 2
!
```

Ein Cisco Gateway versucht jeweils nur, einen Anruf über einen qualifizierten ausgehenden Dial-Peer weiterzuleiten. Wenn beim ersten ausgewählten Dial-Peer eine Fehlerbedingung auftritt, versucht das Gateway, den Anruf an den nächsten qualifizierten Dial-Peer weiterzuleiten. Dieser Vorgang wird so lange fortgesetzt, bis der Anruf erfolgreich war oder fehlschlug, da keine weiteren qualifizierten DFÜ-Peers zum Versuch übrig sind. Ein häufiges Symptom für das Sammeln und Versagen von DFÜ-Peers ist die Verzögerung des Rückrufs bei der Durchführung von Anrufen. In der Regel sind Debugging-Programme erforderlich, um genau zu überprüfen, warum der Anruf auf einem bestimmten Dial-Peer fehlschlägt. Der Befehl huntstop kann auf einem Dial-Peer verwendet werden, wenn ein Administrator nicht möchte, dass ein Gateway nach einem anderen Dial-Peer sucht, wenn eine Fehlerbedingung festgestellt wird.

Szenario: Zwei DFÜ-Peers werden für die Ziffernfolge 2001 mit derselben Länge konfiguriert. Der Administrator hat eine explizite Voreinstellung definiert und möchte für diesen Anruf keine Übereinstimmung mit Dial-Peer 2 herstellen. Da es zwei DFÜ-Peers mit derselben Länge für die Übereinstimmung gibt, wird die Präferenz verwendet, um den DFÜ-Peer zu bestimmen. Dial-Peer 1 hat die niedrigste konfigurierte Einstellungsnummer und wird daher für die Weiterleitung des Anrufs verwendet. Tritt auf der ausgehenden Anrufstrecke unter Verwendung des Dial-Peer 1 eine Fehlerbedingung auf, beendet das Gateway sofort die Dial-Peer-Verfolgung, da der Befehl huntstop konfiguriert ist. In diesem Szenario wird der Dial-Peer 2 nie für das Routing ausgehender Anrufe verwendet.

```
!
dial-peer voice 1 voip
 destination-pattern 2...
 preference 1
 huntstop
!
dial-peer voice 2 voip
 destination-pattern 2...
 preference 2
!
```

Hinweis: Huntstop- und Voreinstellungsbefehle können auch in Verbindung mit URI-Matching-Anweisungen verwendet werden, da es sich um allgemeine Dial-Peer-Konfigurationsbefehle handelt. Darüber hinaus können bei Servergruppenkonfigurationen für Sprachklassen Huntstop-Befehle in 17.4.1a verwendet werden. Weitere Informationen hierzu

---

finden Sie im Abschnitt "Ziel-Server-Gruppen".

URI-DFÜ-Peer-Verfolgung

Das Gateway prüft alle Kriterien für die Übereinstimmung und erschöpft diese, bevor es mit den nächsten Kriterien für die Übereinstimmung fortfährt. Ein Beispiel hierfür ist ein eingehender SIP-Anruf. Basierend auf Tabelle 1. Inbound SIP Dial-Peer Selection Preference (Eingehende SIP-DFÜ-Peer-Auswahl-Voreinstellungen): Das Cisco Gateway überprüft zunächst den URI und wertet alle möglichen URI-Befehle aus, um einen passenden zu finden. Wenn keine Übereinstimmung vorliegt oder keine konfiguriert wurde, wechselt das Gateway zum nächsten übereinstimmenden Element und führt eine Bewertung für dieses Kriterium durch. Dieser Prozess wird wiederholt, bis der Anruf entweder auf Grundlage einer Übereinstimmung weiterleitet oder das Gateway nicht mehr über die zu überprüfenden Kriterien verfügt.

Wenn ein eingehender oder ausgehender Dial-Peer mit einem URI-Befehl konfiguriert wird, überprüft das Gateway den in mehreren Headern empfangenen URI auf eine mögliche Übereinstimmung. Die Übereinstimmungseinstellung basiert auf der spezifischsten Übereinstimmung, und die genaue Einstellung gilt für Vollständige URI-Übereinstimmung, Hostkomponente, Benutzerkomponente oder Telefon-URI. Wenn Sie die Reihenfolge der Vorgänge für den URI-Abgleich kennen, kann dies beim Dial-Peer-Abgleich mit SIP- und CUBE-Bereitstellungen sehr hilfreich sein.

Diese Einstellungsreihenfolge kann mithilfe des Befehls voice class uri sip preference geändert werden, um die Benutzer-ID als erste Option anstatt als Host anzugeben.

URI-Voreinstellung:

1. Der Host-Teil des URI. Beispiele: (@a.b.c.d oder @host.domain.name)
2. Der User-Teil des URI. Beispiele: (sip:8675309 oder sip:user)
3. Das Tele-URI. Beispiel: (tel:18005532447)
4. Genaue Übereinstimmung für den vollständigen URI. Beispiele: (user@host.domain.name, user@a.b.c.d, 8675309@host.domain.name, 8675309@host.domain.name)

Begleitdokument: Konfigurationsleitfaden für Cisco Unified Border Element - ab Cisco IOS XE 17.6

Szenario: Ein Administrator hat diese DFÜ-Peers konfiguriert und sendet einen Anruf an das Gateway. Der Von-Header in der empfangenen Einladung lautet From: <sip:testuser@10.10.10.10>. Das Gateway kann auf Basis dieses Headers zwei verschiedene Dial-Peers zuordnen. Dial-Peer 1 basierend auf dem Benutzerteil und Dial-Peer 2 basierend auf dem Hostteil. Da eine Host-Übereinstimmung jedoch eine Präferenz gegenüber einer Benutzer-Übereinstimmung ist, wird für den eingehenden Dial-Peer im Anruf Dial-Peer 2 verwendet.

```
!
voice class uri URI1 sip
 user-id testuser
!
```

```
voice class uri URI2 sip
 host ipv4:10.10.10.10
!
dial-peer voice 1 voip
 sess protocol sipv2
 incoming uri FROM URI1
!
dial-peer voice 2 voip
 sess protocol sipv2
 incoming uri FROM URI2
!
```

Sprachklassen-URI

Durch den URI-Abgleich für eingehende und ausgehende DFÜ-Peers kann ein Administrator Abgleiche mit mehr als einer Telefonnummernzeichenfolge für VoIP-Protokolle durchführen, die URIs in seinem Messaging unterstützen. Vor IOS 15.4(1)T und IOS-XE 3.11S musste ein Anforderungs-URI eine alphanumerische user@host enthalten. Andernfalls lehnte ein Cisco Gateway den Anruf mit einer 4xx-Nachricht ab. Nun kann ein URI nur den Host-Teil enthalten, und das Gateway leitet den Anruf nur auf Basis des bereitgestellten Hosts weiter. Beispiel: sip:cisco.com.

Außerdem konnten vor IOS 15.4(1)T und IOS-XE 3.11S Sprachklassen-URI-Benutzer-IDs nur numerische e.164-Werte sein (sip:1234@host.com). Dies wurde geändert, damit Administratoren alphanumerische Benutzer-IDs für CUBE konfigurieren können (sip:user@host.com).

Der Host- oder Benutzerteil eines Sprachklassen-URIs kann reguläre Ausdrücke (reguläre Ausdrücke) enthalten, die die möglichen Werte, die zugeordnet werden können, erheblich erweitern.

```
Gateway(config-voice-uri-class)# user-id .)
% unmatched ()user-id pattern can be of format ^([][0-9A-Za-z\|\/()*+^$&?#--.])*$

Gateway(config-voice-uri-class)# host .)
% unmatched ()host pattern can be of format ^([][0-9A-Za-z\|@\/()*+^$&?#--.])*$

Gateway(config-voice-uri-class)# pattern .)
% unmatched ()pattern pattern can be of format ^([][0-9A-Za-z\|@;:=%!~\/()*+^$&?#--.])*$
```

Beispiel: Sprachklassen-URIs

```
!
voice class uri HOST sip
 host webex.com
 host dns:cisco.webex.com
 host ipv4:10.50.244.2
```

```
 host ipv6:[2001:4860:4860::8888]
!
voice class uri USER sip
 user-id username
!
voice class uri PATTERN sip
 pattern 8675309
!
voice class uri HostRegex sip
 host (.*)cisco.com
!
voice class uri ipRegex sip
 host 172\.18\.110\.20[567]
!
voice class uri PatternRegex sip
 pattern 555(.*)
!
voice class uri ipRegex sip
 pattern (172\.18\.110\.10[134]|10\.10\.10\.10)
 ! One Line that matches 172.18.110.101, 172.18.110.103, 172.18.110.104 OR 10.10.10.10
!
voice class uri UserRegex sip
 user-id test(.*)
!
```

Pro Sprachklassen-URI können nur 10 Hosts, 1 Muster oder 1 Benutzer-ID konfiguriert werden, wie in diesem Beispiel veranschaulicht. Wenn weitere Artikel zugeordnet werden müssen, wird empfohlen, Regex zu verwenden.

```
Gateway(config)# voice class uri TEST sip
Gateway(config-voice-uri-class)#host ipv4:10.1.1.1
Gateway(config-voice-uri-class)#host ipv4:10.2.2.2
Gateway(config-voice-uri-class)#host ipv4:10.3.3.3
Gateway(config-voice-uri-class)#host ipv4:10.4.4.4
Gateway(config-voice-uri-class)#host ipv4:10.5.5.5
Gateway(config-voice-uri-class)#host ipv4:10.6.6.6
Gateway(config-voice-uri-class)#host ipv4:10.7.7.7
Gateway(config-voice-uri-class)#host ipv4:10.8.8.8
Gateway(config-voice-uri-class)#host ipv4:10.9.9.9
Gateway(config-voice-uri-class)#host ipv4:10.10.10.10
Gateway(config-voice-uri-class)#host ipv4:10.11.11.11
Error:Maximum of 10 hosts can only be configured.

Gateway(config)# voice class uri TEST2 sip
Gateway(config-voice-uri-class)#host dns:1.com
Gateway(config-voice-uri-class)#host dns:2.com
Gateway(config-voice-uri-class)#host dns:3.com
Gateway(config-voice-uri-class)#host dns:4.com
Gateway(config-voice-uri-class)#host dns:5.com
Gateway(config-voice-uri-class)#host dns:6.com
Gateway(config-voice-uri-class)#host dns:7.com
Gateway(config-voice-uri-class)#host dns:8.com
Gateway(config-voice-uri-class)#host dns:9.com
Gateway(config-voice-uri-class)#host dns:10.com
Gateway(config-voice-uri-class)#host dns:11.com
Error:Maximum of 10 hosts can only be configured.
```

```
Gateway(config)# voice class uri TEST3 sip
Gateway(config-voice-uri-class)#user-id 8675309
Gateway(config-voice-uri-class)#user-id 123456789
Gateway(config-voice-uri-class)#do sh run | s TEST3
voice class uri TEST3 sip
user-id 123456789

Gateway(config)# voice class uri TEST4 sip
Gateway(config-voice-uri-class)#pattern 8675309
Gateway(config-voice-uri-class)#pattern 123456789
Gateway(config-voice-uri-class)#do sh run | s TEST4
voice class uri TEST4 sip
pattern 123456789
```

Eingehende URI-DFÜ-Peer-Zuordnung

Diese Funktion wurde in IOS 15.1(2)T und IOS-XE 3.8S hinzugefügt und verwendet einen Sprachklassen-URI, der konfiguriert und auf einen eingehenden Dial-Peer angewendet wird. Der eingehende URI wurde von vielen Personen über die herkömmliche eingehende Anweisung called-number für SIP-Anrufe übernommen, da er das erste bei der Auswahl von eingehenden Dial-Peers überprüfte Abgleichkriterium ist. Mit diesem Befehl können Administratoren außerdem Anrufe besser zuordnen, die von einem bestimmten Anruf-Agenten oder Benutzer kommen.

Vollständige Dokumentation: Konfigurationsleitfaden für Cisco Unified Border Element - ab Cisco IOS XE 17.6

Häufige Anwendungsfälle

1. Ein eingehender Dial-Peer, der auf dem Host-Teil des URI zum Beantworten von OPTIONS-Ping-Anforderungen vom CUCM übereinstimmt.
2. Ein Dial-Peer für eingehende Anrufe, der auf dem Host-Teil des URI zum Steuern eingehender Anrufe von einem Internettelefonie-Dienstanbieter (ITSP) zugeordnet ist.
3. Ein Dial-Peer-Matching bei eingehenden Anrufen für die Benutzer-ID in der URL zur Anrufbehandlung bei bestimmten Benutzern oder Nummern.

Konfigurationsbeispiel

In diesem Beispiel wird der Dial-Peer 777 für alle SIP-Anfragen von den beiden in der Sprachklassen-URI definierten HOST-IPs abgeglichen. Der überwachte Header wird auf dem Dial-Peer als "From"-Header definiert. Administratoren können jedoch noch viele weitere Header definieren, z. B. VIA, TO und REQUEST (Request URI). Wenn der CUCM einen OPTIONS-Ping an das CUBE sendet, stimmt dieser jetzt mit dem Dial-Peer 777 überein und bezieht meine 200 OK-Antwort von der angegebenen Schnittstelle auf OPTIONS. Wenn der CUCM eine Invite-Nachricht an das CUBE sendet, wird der Dial-Peer 777 als eingehender Dial-Peer abgeglichen.

```
!
voice class uri CUCM sip
 host ipv4:10.50.244.2
```

```
 host ipv4:10.50.244.20
!
dial-peer voice 777 voip
 description INCOMING URI
 session protocol sipv2
 incoming uri from CUCM
 voice-class sip bind control source-interface Loopback777
 voice-class sip bind media source-interface Loopback777
!
```

Ausgehende URI-DFÜ-Peer-Zuordnung

Cisco IOS-Gateways können einen ausgehenden Dial-Peer mithilfe eines URI abgleichen, indem ein Sprachklassen-URI auf einen ausgehenden Dial-Peer angewendet und der globalen Konfiguration eine Anrufweiterleitungs-URL hinzugefügt wird. Wenn dies vorhanden ist, kann CUBE versuchen, Anrufe basierend auf dem Anforderungs-URI weiterzuleiten. Diese Funktion wurde in IOS 12.3(4)T hinzugefügt und ist in allen IOS XE-Versionen enthalten. Beachten Sie, dass der ausgehende SIP-Anforderungs-URI und der To-Header-URI standardmäßig das Sitzungsziel des ausgehenden Dial-Peers aufweisen. Dies kann mithilfe des Befehls request-pass deaktiviert werden, mit dem das Gateway den In-Leg-URI-Hostteil an den Out-Leg übergeben kann, anstatt den URI-Hostteil durch das Sitzungsziel zu ersetzen. Der Befehl request-pass wurde in 15.4(1)T und IOS XE 3.11S hinzugefügt.

Konfigurationsbeispiel

```
voice service voip
 sip
  call-route url
  requri-passing
!
voice class uri CUCM sip
 host dns:.*.com
!
dial-peer voice 777 voip
 description OUTGOING URI
 session protocol sipv2
 destination uri CUCM
 session target sip-uri
!
```

Quelle: Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 und höher

Zusätzlich zur Sprachklassen-URI können Administratoren eine Dial-Peer-Bereitstellungsrichtlinie (DPP) verwenden, um eine In-Leg-URI für eine ausgehende Dial-Peer-Übereinstimmung abzugleichen. Diese Funktion wurde in IOS 15.4(2)T und IOS XE 3.12S hinzugefügt. Für eine Dial-Peer-Bereitstellungsrichtlinie muss ein primäres Zuordnungsattribut definiert werden, wobei ein sekundäres Zuordnungsattribut optional ist. Die Bereitstellungsrichtlinie wird auf einen eingehenden Dial-Peer angewendet. Wenn dieser Dial-Peer für die Verwendung in einem

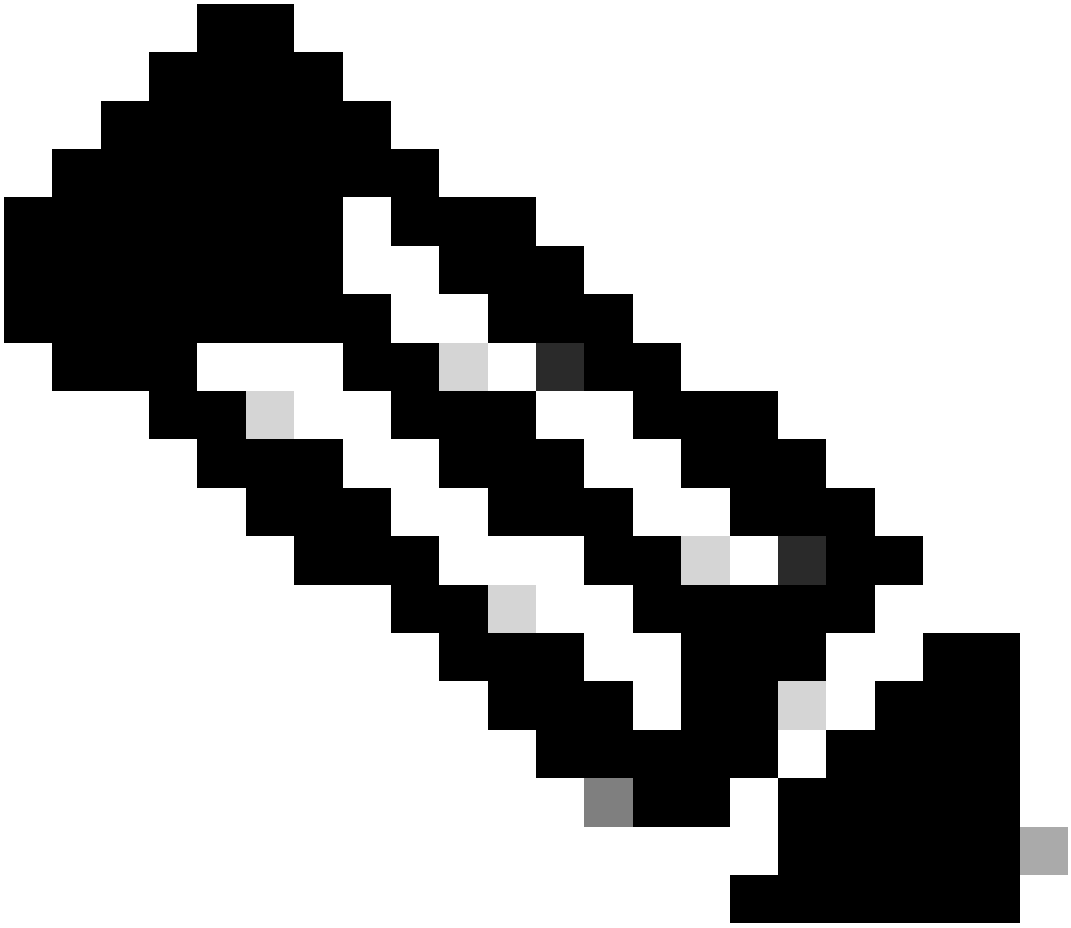
eingehenden Anrufabschnitt ausgewählt wird, wird die Richtlinie aufgerufen. Das Ergebnis ist eine ausgehende Dial-Peer-Auswahl, die auf dem Attribut in der Dial-Peer-Bereitstellungsrichtlinie basiert.

Bei der ausgehenden Übereinstimmung kann es sich um einen einzelnen Header oder um mehrere Header handeln. Alle Header müssen true sein, damit sie mit dem Dial-Peer übereinstimmen.

Im Beispiel gibt es eine Sprachklassen-URI für die Von- und Bis-Header. Für eine OR-Übereinstimmung wird eine Dial-Peer-Bereitstellungsrichtlinie konfiguriert, die zwei Voreinstellungen enthält. Der Von-Header ist die erste Voreinstellung, und der An-Header ist die Sicherungseinstellung. Dial-Peer 1234 wurde entwickelt, um die Bereitstellungsrichtlinie für den eingehenden Abgleich anzuwenden. Anschließend werden die Dial-Peer-Befehle 11111 und 22222 erstellt, die den Befehl "destination uri-from" bzw. den Befehl "destination uri-to" anwenden. Diese Befehle verweisen auf den Sprach-Klassen-URI. Sie können für den Anruf Invite empfangen, Dial-Peer 1234 zuordnen und die Bereitstellungsrichtlinie überprüfen. Das Gerät kann dann versuchen, zuerst eine Route über den Von-Header zu erstellen. Diese Übereinstimmung kann auf Dial-Peer 11111 gefunden werden. Wenn dies fehlschlägt, können Sie auch versuchen, den To-Header mit 22222 weiterzuleiten.

In diesem Beispiel wird auch erläutert, wie eine Und-Übereinstimmung mit Dial-Peer-Bereitstellungsrichtlinien erzielt wird. Wenn dieselbe Einladung empfangen wird, können Sie zwei Header unter einer Präferenz definieren und diese auf den eingehenden Dial-Peer anwenden.

Wenn die Einladung empfangen wird, kann sie prüfen, ob qualifizierte Dial-Peers für ausgehende Anrufe vorhanden sind, die beide in der Bereitstellungsrichtlinie definierten Kriterien erfüllen. In diesem Beispiel muss der Dial-Peer für ausgehende Anrufe mit dem TO- und FROM-Header definiert werden, damit ein Abgleich möglich ist. Wenn keine gültige Übereinstimmung vorliegt, wird dieser Dial-Peer 12345 nicht verwendet.



Hinweis: Obwohl wir den Anruf über den Von-Header weiterleiten, verfügt Invite, das das Gateway verlässt, noch über die ursprüngliche Anforderungs-URI. Wir verwenden einfach die Dial-Peer-Bereitstellungsrichtlinie, um einen ausgehenden Dial-Peer abzugleichen, ohne den Anforderungs-URI zu ändern.

Konfigurationsbeispiel:

<#root>

```
### Received INVITE

Received:
INVITE sip:8675309@172.18.110.58:5060 SIP/2.0
From: sipp <sip:sipp@172.18.110.65>;tag=1
To: sut <sip:cube@172.18.110.58:5060>


### Common Configurations
```

```
!
voice class uri FROM sip
 user-id sipp
!
voice class uri TO sip
 user-id cube
!
```

OR Match

```
!
voice class dial-peer provision-policy 1
 description match from header. If false, try to header
 preference 1 from
 preference 2 to
!
dial-peer voice 1234 voip
 session protocol sipv2
 destination provision-policy 1
 incoming called-number .
!
dial-peer voice 11111 voip
 destination uri-from FROM
 session protocol sipv2
 session target ipv4:172.18.110.48
!
dial-peer voice 22222 voip
 destination uri-to TO
 session protocol sipv2
 session target ipv4:172.18.110.48
!
```

AND Match

```
!
voice class dial-peer provision-policy 2
 description match from AND to headers
 preference 1 from to
!
dial-peer voice 1234 voip
 session protocol sipv2
 destination provision-policy 2
 incoming called-number .
!
dial-peer voice 12345 voip
 destination uri-from FROM
 destination uri-to TO
 session protocol sipv2
 session target ipv4:172.18.110.48
!
```

Quelle: [Cisco Unified Border Element Configuration Guide Through Cisco IOS XE 17.5]

Session-Ziel-SIP-URI

Vor IOS 15.4(1)T und IOS XE 3.11S waren zwei separate ausgehende DFÜ-Peers erforderlich, wenn der Host-Teil einer URI unterschiedlich war, der Benutzer jedoch der gleiche war.

Nach dieser Version kann ein Administrator einen Dial-Peer konfigurieren, um mehrere Hosts für denselben Benutzer zu bedienen. Beispielsweise testuser@cisco.com und testuser@webex.com unter demselben Dial-Peer. Die Verwendung von session target sip-uri löst die DNS-Auflösung der Domäne des eingehenden Invite Req-URIs aus und bestimmt dynamisch die Session target IP.

Beispielkonfiguration:

Das Gateway erhält zwei SIP-Einladungen mit diesen Headern. Invite sip:testuser@cisco.com:5060 SIP/2.0 Invite sip:testuser@webex.com:5060 SIP/2.0 Das Gateway stimmt mit der eingehenden SIP-Anforderung von testuser@cisco.com überein und testuser@webex.com auf dem Dial-Peer 1, da der Befehl incoming URI und die Benutzer-ID-Definition beide mit testuser übereinstimmen. Der Befehl voice-class sip call-route url is present bedeutet, dass Sie ausgehende DFÜ-Peers auf Basis des Anforderungs-URIs dieser eingehenden Einladung auswerten. Sie stimmen mit Dial-Peer 2 überein, weil Sie aus den gleichen Gründen Dial-Peer 1 zugeordnet haben, der Benutzer-ID von testuser. Das Sitzungsziel dieses Dial-Peers ist der ursprüngliche SIP-URI, wie er von "session target sip-uri" (einem FQDN) definiert wurde. Nachdem eine DNS-Auflösung erfolgt ist und cisco.com und webex.com in eine IP für das Layer-3-Routing geändert wurden, wird eine Nachricht vom Gateway gesendet.

```
!
ip host cisco.com 10.10.10.10
ip host webex.com 10.10.10.10
!
voice class uri TEST-IN sip
 user-id testuser
!
dial-peer voice 1 voip
 description INCOMING dial-peer
 incoming uri request TEST
 session protocol sipv2
 voice-class sip call-route url
!
dial-peer voice 2 voip
 description OUTBOUND dial-peer
 destination uri TEST
 session protocol sipv2
 session target sip-uri
!
```

Überprüfen:

```
show voice class uri <uri-name>
show voice class dial-peer provision-policy <number>
debug voip uri
```

DFÜ-Peer-Platzhalter

Ein Administrator kann beim Definieren von Übereinstimmungsmechanismen für ein- und ausgehende Anrufe, die eine Nummernfolge beinhalten, Dial-Peer-Platzhalter verwenden. Dazu gehören das Zielmuster, die eingehende angerufene Nummer, e164-pattern-maps und die Antwortadresse sowie der Präfix-Befehl. Platzhalter für DFÜ-Peers sind reguläre Ausdrücke (reguläre Ausdrücke, "regex"), die konfiguriert werden können und eine größere Flexibilität beim Abgleich von DFÜ-Peers ermöglichen.

Wildcard-Tabelle

Zeichen	Definition	Beispiele
*	Bei einem Dial-Peer ist dies ein literaler Wert von * (Stern) auf der Tastatur.	12345*
Nr.	Bei einem Dial-Peer ist dies ein Literalwert von # (Pfund) auf der Tastatur.	8675309#
,	Fügt eine Pause von 1 Sekunde zwischen Ziffern ein.Ein Komma kann auch in Klammern [ ] verwendet werden, um einen fortlaufenden Bereich aufzuteilen.	9,,,,55591[1-3,5-9]8675309
.	Regex-Zeichen zur Übereinstimmung mit beliebigen Werten 0-9, A-F und *, #, + Pro Dial-Peer können bis zu 15 Dot-Zeichen definiert werden. Mit der CLI kann ein Administrator jedoch so viele Zeichen konfigurieren, wie er möchte. Wenn mehr als 15 Punkte erforderlich sind, verwenden Sie T.	2.... 91[2-9]..[2-9].....
%	Regex für vorangegangene Ziffern, die 0- oder mehrmals vorkommen.	
+	Wenn es am Anfang einer Zeichenfolge verwendet wird, bedeutet es ein Literal +, das in E164-Nummern verwendet wird. Wenn er an einer anderen Stelle in der Zeichenfolge verwendet wird, ist er ein regulärer Wert für die vorangegangene Ziffer, der ein- oder mehrmals vorkommt.	+19191112222

?	Regex für die vorangegangene Ziffer, die null oder einmal vorkommt.	(206)5015111 EUR (0)?(1)?(1)?21933...
^	Regex-Zeichen zur Angabe des Anfangs der Zeichenfolge bei Verwendung außerhalb von Klammern Bei Verwendung in Klammern wird sie als Ausschlussanweisung oder als DO NO MATCH-Anweisung behandelt. Dies ist in späteren Versionen nicht mehr erforderlich, da das Gateway beim Verarbeiten einer Regex-Zeichenfolge ohne ^ automatisch ein ^ annimmt.	^8675309 91[^135]555
USD	Regex-Zeichen, um das Ende einer Zeichenfolge anzugeben.	8675309 USD
\	Escape-Zeichen für einen Literalwert	
[ ]	Klammern definieren einen Zeichenbereich für eine einzelne Position. Kommas müssen verwendet werden, um fortlaufende Zeichenfolgen aufzubrechen.	[1-5]0000 [2,5-8]000
( )	Klammern definieren eine Gruppe von Zeichen in einem Satz.	9(258) 7777
T	Eine variable Längenübereinstimmung von bis zu 32 Ziffern. Der Router wartet auf den Timeout zwischen den Ziffern, bevor er den Anruf weiterleitet. Der Standardwert für die Interdigit-Zeitüberschreitung beträgt 10 Sekunden und kann über die Interdigit-Zeitüberschreitung eines Sprach-Ports geändert werden. Administratoren können die Zeitüberschreitung zwischen den Ziffern mit # auf der Tastatur beenden. Dies kann über den global konfigurierten DFÜ-Peer-Terminator geändert werden. T bezieht sich auch auf den T302-Timer.	9011T
-	Wird in Klammern verwendet, um den Bereich zu definieren.	[5-9]1234

Ausgabe von Gateway, das die möglichen Eingaben für reguläre Ausdrücke anzeigt.

```
Gateway(config-dial-peer)# destination-pattern asdfqw4r3~2
Incorrect format for E.164 Number
        regular expression must be of the form  ^[][^0-9,A-F#*.?+%()-]*T?(\$)?$
```

DFÜ-Peer-Status

DFÜ-Peers können sich in einem von zwei Betriebszuständen befinden.

1. Up
2. Abwärts

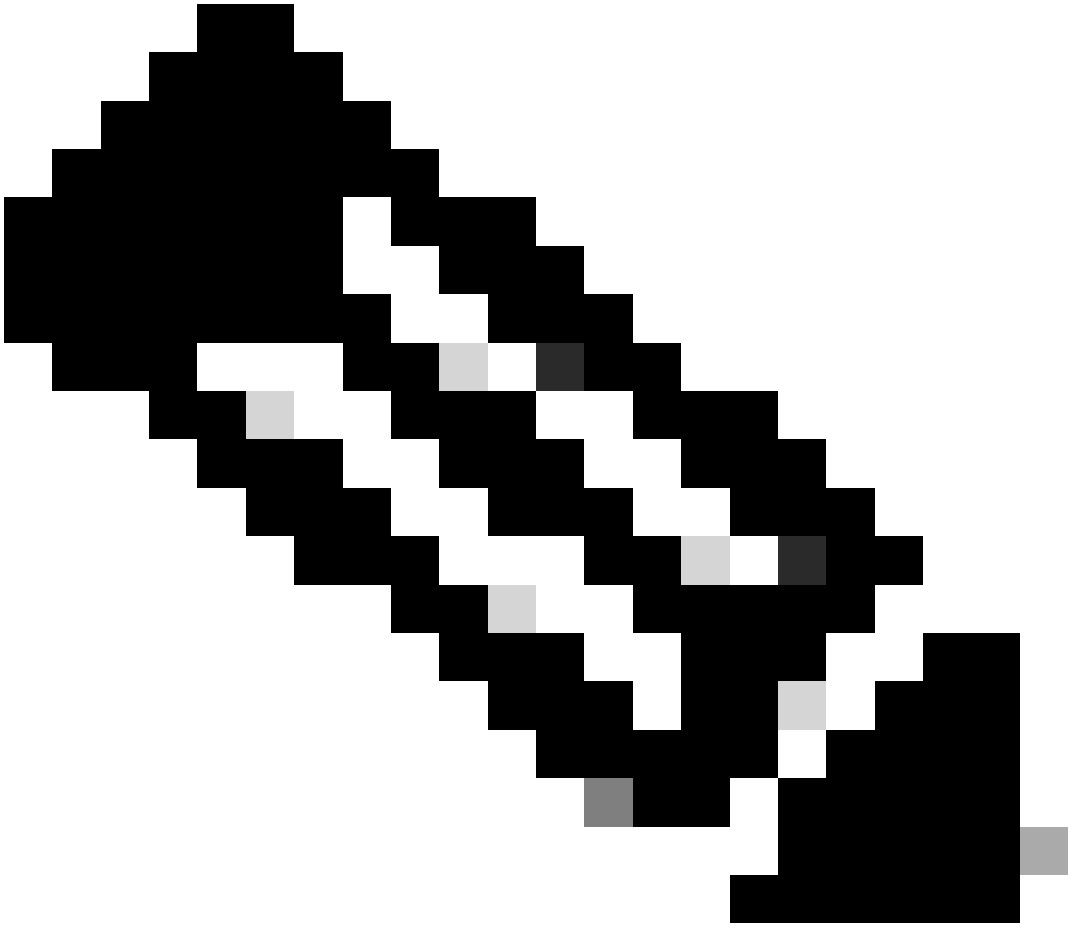
Damit sich ein Dial-Peer in einem gültigen Betriebszustand befindet und für die Anrufweiterleitung verwendet werden kann, muss er den Status "UP" aufweisen. Für ausgehende VoIP-DFÜ-Peers bedeutet dies, dass es einen gültigen Abgleichmechanismus für ausgehende Anrufe sowie ein gültiges Sitzungsziel geben kann, an das der Anruf weitergeleitet wird. Für ausgehende POTS-Dial-Peers können ein gültiger Abgleichmechanismus für ausgehende Anrufe sowie ein gültiger Sprach-Port konfiguriert werden. Nur bei eingehenden Dial-Peers muss ein gültiger Mechanismus für die eingehende Übereinstimmung konfiguriert werden.

Der Busyout-Status wird angezeigt, wenn ein Dial-Peer mit einem Keepalive-Mechanismus konfiguriert ist und das Remote-Ziel die Parameter dieses Keepalive-Mechanismus nicht befolgt hat. Anschließend versetzt das Gateway den Dial-Peer in einen Busyout-Zustand, sodass er nicht mehr für Entscheidungen zur Anrufweiterleitung verwendet wird. Wenn der Keepalive-Mechanismus wieder aktiviert ist, versetzt das Gateway den Dial-Peer wieder in den aktiven Zustand. Wenn ein Dial-Peer als ausgehender Dial-Peer ausgewählt wird und sich dieser Dial-Peer in einem Busyout-Zustand befindet, schlägt der Anruf vom Gateway mit dem Ursachencode 188 fehl.

Neben den Betriebszuständen gibt es auch die Verwaltungszustände.

1. Up
2. Abwärts

Ein Administrator kann einen Dial-Peer deaktivieren, ohne ihn aus der Konfiguration zu entfernen, indem er den Befehl shutdown auf dem Dial-Peer eingibt. Um die Wählhilfe erneut zu aktivieren, geben Sie no shutdown ein.



Hinweis: Ein Dial-Peer mit einem ausgefallenen, heruntergefahrenen oder nicht betriebsbereiten Sprach-Port bleibt im Betriebszustand "Up" (aktiv), während der Status "Out" (Aus) als "Down" (ausgefallen) angezeigt wird.

Verifizierung

```
Gateway# show dial-peer voice summary
dial-peer hunt 0
                AD                                      PRE PASS                 OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN           FER THRU SESS-TARGET     STAT PORT    KEEPALIVE
1      voip  up   up                                     0  syst
777    voip  up   up            9...                    0  syst ipv4:10.50.244.2
555    voip  up   down          555                     0  syst
888    pots  up   up            888                     0                       up   0/2/0
999    pots  up   up            999                     0                       down 0/2/0
123    voip  up   up            123                     0  syst ipv4:10.10.10.10            busyout
```

Virtual Routing and Forwarding (VRF) und Dial-Peer-Hunting

Eingehendes Dial-Peer-Matching mit VRF

Ab IOS 15.6(3)M und IOS-XE 16.3.1 können Cisco Gateways eingehende Dial-Peers mithilfe von VRF-IDs abgleichen. Um dies zu nutzen, muss ein Administrator den eingehenden Dial-Peer an eine Schnittstelle binden, die den Dial-Peer wiederum an die VRF-ID der angegebenen Schnittstelle bindet. Nach Abschluss der Anbindung werden eingehende Anrufe vom Cisco Gateway gefiltert, sodass nur qualifizierte eingehende Dial-Peers berücksichtigt werden, die mit der VRF-ID der Schnittstelle übereinstimmen, auf der das Paket empfangen wurde. Von hier aus wird der eingehende Dial-Peer anhand der regulären Reihenfolge abgeglichen, in der der Dial-Peer abgeglichen wird.

Vor diesen IOS/IOS-XE-Versionen sollte das Cisco Gateway eine eingehende Auswahl treffen, die auf dem regulären Vergleich eingehender Dial-Peers ohne jegliche Filterung basiert. Dies bedeutet, dass ein VRF1-Anruf von einem VRF2-Dial-Peer abgeglichen werden könnte. Da vor diesen Versionen nur eine VRF-Instanz von H323 und SIP unterstützt wurde, treten bei der Verwendung von Multi-VRF-Funktionen weitere Probleme auf. Die Verwendung einer einzelnen VRF-Instanz für Sprachanwendungen wurde als VRF-fähige Konfiguration bezeichnet.

Vollständige VRF-kompatible Dokumentation: VRF-kompatibles H.323 und SIP für Sprach-Gateways

Vollständige Multi-VRF-Dokumentation: Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 und höher

Abgleich ausgehender DFÜ-Peers mit VRF

Cisco Gateways können Anrufe über VRFs hinweg überbrücken, ohne dass Route Leaks konfiguriert werden müssen. Dies bedeutet, dass ein eingehender Anruf bei VRF1 ausgehend auf einem Dial-Peer für VRF2 weitergeleitet werden kann, wenn die normale Auswahl für den ausgehenden Dial-Peer-Abgleich erfüllt ist. DFÜ-Peer-Gruppen können verwendet werden, um das Cisco Gateway zu zwingen, den Anruf innerhalb derselben VRF-Instanz zu halten.

Konfigurationsbeispiel für VRF- und Dial-Peer-Gruppe

Dieses Konfigurationsbeispiel enthält VRF1 und VRF2 mit zwei sich überschneidenden IP-Bereichen und zwei sich überschneidenden Telefonnummernbereichen.

Verwenden Sie die VRF-Bindung, um sicherzustellen, dass der richtige eingehende Dial-Peer zugeordnet wird, und Dial-Peer-Gruppen, um sicherzustellen, dass der richtige ausgehende VRF-Dial-Peer zugeordnet wird. Wenn ein SIP-Paket für einen Anruf bei 8675309 bei gig0/0/1.2 eingeht, filtert das Gateway alle verfügbaren eingehenden Dial-Peers basierend auf der VRF2-ID heraus. Dies bedeutet, dass Sie Dial-Peer 10 nicht zuordnen können. Wenn Sie nun die Ziffernfolge überprüfen, können Sie Dial-Peer 20 zuordnen. Dial-Peer 20 verfügt über eine Dial-Peer-Gruppe, die dem Gateway mitteilt, dass der einzige abgehende Dial-Peer, der zugeordnet

werden kann, auch der Dial-Peer 20 ist. Mit dieser Dial-Peer-Gruppe können Sie eine Übereinstimmung mit dem Dial-Peer 10 und die Weiterleitung eines Anrufs von VRF1 an VRF2 vermeiden. Von dort aus kann der Anruf wie gewohnt fortgesetzt werden.

```
!
interface GigabitEthernet0/0/1.1
 description VRF1
 encapsulation dot1Q 10
 ip vrf forwarding VRF1
 ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/0/1.2
 description VRF2
 encapsulation dot1Q 20
 ip vrf forwarding VRF2
 ip address 10.10.10.10 255.255.255.0
!
voice service voip
 no ip address trusted authenticate
 media-address voice-vrf VRF1
 media-address voice-vrf VRF2
 allow-connections sip to sip
 sip
!
voice class dpg 10
 description INBOUND VRF1 to OUTBOUND VRF1
 dial-peer 10 preference 1
!
voice class dpg 20
 description INBOUND VRF2 to OUTBOUND VRF2
 dial-peer 20 preference 1
!
dial-peer voice 10 voip
 description VRF1
 destination-pattern 8675309
 session protocol sipv2
 session target ipv4:10.10.10.20
 destination dpg 10
 incoming called-number 8675309
 voice-class sip bind control source-interface GigabitEthernet0/0/1.1
 voice-class sip bind media source-interface GigabitEthernet0/0/1.1
!
dial-peer voice 20 voip
 description VRF2
 destination-pattern 8675309
 session protocol sipv2
 session target ipv4:10.10.10.20
 destination dpg 20
 incoming called-number 8675309
 voice-class sip bind control source-interface GigabitEthernet0/0/1.2
 voice-class sip bind media source-interface GigabitEthernet0/0/1.2
!
```

Verifizierung

```
Gateway# show vrf brief | i VRF
  VRF1                             1:1                  ipv4        Gi0/0/1.1
  VRF2                             2:2                  ipv4        Gi0/0/1.2
```

```
Gateway# show dial-peer voice summary
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT    KEEPALIVE    VR
10     voip  up   up             8675309            0  syst ipv4:10.10.10.20                        VR
20     voip  up   up             8675309            0  syst ipv4:10.10.10.20                        VR
```

```
Gateway# show voice class dpg 10
Voice class dpg: 10      AdminStatus: Up
 Description: INBOUND to OUTBOUND VRF1
 Total dial-peer entries: 1

 Peer Tag       Pref
 --------       ----
 10             1
-------------------------------------
```

```
Gateway# show voice class dpg 20
Voice class dpg: 20      AdminStatus: Up
 Description: INBOUND to OUTBOUND VRF2
 Total dial-peer entries: 1

 Peer Tag       Pref
 --------       ----
 20             1
-------------------------------------
```

Erweiterte Anrufweiterleitungsmethoden

Im Laufe der Jahre, in denen die geschäftlichen Anforderungen wachsen, wächst das Unternehmen und benötigt mehr DIDs und Unternehmensadministratoren können feststellen, dass die grundlegenden DFÜ-Peers nicht die richtige Skalierung treffen. Es kann On-Off-Situationen geben, die behoben werden müssen, oder es gibt im Allgemeinen einfach zu viele DFÜ-Peers. Tausende von DFÜ-Peers vereinfachen die Administration und Fehlerbehebung nicht. Ein Dial-Peer für jeden spezifischen CUCM-Server oder Anruf-Agent verschärft das Problem zu vieler Dial-Peers, da ein Administrator nun einen Dial-Peer für jede Ziffernfolge konfigurieren muss. Wenn mehrere SIP-Provider eine Verbindung zu einem Gateway herstellen oder wenn mehrere Benutzer dasselbe CUBE verwenden, gestaltet sich die Isolierung eines bestimmten Tenants sehr schwierig.

Cisco hat dieses Feedback genutzt und eine Reihe von Artikeln erstellt, die diese und andere Probleme behandeln können. Mit DFÜ-Peer-Gruppen, Sprachklassen-Tenants,

Zielservergruppen, e164-Pattern-Maps und POTS-Trunk-Gruppen kann ein Administrator alle aufgeführten und viele andere nicht aufgelistete Probleme lösen.

DFÜ-Peer-Gruppen

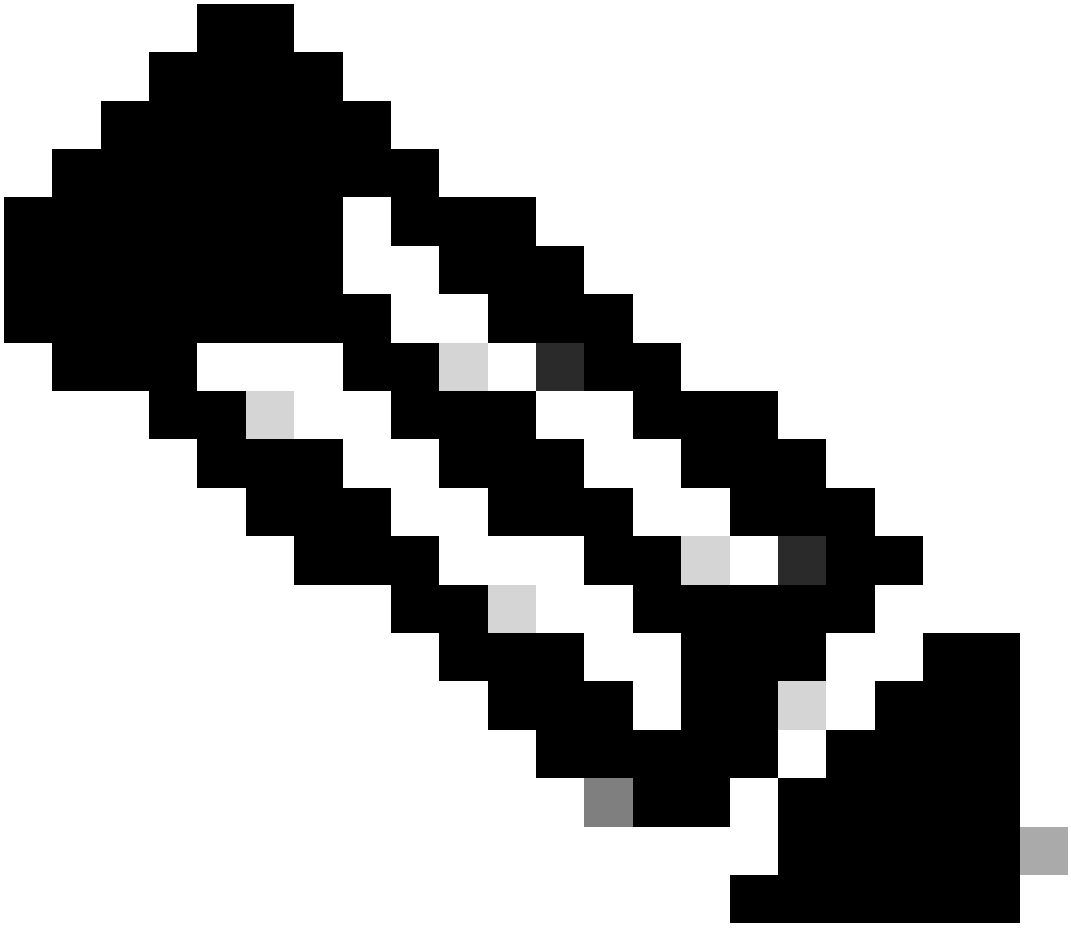
DFÜ-Peer-Gruppen wurden in IOS 15.4(1)T und IOS-XE 3.11S hinzugefügt, und POTS-DFÜ-Peers wurden als Option in IOS 15.5(1)T und IOS-XE 3.14S hinzugefügt. Mit einer Dial-Peer-Gruppe können Administratoren einen genauen Dial-Peer für das ausgehende Routing angeben, basierend auf dem übereinstimmenden eingehenden Dial-Peer. Sobald ein eingehender Dial-Peer mit konfigurierter Dial-Peer-Gruppe zugeordnet wurde, verwendet der Anruf den in der Dial-Peer-Gruppe definierten Dial-Peer, auch wenn das Zielmuster nicht übereinstimmt. Die einzige Voraussetzung ist, dass der ausgehende Dial-Peer "Up" (Aktiviert) sein muss, damit eine Methode zum Zuordnen ausgehender Anrufe konfiguriert werden kann. Dies wird jedoch nicht zum Weiterleiten des Anrufs verwendet.

Die beste Methode, Dial-Peer-Gruppen zu beschreiben, besteht darin, sie mit dem Konzept der statischen Routen in einer Routing-Tabelle zu verknüpfen. Dabei handelt es sich um Entscheidungen bezüglich der Weiterleitung von eingehenden zu ausgehenden Anrufen, die dem Gateway einige Vermutungen ersparen, da sie ihm genau sagen, wie der Anruf weitergeleitet werden soll.

Vollständige Dokumentation: Konfigurationsleitfaden für Cisco Unified Border Element - ab Cisco IOS XE 17.6

Konfigurationsbeispiel

In diesem Beispiel lautet die angerufene Nummer 8675309. Dies entspricht dem Dial-Peer 1234, basierend auf der Anweisung für die eingehende angerufene Nummer. Dieser Dial-Peer wird mit einer Dial-Peer-Gruppe konfiguriert, die angibt, dass der Anruf nun die Dial-Peers 2, dann 3 und schließlich 1 weiterleiten kann, wenn der Dial-Peer 2 ausfällt. Dies veranlasst das Gateway nun, den Call-Out-Dial-Peer 2 weiterzuleiten, da ihm von der Dial-Peer-Gruppe ausdrücklich mitgeteilt wurde, dass dies möglich ist.



Hinweis: Das Zielmuster auf Dial-Peer 1, 2 und 3 entspricht nicht der angerufenen Nummer 8675309. Dies ist in Ordnung, und der Anruf wird trotzdem ohne Problem weitergeleitet.

Denken Sie daran, dass Sie, wie im Abschnitt "Dial-Peer-Status" beschrieben, einen passenden Ausdruck für ausgehende Anrufe benötigen. In diesem Fall dient das Zielmuster lediglich dazu, den DFÜ-Peer in den Betriebszustand "Up" zu versetzen, und die Ziffernfolge dieses Befehls wird nie ausgewertet. Es wird empfohlen, ein Muster wie das Zielmuster AAAA zu konfigurieren, da es sich um ein gültiges Zielmuster handelt. Da es sich technisch gesehen um einen gültigen Dial-Peer handelt, können andere Anrufe mit diesem Peer übereinstimmen. Daher bedeutet die AAAA-Ziffernfolge, dass Sie sie nur für ein bestimmtes Szenario mit einer Dial-Peer-Gruppe verwenden können, da die Wahrscheinlichkeit, dass ein Anruf für AAAA eingeht, sehr, sehr gering ist.

```
!
dial-peer voice 1 voip
 description Server 1
 destination-pattern ^1234$
```

```
 session target ipv4:1.1.1.1
!
dial-peer voice 2 voip
 description Server 2
 destination-pattern ^5678$
 session target ipv4:2.2.2.2
!
dial-peer voice 3 voip
 description Server 3
 destination-pattern AAAA
 session target ipv4:3.3.3.3
!
voice class dpg 1
 description Dial-peer Group for specific called number 8675309
 dial-peer 2 preference 1
 dial-peer 3 preference 2
 dial-peer 1 preference 3
!
dial-peer voice 1234 voip
 description INCOMING dial-peer with DPG
 incoming called-number ^8675309$
 destination dpg 1
!
```

Verifizierung

```
Gateway# show voice class dpg 1
Voice class dpg: 1       AdminStatus: Up
 Description: Dial-peer Group for specific called number 1234
 Total dial-peer entries: 3

 Peer Tag       Pref
 --------       ----
 2              1
 3              2
 1              3
-------------------------------------
```

E164-Musterzuordnungen

Mit dieser Funktion können Administratoren die Anzahl der Dial-Peers reduzieren, indem viele mögliche Nummernübereinstimmungen (Zielmuster, eingehende angerufene Nummer usw.) in einer einzelnen Pattern-Map kombiniert werden. Die Unterstützung für ausgehende Dial-Peer-e164-Pattern-Map wurde in IOS 15.2(4)M und IOS-XE 3.7S hinzugefügt, während die Unterstützung für eingehende Dial-Peer-e164-Pattern-Map in IOS 15.4(1)T und IOS-XE 3.11S hinzugefügt wurde.

Eine e164-pattern-map kann über die CLI konfiguriert oder vorkonfiguriert werden und wird als CFG-Datei gespeichert. Die .cfg-Datei wird dann dem Flash-Speicher des Gateways hinzugefügt und beim Konfigurieren des restlichen Befehls darauf verwiesen. Die .cfg-Datei kann 5000 Einträge enthalten.

Die Einträge in beiden Konfigurationsmethoden können alle normalen Dial-Peer-Platzhalter für die weitere Aggregation verwenden!

Vollständige Dokumentation: Konfigurationsleitfaden für Cisco Unified Border Element - ab Cisco IOS XE 17.6

CLI-Konfigurationsbeispiel - Anrufnummern

```
!
voice class e164-pattern-map 1
 description E164 Pattern Map for calling numbers
 e164 919574100.
 e164 919574300.
 e164 8675309
!
dial-peer voice 1 voip
 description INBOUND Dial-peer based on CALLING #
 incoming calling e164-pattern-map 1
!
dial-peer voice 11 voip
 description OUTBOUND Dial-peer based on CALLING #
 destination calling e164-pattern-map 1
!
```

CLI-Konfigurationsbeispiel - angerufene Nummer

```
!
voice class e164-pattern-map 2
 description E164 Pattern Map for called 800 numbers
 e164 91800T
 e164 91855T
 e164 91888T
!
dial-peer voice 2 voip
 description INBOUND Dial-peer based on CALLED #
 incoming called e164-pattern-map 2
!
dial-peer voice 22 voip
 description OUTBOUND Dial-peer based on CALLED #
 destination e164-pattern-map 2
!
```

Flash-Konfigurationsbeispiel

```
!
voice class e164-pattern-map <tag>
 description FILEPATH for E164 Pattern Map
```

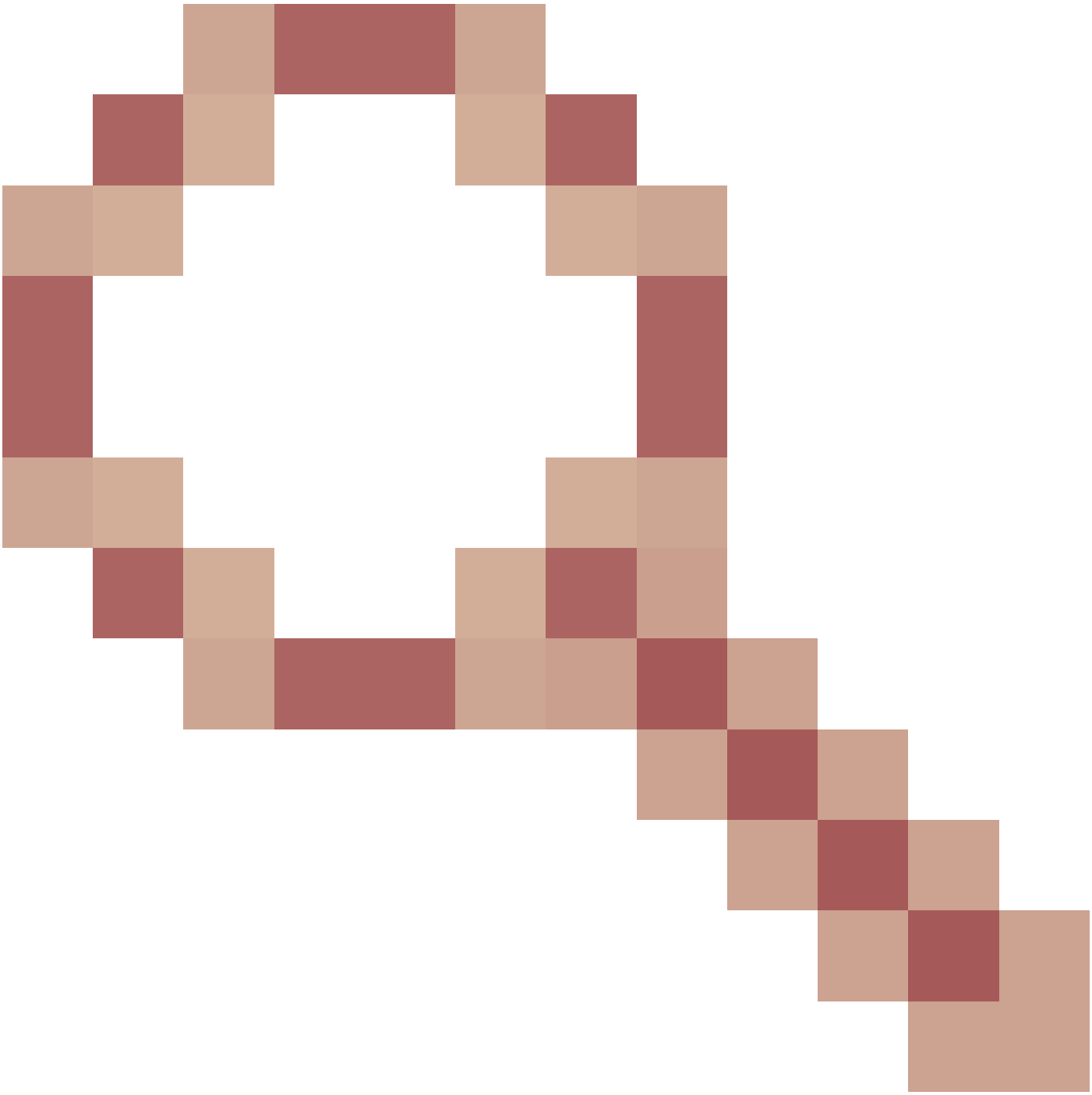
```
 url flash:<filepath>/e164-pattern-list.cfg
!
dial-peer voice ### voip
 description E164 Pattern Map Dial-peer
 incoming calling e164-pattern-map <tag>
!

voice class e164-pattern-map load <tag>
```

Verifizierung

```
Gateway# show voice class e164-pattern-map 1

e164-pattern-map 1
----------------------------------------
  Description: CUCM phones
  It has 3 entries
  It is not populated from a file.
  Map is valid.

E164 pattern
-------------------
8675309
1...
[2-5]...$
```

Erhebliche Mängel

Die Cisco Bug-ID CSCva64393

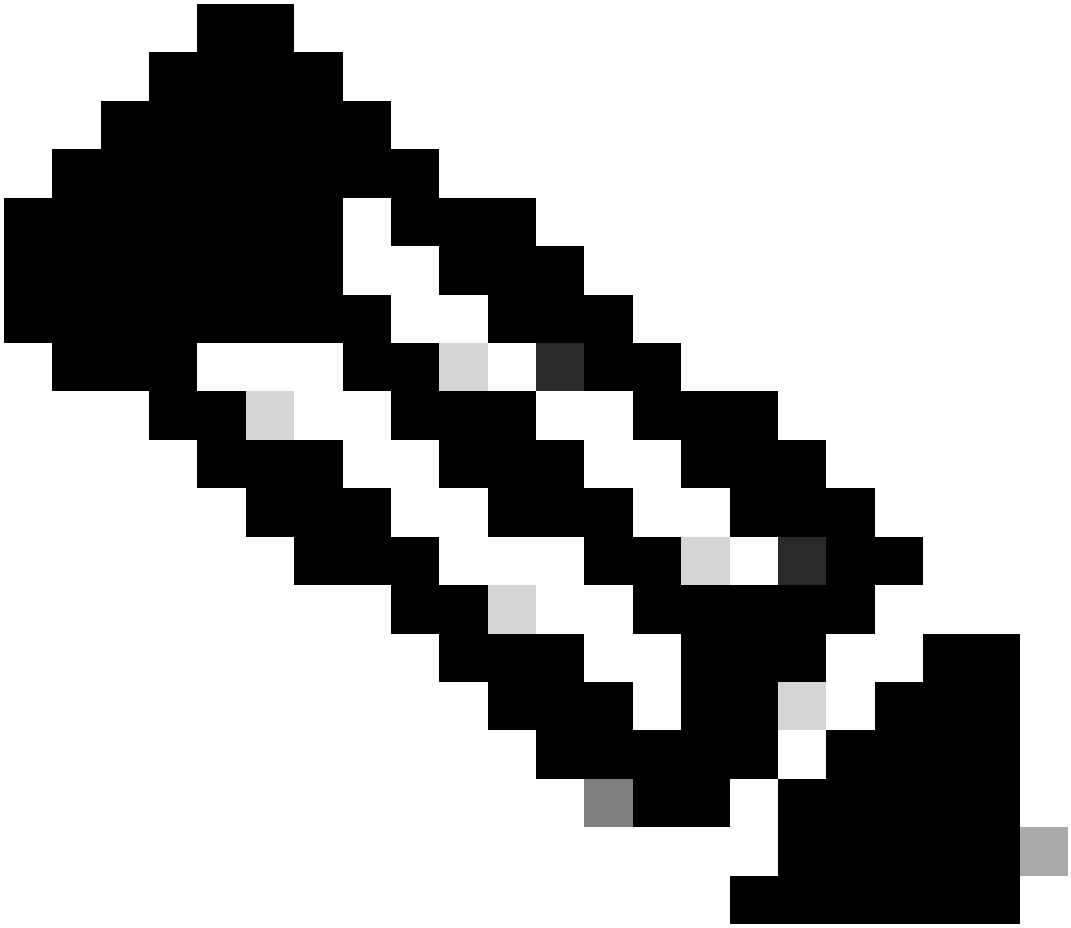


e164-pattern-map analysiert nicht die letzte Zeile der Konfigurationsdatei.

Ziel-Server-Gruppen

Mit Servergruppen können Administratoren mehrere Ziele (Sitzungsziele) auf demselben VOIP-Dial-Peer konfigurieren. Standardmäßig ist die Sortierreihenfolge die in den Servergruppeneinträgen definierte Voreinstellung. Round-Robin Hunting kann verwendet werden, wenn Sie den Befehl hunt-schema round-robin verwenden. Servergruppen wurden in Cisco IOS 15.4(1)T und Cisco IOS XE 3.11S hinzugefügt. In Cisco IOS XE 17.4.1a wurden konfigurierbare Huntstop-Fehlercodes zu Sprachklassen-Server-Gruppenkonfigurationen hinzugefügt. Das heißt, Sie können einen einzelnen Fehlercode konfigurieren, z. B. 404 Not Found (Nicht gefunden), und ein SIP-Fehler löst normalerweise das Gerät aus, um die nächste Option in der Servergruppe auszuprobieren. Wenn die Konfiguration huntstop 1 bzw. 404 in der Servergruppe aktiviert ist,

kann das Hunting stoppen. Diese können auch für einen Bereich wie: huntstop 1 resp-code 401 bis 599 konfiguriert werden.



Hinweis: Pro Servergruppe sind maximal 5 Einträge möglich.

Vollständige Dokumentation: Konfigurationsleitfaden für Cisco Unified Border Element - ab Cisco IOS XE 17.6

Konfigurationsbeispiel - Normal

```
!
voice class server-group 1
 hunt-scheme round-robin
 ipv4 10.50.244.2 port 5060 preference 1
 ipv4 10.50.244.62
 ipv6 2010:AB8:0:2::1 port 2323 preference 3
 ipv6 2010:AB8:0:2::2 port 2222
!
```

```
dial-peer voice 1 voip
 session protocol sipv2
 destination-pattern 8675309
 session server-group 1
!
```

Verifizierung

```
Gateway# show voice class server-group 1
Voice class server-group: 1
 AdminStatus: Up OperStatus: Up
 Hunt-Scheme: round-robin Last returned server:
 Description:
 Total server entries: 4

 Pref Type IP Address IP Port
 ---- ---- ---------- -------
 1 ipv4 10.50.244.2     5060
 0 ipv4 10.50.244.62
 3 ipv6 2010:AB8:0:2::1 2323
 0 ipv6 2010:AB8:0:2::2 2222
[..truncated..]
```

Zielservergruppe und OPTIONS Keepalive

Beachten Sie, dass Servergruppen nicht den normalen Out-of-Dialog OPTIONS Keepalive-Mechanismen folgen. Sie verwenden eine Funktion, die als option-keepalive-Profil bezeichnet wird. Dadurch kann das Gateway jeden Anruf-Agenten überwachen, der in der jeweiligen Servergruppe definiert ist.

Beispiel für Option-Keepalive mit Servergruppe

```
!
voice class server-group 1
 hunt-scheme round-robin
 ipv4 10.50.244.2
 ipv4 10.50.244.62
!
dial-peer voice 1 voip
 session protocol sipv2
 session server-group 1
 voice-class sip options-keepalive profile 1
!
```

Verifizierung

<#root>

```
Gateway#

show voice class sip-options-keepalive 1

Voice class sip-options-keepalive: 1             AdminStat: Up
 Description:
 Transport: system               Sip Profiles: 0
 Interval(seconds) Up: 5                 Down: 5
 Retry: 5

  Peer Tag      Server Group    OOD SessID      OOD Stat        IfIndex
  --------      ------------    ----------      --------        -------
  1             1                               Active          87

  Server Group: 1                OOD Stat: Active
   OOD SessID   OOD Stat
   ----------   --------
   1            Active
   2            Active

 OOD SessID: 1                   OOD Stat: Active
  Target: ipv4:10.50.244.2
  Transport: system              Sip Profiles: 0

 OOD SessID: 2                   OOD Stat: Active
  Target: ipv4:10.50.244.62
  Transport: system              Sip Profiles: 0
```

Ausgehender Proxy

Die Konfiguration des ausgehenden SIP-Proxys kann der Sprachdienst-VoIP-, Sprachklassen-Tenant- oder Dial-Peer-Konfiguration hinzugefügt werden, um das Ziel für ein Layer-3-SIP-Paket anzugeben.

Das Sitzungsziel auf einem Dial-Peer kann zum Erstellen des SIP-Pakets verwendet werden, der ausgehende Proxy kann jedoch den Ort bestimmen, an den das Paket auf Layer 3 gesendet wird.

```
!
voice service voip
 sip
  outbound-proxy dns:la01.sipconnect-us10.cisco-bcld.com
!
voice class tenant 100
 outbound-proxy dns:la01.sipconnect-us10.cisco-bcld.com
!
dial-peer voice 100 voip
 session target ipv4:192.168.1.1
 voice-class sip outbound-proxy dns:la01.sipconnect-us10.cisco-bcld.com
!
```

Es ist zu beachten, dass die Standardkonfiguration für einen Dial-Peer ein ausgehenden SIP-Proxysystem der Sprachklasse ist, das einen Dial-Peer dazu veranlassen kann, die globale

Sprachdienst-VoIP- > SIP-Konfiguration zu verwenden.

Dieses Verhalten kann deaktiviert werden und einen Dial-Peer zwingen, zurückzufallen und das Sitzungsziel als Layer-3-Ziel pro Dial-Peer mit der folgenden Konfiguration zu verwenden:

```
dial-peer voice 777 voip
 no voice-class sip outbound-proxy
```

POTS-Trunk-Gruppen

Trunk-Gruppen sind eine Zusammenstellung physischer Sprach-Ports mit ähnlichen Signalisierungsfunktionen. Mit dieser Funktion kann die Gesamtzahl der zu konfigurierenden POTS-Dial-Peers reduziert werden. Trunk-Gruppen wurden in 12.1(3)T in IOS eingeführt und sind in allen Versionen von Cisco IOS XE vorhanden.

Vollständige Dokumentation: Gateway-Trunk- und Carrier-basierte Routing-Verbesserungen

Konfigurationsbeispiel

```
!
trunk group PSTN
 description PSTN voice-ports
!
trunk group FXO
 description FXO voice-ports
!
voice-port 0/2/0
 trunk-group PSTN 1
!
voice-port 0/2/1
 trunk-group PSTN 2
!
voice-port 0/2/2
 trunk-group FXO 1
!
voice-port 0/2/3
 trunk-group FXO 2
!
dial-peer voice 1234 pots
 trunkgroup PSTN 1
 trunkgroup FXO 2
!
```

Sprachklassen-Tenants

Mit Cisco IOS 15.6(2)T und Cisco IOS XE 16.3.1 wurden Tenants der Sprachklasse eingeführt, die es jedem Tenant ermöglichen, eigene individuelle Konfigurationen zu erstellen. Ein Tenant

kann ein Telefonieanbieter, Cisco Unified Communication Manager (CUCM) oder ein beliebiger anderer Drittanbieter-Anruf-Agent sein, für den ein Administrator spezifische globale Einstellungen benötigt. Zunächst erstellt ein Administrator einen Tenant für die Sprachklasse und definiert die Parameter. Der Tenant der Sprachklasse wird dann auf den gewünschten Dial-Peer oder die gewünschte Auswahl angewendet. Mit dieser neuen Konfiguration erhalten Administratoren eine weitere Steuerungsebene über die DFÜ-Peers und die globale Konfiguration hinaus.

Mit Version 17.8.1a können Sprachklassen-Tenant-Konfigurationen mit einem SIP-Listen-Befehl (in Verbindung mit dem entsprechenden SIP-Steuerungs-Bindungsbefehl) konfiguriert werden, um den nicht sicheren Port für diesen Tenant zu definieren. Das bedeutet, dass Tenant 1 auf unsicheres SIP auf UDP 5060 + VRF Rot hören kann, während Tenant 2 auf SIP auf TCP TLS 5070 + VRF Blau hört. Nachdem der Tenant anhand von "listen-port + bind + optional vrf" abgeglichen wurde, werden eingehende Dial-Peers an diejenigen gefiltert, auf die der Tenant angewendet wurde.

Vollständige Dokumentation: Konfigurationsleitfaden für Cisco Unified Border Element - ab Cisco IOS XE 17.6

Normale Reihenfolge der Befehlspräferenzen ohne Tenants

1. DFÜ-Peer-Befehl
2. Global Command (Sprachservice-VoIP und SIP-UA)

Reihenfolge der Befehlspräferenz für Tenants

1. Dial-Peer-Befehl
2. Tenant-Befehl
3. Globaler Befehl (Sprachdienst-VoIP und SIP-UA)

Multi-Tenant-Konfigurationsbeispiel

Sie haben zwei Mieter 777 und 999. Sie haben diese mit leicht unterschiedlichen Konfigurationen konfiguriert und auf die DFÜ-Peers angewendet. Das bedeutet, dass Anrufe, die unterschiedliche DFÜ-Peers verwenden, sowohl die DFÜ-Peer-basierten Konfigurationen als auch die Tenant-spezifischen Konfigurationen aufweisen. Bei den aufgeführten Optionen handelt es sich lediglich um einen Ausschnitt aus der Leistung von Tenants der Sprachklasse. Sehen Sie in der Dokumentation nach, was auf einem Tenant konfiguriert werden kann. Es wird empfohlen, strikte Übereinstimmungsmechanismen wie Sprachklassen-URIs einzusetzen oder Nummern mit bestimmten Ziffernfolgen zu taggen, um das Dial-Peer-Matching für Tenants zu trennen, oder sogar VRFs so zu konfigurieren, dass Tenant A sich nie mit Tenant B überschneidet und versehentlich mit einem Dial-Peer übereinstimmt, den sie nicht erreichen können.

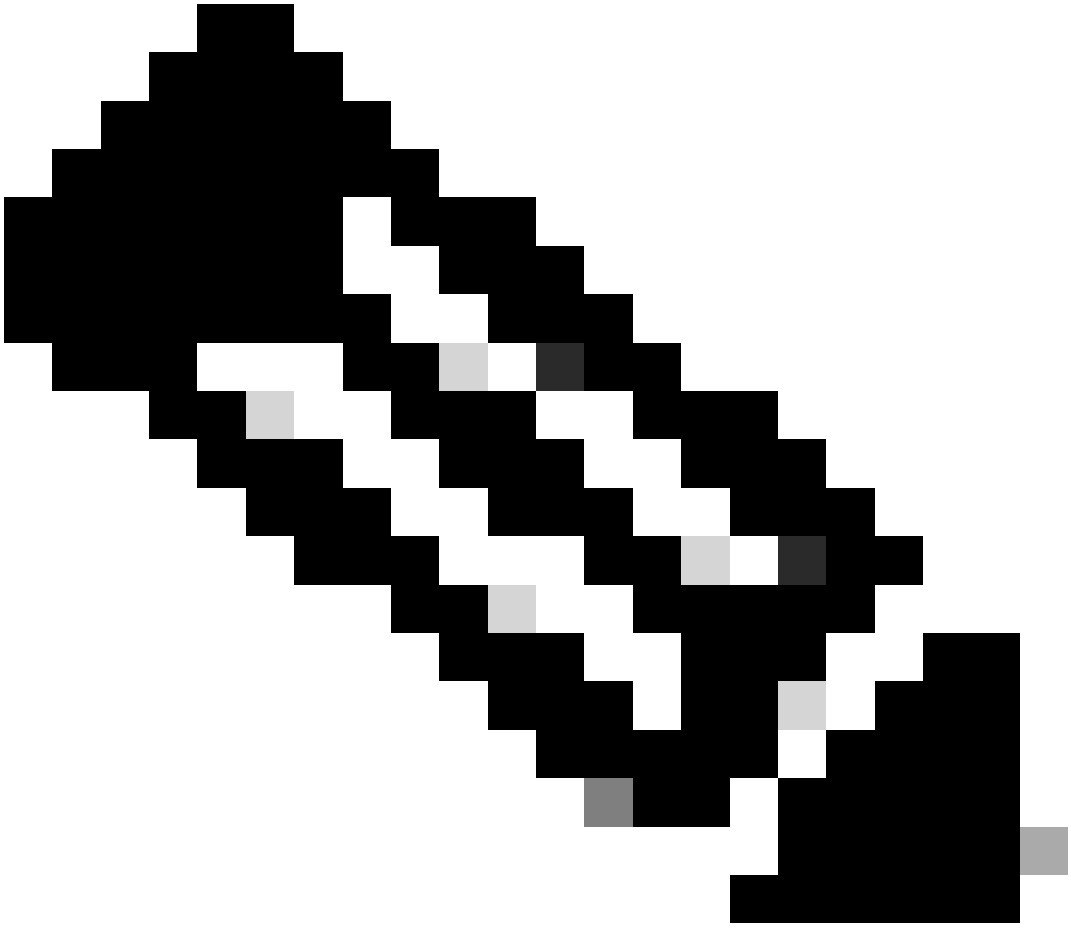
```
!
voice class tenant 999
 asymmetric payload full
 bind control source-interface GigabitEthernet0/0/0.228
 bind media source-interface GigabitEthernet0/0/0.228
 g729 annexb-all
!
```

```
voice class tenant 777
 sip-server ipv4:192.168.1.2
 bind control source-interface Loopback0
 bind media source-interface Loopback0
 pass-thru content sdp
!
dial-peer voice 999 voip
 destination-pattern 8675309
 session protocol sipv2
 incoming called-number 8675309
 voice-class sip tenant 999
!
dial-peer voice 777 voip
 destination-pattern 8675309
 session protocol sipv2
 session target sip-server
 voice-class sip tenant 777
!
```

Verifizierung

Derzeit gibt es keine einzelnen Befehle zur Anzeige der Sprachklassen-Tenant-Konfigurationen. Dieser Befehl kann ausreichen, um die aktuelle Konfiguration nur nach den Tenant-Informationen zu filtern.

```
show run | sec tenant
```



Hinweis: Die Cisco Bug-ID CSCvf28730 gibt an, dass der Status "sip-ua register" den Status der SIP-Trunk-Registrierung bei einem Tenant der Sprachklasse nicht angibt.

ILS URI-Aufrufe CUBE (Voice Class Route-String)

Routenzeichenfolgen werden mit dem CUCM-Intercluster-Suchdienst (ILS) verwendet und können so konfiguriert werden, dass Cisco Gateways VoIP-Anrufe über die Routenzeichenfolge weiterleiten können, die in der SIP-Einladung enthalten ist, die von einem CUCM 9.5+ empfangen wurde, auf dem der ILS-Dienst ausgeführt wird. Diese Funktion wurde in Cisco IOS 15.3(3)M und Cisco IOS XE 3.10S hinzugefügt. Die meisten ILS-Verbindungen bestehen zwischen CUCM und CUCM, und Administratoren müssen für Intercluster-Trunking kein CUBE verwenden. Wenn Sie die Funktion jedoch mit CUBE in der Mitte ausführen müssen, sind die Optionen vorhanden. CUCM muss die Einstellung "Send ILS Learned Destination Route String" im SIP-Profil aktivieren, um den x-cisco-dest-route-string-Header an CUBE zu senden.

Vollständige Dokumentation: Enterprise Application Interoperability for H.323-to-SIP and SIP-to-SIP Configuration Guide, Cisco IOS Release 15M&T

Konfigurationsbeispiel CUCM - SIP - CUBE - SIP - CUCM

```
!
voice service voip
 sip
  call-route dest-route-string
!
voice class route-string rt1
 pattern london.uk.eu
!
voice class sip route-string rt2
 pattern *.eu
!
voice class sip-hdr-passthrulist hdr1
 passthru-hdr x-cisco-dest-route-string
!
dial-peer voice 1 voip
 description INBOUND dial-peer
 session protocol sipv2
 voice-class sip pass-thru headers hdr1
 incoming called-number .
!
dial-peer voice 2 voip
 description OUTBOUND dial-peer
 destination route-string rt2
 session protocol sipv2
 session target ipv4:172.16.104.178
!
```

Verifizierung

```
show voice class route-string
```

Ältere Anrufweiterleitungsverfahren

Bei den in diesem Abschnitt behandelten Punkten handelt es sich um veraltete Techniken. Die Möglichkeit, diese Befehle zu konfigurieren, ist zwar weiterhin in einem Cisco Gateway vorhanden, es wird jedoch nicht empfohlen, diese Befehle in modernen Konfigurationen zu verwenden. In diesem Dokument werden sie nur behandelt, da sie bei der Arbeit mit älteren Konfigurationen oder bei Upgrades auftreten können.

DNIS-Map

DNIS-Maps könnten als Vorläufer für eine E164-Pattern-Map betrachtet werden. DNIS-Zuordnungen wurden Cisco IOS in 12.2(2)XB hinzugefügt und gab es schon immer in Cisco IOS

XE.

Wenn DNIS-Maps konfiguriert sind, lohnt es sich, diese in die robustere e164-pattern-map-Funktion umzuwandeln.

Befehlssyntax: Cisco IOS-Sprachbefehlsreferenz - D bis I

Konfigurationsbeispiel

```
!
voice dnis-map 34
 dnis 8675309
!
dial-peer voice 88 voip
 dnis-map 34
!
```

Trunk-Gruppen-Labels

Trunk-Gruppen-Labels wurden in Cisco IOS 12.2(11)T hinzugefügt und existieren in allen Cisco IOS XE-Versionen. Der Zweck eines Trunk-Gruppen-Labels ähnelt insofern einer Carrier-ID, als es dazu verwendet werden kann, die Übereinstimmung von DFÜ-Peers zu verbessern. Diese Funktion steht für die Konfiguration in POTS-Trunk-Gruppen, VoIP- und POTS-Dial-Peers sowie Sprachquellengruppen zur Verfügung. Die Verwendung von Trunk Group Labels ist in modernen Cisco Gateway-Konfigurationen selten vorzufinden.

Befehlssyntax: Cisco IOS-Sprachbefehlsreferenz - T bis Z

Konfigurationsbeispiel

```
!
dial-peer voice 112 pots
 trunk-group-label source north3
 trunk-group-label target east17
!
```

Numbering-Typ

Mit ISDN Q.931-Integrationen besteht die Möglichkeit, einen Dial-Peer basierend auf der anrufenden oder angerufenen Nummer sowie dem spezifischen ITU-Nummerntyp aus dem Q.931 SETUP-Messaging abzugleichen. Dies kann über den Nummerierungstyp-Befehl auf einem VOIP- oder POTS-DFÜ-Peer konfiguriert werden. Der Nummerntyp kann nicht allein verwendet werden und muss zusammen mit dem Zielmuster, der Antwortadresse oder der eingehenden angerufenen Nummer verwendet werden. Dies bedeutet, dass sowohl die Bedingung der Übereinstimmungsanweisung für ein-/ausgehende Anrufe als auch der Nummerntyp

übereinstimmen müssen, damit der Dial-Peer für die Weiterleitung ein- und ausgehender Anrufe berücksichtigt werden kann.

Die Numbering-Übereinstimmung kann als Dial-Peer-Filtermechanismus anstatt als Übereinstimmungsmechanismus betrachtet werden. Dies liegt daran, dass ein Dial-Peer mit und ohne angewendetem Nummerntyp-Befehl als die gleiche Standardeinstellungsgewichtung gilt, wenn keine Administratoreinstellung angewendet wird. Dies unterscheidet sich von der Carrier-ID, die bei Anwendung auf einen Dial-Peer neben einem anderen Übereinstimmungsmechanismus diesen Dial-Peer gegenüber anderen bevorzugt, wenn beide Bedingungen zutreffen.

Die Zuordnung des Nummerntyps wurde in Cisco IOS 12.0(7)XR1 hinzugefügt und ist in allen Cisco IOS XE-Versionen vorhanden. Da die Anzahl herkömmlicher POTS ISDN-Leitungen in Collaboration-Netzwerken stark abnimmt, ist die Verwendung von Nummerntypen in modernen Bereitstellungen eher selten.

Befehlssyntax: Cisco IOS-Sprachbefehlsreferenz - K bis R

Konfigurationsbeispiel

Dieser Dial-Peer kann nur 4085150000 bis 4085159999 abgleichen, wenn der ISDN-Nummerntyp National ist.

```
!
dial-peer voice 408 voip
 numbering-type national
 destination-pattern 408515....
 session target ipv4:10.1.1.2
!
```

Mögliche Nummerntypen:

Abgekürzt	Abgekürzte Darstellung der vollständigen Nummer, wie von diesem Netzwerk unterstützt
International	Angerufene Nummer, die einen Teilnehmer in einem anderen Land erreicht
Nationaler	Angerufene Nummer, um einen Teilnehmer im gleichen Land, aber außerhalb des lokalen Netzwerks zu erreichen
Netzwerk	Administrations- oder Servicenummer für das bereitstellende Netzwerk

Reserviert	Reserviert für Erweiterung
Abonnent	Nummer, die angerufen wird, um einen Teilnehmer im gleichen lokalen Netzwerk zu erreichen
Unbekannt	Art der Nummer ist vom Netzwerk unbekannt

DFÜ-Peer-Daten

Data Dial-Peers wurden in Cisco IOS 12.2(13)T eingeführt, und die Verwendung solcher Dial-Peers erfolgte für eingehende Datenmodemanrufe auf einem Cisco Gateway. Dieser Dial-Peer wird nur für eingehende Anrufe verwendet und ist in modernen Bereitstellungen nur selten zu finden.

Befehlssyntax: Cisco IOS-Sprachbefehlsreferenz - D bis I

Konfigurationsbeispiel

```
!
dial-peer data 100 pots
 incoming called-number 100
!
```

Sprachquellengruppe

Diese Funktion wurde in 15.1(2)T hinzugefügt, ist jedoch in vielen modernen Bereitstellungen nicht implementiert. Andere Sicherheitsmethoden für IOS/CUBE werden in der Regel bereitgestellt.

Die CUBE Application Security-Übersicht finden Sie in diesem Whitepaper ab Abschnitt 4.2.

Cisco Unified Border Element (CUBE) - Spezifikation für Management und Verwaltbarkeit

Befehlssyntax: Funktion "Sprachquellengruppe"

DFÜ-Peer-Berechtigungen

Mit dieser Konfiguration kann ein Administrator einen Dial-Peer so einschränken, dass er entweder nur eingehende Verbindungen (Laufzeit/Terminierung) oder Ausgangsverbindungen (Ursprung/Ursprung) zulässt. Dies wäre so, als würde ein eingehender Dial-Peer explizit so konfiguriert, dass er nur für eingehende Anrufe und ein ausgehender Dial-Peer für ausgehende Anrufe verwendet wird. Standardmäßig sind eingehende und ausgehende Verbindungen bei allen Dial-Peers zulässig. Diese CLI wird in modernen Bereitstellungen häufig nicht bereitgestellt.

```
Router(config)# dial-peer voice 1 voip
Router(config-dial-peer)# permission ?
 both allow both orig/term on this dialpeer
 none no orig/term allowed on this dialpeer
 orig allow only orig on this dialpeer
 term allow only term on this dialpeer
```

URI- und Ziffernmanipulation

An einem bestimmten Punkt in einer Collaboration-Bereitstellung kann der Administrator Ziffern oder einen URI-/SIP-Header bearbeiten müssen. Cisco Gateways verfügen über zahlreiche Methoden zur Nummernänderung, sodass der Administrator vollständige Kontrolle darüber hat, wie und wann eine Ziffer geändert werden kann. Dies ist jedoch nicht immer einfach, und einige Leute sind mit den verschiedenen Optionen überfordert, oder der Administrator weiß nicht, dass eine Option existiert.

Nummernmanipulation über POTS-DFÜ-Peers

POTS-DFÜ-Peers verfügen über einige einzigartige Ziffernmanipulationstechniken, die auf sie zutreffen, die VoIP-DFÜ-Peers nicht bieten.

Die erste ist das Entfernen von explizit definierten, linksbündig gerechtfertigten Ziffern in einem Zielmuster. Dies kann mithilfe des Befehls no digit-strip (Kein Ziffernstreifen) auf dem POTS-Dial-Peer deaktiviert werden.

Beispiel:

In diesem Beispiel wird 9011T als Zeichenfolge für das Zielmuster definiert.

Wenn diese Nummer eingerichtet ist, können Sie einen Anruf für die Nummer 90113227045555 erhalten. Dies entspricht dem Dial-Peer für die Weiterleitung ausgehender Anrufe, und die explizit definierten Ziffern 9011 werden entfernt, bevor der Anruf über den Sprach-Port weitergeleitet wird.

```
!
dial-peer voice 1 pots
 destination-pattern 9011T
 port 0/0/0:23
!
```

Dieses Beispiel zeigt eine Konfiguration ohne Ziffernleiste.

Wenn dieselbe Nummer gewählt wird, wird die Nummer 9011 gesendet.

```
!
dial-peer voice 1 pots
 destination-pattern 9011T
 port 0/0/0:23
 no digit-strip
!
```

Die zweite Möglichkeit besteht in der Angabe, wie viele Ziffern auf dem POTS-DFÜ-Peer weitergeleitet werden sollen.

Nehmen wir dieses Beispiel, in dem Sie einen Anruf für die Nummer 918005532447 vom CUCM erhalten. In dieser Situation möchten Sie die 9 entfernen, aber den Rest der Nummer beginnend mit der 1 senden.

Wenn Sie den Befehl forward-digits auf dem POTS-DFÜ-Peer konfigurieren, können Sie genau angeben, wie viele Ziffern Sie senden.

```
!
dial-peer voice 1 pots
 destination-pattern 918005532447
 forward-digits 11
 port 0/2/0
!
```

Schließlich können POTS-DFÜ-Peers den Präfix-Befehl verwenden, um einem Anruf Nummern hinzuzufügen, bevor sie den Sprach-Port weiterleiten. In diesem Beispiel wird die explizit definierte 91 entfernt und der Nummer 007 das Präfix 007 vorangestellt, bevor der Anruf über den Sprach-Port gesendet wird.

```
!
dial-peer voice 1 pots
 destination-pattern 91T
 prefix 007
 port 0/1/0:15
!
```

Nummernmanipulation über Sprachübersetzungsregeln und -profile

Sprachübersetzungsregeln sind reguläre Ausdrücke (reguläre Ausdrücke, reguläre Ausdrücke), die zum Umwandeln von Ziffern verwendet werden. In 12.0(7)XR1 wurden Übersetzungsregeln und Profile zu Cisco IOS hinzugefügt. Eine Übersetzungsregel wird auf Sprachübersetzungsprofile angewendet, die dann auf einen Dial-Peer oder Voice-Port angewendet werden. Übersetzungsregeln enthalten eine Übereinstimmungseingabe und eine Änderungsausgabe. Zusammen mit der Übereinstimmungseingabe für die Nummer gibt es eine Übereinstimmungs-

und Änderungseingabe für den ISDN-Plan und -Typ. Die Kombination aus einer Zeichenfolge, einem Plan und einem Typ für die Übereinstimmungsnummer wird als übereinstimmend angesehen. Dies bedeutet, dass alle definierten Übereinstimmungseingaben für die Übersetzung wahr sein müssen.

Übersetzungsregeln können in ISDN-, SIP- und H323-Signalisierungsprotokollen die Rufnummern Angerufener, Anrufer, Umgeleiteter, Umleitungsziel und Rückrufnummer ändern. Die Übersetzungsregeln werden anhand einer Top-Down-Suche zugeordnet, daher ist die Reihenfolge der Regeln von größter Bedeutung. Wenn eine Übereinstimmung in einer höheren Regel gefunden wird, beendet das Gateway sofort die Suche und verarbeitet die Übersetzung. Übersetzungsregeln können nicht numerische SIP-Header wie testuser@10.10.10.10 nicht ändern. Verwenden Sie für diese Manipulation ein SIP-Profil.

Mit Übergangsregeln können Anrufe auf Cisco Gateways blockiert werden.

Übersetzungsprofil-Auswahlpräferenz

1. Eingangs-Sprachübersetzungsprofil am Sprach-Port
2. Eingangs-Sprachübersetzungsprofil in der Trunk-Gruppe auf serielle Schnittstelle angewendet
3. Eingangs-Sprachübersetzungsprofil auf dem eingehenden Dial-Peer
4. Über Sprachservice-Ports definiertes eingehendes Sprachübersetzungsprofil
5. Übersetzungsprofil für eingehende Sprachnachrichten über globales "voip-incoming translation-profile" definiert
6. Über Sprachservice-Ports definiertes ausgehendes Sprachübersetzungsprofil
7. Outbound-Sprachübersetzungsprofil oder translate-outgoing auf dem Outbound-Dial-Peer
8. Übersetzungsprofil für ausgehende Sprache in der Trunk-Gruppe angewendet auf serielle Schnittstelle
9. Übersetzungsprofil für ausgehende Sprachnachrichten am Sprach-Port

Zusätzlich zu Dial-Peer-regulären und Platzhalter-Übersetzungsregeln haben ihre eigenen regulären Zeichen.

Zeichen	Definition
*	Bei Verwendung in Übersetzungsregeln ist dies ein regulärer Ausdruck für 0 oder mehr des vorherigen Zeichens. Um einem Literal zu entsprechen * verwenden Sie ein Escapezeichen: *
\	Wird häufig zum Escapen von Sätzen in Übersetzungsregel \(\) verwendet
u.	Das Ampersand-Zeichen wird verwendet, um alle Übereinstimmungen im ursprünglichen Übereinstimmungssatz für den Änderungssatz hervorzuheben.

( )	In Klammern eingeschlossene Elemente gelten als Gruppe.
^	Definiert den expliziten Start einer Zeichenfolge. Im Gegensatz zu DFÜ-Peers definieren Übersetzungsregeln nicht den Anfang der Zeichenfolge. Dies bedeutet, dass das Definieren einer Zeichenfolge ohne ^ an einer beliebigen Stelle der Eingabezeichenfolge möglich ist, was zu unerwünschten Übersetzungen in der Mitte einer Zahl führen kann.

Änderungssätze

- Sets werden als \0, \1, \2 usw. angegeben.
- \0 steht für alles, was zwischen der ersten Übereinstimmungsgruppe liegt. Dies kann auch durch einen kaufmännischen Charakter erreicht werden: &.
- \1 entspricht dem ersten Satz von ( ) in der Übereinstimmungsgruppe
- \2 stimmt mit dem zweiten Satz von ( ) in der Übereinstimmungsgruppe überein
- So weiter und so fort.

Beispiel für eine Übersetzungsregel mit zwei Sätzen

In diesem Beispiel können Sie die Zahl 000111000222 untersuchen.

Sie möchten die 0 aus der Zahl entfernen und eine endgültige Zahl von 111222 realisieren.

Dazu konfigurieren Sie den 1 und 2 so, dass die 111 bzw. 222 beim Verwerfen der 0 ergriffen werden.

```
!
voice translation-rule 333
 rule 1 /000\(111\)000\(222\)/ /\1\2/
!
voice translation-profile SET-EXAMPLE
 translate called 333
!

Gateway# test voice translation-rule 333 000111000222
Matched with rule 1
Original number: 000111000222   Translated number: 111222
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

Beispiel zum Entfernen des Hinauswahl-Musters "9" aus einer angerufenen Nummer

```
!
voice translation-rule 9
```

```
 rule 1 /^9\(.*\)/ /\1/
!
voice translation-profile STRIP-9
 translate called 9
!
dial-peer voice 9 voip
 translation-profile outgoing STRIP-9
!
voice-port 0/0/0
 translation-profile outgoing STRIP-9
!

Gateway# test voice translation-rule 9 918675309
Matched with rule 1
Original number: 918675309      Translated number: 18675309
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

Angerufene Nummer auf 4 Ziffern kürzen

```
!
voice translation-rule 4
 rule 1 /.*\(....\)/ /\1/
!
voice translation-profile STRIP-TO-4
 translate called 4
!

Gateway# test voice translation-rule 4 8675309
Matched with rule 1
Original number: 8675309        Translated number: 5309
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

Entfernen von Plus + aus der angerufenen Nummer

```
!
voice translation-rule 999
 rule 1 /\+\(.*\)/ /\1/
!
voice translation-profile STRIP-PLUS
 translate called 999
!
Gateway# test voice translation-rule 999 +8675309
Matched with rule 1
Original number: +8675309       Translated number: 8675309
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

Übersetzungsregeln können auch direkt auf einen Dial-Peer angewendet werden, ohne zuvor auf

ein Übersetzungsprofil angewendet zu werden.

```
!
voice translation-rule 1
 rule 1 /1234/ /8678309/
!
voice translation-rule 2
 rule 2 /^4...$/ /1408515\0/
!
dial-peer voice 1 voip
 translate-outgoing called 1
!
dial-peer voice 2 voip
 translate-outgoing calling 2
!
```

Übersetzungsprofil für Trunk-Gruppe

```
!
trunk group <name>
 translation-profile incoming <profile-name>
 translation-profile outgoing <profile-name>
!
```

Sprachübersetzungsregeln und -profile debuggen

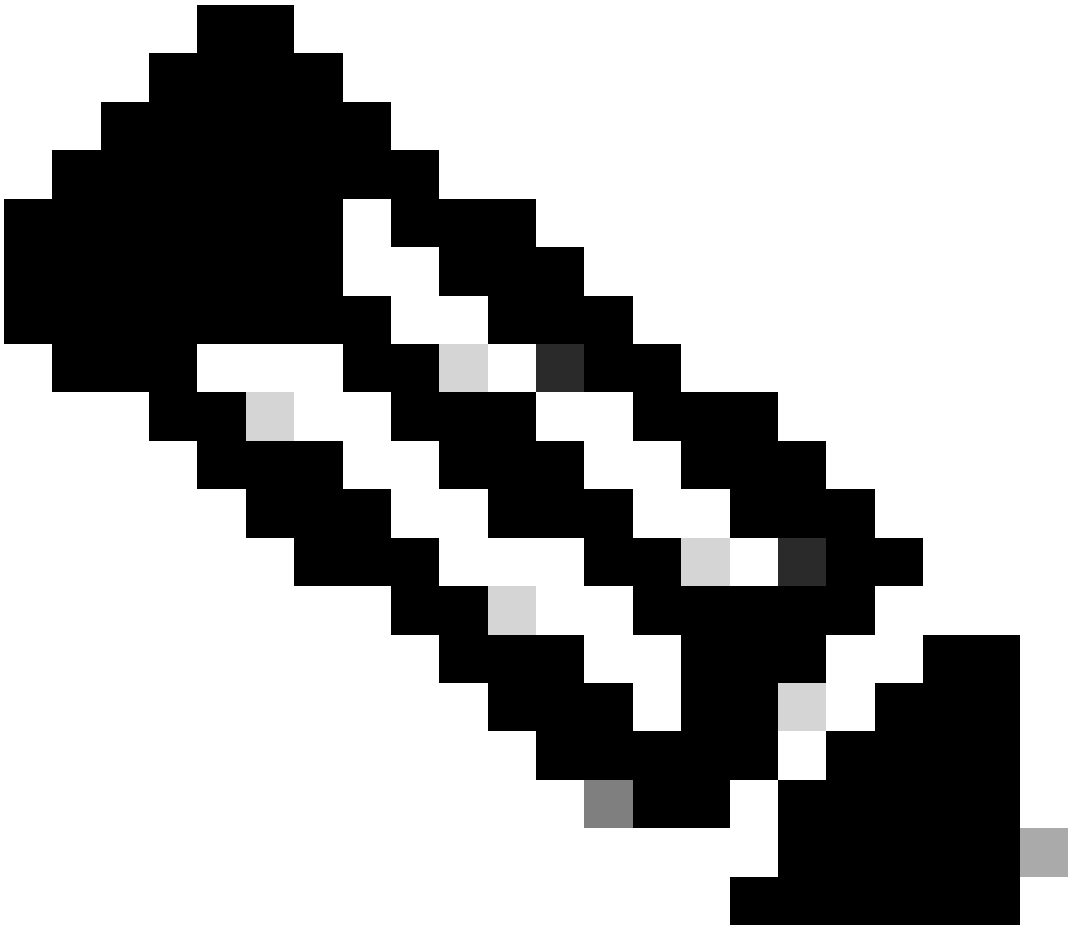
```
debug voip ccapi inout
debug voice translation
debug dialpeer
test voice translation-rule <number> <string> type <type> plan <plan>
```

Sprachklasse e164 - Übersetzung

Die Sprachklasse e164-translation-Funktion ist eine neuere Cisco IOS XE-Funktion, mit der ein Administrator eine Liste von Match-Anweisungen erstellen und Anweisungen ändern kann, die über eine Konfigurationsdatei aus dem Flash-Speicher oder einem Netzwerkverzeichnis geladen werden. Dies ähnelt dem Konzept für die in diesem Dokument beschriebene Funktion e164-pattern-map. Dadurch kann ein Administrator bis zu 100 Übersetzungen innerhalb einer Konfigurationsdatei konfigurieren und sie in einem einzigen Übersetzungsprofil anwenden. Weitere Informationen finden Sie in der Cisco IOS Voice Command Reference.

Befolgen Sie diese Syntax für die .cfg-Datei:

```
pattern1_to_be_matched<tab>replaced_pattern<space><enter>
pattern1_to_be_matched<tab>replaced_pattern<space><enter>
```



> Hinweis: Das nachfolgende Leerzeichen ist sehr wichtig, und der Import kann ohne diesen zusätzlichen Formatierungsschritt fehlschlagen.

Beispiel.cfg

```
+111111     8897
+222222     8312
928747     +123456789
737362     +987654321
```

Diese Datei referenziert dann als solche:

```
voice class e164-translation 164
 url ftp://username:password@10.10.10.10/sample.cfg
```

Jetzt wenden Sie sich ganz normal an ein Übersetzungsprofil und anschließend an DFÜ-Peers, die die normale Übersetzungsprofilsyntax verwenden.

```
voice translation-profile e164
 translate calling voice-class e164-translation 164
 translate called voice-class e164-translation 164
```

Der Befehl show voice class e164-translation e164-translation-number kann verwendet werden, um den Inhalt des Übersetzungsprofils anzuzeigen.

Ziffernmanipulation über ISDN-Karten

ISDN-MAPS sind eine ältere Technik zum Ändern von Ziffern. Dies wurde in Cisco IOS 12.0(6)T hinzugefügt, und die meisten neuen Konfigurationen nutzen diese Funktion nicht, da sie nicht so robust sind wie Sprachübersetzungsregeln und -profile. ISDN-Zuordnungen werden unter der seriellen Schnittstelle definiert.

Konfigurationsbeispiel

```
Serial0/0/0:23
 isdn map address ^911 plan isdn type unknown
 isdn map address ^1.......... plan isdn type national
 isdn map address ^2......... plan isdn type national
 isdn map address ^3......... plan isdn type national
 isdn map address ^4......... plan isdn type national
 isdn map address ^5......... plan isdn type national
 isdn map address ^6......... plan isdn type national
 isdn map address ^7......... plan isdn type national
 isdn map address ^8......... plan isdn type national
 isdn map address ^9......... plan isdn type national
```

Nummernmanipulation über Nummernerweiterung (num-exp)

Wie ISDN Maps ist auch die Nummernerweiterung eine ältere, in Cisco IOS 11.3(1)T hinzugefügte Technik, die in neuen Netzwerken nur wenig verwendet wird. Diese Funktion wurde hinzugefügt, bevor Sprachübersetzungsregeln und -profile existierten. Die Nummernerweiterung ist eine globale Änderung der Ziffern, die auf alle DFÜ-Peers auf einem Cisco Gateway angewendet werden. Die Änderung wird auf die angerufene Nummer angewendet, nachdem der Dial-Peer zugeordnet wurde und unmittelbar bevor der Anruf an den nächsten Anruf-Agenten gesendet wird.

Konfigurationsbeispiel

```
num-exp 4... 18005554...
num-exp 1234 8675309
```

Eingehende/ausgehende SIP-Profile

SIP-Profile sind robuste Match-Anweisungen für reguläre Ausdrücke (Regex), mit denen ein Administrator jeden Aspekt einer SIP-Nachricht ändern kann, die SDP- und SIP-Header enthält. Diese können global, pro Dial-Peer oder pro Tenant aktiviert werden. SIP-Profile sind für eingehende Änderungen verfügbar, beginnend mit Cisco IOS 15.4(2)T und Cisco IOS XE 3.12S. Da SIP-Profile so robust sind, werden in diesem Dokument nur einige konkrete Beispiele erläutert. SIP-Profile ermöglichen außerdem das Ändern oder Hinzufügen benutzerdefinierter SIP-Header in IOS 15.5(2)T und IOS-XE 3.13S.

Wichtige Informationen zu eingehenden und ausgehenden SIP-Profilen

- Eingehende SIP-Profile ändern die Nachricht, BEVOR das CUBE die Nachricht für die Anrufweiterleitung verarbeitet.
- Ausgehende SIP-Profile ändern die Nachricht, NACHDEM CUBE die Anrufweiterleitung verarbeitet hat und bevor die Nachricht an den nächsten Hop gesendet wird.

Weitere Hinweise zur SIP-Profilkonfiguration:

- SIP-Profile können m=image SDP-Attribute nicht bearbeiten. Die Erweiterung wurde unter der Cisco Bug-ID CSCsr20474 hinterlegt.
  Darüber hinaus können SIP-Profile SDP weder Werte entfernen noch Werte hinzufügen. Nur Sie können diese Werte ändern. Es ist jedoch möglich, einen SDP-Wert in einen NULL-

Wert zu ändern, indem Sie den gesamten Wert angeben und dann die Ausgabe auf einen Satz leerer Anführungszeichen ohne Leerzeichen setzen.

- Bei der Eingabe von Befehlen in das Sprachklassen-SIP-Profil werden keine Prüfungen durchgeführt, um festzustellen, ob der aktuelle eingegebene Befehl bereits vorhanden ist oder ob bereits eine Version dieses Befehls vorhanden ist. Wenn ein Administrator eine Zeile sieben Mal in ein SIP-Profil einfügt, wird sie in der aktuellen Konfiguration sieben Mal angezeigt. Es wird empfohlen, den zu ändernden Befehl zu entfernen und dann den neuen Befehl beim Bearbeiten von SIP-Profilen einzugeben, um zu vermeiden, dass mehrere Befehle vorhanden sind.

Vollständige Dokumentation: Konfigurationsleitfaden für Cisco Unified Border Element - ab Cisco IOS XE 17.6

SIP Profile Testing Tool: SIP Profile Test Tool

Beispielsyntax für ein- und ausgehende SIP-Profile

```
!
voice class sip-profiles <number>
 request <message-type> sip-header <header> modify "match-pattern" "replace-pattern"
 request <message-type> sip-header <header> add "add-pattern"
 request <message-type> sip-header <header> remove

 request <message-type> sdp-header <header> modify "match-pattern" "replace-pattern"
 request <message-type> sdp-header <header> add "add-pattern"
 request <message-type> sdp-header <header> remove

 response <number> sip-header <header> modify "match-pattern" "replace-pattern"
 response <number> sip-header <header> add "add-pattern"
 response <number> sip-header <header> remove

 response <number> sdp-header <header> modify "match-pattern" "replace-pattern"
 response <number> sdp-header <header> add "add-pattern"
 response <number> sdp-header <header> remove
!
```

Eingehendes/ausgehendes SIP-Profilbeispiel mit Zahlen

```
voice class sip-profiles 200
 rule 1 response ANY sip-header Remote-Party-ID modify "match-pattern" "replace-pattern"
 rule 2 response ANY sdp-header Audio-Attribute modify "match-pattern" "replace-pattern"
```

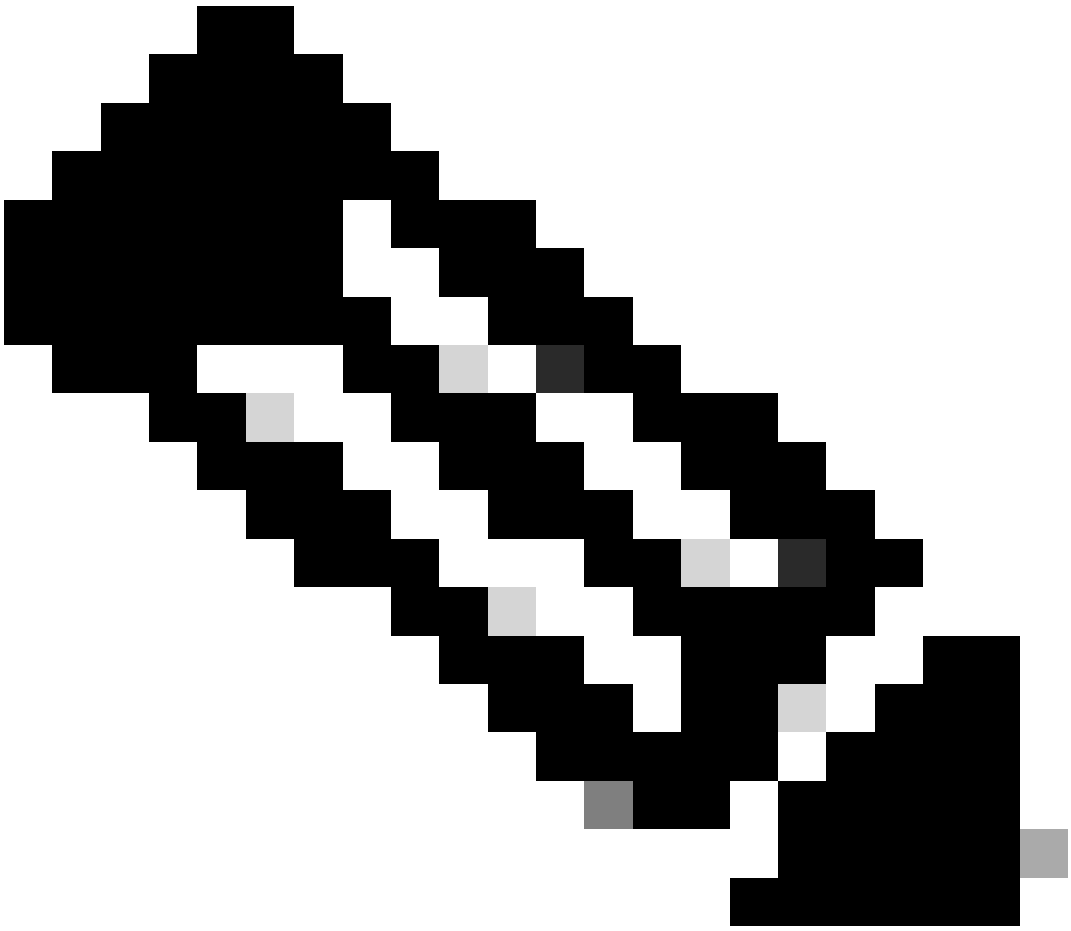
Ausgehende SIP-Profil-Anwendungsmethoden

<#root>

```
! Global Application
```

```
voice service voip
 sip
  sip-profiles <number>
!

! Tenant Application


voice class tenant <tag>
 sip-profiles <tag>
!

! Dial-peer Application


dial-peer voice <tag> voip
 voice-class sip profiles <number>
!
```

Eingehende SIP-Profil-Anwendungsmethoden



Hinweis: Es ist erforderlich, eingehende SIP-Profile im Rahmen des Voice-Service-VoIP-

SIP zu aktivieren, unabhängig davon, ob die globale Anwendung, der Tenant oder die Dial-Peer-Anwendung verwendet wird.

<#root>

```
! Global Application

voice service voip
 sip
  sip-profiles inbound
  sip-profiles <number> inbound
!
```

<#root>

```
! Tenant Application


voice service voip
 sip
  sip-profiles inbound
!
voice class tenant <tag>
 sip-profiles <tag> inbound
!
```

<#root>

```
! Dial-Peer Application


voice service voip
 sip
  sip-profiles inbound
!
dial-peer voice <tag> voip
 voice-class sip profiles <number> inbound
!
```

SIP-Beispielprofil zum Ändern von OPTIONS Keepalive-Nachrichten.

```
!
voice class sip-options-keepalive 200
 transport tcp tls
 sip-profiles 299
!
```

SIP-Beispielprofil zum Ändern des Hosts, der Domäne oder beider Teile eines URIs.

<#root>

```
! Host

!
voice class sip-profiles 1
 request ANY sip-header Contact modify "sip:(.*)@" "sip:8675309@"
!

! Domain

!
voice class sip-profiles 2
 request ANY sip-header Contact modify "10.67.138.241:5060" "cisco.com"
!

! Note: Port is optional

!

! Modify Both User and Host

!
voice class sip-profiles 3
 request ANY sip-header Contact modify "sip:(.*)>" "sip:8675309@cisco.com>"
!
```

SIP-Beispielprofil zum Hinzufügen, Ändern oder Entfernen von Diversion-Headern.

<#root>

```
! Add

!
voice class sip-profiles 777
 request INVITE sip-header Diversion add "Diversion: <sip:1234@cisco.com>"
!
!

! Modify

!
voice class sip-profiles 888
 request INVITE sip-header Diversion modify "sip:(.*)>" "sip:1234@cisco.com>"
!
!

! Remove

!
voice class sip-profiles 999
 request INVITE sip-header Diversion remove
!
```

SIP-Beispielprofil zum Ändern des Namensbereichs der Anrufer-ID in SIP-Headern.

```
!
voice class sip-profiles 123
 request INVITE sip-header From modify "\".*\"" "\"TEST CLID*\""
!
```

Beispiel für ein SIP-Profil zum Ändern des Werts von "183 Sitzung in Bearbeitung" in "180 Ringing".

```
!
voice class sip-profiles 789
 response 183 sip-header SIP-StatusLine modify "SIP/2.0 183 Session in Progress" "SIP/2.0 180 Ringing"
!
```

SIP-Beispielprofil für unidirektionale oder unidirektionale Audiointeroperabilität mit einem Anbieter

<#root>

```
!
voice class sip-profiles 200
 request ANY sdp-header Audio-Attribute modify "a=inactive" "a=sendrecv"
 request ANY sdp-header Audio-Connection-Info modify "0.0.0.0" "10.10.10.10"
!

! where 10.10.10.10 is CUBE's provider facing IP address
```

SIP-Beispielprofil zum Entfernen der UPDATE-Methode bei Interoperabilitätsproblemen.

```
!
voice class sip-profiles 200
 request ANY sip-header Allow-Header modify ", UPDATE" ""
!
```

SIP-Beispielprofil mit SET-Verwendung im SIP-Profil. Dies ist das gleiche Konzept von Sets, das im Abschnitt für Sprachübersetzungsregeln beschrieben wird.

```
!
voice class sip-profiles 1
 request ANY sip-header Contact modify "sip:(.*)@" "sip:\1@"
!
```

Konfiguration der IF-Logik und von Zeilenumbrüchen mit einem SIP-Profil.

In SIP-Profilen werden Zeilenumbrüche unterstützt, es gibt jedoch nur einen sehr spezifischen Anwendungsfall dafür. Da SIP-Profile keine "If, Then, Else"-Logik haben, besteht jetzt die Möglichkeit, Änderungen an einem Header auf der Grundlage einer Eingabe von einem anderen Header durchzuführen. Beispielsweise möchte ein Administrator einen Diversion-Header nur ändern, wenn der FROM-Header 1234@cisco.com enthält. Mit dem Zeilenumbruch kann die IF-Anweisung innerhalb eines SIP-Profils gefälscht werden. Siehe Beispielkonfiguration: Sie gleichen 1234 in einer beliebigen Domäne im Von-Header ab. Dann bringen Sie den ersten Satz und fügen Sie einen neuen Zeilenumbruch \x0D\x0AD. Schließlich fügen Sie den gewünschten Header hinzu. Beachten Sie, dass Sie mit dieser Methode nur einen Header HINZUFÜGEN können. Es ist nicht möglich, einen anderen Header zu ändern. Dies erfüllt also nur teilweise die Anforderungen, die ein Administrator zuvor erfüllen wollte.

```
!
voice class sip-profiles 1
 request INVITE sip-header From modify “(.*sip:1234@.*)” “\1\x0D\x0ADiversion: <sip:5678@example.com>”
!
```

Beispiel eines SIP-Profils mit ODER-Logik.

```
!
voice class sip-profiles 123
 request ANY sdp-header Audio-Attribute modify "(a=sendonly|a=recvonly|a=inactive)" "a=sendrecv"
 response ANY sdp-header Audio-Attribute modify "(a=sendonly|a=recvonly|a=inactive)" "a=sendrecv"
!
```

Beispiel für Layer-7-SIP-Inspektion über SIP-Profil.

<#root>

```
### Usage

10.21.15.10 replace with private IP of CUBE
a.b.c.d replace with public IP
-----------------------------------------------------


### Inbound from ITSP Layer 7 Fixup

!
voice class sip-profiles 888
 request INVITE sip-header SIP-Req-URI modify "@.*;" "@10.21.15.100;"
!
voice service voip
 sip
```

```
  sip-profiles inbound
!
```

Outbound Layer 7 Fixup

```
!
voice class sip-profiles 777
 request ANY sip-header Contact modify "<sip:(.*)@10.21.15.100:5060>" "<sip:\1 a.b.c.d:5060>"
 response ANY sip-header Contact modify "<sip:(.*)@10.21.15.100:5060>" "<sip:\1 a.b.c.d:5060>"
 request ANY sip-header Via modify "SIP(.*) 10.21.15.100(.*)" "SIP\1 a.b.c.d\2"
 request ANY sdp-header Session-Owner modify "(.*IP4 ).*" "\1a.b.c.d"
 request ANY sdp-header Connection-Info modify "IN IP4 10.21.15.100" "IN IP4 a.b.c.d"
 request ANY sdp-header Audio-Connection-Info modify "IN IP4 10.21.15.100" "IN IP4 a.b.c.d"
 response ANY sdp-header Session-Owner modify "(.*IP4 ).*" "\1a.b.c.d"
 response ANY sdp-header Audio-Connection-Info modify "IN IP4 10.21.15.100" "IN IP4 a.b.c.d"
 response ANY sdp-header Connection-Info modify "IN IP4 10.21.15.100" "IN IP4 a.b.c.d"
 request ANY sip-header Remote-Party-ID modify "<sip:(.*)@10.21.15.100>" "<sip:\1 a.b.c.d>"
 response ANY sip-header Remote-Party-ID modify "<sip:(.*)@10.21.15.100>" "<sip:\1 a.b.c.d>"
!
```

Apply to dial-peers for the side of the CUBE facing the ITSP

```
!
dial-peer voice 1 voip
 voice-class sip profiles 777
 voice-class sip profile 888 inbound
!
dial-peer voice 2 voip
 voice-class sip profiles 777
 voice-class sip profile 888 inbound
!
```

SIP-Copylist

SIP-Copylists sind eine Erweiterung von SIP-Profilen, mit der das Gateway einen Header aus dem eingehenden Anruf KOPIEREN und dann PASTE an einen anderen Punkt in der ausgehenden SIP-Nachricht am ausgehenden Anruf übernehmen kann. Die Unterstützung von SIP Copylist wurde in Cisco IOS 15.1(3)T und Cisco IOS XE 3.6S hinzugefügt. Dies ist eine sehr effektive Methode, um dynamische Header zu erstellen, die auf anderen Headern basieren, nachdem der Anruf getätigt wurde.

Der häufigste Anwendungsfall ist das dynamische Kopieren eines FROM-Headers in einen anderen Header, z. B. diversion oder p-asserted-id, sodass der Wert des Benutzerteils der Wert von user ist. Dies geschieht hauptsächlich zur Authentifizierung und für die Anrufer-ID.

Vollständige Dokumentation: Konfigurationsleitfaden für Cisco Unified Border Element - ab Cisco IOS XE 17.6

SIP-Copylist - Beispiel

<#root>

```
!
! Create Copylist to copy the FROM header on the inbound message specified later.

!
voice class sip-copylist <number>
 sip-header From
!
! Apply this to the inbound dial-peer of the call.

!
dial-peer voice <tag> voip
 voice-class sip copy-list <number>
!
! Create SIP Profile to take From (peer-header) stored as variable "u01" and apply to a header of choice
! This example modifies the user portion of the Contact by copying the user portion of the From header t

!
voice class sip-profiles <number>
 request INVITE peer-header sip From copy "<sip:(.*)@" u01
 request INVITE sip-header Contact modify "<sip:(.*)>" "<sip:\u01@10.50.244.2>"
!
! Apply the SIP profile to an outbound dial-peer

!
dial-peer voice <tag> voip
 voice-class sip profiles <number>
!
```

Debuggen von SIP-Profilen und Copylist

```
debug voip ccapi inout
debug ccsip mess
debug ccsip info
debug ccsip feature sip-profile
```

Debug-Ausgabe aus der Beispielkopieliste für SIP

```
### Ingress from CUCM
Received:
INVITE sip:1001@10.50.228.61:5060 SIP/2.0
Via: SIP/2.0/TCP 10.50.244.3:5060;branch=z9hG4bKaad21bc3ae7e
From: "5001" <sip:5001@10.50.244.3>;tag=100442~cdffff43-5020-4e79-a10b-99d406971010-36470319
Contact: <sip:5001@10.50.244.3:5060;transport=tcp>

### Copylist Details
000440: Mar  8 18:59:49.796: //-1/xxxxxxxxxxxx/SIP/Info/info/64/sip_profiles_application_peer_copy_patte
000441: Mar  8 18:59:49.797: //187/D6138E000000/SIP/Info/info/64/sip_profiles_application_peer_copy_pat
000442: Mar  8 18:59:49.797: //-1/xxxxxxxxxxxx/SIP/Info/info/64/sip_profiles_prefix_slash_in_copy_var_v
000443: Mar  8 18:59:49.797: //187/D6138E000000/SIP/Info/info/64/sip_profiles_application_peer_copy_pat
000444: Mar  8 18:59:49.797: //-1/xxxxxxxxxxxx/SIP/Info/info/64/sip_profiles_application_modify_remove_
000445: Mar  8 18:59:49.797: //187/D6138E000000/SIP/Info/info/64/sip_profiles_check_and_get_variables_i
```

```
000446: Mar  8 18:59:49.797: //187/D6138E000000/SIP/Info/info/64/sip_profiles_check_and_get_variables_i
000448: Mar  8 18:59:49.797: //187/D6138E000000/SIP/Info/info/64/sip_profiles_check_and_get_variables_i
000449: Mar  8 18:59:49.797: //-1/xxxxxxxxxxxx/SIP/Info/info/64/sip_profiles_app_modify_header: Passing
000450: Mar  8 18:59:49.798: //-1/xxxxxxxxxxxx/SIP/Info/info/64/sip_profiles_application_modify_remove_
000451: Mar  8 18:59:49.798: //187/D6138E000000/SIP/Msg/ccsipDisplayMsg:

### Egress from CUBE
Sent:
INVITE sip:1001@14.50.228.63:5060 SIP/2.0
Via: SIP/2.0/UDP 10.50.228.61:5060;branch=z9hG4bK3C7CD
Remote-Party-ID: "5001" <sip:5001@10.50.228.61>;party=calling;screen=yes;privacy=off
From: "5001" <sip:5001@10.50.228.61>;tag=34C458-D6
Contact: <sip:5001@168.117.64.94>
```

Besondere Hinweise

Protokollsignalisierung und Medienbindung

Alle Signalisierungsprotokolle ermöglichen es Administratoren, die Signalisierung an eine bestimmte Schnittstelle zu binden. Standardmäßig bezieht ein Gateway ohne statische definierte Bindung die Signalisierung für einen Anruf von der physischen Schnittstelle, über die das Paket übertragen wird. Mit der Bindung an einen Dial-Peer umfasst das Paket Quell-Header, Messaging und Pakete von der angegebenen Schnittstelle, aber das eigentliche Paket wird weiterhin über die physische Schnittstelle geroutet. Die DFÜ-Peer-Bindung ersetzt immer die Sprachklassen-Tenant- und globale Sprachservice-VoIP-Bindung mit Session Initiation Protocol (SIP).

Häufig binden Administratoren die Signalisierung an ein Loopback. Da es sich um eine logische Schnittstelle handelt, werden keine Pakete über diese Schnittstelle übertragen. Um eine Paketerfassung durchzuführen, muss diese an einer physischen Schnittstelle erfolgen. Der Befehl show ip cef <remote-ip> zeigt die physische Schnittstelle an, die ein Paket für die Weiterleitung an die Ziel-/Remote-IP-Adresse verwendet, selbst wenn die Konfiguration an eine virtuelle Schnittstelle gebunden ist.

Die Medien- und Signalisierungsbindung muss nicht immer dieselbe IP-Adresse sein. Wenn ein Administrator für die Signalisierung an/von einem CUCM eine Bindung an eine bestimmte Schnittstelle herstellen muss, die Audio-/Medienverbindung zwischen dem Telefon und dem Gateway jedoch möglicherweise an eine andere Schnittstelle gebunden werden muss.

Konfigurationsbeispiel

Dieses Beispiel zeigt einen Dial-Peer, der an Loopback 1 gebunden ist und einen Anruf vom CUCM empfängt.

Obwohl die Medien und die Signalisierung (Steuerung) an Loopback 1 gebunden sind, zeigt der Befehl show ip cef an, dass alle an CUCM gesendeten Pakete an der physischen Schnittstelle GigabitEthernet0/0/1 verbleiben.

```
!
dial-peer voice 2 voip
 description "Incoming call from CUCM"
 session protocol sipv2
 incoming called-number .
 voice-class sip bind control source-interface Loopback1
 voice-class sip bind media source-interface Loopback1
!
```

Reihenfolge der Vorgänge für die Layer-7-Anwendungsbindung

1. Gemäß der bind-Anweisung auf dem übereinstimmenden eingehenden/ausgehenden Dial-Peer.
2. Gemäß den Bindungen unter dem Sprachklassen-Tenant, der dem entsprechenden eingehenden/ausgehenden Dial-Peer zugewiesen ist.
3. Gemäß globaler Bindungserklärung.
4. Gemäß der physischen Layer-3-Schnittstelle wird das Paket gemäß der Routing-Tabelle voraussichtlich beendet.

SIP-Bindungsbefehle

<#root>

```
! Per Dial-peer


!
dial-peer voice 1 voip
 voice-class sip bind control source-interface <interface>
 voice-class sip bind media source-interface <interface>
!
```

```
! Global Binding


!
voice service voip
 sip
   bind control source-interface <interface>
   bind media source-interface <interface>
!
```

MGCP-Bindungsbefehle

```
!
mgcp bind control source-interface <interface>
mgcp bind media source-interface <interface>
!
```

SCCP-Bindungsbefehle

```
!
sccp local <interface>
!
sccp ccm group <number>
 bind interface <interface>
!
```

H323-Bindungsbefehle

<#root>

```
!
inteface <interface>
 !
 ! Media Bind Command:
 h323-gateway voip interface
 !
 ! Signaling Bind Command:
 h323-gateway voip bind srcaddr <a.b.c.d>
!
```

DNS- und VoIP-DFÜ-Peers

DNS mit VoIP wird wie jede andere DNS-Lösung eingesetzt. Eine gängige Konfiguration ist die Verwendung von Session Target dns:FQDN.com.

Ein Cisco Gateway führt eine DNS-Auflösung aus, selbst wenn auf dem Gateway keine globale IP-Domänensuche konfiguriert wurde. Das bedeutet, dass die VoIP-DFÜ-Peers den DNS-Eintrag zwar deaktivieren, aber trotzdem auflösen. In letzter Zeit gab es jedoch einige Änderungen an der DNS-Funktionalität innerhalb der Cisco IOS XE-Plattformen.

Nach dieser Änderung gehorchen DFÜ-Peers, die mit dem Sitzungsziel dns:FQDN.com konfiguriert wurden, nun der Tatsache, dass DNS deaktiviert ist und keine IP-Domänensuche stattfindet.
Ich empfehle, stets sicherzustellen, dass der Befehl "ip domain lookup" bei der Verwendung von DNS konfiguriert ist, um dieses Problem zu vermeiden.

Bei ausgehenden SIP-Verbindungen führt CUBE diese Reihenfolge für die DNS-Auflösung aus.

1. SRV-Abfragesuche
2. Suche nach Datensätzen

3. Suche nach AAAA-Datensätzen

Informationen zur Erstellung der SRV oder zum Überspringen der SRV und zum Durchführen einer A-Datensatzabfrage für ein Sitzungsziel finden Sie in der vollständigen Dokumentation: Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 Onwards.

Bei eingehenden SIP-Verbindungen, bei denen ein IOS-Gateway einen Header auflösen muss, um auf eine Nachricht zu reagieren, kann das Gateway diese Reihenfolge für die DNS-Auflösung verwenden.

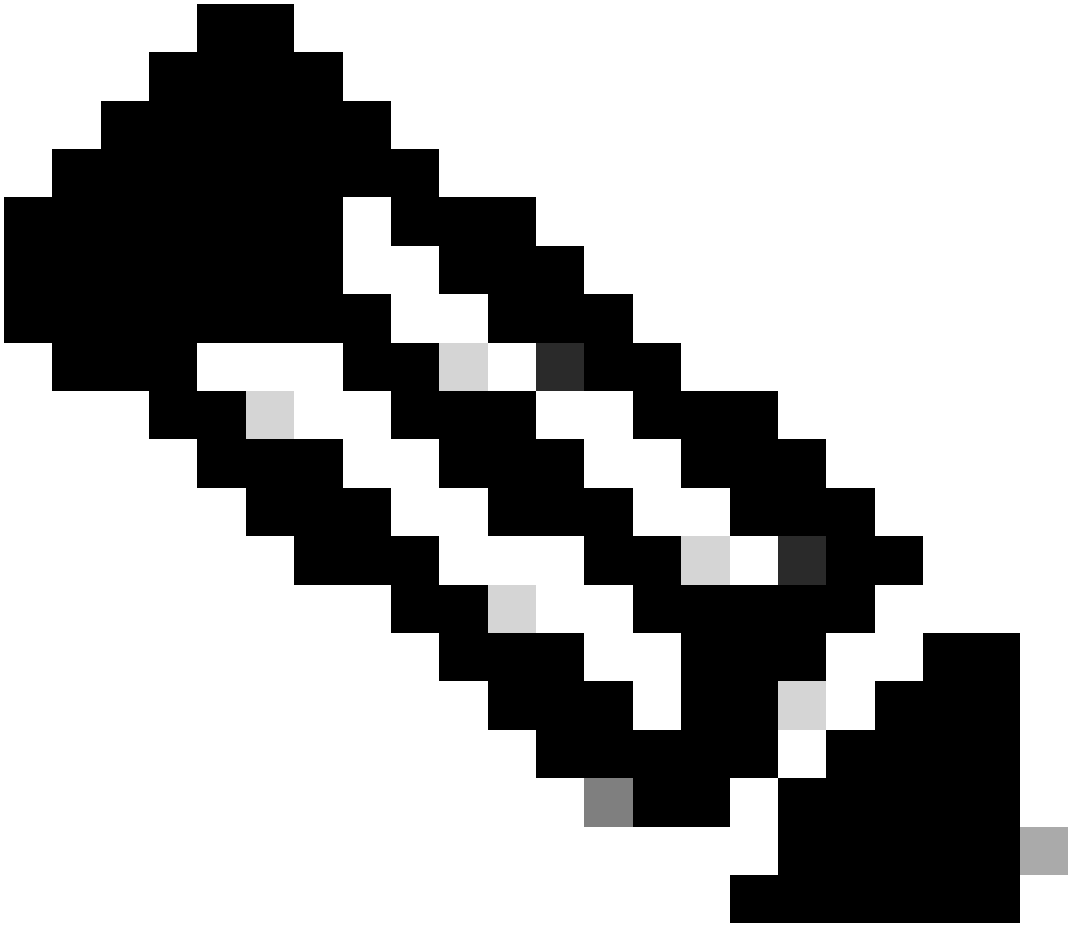
1. Suche nach Datensätzen
2. Suche nach AAAA-Datensätzen

In Cisco IOS XE 17.9.1 kann CUBE die Erreichbarkeit von DNS-Sitzungszielen mithilfe von Keepalive-Mechanismen überprüfen. Vollständige Dokumentation:

Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 und höher

IOS DNS-Konfigurationsbeispiele

```
ip host _sip._udp.cucmgroup.lab.local srv 1 50 5060 cucm1.lab.local
ip host _sip._udp.cucmgroup.lab.local srv 1 50 5060 cucm2.lab.local
ip host _sip._udp.cucmgroup.lab.local srv 1 50 5060 cucm3.lab.local

ip host cucm1.lab.local 10.0.0.1
ip host cucm2.lab.local 10.0.0.2
ip host cucm3.lab.local 10.0.0.3

ip domain name lab.local
ip name-server 8.8.8.8
```



Hinweis: Die Unterstützung von DNS SRV auf Cisco IOS XE wird unter 15.6(1)S/3.17.00.S und höher unterstützt.

DNS-Debugger und Verifizierungsbefehle

<#root>

```
show host
clear host all *
!
debug ip dns view
debug ip domain
debug ccsip info
debug ccsip error
```

DNS-Tests 3.15S und höher

<#root>

Domain Name Verification

```
Gateway# sh run | s lookup
no ip domain lookup
```

Checking the host table for no entry

```
Gateway# show host
Name lookup view: Global
Default domain is cisco.com
Name/address lookup uses static mappings

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                      Port  Flags      Age Type   Address(es)
```

Verification of no PING on a FQDN

```
Gateway# ping cucm.cisco.com
Translating "cucm.cisco.com"
% Unrecognized host or address, or protocol not running.
```

Made a test call here

Checking logs to see if it worked

```
Gateway# sh log | s INVITE sip:
INVITE sip:9001@14.50.228.70:5060 SIP/2.0
INVITE sip:5001@cucm.cisco.com:5060 SIP/2.0
```

Host Table now has an entry

```
Gateway# sh host
Name lookup view: Global
Default domain is cisco.com
Name/address lookup uses static mappings

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                      Port  Flags      Age Type   Address(es)
cucm.cisco.com            None  (temp, OK)  0   IP    10.50.244.2
```

CCSIP All output showing a proper DNS Query for the FQDN on the dial-peer.

```
001338: Mar  9 15:29:07.437: //-1/xxxxxxxxxxxx/SIP/Info/info/1024/httpish_msg_free: Freed msg=0x7FE9873
001339: Mar  9 15:29:07.437: //-1/xxxxxxxxxxxx/SIP/Info/notify/8192/sip_dns_type_srv_query: TYPE SRV qu
001340: Mar  9 15:29:07.438: //-1/xxxxxxxxxxxx/SIP/Info/info/8192/sip_dns_type_a_aaaa_query: DNS query
001341: Mar  9 15:29:07.441: //-1/xxxxxxxxxxxx/SIP/Info/notify/8192/sip_dns_type_a_query: TYPE A query
001342: Mar  9 15:29:07.441: //-1/xxxxxxxxxxxx/SIP/Info/info/8192/sip_dns_type_a_query: ttl for A recor
001343: Mar  9 15:29:07.441: //-1/xxxxxxxxxxxx/SIP/Info/info/8192/sip_dns_type_a_aaaa_query: IP Address
001344: Mar  9 15:29:07.441: //-1/xxxxxxxxxxxx/SIP/Info/info/8192/sip_dns_type_a_aaaa_query: 10.50.244.
```

DNS-Tests 3.16S und höher.

<#root>

```
### Checking the command is present

Gateway# sh run | s lookup
no ip domain lookup


### Verifying the gateway cannot ping a FQDN

Gateway# ping cucm.cisco.com
% Unrecognized host or address, or protocol not running.


### Checking the Host Table for entries

Gateway# sh host
Default domain is cisco.com
Name servers are 10.50.244.52
NAME  TTL  CLASS   TYPE      DATA/ADDRESS
-----------------------------------------


### Made a test call here

### CCSIP All Outbound showing the failed call

000974: *Mar  9 15:53:01.222: //-1/xxxxxxxxxxxx/SIP/Info/info/1024/httpish_msg_free: Freed msg=0x7FF31D
000975: *Mar  9 15:53:01.222: //-1/xxxxxxxxxxxx/SIP/Info/notify/8192/sip_dns_type_srv_query: TYPE SRV q
000976: *Mar  9 15:53:01.224: //-1/xxxxxxxxxxxx/SIP/Info/info/8192/sip_dns_type_a_aaaa_query: DNS query
000977: *Mar  9 15:53:01.225: //-1/xxxxxxxxxxxx/SIP/Error/sip_dns_type_a_query:
 TYPE A query failed for cucm.cisco.com
000978: *Mar  9 15:53:01.225: //-1/xxxxxxxxxxxx/SIP/Error/_send_dns_fail:
 DNS Query for cucm.cisco.com failed
000984: *Mar  9 20:53:01.225: %VOICE_IEC-3-GW: SIP: Internal Error (DNS query fail): IEC=10.1.128.7.47.
```

Maximale Verbindungen und Bandbreite

Standardmäßig ermöglichen VoIP- und POTS-Dial-Peers unbegrenzte Verbindungen (Anrufe) und Bandbreite (nur VoIP-Dial-Peers). Für Trunks mit einer Beschränkung für die Anzahl von Anrufen oder die nutzbare Bandbreite kann es hilfreich sein, die Befehle max-conn oder max-bandwidth zu verwenden.max-conn wurde in Cisco IOS 11.3(1)T hinzugefügt und ist in allen Cisco IOS XE-Versionen vorhanden, während max-bandwidth in 15.2(2)T hinzugefügt wurde und IOS-XE 3.7S:

Konfigurationsbeispiel:

Hier weisen Sie das Gateway an, mithilfe von "max-conn 30" den DFÜ-Peer auf 1 bis 30 Anrufe zu begrenzen.
Dial-Peer 2 schränkt die Bandbreite für diesen Dial-Peer ein, sodass der zugewiesene Grenzwert nicht überschritten wird.

```
!
```

```
dial-peer voice 1 voip
 description ITSP SIP Trunk - 30 Max Calls!
 session protocol sipv2
 sess target ipv4:10.10.10.10
 destination-pattern 8675309$
 max-conn 30
!
dial-peer voice 2 voip
 description SIP Trunk with Bandwidth Restrictions!
 session protocol sipv2
 sess target ipv4:10.10.10.10
 destination-pattern 123456789$
 max-bandwidth 400
!
```

Beispielfehler beim Überschreiten des Grenzwerts für die maximale Verbindung.

```
000308: Oct  5 19:01:02.603: %CALL_CONTROL-6-MAX_CONNECTIONS: Maximum number of connections reached for

000309: Oct  5 19:01:02.603: %VOICE_IEC-3-GW: CCAPI: Internal Error (Dial-peer connections exceeded): I
000310: Oct  5 19:01:02.604: %SIP-3-MAXCONNCAC: Call rejected due to CAC based on maximum number of con

000311: Oct  5 19:01:02.604: //17084/86B070800000/SIP/Msg/ccsipDisplayMsg:
Sent:
SIP/2.0 503 Service Unavailable
Via: SIP/2.0/TCP 10.50.244.62:5060;branch=z9hG4bKb78c35aa21b0
From: <sip:9001@10.50.244.62>;tag=72531~2e8ca155-3f0b-4f07-a1b2-b14ef77ceb7f-26250846
To: <sip:1234@10.50.245.70>;tag=3E19564D-1684
Date: Thu, 05 Oct 2017 19:01:02 GMT
Call-ID: 86b07080-9d61816e-b762-3ef4320e@10.50.244.62
CSeq: 101 INVITE
Allow-Events: telephone-event
Warning: 399 10.50.245.70 "Maximum Number of Connections reached for dial-peer 1"
Server: Cisco-SIPGateway/IOS-15.4.3.S4
Content-Length: 0
```

Durchwahl (Direct Inward Dial, DID)

Stufenwahl

Wenn Direct Inward Dial (Eingehende Direktwahl) auf POTS-DFÜ-Peers aktiviert ist, kann die eingehende Nachricht alle zum Weiterleiten des Anrufs erforderlichen Ziffern enthalten. Das Cisco Gateway kann keine weiteren Ziffern erfassen. Wenn der Router oder das Gateway nach einem ausgehenden Dial-Peer sucht, verwendet das Gerät die gesamte Zeichenfolge für eingehende Anrufe. Diese Übereinstimmung ist standardmäßig variabel. Diese Übereinstimmung wird nicht für jede Ziffer einzeln durchgeführt, da laut DID-Definition alle Ziffern empfangen wurden. Dies ist die Standardkonfiguration für POTS-DFÜ-Peers.

Vollständige Dokumentation: DID (Direct-Inward-Dial) an IOS-Sprachschnittstellen (T1/E1)

Konfigurationsbeispiel

```
!
dial-peer voice 1 pots
 incoming called-number 8675309
 voice-port 0/0/0
 direct-inward-dial
!
```

Zweistufiges Wählen

Wenn der eingehende POTS-Dial-Peer ohne Direktwahl nach innen konfiguriert ist, wechselt der Router oder das Gateway in den Ziffernsammelmodus (Ziffernsammlung in Band). Das Dial-Peer-Matching für ausgehende Anrufe erfolgt auf einer Ziffernbasis. Der Router oder das Gateway sucht nach Dial-Peer-Übereinstimmungen, nachdem das Gerät jede Ziffer empfangen hat, und leitet den Anruf dann weiter, wenn eine vollständige Übereinstimmung erfolgt ist.

Konfigurationsbeispiel

```
!
dial-peer voice 1 pots
 incoming called-number 8675309
 voice-port 0/0/0
 no direct-inward-dial
!
```

Anrufe blockieren

Jedes Protokoll behandelt die Anrufblockierung etwas anders. Die meisten Protokolle können das Ablehnungsmuster der Übersetzungsregel verwenden, das auf einer Ziffernfolge basierende Blöcke enthält. Wenn ein Administrator weiterhin ein eingehendes Übersetzungsprofil für die normale Nummernänderung verwenden möchte, jedoch keine darin enthaltenen Nummern blockieren möchte, besteht die Möglichkeit, mithilfe des Befehls call-block translation-profile eine Anrufblockierung zu implementieren.

```
!
voice translation-rule 164
 rule 1 reject /8675309/
!
voice translation-profile CALLBLOCK
 translate calling 164
!
```

```
dial-peer voice 1 pots
 desc INCOMING VOICE-PORT with BLOCK
 translation-profile incoming ANOTHER
 call-block translation-profile incoming CALLBLOCK
 call-block disconnect-cause incoming invalid-number
 incoming called-number .
 port 0/0/0:23
!

Gateway#test voice translation-rule 164 8675309
8675309 blocked on rule 1
```

Innerhalb von E1 R2 kann ein Administrator Collect Calls blockieren. Dies wird hauptsächlich in Bereitstellungen in Brasilien verwendet, kann jedoch über jede benutzerdefinierte Gruppe konfiguriert werden.

Die beiden Optionen sind:

1. Blockieren Sie den eingehenden Collect-Anruf auf Basis der Kategorie II-8, die vom Telco-Switch empfangen wird. Dies ist der Standardmechanismus, der von allen Cisco Gateways ohne Konfiguration ausgeführt wird. Für diese Blockierungsmethode ist ein neuerer Telco-Switch erforderlich, der eine kategoriebasierte Markierung unterstützt. Um diese Methode zu deaktivieren, verwenden Sie den Befehl collect-call-enable in der case-customer-Gruppe.
2. Verwenden Sie die Funktion doppelte Antwort für eine benutzerdefinierte r2-digitale E1 R2-Gruppe. Bei der Konfiguration mit doppelter Antwort wird die kategoriebasierte Blockierung deaktiviert und durch die Funktion mit doppelter Antwort ersetzt. Hierzu muss zunächst der eingehende Anruf beantwortet und ein 1-Sekunden-Timer gestartet werden. Nach 1 Sekunde sendet das Gateway eine Freigabe in Form des CLEAR BWD-Befehls. Die Telekommunikation kann dann eine CLEAR-FWD an das Gateway senden, und der Anruf kann beendet werden. Ein Timer startet, nachdem das Gateway CLEAR BWD gesendet hat. Wenn dieser Timer abläuft, sendet das Gateway ein weiteres ANSWER-Signal. Dabei wird davon ausgegangen, dass es sich bei dem Anruf nicht um einen Collect-Anruf handelt, und der Anruf wird von hier aus wie gewohnt fortgesetzt. Dieser Timer kann mithilfe von "cc-reanswer-to" in der benutzerdefinierten Gruppe konfiguriert werden.

Kategorie II-8 Nachricht blockieren (debug vpm signal)

<#root>

```
009228: Nov 21 12:02:00.955 GMT: //-1/BF12BE36BAC8/VTSP:(0/0/0:0):-1:1:2/vtsp_report_cas_digit:
   Begin Digit=8, Mode=CC_TONE_R2_MF_BACKWARD_MODE
009229: Nov 21 12:02:00.955 GMT: htsp_digit_ready_up(0/0/0:0(2)):
```

Rx digit='8'

```
009230: Nov 21 12:02:00.955 GMT: R2 Incoming Voice(0/0): DSX (E1 0/0/0:1): STATE: R2_IN_CATEGORY R2 Got
009231: Nov 21 12:02:00.955 GMT: Enter r2_comp_category
009232: Nov 21 12:02:00.955 GMT:
```

R2 Event : 8

```
009233: Nov 21 12:02:00.955 GMT:
```

```
#######R2_II8 TRUE########

009234: Nov 21 12:02:00.955 GMT:

####### collect_call_enable = 0

009235: Nov 21 12:02:00.955 GMT:

############sending B7 ##########

009236: Nov 21 12:02:00.955 GMT: r2_reg_generate_digits(0/0/0:0(2)):

Tx digit '7'

009237: Nov 21 12:02:01.055 GMT: //-1/BF12BE36BAC8/VTSP:(0/0/0:0):-1:1:2/vtsp_report_cas_digit:
   End Digit=8, Mode=CC_TONE_R2_MF_BACKWARD_MODE
009238: Nov 21 12:02:01.055 GMT: htsp_digit_ready(0/0/0:0(2)): Rx digit='#'
009239: Nov 21 12:02:01.055 GMT: R2 Incoming Voice(0/0): DSX (E1 0/0/0:1): STATE: R2_IN_CATEGORY R2 Got
009240: Nov 21 12:02:01.055 GMT: Enter r2_comp_category
009241: Nov 21 12:02:01.055 GMT: r2_reg_generate_digits(0/0/0:0(2)): Tx digit '#'
009242: Nov 21 12:02:01.359 GMT: htsp_dsp_message: SEND_SIG_STATUS: state=0x8 timestamp=22365 systime=2
009243: Nov 21 12:02:01.359 GMT: htsp_process_event: [0/0/0:0(2), R2_Q421_IC_WAIT_ANSWER, E_DSP_SIG_100
009244: Nov 21 12:02:01.359 GMT: r2_q421_ic_clr_fwd_idle(0/0/0:0(2)) Rx CLEAR FWD
009245: Nov 21 12:02:01.359 GMT: r2_reg_channel_disconnected(0/0/0:0(2))
009246: Nov 21 12:02:01.359 GMT: R2 Incoming Voice(0/0): DSX (E1 0/0/0:1): STATE: R2_IN_CATEGORY R2 Got
009247: Nov 21 12:02:01.359 GMT: Enter r2_comp_category
009248: Nov 21 12:02:01.359 GMT: htsp_timer - 2000 msec
009249: Nov 21 12:02:01.359 GMT: htsp_process_event: [0/0/0:0(2), R2_Q421_IC_CLR_FWD, E_HTSP_RELEASE_REQ
009250: Nov 21 12:02:01.359 GMT: r2_q421_null_release(0/0/0:0(2)) E_HTSP_RELEASE_REQ
009251: Nov 21 12:02:01.359 GMT: r2_reg_process_event: [0/0/0:0(2), R2_REG_COLLECTING, E_R2_REG_DISCONN
009252: Nov 21 12:02:01.359 GMT: r2_reg_disconnect_collect(0/0/0:0(2))
009253: Nov 21 12:02:01.359 GMT: r2_reg_timer_stop(0/0/0:0(2))
009254: Nov 21 12:02:01.711 GMT: htsp_process_event: [0/0/0:0(1), R2_Q421_IC_CLR_FWD, E_HTSP_EVENT_TIME
009255: Nov 21 12:02:01.711 GMT: htsp_timer_stop
009256: Nov 21 12:02:01.711 GMT: r2_q421_clr_fwd_idle(0/0/0:0(1)) Tx IDLEvnm_dsp_set_sig_state:[R2 Q.42
009257: Nov 21 12:02:01.711 GMT: r2_reg_channel_disconnected(0/0/0:0(1))
009258: Nov 21 12:02:01.711 GMT: //682206/0C63B263B9C9/VTSP:(0/0/0:0):0:1:1/vtsp_do_call_history:
   Coder Rate=5
009259: Nov 21 12:02:01.711 GMT: r2_reg_process_event: [0/0/0:0(1), R2_REG_IDLE, E_R2_REG_DISCONNECT(91
```

Konfigurationsbeispiel für Doppelantwort

```
!
controller e1 0/0/0
 ds0-group 0 timeslots 1-15,17-31 type r2-digital r2-compelled ani
 cas-custom 0
  country brazil
  double-answer
  cc-reanswer-to 3000
!
```

Double-Answer Debugs (debug vpm signal)

<#root>

```
### Answer the call and start a 1 second timer
```

```
May 23 09:52:59.180 BR: r2_q421_ic_answer(0/0/0:0(18))
```

Tx ANSWER

```
 seizure: delay 0 ms,elapsed 12404 msvnm_dsp_set_sig_state:[R2 Q.421 0/0/0:0(18)] set signal state = 0x
May 23 09:52:59.180 BR: r2_reg_channel_connected(0/0/0:0(18))
May 23 09:52:59.180 BR:
```

htsp_timer - 1000 msec

```
May 23 09:52:59.180 BR: //23899578/92233E71B421/CCAPI/cc_api_voice_mode_event:
   Call Id=23899578
May 23 09:52:59.180 BR: //23899578/92233E71B421/CCAPI/cc_api_voice_mode_event:
   Call Entry(Context=0x1E73AD8)
May 23 09:52:59.180 BR: htsp_process_event: [0/0/0:0(18), R2_Q421_IC_DOUBLE_ANS_ANS, E_HTSP_VOICE_CUT_T
May 23 09:52:59.184 BR: //23899578/92233E71B421/CCAPI/cc_process_notify_bridge_done:
   Conference Id=0x10AD1, Call Id1=23899578, Call Id2=23899579
May 23 09:52:59.184 BR: r2_reg_process_event: [0/0/0:0(18), R2_REG_WAIT_FOR_CONNECT, E_R2_REG_CONNECT(9
May 23 09:52:59.184 BR: r2_reg_connect(0/0/0:0(18))
```

One Second Passes and we clear the call and start a 2 second timer

```
May 23 09:53:00.180 BR: htsp_process_event: [0/0/0:0(18), R2_Q421_IC_DOUBLE_ANS_ANS, E_HTSP_EVENT_TIMER
May 23 09:53:00.180 BR: r2_q421_ic_d_answ_answ_to(0/0/0:0(18)) E_TIMER_EVENT
May 23 09:53:00.180 BR: htsp_timer - 2000 msec
May 23 09:53:00.180 BR: r2_q421_ic_d_answ_answ_to(0/0/0:0(18))
```

Tx CLEAR BWD

```
vnm_dsp_set_sig_state:[R2 Q.421 0/0/0:0(18)] set signal state = 0xC
May 23 09:53:00.824 BR: htsp_process_event: [0/0/0:0(18), R2_Q421_IC_DOUBLE_ANS_RLS, E_DSP_SIG_1000]
May 23 09:53:00.824 BR: r2_q421_ic_answer_clr_fwd(0/0/0:0(18))
```

Rx CLEAR FWD

```
May 23 09:53:00.824 BR: r2_reg_channel_disconnected(0/0/0:0(18))
May 23 09:53:00.824 BR:
```

htsp_timer - 2000 msec

```
May 23 09:53:00.824 BR: r2_reg_process_event: [0/0/0:0(18), R2_REG_CONNECTED, E_R2_REG_DISCONNECT(91)]
May 23 09:53:00.824 BR: r2_reg_disconnect_idle(0/0/0:0(18))
May 23 09:53:00.824 BR: R2 Incoming Voice(0/0): DSX (E1 0/0/0:17): STATE: R2_IN_IDLE R2 Got Event R2_ST
May 23 09:53:00.824 BR: r2_reg_timer_stop(0/0/0:0(18))
```

2 second passes and the gateway release the call

```
May 23 09:53:02.824 BR: htsp_process_event: [0/0/0:0(18), R2_Q421_IC_CLR_FWD, E_HTSP_EVENT_TIMER]
May 23 09:53:02.824 BR: htsp_timer_stop
May 23 09:53:02.824 BR: r2_reg_channel_disconnected(0/0/0:0(18))
May 23 09:53:02.824 BR: //23899578/92233E71B421/VTSP:(0/0/0:0):17:1:1/vtsp_cc_call_disconnected:
   Cause Value=16
May 23 09:53:02.824 BR: //23899578/92233E71B421/CCAPI/cc_api_call_disconnected:
   Cause Value=16, Interface=0xB41CEBC, Call Id=23899578
```

ISDN-Überlappungs-Empfang

Wenn der Befehl isdn overlap-receive auf ISDN-Schnittstellen konfiguriert ist, wirkt sich dies auf den Vergleich eingehender Dial-Peers aus. Nachdem jede Ziffer auf der ISDN-Ebene empfangen

wurde, werden DFÜ-Peers auf Übereinstimmungen überprüft. Bei vollständiger Übereinstimmung wird der Anruf sofort (in diesem Fall an die Sitzungs-App) weitergeleitet, ohne auf weitere Nummern zu warten. Der T-Terminator kann verwendet werden, um die Zuordnung einzelner Ziffern auszusetzen und den Router oder das Gateway zu zwingen, auf den Empfang aller Ziffern zu warten. Das T bezieht sich auf den T302-Interdigit-Timer auf ISDN-Ebene, der über die mit der ISDN-Schnittstelle verknüpfte serielle Schnittstelle konfiguriert werden kann. ISDN bietet auch andere Mechanismen zur Angabe des Ziffernendes, z. B. die Einstellung des Sending Complete Information Element (IE) in Q.931-Informationsmeldungen.

Leere angerufene Nummer

Die angezeigte Warnmeldung wird angezeigt, wenn der Dial-Peer mit der eingehenden angerufenen Rufnummer T konfiguriert wurde.

Beispiel für das Ergebnis

```
Gateway(config)# dial-peer voice 1 pots
Gateway(config-dial-peer)# incoming called-number T
Warning: Pattern T defines a match with zero or more digits and hence could
match with an empty number. If this is not the desired behaviour please
configure pattern .T instead to match on one or more digits
```

Besondere Hinweise zu einer eingehenden DFÜ-Peer-Übereinstimmung mit einer leeren angerufenen Nummer.

- Eine angerufene Null-Nummer gilt als weniger qualifiziert im Vergleich zu einem Sprach-Port und/oder in einigen Fällen als Antwortadresse. Aus diesem Grund kann eine Übereinstimmung auf der Basis einer Null-angerufenen Nummer nur dann auftreten, wenn keine Übereinstimmung auf der Basis der Antwortadresse oder der Portnummer vorliegt.
- Bei überlappenden Wählvorgängen stimmt die angerufene Null-Nummer nicht mit der eingehenden angerufenen Nummer T überein, da kein Timeout aufgetreten ist.
- Eine Null-angerufene Nummer kann nur im Fall von ENBLOCK mit der eingehenden angerufenen Nummer T übereinstimmen, und es gibt auch keine Übereinstimmung aufgrund von Antwortadresse und Portnummer. Die Warnung, die angezeigt wird, wenn ein Administrator die eingehende Rufnummer T konfiguriert, bezieht sich auf diesen speziellen Fall.

Einschränkungsklasse

Class of Restriction (COR) ist eine Möglichkeit, Anrufe auf einem Cisco Gateway zu begrenzen. COR wird oft als Schlüssel-Schloss-Mechanismus bezeichnet. Sperren werden DFÜ-Peers mit einer ausgehenden COR-Liste zugewiesen. Schlüssel werden DFÜ-Peers mit einer eingehenden COR-Liste zugewiesen. Bei Anwendung von COR-Listen sind die verfügbaren ausgehenden DFÜ-Peers diejenigen, die der Schlüssel entsperren kann. Diese Filterung erfolgt, bevor die übrigen

Methoden zum Abgleich ausgehender Dial-Peers überprüft werden.

Zwei wichtige Regeln für die Einschränkungsklasse:

1. Wenn keine COR-Liste ausgehender Anrufe angewendet wird, wird der Anruf immer weitergeleitet.
2. Wenn keine COR-Liste eingeht, wird der Anruf immer weitergeleitet.

Die Konfiguration von Class of Restriction (COR), Logical Partitioning Class of Restriction (LPCOR) und LPCOR mit Forced Authorization Codes (FAC) geht über den Umfang dieses Dokuments hinaus. Auf diese Dokumente kann jedoch zum weiteren Lesen verwiesen werden.

COR	Konfigurieren der Einschränkungsklasse (Class of Restrictions, COR)
LPCOR mit CME	CME mit LPCOR-Konfigurationsbeispiel
LPCOR mit CME und FAC	Administratoranleitung für das Cisco Unified Communications Manager Express-System

Cisco Unified Communications Manager Express (CUCME) Dial-Peers

CME erstellt Dial-Peers für das System für Ephones und Sprachregisterpools. Diese sind in der aktuellen Konfiguration nicht sichtbar. Um Änderungen an den CME-DFÜ-Peers vorzunehmen, müssen die Änderungen am tatsächlichen Telefon- oder Sprachregisterpool vorgenommen werden. Beim Anzeigen von Anzeigeausgängen für die Dial-Peer-Sprachübersicht handelt es sich bei dem Dial-Peer ab 2000 um SCCP-Ephones, und bei den Dial-Peers ab 4000 um SIP-Sprachregisterpools. Dieser Dial-Peer wird bei Anrufen von CME-registrierten Telefonen als eingehender Dial-Peer angezeigt, während der ausgehende Dial-Peer bei Debug-Anrufen von CME-registrierten Telefonen als eingehender Dial-Peer angezeigt wird.

Beispielausgabe zur Anzeige einer Dial-Peer-Sprachübersicht mit CME.

```
Gateway# show dial-peer voice sum | s 2000|4000
20001  pots  up   up             1001$             0                              50/0/1
20002  pots  up   up             4001$             0                              50/0/2
20003  pots  up   up             4002$             0                              50/0/3
20004  pots  up   up             7001$             0                              50/0/4
20005  pots  up   up             3009$             0                              50/0/5
20006  pots  up   up             8810....$         0                              50/0/10
20007  pots  up   up             8811....$         0                              50/0/11
40001  voip  up   up             14085151111$      0  syst ipv4:14.50.214.67:50
40002  voip  up   up             19725252222$      0  syst ipv4:14.50.214.67:50
40003  voip  up   up             85225353333$      0  syst ipv4:14.50.214.67:50
40004  voip  up   up             442084445555$     0  syst ipv4:14.50.214.67:50
40005  voip  up   up             911$              0  syst ipv4:14.50.214.67:50
40006  voip  up   up             18005550100$      0  syst ipv4:14.50.214.67:50
40008  voip  up   up             2001$             0  syst ipv4:14.50.214.51:50
```

Beispielausgabe für die Anzeige von Sprachregister-Dial-Peers mit SIP CME.

```
Gateway# show voice register dial-peers
Dial-peers for Pool 2:

dial-peer voice 40006 voip
 destination-pattern 14085151111$
 session target ipv4:14.50.214.67:5060
 session protocol sipv2
 dtmf-relay rtp-nte
 digit collect kpml
 codec  g711ulaw bytes 160
 no vad
  call-fwd-all         8888
  after-hours-exempt   FALSE

dial-peer voice 40005 voip
 destination-pattern 19725252222$
 session target ipv4:14.50.214.67:5060
 session protocol sipv2
 dtmf-relay rtp-nte
 digit collect kpml
 codec  g711ulaw bytes 160
 no vad
  after-hours-exempt   FALSE
```

MGCP und SCCP mit Dial-Peers

MGCP und SCCP befolgen ihre eigenen Regeln für Dial-Peers. Sie verwenden lediglich das Konzept, dass der gewünschte Sprach-Port für den Anruf konfiguriert werden muss. Der Rest wird über den STCAPP- und MGCPAPP-Prozess abgewickelt. Wenn Sie die Konfiguration dieser DFÜ-Peers untersuchen, verfügen sie entweder über den Befehl service mgcappp oder service stcapp. Diese aktivieren den Dial-Peer für die gewünschte Anwendung und teilen der Anwendung mit, mit welchem Dial-Peer sie umgehen kann.

Beim Debuggen dieser Protokolle wird in der Ausgabe nie eine Übereinstimmung mit einem eingehenden Dial-Peer angezeigt. Dies kann immer als Dial-Peer 0 angezeigt werden. Weil es sie nicht gibt. Der Anruf-Agent, der die Anwendung verarbeitet, hat bereits den Port ausgewählt, an den der Anruf gesendet werden soll, und der Dial-Peer-Abgleich für eingehende Anrufe ist nutzlos, da das Gateway keine Kontrolle über diesen Teil des Anrufs hat. Es kann jedoch ein Dial-Peer-Abgleich bei ausgehenden Anrufen beobachtet werden. Dies dient lediglich zur Veranschaulichung, da der Anruf-Agent, der den Prozess verarbeitet, letztlich auch diese Seite des Anrufs steuert.

Denken Sie daran, dass der Dial-Peer der Anwendung nur mitteilt, welcher physische Sprach-Port gesteuert werden soll. Da der Großteil dieser Aufgaben von einem externen Anruf-Agenten und dem Gateway gesteuert wird, übernimmt das Gerät einfach das, was ihm gesagt wird. Sie überspringen die grundlegende Vorgehensweise in diesem Abschnitt und stellen einige

Konfigurationen für die ersten Schritte bereit.

MGCP-Beispielkonfiguration [mit CUCM-Autokonfiguration*]

```
!
mgcp call-agent 10.10.10.10
mgcp
!
ccm-manager mgcp [codec-all]
ccm-manager config server 10.10.10.10
ccm-manager config
ccm-manger redundant-host 10.10.10.20
!
voice-port 0/0/0
 description The MGCP port to register
 no shut
!
dial-peer voice 1 pots
 description Defining the Port for the MGCP application
 service mgcpapp
 port 0/0/0
!
hostname myrouter
ip domain name cisco.com
ip name server 10.10.10.30
!
ip tftp source-interface gig0/0/0
!
```

Vollständige MGCP-Dokumentation: Cisco Unified Communications Manager and Interoperability Configuration Guide, Cisco IOS Release 15M&T

SCCP-/STCAPP-Beispielkonfiguration [mit CUCM-Autokonfiguration*]

```
!
stcapp ccm-group 1
stcapp
!
sccp local gig0/0/0
sccp ccm 10.10.10.10 id 1 priority 1 version 7.0+
sccp ccm 10.10.10.20 id 1 priority 2 version 7.0+
sccp
!
sccp ccm group 1
 bind interface gig0/0/0
 associate ccm 1 priority 1
 associate ccm 2 priority 2
!
ccm-manager config server 10.10.10.10
ccm-manager sccp local gig0/0/0
ccm-manager sccp
!
voice-port 0/0/0
 description The SCCP port to register
```

```
 no shut
!
dial-peer voice 1 pots
 description Defining the Port for the SCCP application
 service stcapp
 port 0/0/0
!
ip tftp source-interface gig0/0/0
!
```

Wenn ein Administrator nicht möchte, dass der CUCM das Gateway konfiguriert, entfernen Sie einfach die ccm-manager-Befehle. Die Dial-Peer-Konfiguration ist enthalten, um die Funktionsweise des Konzepts zu verdeutlichen. Wenn die CCM-Manager-Konfigurationen vorhanden sind, erstellt CUCM diese Dial-Peers basierend auf der Port-Konfiguration im CUCM, sodass der Dial-Peer nicht definiert werden muss. Die vom CUCM erstellten DFÜ-Peers beginnen in der Regel mit 999 und enthalten dann drei weitere Ziffern.

SIP DSAPP mit Dial-Peers

SIP DSAPP wurde in Cisco IOS XE 16.12.1+ und CUCM 12.5.1SU+ hinzugefügt

Mit dieser Funktion können analoge Sprach-Ports wie FXS vom CUCM registriert und verwaltet werden. Die Anrufweiterleitung mit DSAPP unterscheidet sich geringfügig von MGCP oder SCCP, da die DFÜ-Peers weiterhin normal zugeordnet sind. Das Gateway kann also Nummern vom FXS-Port sammeln und eine Dial-Peer-Suche bei den VoIP-Dial-Peers durchführen. Nachdem eine Übereinstimmung gefunden wurde, wird die INVITE-Nachricht an den CUCM-Enblock gesendet, damit der CUCM eine weitere Ziffernanalyse durchführen kann.

SIP-DSAPP-Beispielkonfiguration [mit CUCM-Autokonfiguration*] | IOS-XE 16.12.1+ und CUCM 12.5.1SU+

```
!
dsapp line
!
voice service voip
 sip
  bind control source-interface GigabitEthernet0/0/0
  bind media source-interface GigabitEthernet0/0/0
  session transport tcp
!
application
 service dsapp
  param dialpeer 777
!
global
 service default dsapp
!
ccm-manager config server 10.10.10.10
ccm-manager sipana auto-config local GigabitEthernet0/0/0
!
dial-peer voice 777 voip
 destination-pattern 9T
```

```
 session protocol sipv2
 session target ipv4:10.10.10.10
 session transport tcp
 incoming called-number .
 voice-class sip extension gw-ana
 voice-class sip bind control source-interface GigabitEthernet0/0/0
 dtmf-relay rtp-nte
 codec g711ulaw
!
dial-peer voice 19990100 pots
 service dsapp
 destination-pattern 7776
 voice-class sip extension gw-ana
 port 0/1/0
!
sip-ua
 registrar ipv4:10.10.10.10 expires 3600 tcp
!
```

Vollständige SIP DSAPP-Dokumentation: Cisco VG450 Voice Gateway Software Configuration Guide

Fehlerbehebung und Überprüfung der Anrufweiterleitung

Weitere Informationen finden Sie in diesem Dokument.

Konfigurieren der Debugsammlung für Unified Border Element (CUBE)- und Time Division Multiplexing (TDM)-Gateways

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.