

# Informazioni sul routing delle chiamate in Cisco IOS e IOS XE

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Definizioni comuni](#)

[Roadmap dei comandi e delle funzionalità](#)

[Nozioni fondamentali di Cisco IOS / Cisco IOS XE Call Routing](#)

[Tipi Voice Dial-Peer](#)

[Corrispondenza Dial-Peer In Entrata](#)

[Se non esistono corrispondenze /Default Dial-Peer 0 peer\\_tag=0\\_pid:0](#)

[Corrispondenza Dial-Peer In Uscita](#)

[Stringa numerica Dial-Peer Hunting](#)

[URI Dial-Peer Hunting](#)

[URI classe voce](#)

[Corrispondenza Dial-Peer URI in entrata](#)

[Corrispondenza Dial-Peer URI in uscita](#)

[Caratteri jolly Dial-Peer](#)

[Stati Dial-Peer](#)

[Virtual Routing and Forwarding \(VRF\) e Dial-Peer Hunting](#)

[Corrispondenza Dial-Peer in entrata con VRF](#)

[Corrispondenza Dial-Peer in uscita con VRF](#)

[Tecniche avanzate di routing delle chiamate](#)

[Dial-Peer Group](#)

[Mappe modello E164](#)

[Gruppi-server di destinazione](#)

[Gruppo server di destinazione e OPZIONI attive](#)

[Proxy in uscita](#)

[Gruppi trunk POTS](#)

[Tenant classe voce](#)

[Chiamate URI ILS a CUBE \(Voice Class Route-String\)](#)

[Tecniche di routing delle chiamate legacy](#)

[Mappa DNIS](#)

[Etichette gruppi trunk](#)

[Tipo di numerazione](#)

[Dial-Peer Data](#)

[Voice Source-Group](#)

---

[Autorizzazioni Dial-Peer](#)

## [Manipolazione dell'URI e della cifra](#)

[Manipolazione della cifra tramite Dial-Peer POTS](#)

[Manipolazione della cifra tramite regole e profili di conversione vocale](#)

[Traduzione della classe voce e164](#)

[Manipolazione della cifra tramite mappe ISDN](#)

[Manipolazione della cifra tramite espansione del numero \(num-exp\)](#)

[Profili SIP in entrata/in uscita](#)

[Copylist SIP](#)

## [Note speciali](#)

[Segnalazione protocollo e associazione supporti](#)

[DNS e VoIP Dial-Peer](#)

[Connessioni e larghezza di banda massime](#)

[Direct Inward Dial \(DID\)](#)

[Composizione in una fase](#)

[Composizione in due fasi](#)

[Blocco delle chiamate](#)

[Ricezione sovrapposizione ISDN](#)

[Numero chiamato vuoto](#)

[Classe di restrizione](#)

[Peer di connessione remota Cisco Unified Communications Manager Express \(CUCME\)](#)

[MGCP e SCCP con Dial-Peer](#)

[SIP DSAPP con Dial-Peer](#)

[Risoluzione dei problemi e verifica del routing delle chiamate](#)

---

# Introduzione

In questo documento viene fornita una spiegazione del routing delle chiamate in Cisco IOS® e in Cisco IOS XE.

## Prerequisiti

### Requisiti

Sebbene non siano richiesti prerequisiti formali per la lettura di questo documento, il lettore è comunque in grado di leggere i protocolli di segnalazione vocale utilizzati per stabilire e connettere le chiamate. I riferimenti a questi protocolli vengono ripetuti più volte in.

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

Protocolli multimediali: Real Time Protocol (RTP), codec voce, codec video.

Tecnologie analogiche: Ear and Mouth (E&M), Foreign Exchange Subscriber (FXS) e Foreign Exchange Office (FXO).

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS e IOS XE Gateway
- 2800 / 3800 / 2900 / 3900 / 4300 / 4400 / CSR1000v / CAT8000v / ASR100X / C8200 / C8300 / ISR1100

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

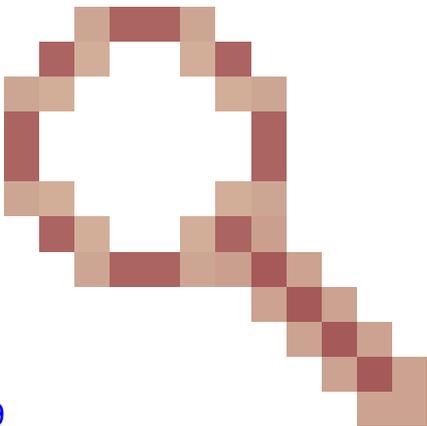
In questo documento vengono illustrati i meccanismi alla base della corrispondenza dial-peer in entrata e in uscita con i servizi POTS (Plain Old Telephone Service) e VoIP (Voice over IP).

Oltre alle informazioni sui dial-peer, questo documento tratta argomenti importanti relativi al routing delle chiamate. Queste includono la manipolazione delle cifre, una rapida panoramica della manipolazione dei messaggi SIP (Session Initiation Protocol), alcuni metodi per limitare le funzionalità di chiamata, una rapida panoramica del supporto e del binding di segnalazione e infine un po' di risoluzione dei problemi.

In questo documento vengono usati come punti di riferimento gli esempi di configurazione e gli output dei comandi debug e show. Le numerose funzionalità di questo documento sono chiaramente contrassegnate con la versione in cui è stata introdotta la funzionalità in Cisco IOS e Cisco IOS XE. È possibile fare rapidamente riferimento a queste informazioni anche nella sezione [Roadmap dei comandi e delle funzionalità](#). Se si verifica un difetto notevole, questo viene collegato all'interno del testo in modo che i lettori ne siano consapevoli.

## Definizioni comuni

Attributo	Descrizione
Stringa di cifre	Definito anche stringa numerica, numero di telefono, numero o numero E164. È costituito interamente da cifre comprese tra 0 e 9 con un segno più (+) iniziale facoltativo.  Esempio: 8675309 123456789 +1972525222

Attributo	Descrizione
	+442084445555 +85225353333
DNIS (Dialed Number Identification Service)	Si tratta del numero chiamato o del numero di destinazione di una chiamata.
ANI (Automatic Number Identification)	Numero di chiamata o numero di chiamata di origine per una chiamata. Questo identificatore può anche essere denominato CLID (Calling Line Identifier) e può anche essere denominato ID chiamante.
URI (Uniform Resource Identifier)	Un URI è una stringa sip: o tel: comunemente utilizzata con i protocolli VoIP SIP e H323.  Esempi di URL: 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
ID vettore	Esempi di CID: cid:orange@host.com cid:orange@sub.host.com cid:orange@10.10.10.10 cid:orange@2001:4860:4860:8888    <p data-bbox="576 1984 1278 2056">Nota: l'ID bug Cisco <a href="https://tools.cisco.com/bugtools/bugsearch/show/CSCua14749">CSCua14749</a> Carrier-ID non funziona sulle piattaforme IOS XE.</p>

Attributo	Descrizione
Route-String	Un'intestazione proprietaria Cisco per le stringhe di route ILS utilizzate con il SIP.  Esempio: Stringa-route-destinazione-X-cisco: <sip:configure-value>
ENUMERAZIONE	ENUM è un protocollo che utilizza il DNS (Domain Name Service) per convertire i numeri telefonici E164 in URI. Argomento non trattato nel presente documento.
PSTN	Rete telefonica pubblica commutata
ITSP	Provider di servizi di telefonia Internet
SBC	Controller del bordo di sessione.  Si tratta del dispositivo che funge da punto di distinzione tra la LAN del cliente e una rete ITSP/PSTN

## Roadmap dei comandi e delle funzionalità

Funzionalità	Versione IOS	Versione IOS XE
Espansione numero (num-exp)		
Dial-peer (POTS e VOIP)		
indirizzo-risposta		
schema di destinazione	11.3(1)T	Tutto
numero chiamato in ingresso		
destinazione sessione (IPv4 e DNS)		

Numero massimo di connessioni (max-conn) chiamata diretta verso l'interno POTS (forward-cifre) prefisso (POTS) timeout a quattro cifre (voice-port)		
dial-peer terminator	12.0	Tutto
cacciatrice	12.0(5)T	Tutto
Mappe ISDN	12.0(6)T	Tutto
Schemi di caccia Dial-peer	12.0(7)XK	Tutto
Regola e profilo di conversione vocale translate-outgoing tipo numerico Nastro numerico (POTS)	12.0(7)XR1	Tutto
destinazione sessione (sip-server)	12.1(1)T	Tutto
Gruppo trunk POTS	12.1(3)T	Tutto
Mappa DNIS (in uscita)	12.2(2)XB	Tutto
trunk-group-label	12.2(11)T	Tutto
Dial-peer (dati)	12.2(13)T	Tutto

URI classe voce (in uscita)	12.3(4)T	Tutto
proxy in uscita	12.4(15)T	Tutto
destinazione sessione (IPv6)	12.4(22)T	Tutto
Profili SIP (in uscita)	15.0(1)M	Tutto
URI classe voce (in entrata) voice source-group	15.1(2)T	3,8 S
Copylist SIP destinazione sessione (Registrar)	15.1(3)T	3,6 S
url (call-route)	15.2(1)T	3,3S
massima larghezza di banda	15.2(2)T	3,7 S
E164-Pattern-Maps (In Uscita)	15.2(4)M	3,7 S
Route-String classe voce call-route (dest-route-string)	15.3(3)M	3,10 S
VOIP (Dial-Peer Group) E164-Pattern-Maps (In Entrata) Gruppo server di destinazione	15.4(1)T	3.11S

passaggio obbligatorio destinazione sessione (sip-uri)		
Criteri di provisioning Dial-peer Profili SIP (in entrata)	15.4(2)T	3,12S
Dial-Peer Group (POTS)	15.5(1)T	3,14S
Tenant classe voce	15.6(2)T	16.3.1
Filtraggio VRF per dial- peer	15.6(3)M	16.3.1
e164-traduzione	n/d	16.8.1
DSAPP SIP	n/d	16.12.1
Huntstop per i gruppi di server	n/d	17.4.1
sip porta di ascolto per il tenant Filtro per dial-peer	n/d	17.8.1
Opzione keepalive basata su DNS SRV	n/d	17.9.1

## Nozioni fondamentali di Cisco IOS / Cisco IOS XE Call Routing

I gateway Cisco IOS e Cisco IOS XE utilizzano il concetto di dial-peer per controllare il routing delle chiamate e la negoziazione delle funzionalità per ciascuna gamba di una chiamata. Una gamba di richiamo è la comunicazione bidirezionale tra due agenti di richiamo. Un agente di chiamata è un dispositivo che avvia, elabora o inoltra chiamate di telefonia. Questa operazione può essere eseguita, e non è limitata a, da un provider di telefonia, un gateway Cisco, un telefono IP, un Cisco Unified Communications Manager (CUCM), una Cisco Unity Connection (CUC) e così via. Troppi agenti di chiamata da elencare.

Scenario: una chiamata arriva a un gateway Cisco da un altro agente di chiamata ed è la coda di chiamata in entrata (nella coda). Il gateway elabora la chiamata e, in base alla relativa elaborazione, la invia all'agente di chiamata successivo. Questa è la gamba di richiamo in uscita (out-leg).

Nell'immagine 1 viene mostrata una chiamata dal PSTN al routing CUCM tramite Cisco Voice Gateway e le informazioni sulla coda delle chiamate in entrata e in uscita rispettive.

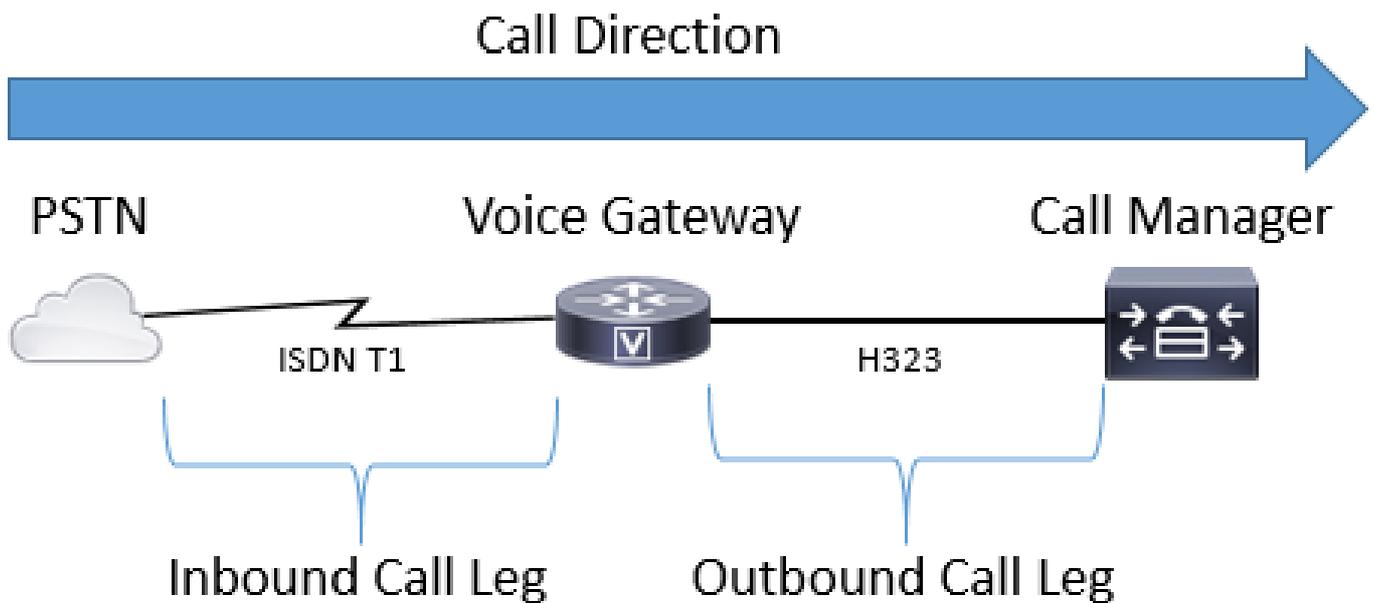


Immagine 1 - Illustrazione dei segmenti di chiamata in entrata e in uscita

Una chiamata effettuata tramite un Cisco Gateway ALWAYS (vedere la nota) corrisponde a una connessione dial-peer in entrata o in uscita per il routing corretto. I dial-peer in entrata e in uscita sono simili ai call-leg menzionati in precedenza. Nell'immagine 1, la chiamata arriva dalla PSTN sul gateway Cisco e deve corrispondere a una connessione dial-peer in entrata. Il gateway quindi utilizza un dial-peer in uscita per instradare la chiamata all'agente di chiamata successivo. È importante ricordare che questi termini vengono definiti dalla prospettiva di Cisco Gateway.

Abbinando un dial-peer per ogni lato della chiamata, un amministratore ha il potere di controllare molti aspetti di ogni specifico tappa della chiamata. Esempi di queste includono codec voce, preferenze DTMF, manipolazione delle cifre, dove instradare la chiamata e molte altre impostazioni. I peer di composizione possono essere configurati con istruzioni di corrispondenza in entrata e in uscita, in modo che sia possibile far corrispondere lo stesso peer di composizione sia per il segmento in entrata che per il segmento in uscita, se a tale peer di composizione specifico viene applicata una configurazione di corrispondenza in entrata e in uscita valida.

 Nota: l'eccezione a questa regola si ha con le porte vocali MGCP e SCCP. Questi protocolli di segnalazione non seguono il normale meccanismo di corrispondenza dial-peer durante il routing delle chiamate. Per ulteriori informazioni, vedere la sezione [SCCP e MGCP](#).

Nella figura 2 vengono illustrati gli stessi livelli di chiamata in entrata e in uscita dell'immagine 1, ma con i rispettivi dial-peer per una chiamata dalla PSTN al routing CUCM tramite Cisco Voice Gateway.

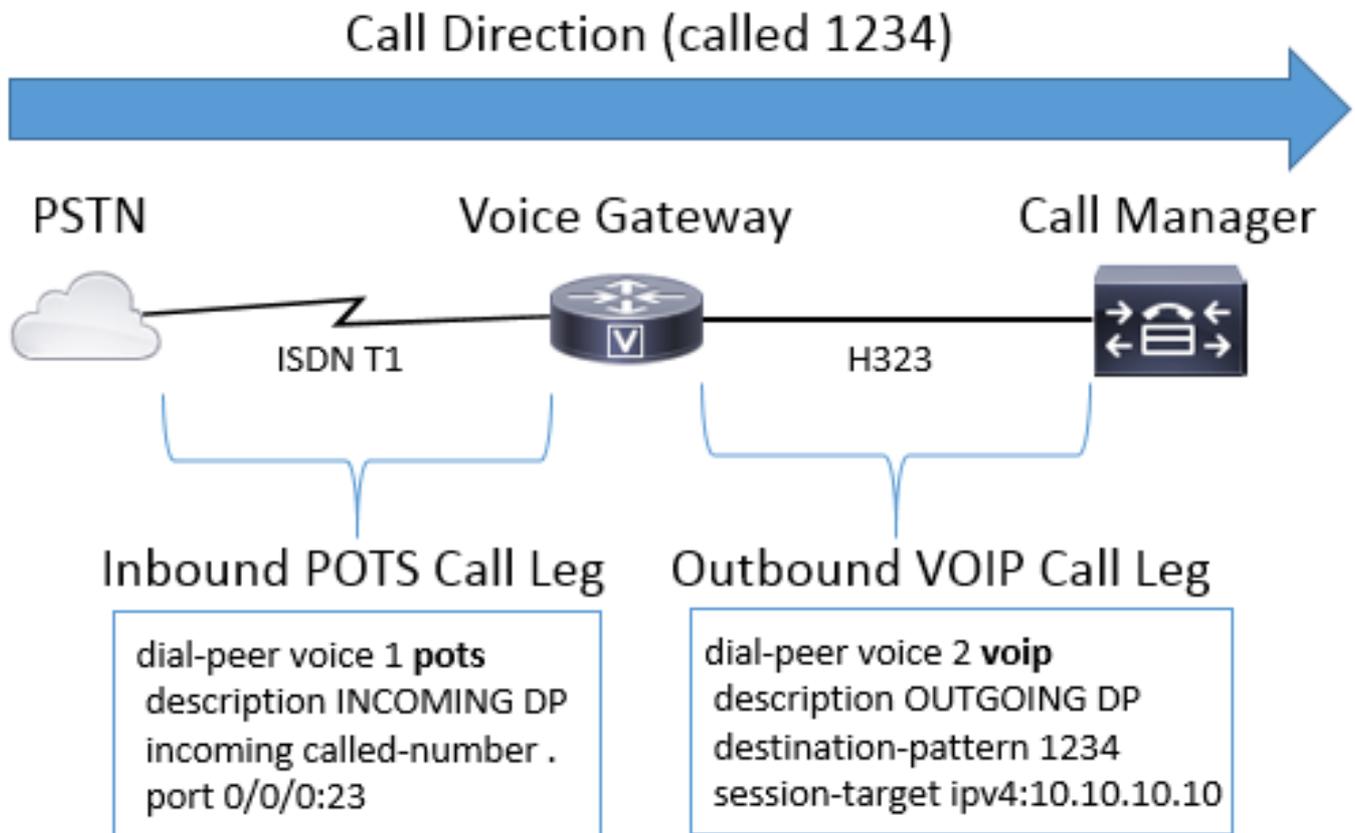


Immagine 2 - Elenco dei dial-peer in entrata e in uscita

I Cisco Voice Gateway possono interagire con molti tipi diversi di chiamate vocali e protocolli, tra cui IP-IP, POTS-POTS e IP-POTS o viceversa.

L'immagine 3 mostra una chiamata da VoIP a VoIP tramite Cisco Unified Border Element (CUBE).

## Call Direction (called 1234)

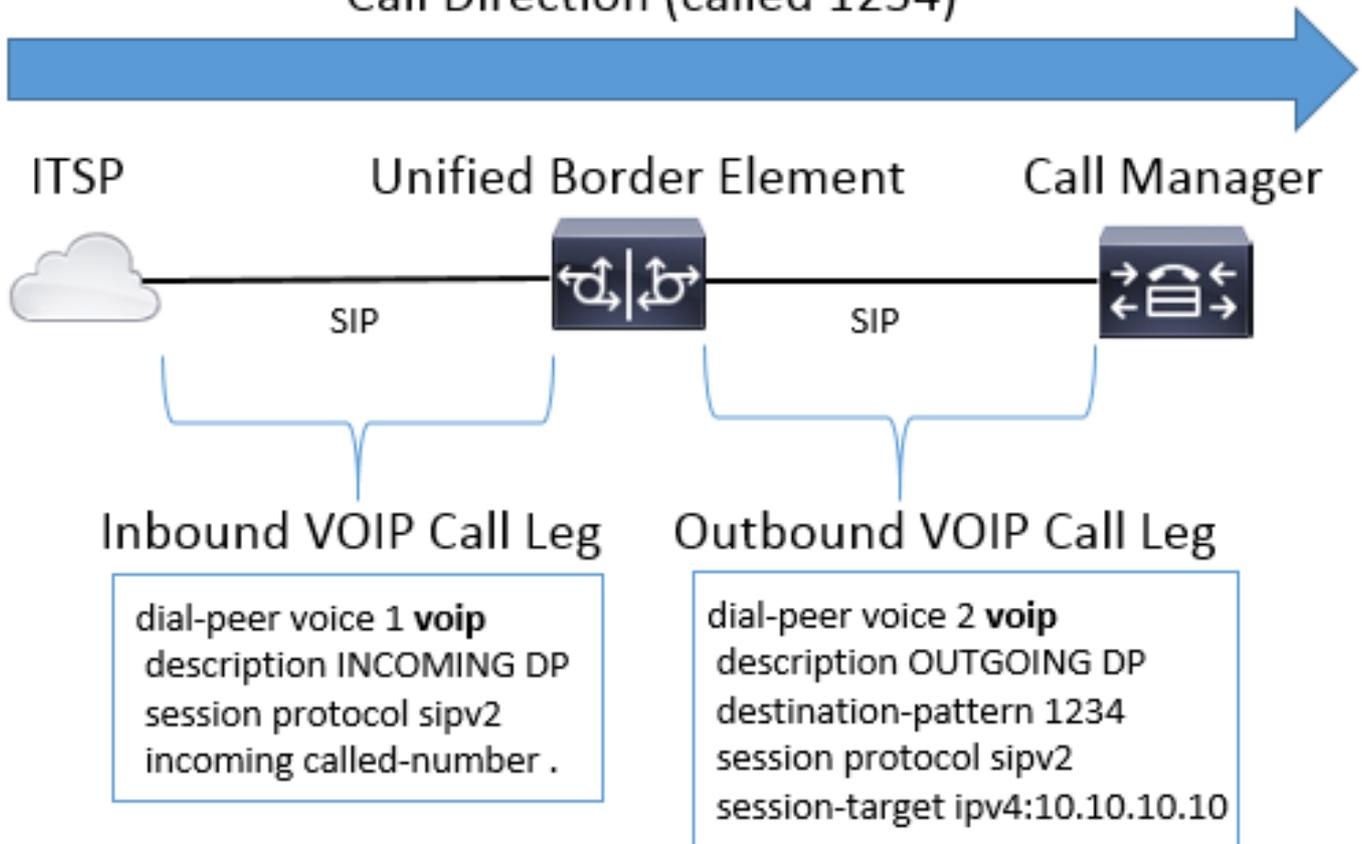


Immagine 3 - Dial-peer in entrata e in uscita per una chiamata Voip to VoIP

L'immagine 4 mostra una chiamata POTS a POTS tramite un gateway Cisco.

## Call Direction (called 1234)

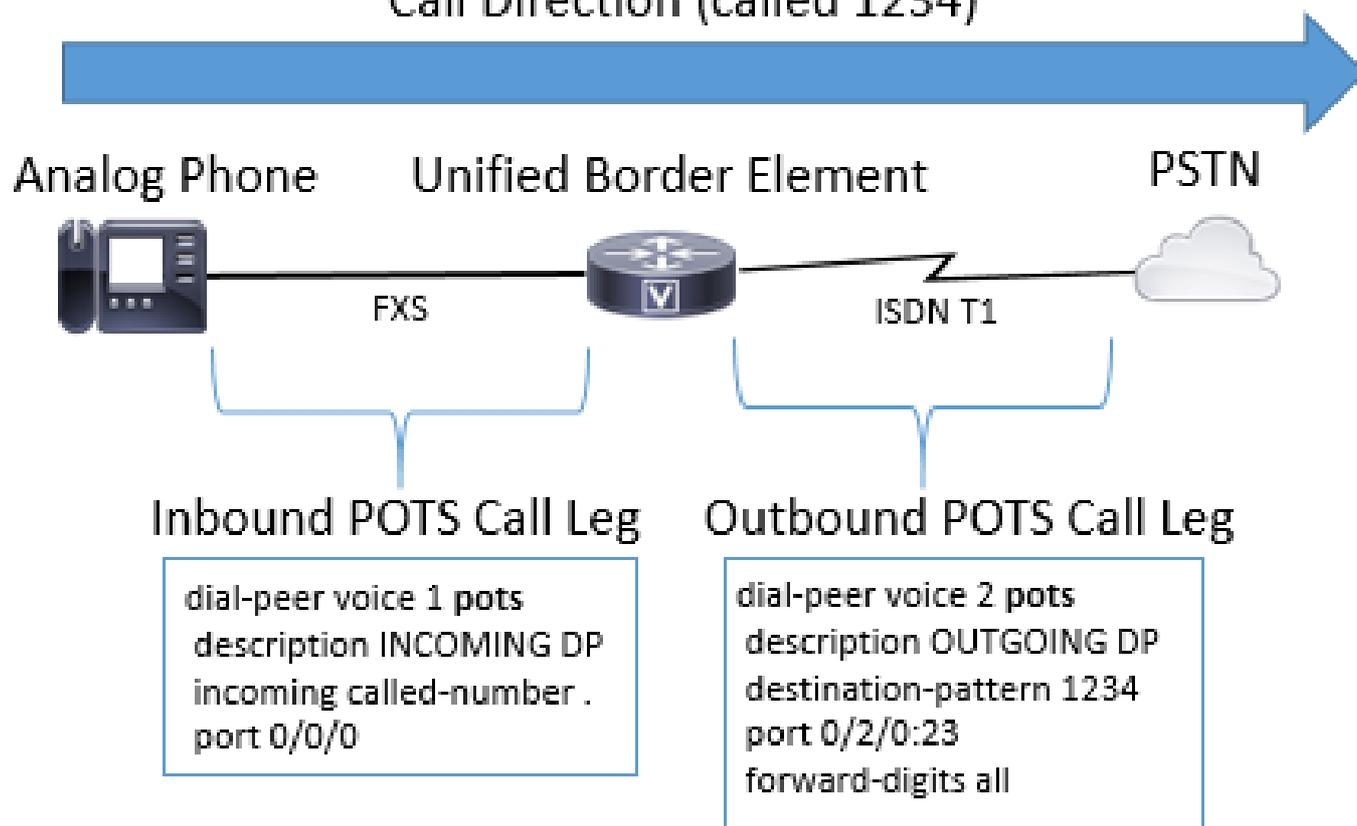


Immagine 4 - Dial-peer in entrata e in uscita per una chiamata POTS a POTS

### Tipi Voice Dial-Peer

PENTOLE	<p>I dial-peer dei servizi di telefonia tradizionali vengono usati per connessioni analogiche come FXS analogico, FXO, ISDN T1 / E1, E1 R2 e connessioni Ear and Mouth (E&amp;M). Questi inviano o ricevono una chiamata a/da una porta vocale fisica sul gateway.</p>
VOIP	<p>I dial-peer Voice Over IP vengono usati principalmente per controllare le connessioni H323 e SIP da e verso il gateway. Questi peer di composizione inviano e ricevono segnali da indirizzi IPv4 e IPv6 e da nomi di dominio completi (FQDN) tramite DNS (Domain Name System).</p> <p>I dial-peer VoIP possono essere utilizzati anche per i segnali Voice over Frame Relay (VoFR), Voice over ATM (VoATM), Voice over High-Level Data Link Control (VoHDLC) e la segnalazione Registration, Admission, and Status (RAS) e per le destinazioni di sessione per questi dial-peer possono includere anche i valori dei regolamenti e dei valori ENUM.</p>

	Nota: alcuni di questi tipi di configurazioni sono tecnologie meno recenti non visibili nelle reti più recenti e con IOS XE alcune non sono più supportate. Di conseguenza, non sono trattate nel presente documento.
MMOIP	I dial-peer Multimedia Mail Over IP vengono utilizzati per inviare e-mail ai server di scambio. Questi sono utilizzati principalmente per il fax on-ramp/off-ramp t t37. Questi tipi di dial-peer non rientrano nell'ambito di questo documento.

 Nota: il numero massimo di peer di chiamata che possono essere configurati su un gateway Cisco dipende dalla memoria disponibile (DRAM). Ogni dial-peer occupa circa 6 KB di memoria, quindi assicurarsi che il gateway disponga almeno del 20% della memoria totale riservata ad altri processi CPU. Un numero elevato di dial-peer configurati può aggiungere al ritardo per indirizzare una chiamata. Ciò può essere significativo se l'applicazione voce Cisco guarda attraverso i dispositivi peer di connessione dall'alto verso il basso, in modo simile a un Access Control List (ACL). Di solito questo non è un problema sui gateway Cisco più recenti.

Errore di esempio:

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

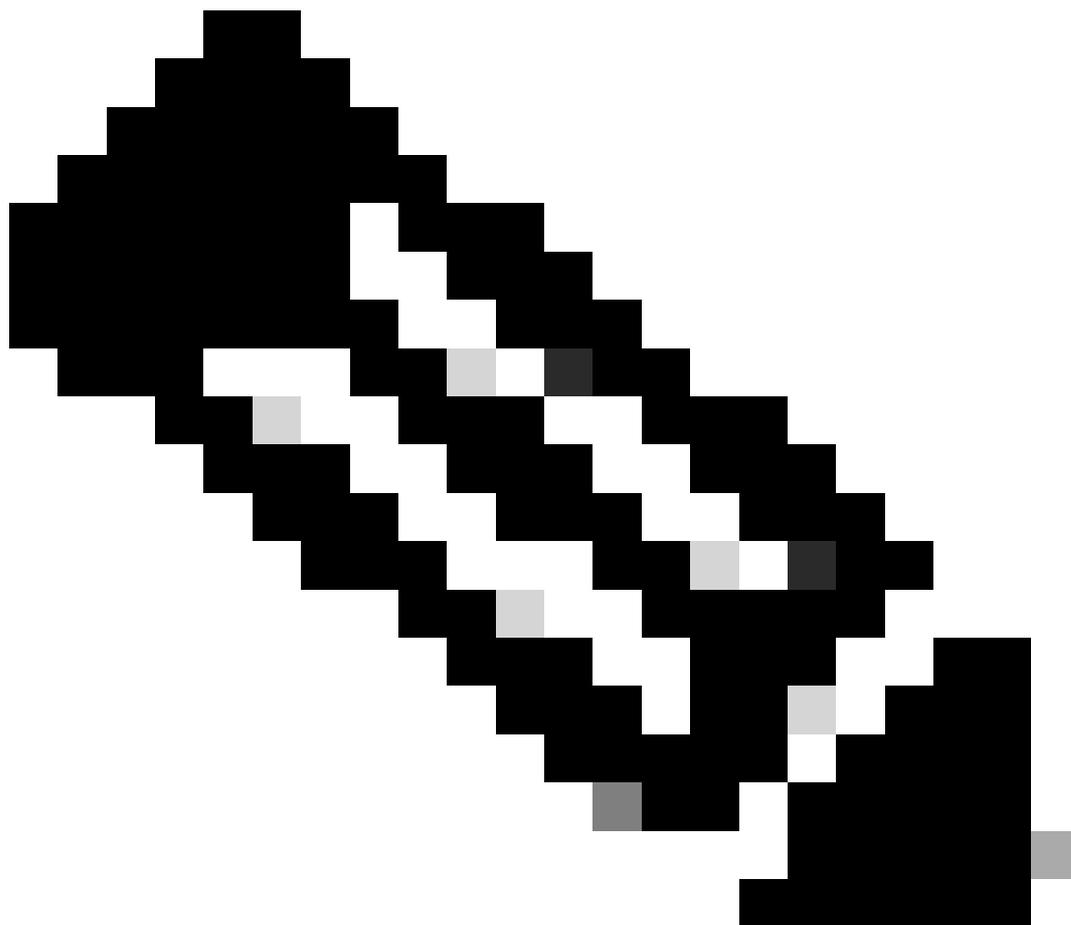
## Corrispondenza Dial-Peer In Entrata

Quando un gateway Cisco riceve una richiesta di configurazione di chiamata, inizia la ricerca di un dial-peer in arrivo applicabile per questa chiamata. Non si tratta di un'analisi cifra per cifra, ma viene utilizzato il messaggio completo per determinare quale dial-peer in ingresso è selezionato. L'ordine degli elementi nel messaggio controllato dipende in larga misura dal protocollo per la chiamata, come indicato dagli elenchi di preferenze definiti nella tabella 1, nella tabella 2 e nella tabella 3. Un dial-peer deve soddisfare solo una delle condizioni per la corrispondenza. Non è necessario configurare tutti gli attributi nel dial-peer o che ogni attributo corrisponda alle informazioni di impostazione della chiamata. La ricerca viene eseguita in base ai primi criteri di corrispondenza in tutti i peer di composizione. Il gateway passa ai criteri successivi solo se non viene trovata alcuna corrispondenza.

Tabella 1. Preferenza selezione Dial-Peer SIP in entrata

Preferenza	Criteri di corrispondenza	Comandi Dial-peer
------------	---------------------------	-------------------

1	URI	uri in ingresso tramite <uri-tag>
2	URI	richiesta uri in ingresso <uri-tag>
3	URI	uri in ingresso in <uri-tag>
4	URI	uri in ingresso da <uri-tag>
5	Numero chiamato	call-number <stringa-numero> in arrivo chiamata in arrivo e164-pattern-map <pattern-map-number>
6	Numero chiamante	chiamata in arrivo e164-pattern-map <pattern-map-number> answer-address <stringa-numero>
7	Modello di destinazione (ANI)	destination-pattern <stringa-numero>
8	ID vettore	carrier-id source <stringa>



Nota: i dial-peer in ingresso idonei possono essere filtrati in base al VRF o al tenant. se è configurata la funzionalità applicabile. Per ulteriori informazioni, vedere le sezioni VRF (Virtual Routing and Forwarding) e Dial-Peer Hunting e Voice Class Tenants.

Tabella 2. Preferenza di selezione Dial-Peer H323 in entrata

Preferenza	Criteri di corrispondenza	Comandi Dial-peer
1	URI	uri in ingresso chiamato <uri-tag> chiamata uri in ingresso <uri-tag>
2	Numero chiamato	call-number <stringa-numero> in arrivo chiamata in arrivo e164-pattern-map <pattern-map-

		number>
3	Numero chiamante	chiamata in arrivo e164-pattern-map <pattern-map-number> answer-address <stringa-numero>
4	Modello di destinazione (ANI)	destination-pattern <stringa-numero>
5	ID vettore	carrier-id source <stringa>

Tabella 3. Preferenza di selezione Dial-Peer POTS Enbloc in entrata

Preferenza	Criteri di corrispondenza	Comandi Dial-peer
1	Numero chiamato	call-number <number-string> in arrivo
2	Numero chiamante	answer-address <number-string>
3	Modello di destinazione (ANI)	destination-pattern <stringa-numero>
4	Voice-port	port <voice-port-number>

Se non esistono corrispondenze / Dial-Peer predefinito 0 peer\_tag=0, pid:0

Quando non esistono corrispondenze idonee per un dial-peer in entrata per chiamate POTS o VoIP, il gateway alloca il dial-peer 0. Ciò non è ideale in quanto il dial-peer 0 dispone di funzionalità limitate e può causare problemi con le chiamate. L'outlier a questo è il protocollo SCCP e MGCP che non usano i dial-peer per instradare le chiamate. Per ulteriori informazioni, vedere la sezione [MGCP e SCCP](#).

funzionalità dial-peer 0

- Nessun meccanismo di relay dtmf.
- Sono stati annunciati tutti i codec voce per le chiamate VoIP.
- Velocità fax per voce.
- Rilevamento attività voce (VAD) abilitato.

- Nessun supporto RSVP.
- Nessun supporto per applicazioni IVR per chiamate POTS.
- Direct-inward-dial abilitato.
- VRF non è supportato.

## Corrispondenza Dial-Peer In Uscita

I dial-peer in uscita vengono utilizzati per indirizzare le chiamate POTS o VoIP dal gateway all'agente di chiamata successivo. Analogamente alla corrispondenza dial-peer in ingresso, esiste un elenco di elementi che il gateway può utilizzare per individuare i dial-peer in base all'ordine di preferenza per il protocollo specifico. Tuttavia, a differenza dei dial-peer in ingresso, se non è disponibile alcun dial-peer in uscita idoneo per instradare la chiamata, la chiamata ha esito negativo. Come la corrispondenza dial-peer in entrata, la ricerca viene eseguita in tutti i dial-peer in base ai primi criteri di corrispondenza. Il gateway passa ai criteri successivi solo se non viene trovata alcuna corrispondenza.

Tabella 4. Preferenza selezione dial-peer SIP in uscita

Preferenza	Criteri di corrispondenza	Comandi Dial-peer
1	Dial-Peer Group Dial-Peer	dpg di destinazione <tag-dpg> (DPG configurato sul dial-peer in entrata)
2	URI criterio di provisioning dial-peer	uri-from di destinazione <uri-tag> uri-to <uri-tag> di destinazione uri-via di destinazione <uri-tag> diversione uri di destinazione <uri-tag> uri-referring-by di destinazione <uri-tag> (DPP configurato su dial-peer in entrata)
3	Stringa route ILS	destination route-string <tag-string-route>
4	URI e Carrier-ID	URI di destinazione <uri-tag> AND carrier-id target <string>
5	Numero chiamato e ID vettore	destination-pattern <stringa-numero> AND carrier-id target <stringa>
6	URI	uri di destinazione <uri-tag>

7	Numero chiamato	destination-pattern <numero-DNIS> destination-e164-pattern-map <numero-mappa-pattern> dnis-map <numero-mappa-dnis>
8	Numero chiamante	destinazione chiamata e164-pattern-map <pattern-map-number>

Tabella 5. Preferenza selezione dial-peer H323 in uscita

Preferenza	Criteri di corrispondenza	Comandi Dial-peer
1	Dial-Peer Group Dial-Peer	dpg di destinazione <tag-dpg> (configurato su dial-peer in entrata)
2	URI e Carrier-ID	URI di destinazione <uri-tag> AND carrier-id target <string>
3	Numero chiamato e ID vettore	destination-pattern <stringa-numero> AND carrier-id target <stringa>
4	URI	uri di destinazione <uri-tag>
5	Numero chiamato	destination-pattern <stringa-numero> destination-e164-pattern-map <numero-mappa-pattern> dnis-map <numero-mappa-dnis>
6	Numero chiamante	destinazione chiamata e164-pattern-map <pattern-map-number>

Tabella 6. Preferenza selezione dial-peer POTS in uscita

Preferenza	Criteri di corrispondenza	Comandi Dial-peer*
1	Dial-Peer Group Dial-Peer	dpg di destinazione <dpg-tag>(configurato sul dial-peer in

		entrata)
2	URI e Carrier-ID	URI di destinazione <uri-tag> AND carrier-id target <string>
3	Numero chiamato e ID vettore	destination-pattern <stringa-numero> E carrier-id target <stringa>
4	URI	uri di destinazione <uri-tag>
5	Numero chiamato	destination-pattern <numero-DNIS>mappa-dnis <numero-mappa>

 Nota: la sezione [Numero di stringhe di chiamata](#) e [URI di chiamata](#) di [peer](#) analizza il modo in cui il gateway valuta un elenco di comandi potenziali per ogni riga di criteri di corrispondenza prima di passare ai criteri di corrispondenza successivi. Ad esempio, valuta tutte le potenziali corrispondenze del modello di destinazione e i comandi di corrispondenza del modello e164 della destinazione prima di esaminare i comandi del numero chiamante.

## Stringa numerica Dial-Peer Hunting

Preferenza stringa numero:

Analogamente agli URI, che dispongono di un ordine specifico di operazioni per la valutazione delle corrispondenze, esiste anche un insieme di regole utilizzate per la valutazione di una stringa numerica di cifre. Lo schema di ricerca dial-peer predefinito per un gateway Cisco è impostato su 0. Il gateway cerca quindi un modello con la corrispondenza più lunga (più specifica). Se esistono due peer di connessione con la stessa lunghezza, il gateway considera la preferenza del peer di connessione definita in modo esplicito. Infine, se entrambi sono uguali, ne sceglie uno in ordine casuale.

Per la configurazione sono disponibili altri schemi di ricerca dial-peer. Tuttavia, la maggior parte delle distribuzioni mantiene il valore predefinito 0.

 Suggerimento: se i dial-peer vengono abbinati al di fuori dell'ordine predefinito, un amministratore può esaminare la configurazione in esecuzione per uno schema di risposta dial-peer non predefinito.

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.

L'algoritmo dial-peer della stringa di numeri di corrispondenza più lunga trova il dial-peer con il maggior numero di numeri in una sequenza che corrisponde esattamente a una sequenza di numeri in una stringa di numeri. Questo concetto è chiarito nello scenario successivo.

Scenario: sono stati configurati peer di composizione idonei con queste possibili corrispondenze e il gateway sta valutando una stringa di cifre del 2001. Dial-peer 1 può corrispondere a qualsiasi numero compreso tra 2000 e 2999, mentre dial-peer 2 può corrispondere a 2000 e 2009. Dial-Peer 2 verrebbe abbinato per questa chiamata poiché è la corrispondenza più lunga (più specifica) per la stringa numerica 2001 quando viene utilizzato il meccanismo di caccia dial-peer predefinito (dial-peer hunt 0). In altre parole, la sequenza di numeri 200 è la sequenza più grande che corrisponde esattamente a una sequenza di numeri nella stringa di numeri 2001.

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

Per preferenza si intende il peso definito dall'amministratore per ogni dial-peer. Gli amministratori possono configurare una preferenza in modo che la chiamata utilizzi sempre un dial-peer specifico prima degli altri. Per impostazione predefinita, tutti i peer della connessione remota hanno la preferenza 0. Un dial-peer con preferenza 0 viene abbinato a un dial-peer con preferenza da 1 a 10. La maggior parte degli amministratori imposta più peer di chiamata per inviare una chiamata a un sottoscrittore CUCM specifico con un sottoscrittore di backup o un altro agente di chiamata configurato utilizzando un altro peer di chiamata con una preferenza inferiore (configurato con un numero più alto).

Scenario: due dial-peer configurati con la stessa lunghezza di corrispondenza per la stringa di cifre del 2001. L'amministratore definisce una preferenza esplicita. Il gateway valuta entrambi i peer di composizione allo stesso modo, poiché la lunghezza della corrispondenza è la stessa. Tuttavia, l'amministratore imposta il dial-peer 1 con una preferenza maggiore in modo che il dial-peer venga scelto come primo dial-peer utilizzato per il routing della chiamata. Dial-Peer 2 rimane come opzione secondaria se si verifica un errore sul primo dial-peer.

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

Un gateway Cisco tenta di indirizzare una chiamata solo tramite un dial-peer in uscita idoneo alla volta. Se si verifica una condizione di errore sul primo dial-peer selezionato, il gateway tenta di indirizzare la chiamata verso l'esterno del dial-peer successivo idoneo. L'operazione continua finché la chiamata non riesce o non riesce perché non sono più disponibili peer idonei da provare. Un sintomo comune della caccia e del fallimento di dial-peer è un notevole ritardo nella richiamata durante le chiamate. I debug sono in genere necessari per verificare esattamente il motivo per cui la chiamata non riesce su un determinato dial-peer. Il comando `huntstop` può essere utilizzato su un dial-peer se un amministratore non desidera che un gateway cerchi un altro dial-peer quando si verifica una condizione di errore.

Scenario: due dial-peer configurati con la stessa lunghezza di corrispondenza per la stringa di cifre del 2001. L'amministratore ha definito una preferenza esplicita e non desidera trovare una corrispondenza con il dial-peer 2 per questa chiamata specifica. Poiché esistono due peer di composizione con la stessa lunghezza di corrispondenza, la preferenza viene utilizzata per determinare il peer di composizione. Dial-Peer 1 ha il numero di preferenza configurato più basso, quindi viene utilizzato per instradare la chiamata. Se si verifica una condizione di errore nella coda di chiamata in uscita utilizzando il dial-peer 1, il gateway interrompe immediatamente la ricerca del dial-peer poiché il comando `huntstop` è configurato. In questo scenario, il dial-peer 2 non viene mai utilizzato per il routing in uscita.

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

---

 Nota: i comandi `huntstop` e `preferred` possono essere utilizzati anche insieme alle istruzioni `URI matching` in quanto sono comandi generali di configurazione dial-peer. Inoltre, le configurazioni dei gruppi di server di classe voce possono utilizzare i comandi `huntstop` della versione 17.4.1a. Per ulteriori informazioni, consultare la sezione `Gruppi di server di destinazione`.

---

## URI Dial-Peer Hunting

Il gateway esamina ogni criterio di corrispondenza e lo esaurisce prima di passare al criterio di corrispondenza successivo. Un esempio potrebbe essere in una chiamata SIP in ingresso. In base alla [tabella 1. Preferenza selezione Dial-Peer SIP in entrata](#), la prima cosa che il gateway Cisco controlla è l'URI e valuta tutti i potenziali comandi URI per trovarne uno adatto. Se non esiste alcuna corrispondenza o se non ne è stata configurata alcuna, il gateway passa all'elemento corrispondente successivo ed esegue una valutazione su tale criterio. Questo processo viene ripetuto fino a quando la chiamata viene instradata in base a una corrispondenza o fino a quando il gateway non supera i criteri di corrispondenza da controllare.

Quando un dial-peer in entrata o in uscita è configurato con un comando URI, il gateway esamina l'URI ricevuto in più intestazioni per individuare una potenziale corrispondenza. La preferenza di corrispondenza si basa sulla corrispondenza più specifica e la preferenza esatta è Corrispondenza URI completo, Porzione host, Porzione utente o URI telefono. La conoscenza dell'ordine delle operazioni per la corrispondenza URI può semplificare notevolmente la corrispondenza dial-peer con le distribuzioni SIP e CUBE.

Questo ordine di preferenza può essere modificato utilizzando il comando `voice class uri sip preferenza` per specificare l'id utente come prima opzione anziché l'host.

Preferenza URI:

1. Parte host dell'URI. Esempi: (@a.b.c.d o @host.domain.name)
2. Parte User dell'URI. Esempi: (sip:8675309 o sip:user)
3. Il tele-uri. Esempio: (tel:18005532447)
4. Corrispondenza esatta per l'URI completo. Esempi: (user@host.domain.name, user@a.b.c.d, 8675309@host.domain.name, 8675309@host.domain.name)

Documento di supporto: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

Scenario: un amministratore ha configurato questi peer di connessione remota e invia una chiamata al gateway. L'intestazione Da nell'invito ricevuto è Da: <sip:testuser@10.10.10.10>. Il gateway può potenzialmente corrispondere a due dial-peer diversi in base a questa intestazione. Dial-Peer 1 basato sulla parte utente e dial-peer 2 basato sulla parte host. Tuttavia, poiché una corrispondenza host è una preferenza rispetto a una corrispondenza utente, il dial-peer 2 viene utilizzato per il dial-peer in ingresso nella chiamata.

```
!  
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
!
```

## URI classe voce

La corrispondenza URI per i dial-peer in entrata e in uscita consente a un amministratore di poter eseguire le corrispondenze su più di una stringa di numero di telefono per i protocolli VoIP che supportano gli URI nei messaggi. Nelle versioni precedenti a IOS 15.4(1)T e IOS-XE 3.11S, l'URI della richiesta doveva contenere un user@host alfanumerico, altrimenti un gateway Cisco rifiutava la chiamata con un messaggio 4xx. Ora un URI può contenere solo la parte host e il gateway instrada la chiamata solo in base all'host fornito. Ad esempio, sip:cisco.com.

Inoltre, prima di IOS 15.4(1)T e IOS-XE 3.11S, gli ID utente degli URI della classe vocale potevano essere solo valori numerici e.164 (sip:1234@host.com). La modifica è stata apportata in modo che gli amministratori possano configurare gli ID utente alfanumerici su CUBE (sip:user@host.com).

La parte host o utente di un URI di classe vocale può contenere espressioni regolari (regex) pattern che espandono notevolmente i valori che è possibile associare.

```
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\|@;:=%!\~\/()]*+^$&?#--.)*$
```

## Esempio: URI classe voce

```
!
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(.*)
!

```

Come mostrato nell'esempio, per ogni URI di classe voce è possibile configurare solo 10 host, 1 modello o 1 ID utente. Se è necessario abbinare più elementi, si consiglia di utilizzare Regex.

```

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
```

## Corrispondenza Dial-Peer URI in entrata

Questa funzionalità è stata aggiunta in IOS 15.1(2)T e IOS-XE 3.8S e utilizza un URI di classe voce configurato e applicato a un dial-peer in entrata. L'URI in ingresso è stato adottato da molte persone tramite l'istruzione call-number tradizionale in ingresso per le chiamate SIP, in quanto è stato verificato il primo criterio di corrispondenza durante la selezione dei dial-peer in ingresso. Il comando consente inoltre agli amministratori di stabilire una corrispondenza migliore tra le chiamate provenienti da un determinato agente di chiamata o utente.

Documentazione completa: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

## Casi di utilizzo comuni

1. Corrispondenza dial-peer in entrata nella parte host dell'URI per rispondere alle richieste ping OPTIONS da CUCM.
2. Corrispondenza dial-peer in entrata nella parte host dell'URI per controllare le chiamate in entrata da un provider di servizi di telefonia Internet (ITSP)
3. Corrispondenza dial-peer in entrata nella parte user-id dell'URI per il trattamento delle chiamate da parte di determinati utenti o numeri.

## Esempio di configurazione

In questo output di esempio viene trovata una corrispondenza tra dial-peer 777 e qualsiasi richiesta SIP proveniente dai due IP HOST definiti nell'URI della classe voce. L'intestazione controllata è definita come l'intestazione From sul dial-peer; tuttavia, un amministratore può definirne molte altre, tra cui VIA, TO e REQUEST (Request URI). Se il CUCM invia un ping OPTIONS al CUBE ora corrisponde a dial-peer 777 e l'origine my 200 OK risponde alle OPZIONI dall'interfaccia specificata. Se CUCM invia un invito al CUBE corrisponde a dial-peer 777 come dial-peer in entrata.

```
!
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
```

!

## Corrispondenza Dial-Peer URI in uscita

I gateway Cisco IOS possono far corrispondere un dial-peer in uscita utilizzando un URI applicando un URI di classe voce a un dial-peer in uscita e aggiungendo l'URL del call-route alla configurazione globale. Quando questo è presente, il CUBE può tentare di instradare le chiamate in base all'URI della richiesta. Questa funzione è stata aggiunta in IOS 12.3(4)T ed è presente in tutte le versioni di IOS XE. Si noti che per impostazione predefinita l'URI di richiesta SIP in uscita e l'URI di intestazione A hanno la destinazione di sessione del dial-peer in uscita. Questa condizione può essere disabilitata utilizzando il comando request-pass che consente al gateway di passare la parte host URI inclusa nella gamba all'uscita invece di sostituire la parte host URI con la parte target della sessione. Il comando quri-pass è stato aggiunto nella versione 15.4(1)T e IOS XE 3.11S.

## Esempio di configurazione

```
voice service voip
  sip
    call-route url
    request-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
!
```

Fonte: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

Oltre all'URI della classe vocale, gli amministratori possono utilizzare un dial-peer provision-policy (DPP) per far corrispondere un URI interno per una corrispondenza dial-peer in uscita. Questa funzione è stata aggiunta in IOS 15.4(2)T e IOS XE 3.12S. Un criterio di provisioning dial-peer richiede la definizione di un attributo di corrispondenza primario con un attributo di corrispondenza secondario facoltativo. Il criterio di provisioning viene applicato a un dial-peer in ingresso e quando tale dial-peer viene selezionato per l'utilizzo in una call-leg in ingresso, viene richiamato. Il risultato è una selezione dial-peer in uscita basata sull'attributo del criterio di provisioning dial-peer.

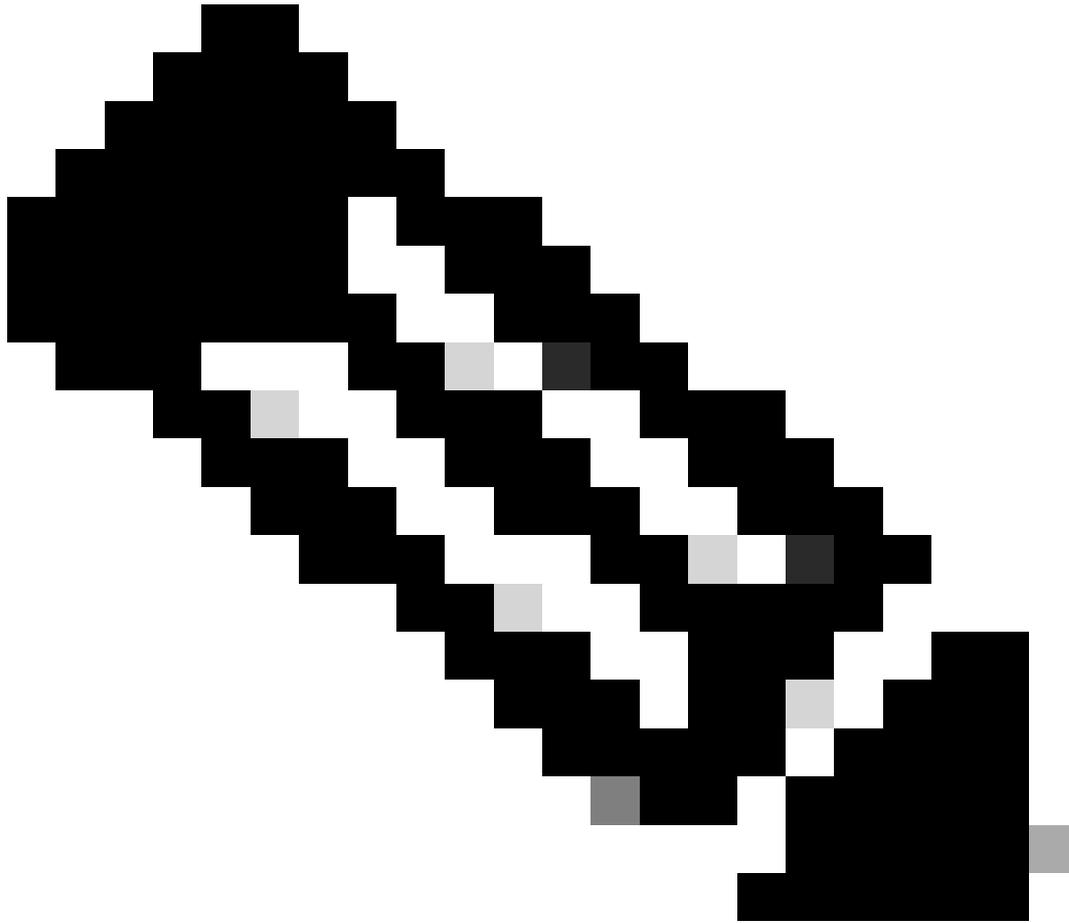
La corrispondenza in uscita può essere costituita da una singola intestazione o da più intestazioni, tutte vere per consentire la corrispondenza con il dial-peer.

Nell'esempio, è presente un URI di classe vocale per le intestazioni From e To. Per una

corrispondenza OR, viene configurato un criterio di provisioning dial-peer che contiene due preferenze. L'intestazione Da rappresenta la prima preferenza, mentre l'intestazione A rappresenta la preferenza di backup. Dial-Peer 1234 è progettato per applicare i criteri di provisioning per la corrispondenza in ingresso. Vengono quindi generati i dial-peer 1111 e 2222 che applicano rispettivamente i comandi uri-from e uri-to di destinazione. Questi comandi puntano all'URI della classe vocale corrispondente. Per la chiamata, è possibile ricevere l'invito, confrontare dial-peer 1234 e controllare il provision-policy. Il dispositivo può quindi tentare di eseguire il routing sull'intestazione From che corrisponde al dial-peer 1111. Se l'operazione non riesce, è inoltre possibile provare a eseguire il routing sull'intestazione a con 2222.

Nell'esempio viene inoltre descritto come ottenere un E corrispondente alle policy di provisioning dial-peer. Supponendo che venga ricevuto lo stesso invito, è possibile definire due intestazioni in base a una preferenza e applicarle al dial-peer in ingresso.

Ora, quando l'invito viene ricevuto, è possibile verificare la presenza di dial-peer in uscita idonei che soddisfano entrambi i criteri di corrispondenza definiti nel criterio di provisioning. In questo esempio, il dial-peer in uscita deve essere definito sia con l'intestazione TO che con l'intestazione FROM per poter corrispondere. Se uno dei due non è una corrispondenza valida, il dial-peer 12345 non viene utilizzato.



Nota: anche se si sta instradando la chiamata sull'intestazione From, l'invito che lascia il gateway ha ancora l'URI della richiesta originale. È sufficiente utilizzare il criterio di provisioning Dial-peer per trovare una corrispondenza con un dial-peer in uscita e non modificare l'URI della richiesta.

---

Esempio di configurazione:

```
<#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  
!
```

Fonte: [Guida alla configurazione di Cisco Unified Border Element con Cisco IOS XE 17.5](#)

sip-uri destinazione sessione

Nelle versioni precedenti a IOS 15.4(1)T e IOS XE 3.11S, se la parte host di un URI è diversa ma l'utente è lo stesso, sono necessari due dial-peer in uscita distinti.

Dopo questa release, un amministratore può configurare un dial-peer per servire più host per lo stesso utente. Ad esempio, testuser@cisco.com e testuser@webex.com nello stesso dial-peer. L'utilizzo dell'URI sip di destinazione della sessione attiva la risoluzione DNS del dominio dell'URI di richiesta di invito in ingresso e determina dinamicamente l'IP di destinazione della sessione.

Configurazione di esempio:

Il gateway riceve due inviti SIP con queste intestazioni Invite sip:testuser@cisco.com:5060 SIP/2.0 Invite sip:testuser@webex.com:5060 SIP/2.0 Il gateway corrisponde alla richiesta SIP in ingresso di testuser@cisco.com e testuser@webex.com sul dial-peer 1 a causa del comando URI in ingresso e della definizione dell'ID utente che corrispondono entrambi a testuser. Il comando sip call-route url della classe vocale indica che i dial-peer in uscita vengono valutati in base all'URI della richiesta di questo invito in ingresso. La corrispondenza con il dial-peer 2 dipende dagli stessi motivi per cui è stata trovata la corrispondenza con il dial-peer 1, l'ID utente di testuser. La destinazione della sessione di questo peer di connessione remota è l'URI sip originale definito dall'URI sip della destinazione della sessione, che era un nome di dominio completo (FQDN). Dopo una risoluzione DNS e la modifica di cisco.com e webex.com in un IP per il routing di layer 3, si invia un messaggio dal gateway.

```
!  
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  
!
```

Verifica:

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

## Caratteri jolly Dial-Peer

Un amministratore può utilizzare i caratteri jolly dial-peer per definire meccanismi di corrispondenza in entrata e in uscita che implicano una stringa numerica. Tra questi sono inclusi il modello di destinazione, il numero chiamato in ingresso, le mappe modello e164 e l'indirizzo di risposta, nonché il comando prefix. I caratteri jolly dei dial-peer sono espressioni regolari (regex) disponibili per la configurazione che consentono una maggiore flessibilità sulla corrispondenza dei dial-peer.

Tabella con caratteri jolly

Carattere	Definizione	Esempi
*	Su un dial-peer questo è un valore letterale di * (stella) sul tastierino.	12345*
N.	Su un dial-peer questo è un valore letterale di # (libbra) sul tastierino.	8675309#
,	Inserisce una pausa di 1 secondo tra le cifre. È inoltre possibile utilizzare una virgola tra parentesi quadre [ ] per suddividere un intervallo continuo.	9,,,,55591[1-3,5-9]8675309
.	Carattere Regex per la corrispondenza di qualsiasi valore 0-9, A-F e *, #, +  È possibile definire fino a 15 caratteri punto per ogni dial-peer, anche se la CLI consente all'amministratore di configurarne tutti i numeri che ritiene appropriati.  Se sono necessari più di 15 punti, utilizzare T.	2.... 91[2-9]...[2-9].....
%	Regex per la cifra che precede zero o più volte.	
+	Se utilizzato all'inizio di una stringa, significa un valore letterale + utilizzato nei numeri E164.  Se utilizzato in qualsiasi altro punto della stringa, è un valore regex per la cifra precedente che si verifica una o più volte.	+19191112222
?	Regex per la cifra che precede zero o una volta.	(206)?5015111

		(0)?(1)?(1)?21933...
^	<p>Carattere Regex per indicare l'inizio della stringa quando viene utilizzato all'esterno delle parentesi quadre</p> <p>Se utilizzata all'interno di parentesi quadre, viene considerata un'istruzione exclude o DO NO MATCH</p> <p>Nelle versioni più recenti, questa condizione non è più necessaria in quanto il gateway assume automaticamente un ^ quando elabora una stringa regex senza un ^.</p>	<p>^8675309</p> <p>91[^135]55</p>
\$	Carattere Regex per indicare la fine di una stringa.	8675309\$
\	Carattere di escape per indicare un valore letterale	
[ ]	<p>Le parentesi definiscono un intervallo di caratteri per una singola posizione.</p> <p>Per separare le stringhe continue è necessario utilizzare le virgole.</p>	<p>[1-5]0000</p> <p>[2,5-8]0000</p>
( )	Le parentesi definiscono un gruppo di caratteri in un set.	9(258) 7777
T	<p>Corrispondenza di lunghezza variabile fino a 32 cifre.</p> <p>Il router attende il timeout tra le cifre prima di instradare la chiamata.</p> <p>Il valore predefinito per il timeout a intercifre è 10 secondi ed è modificabile tramite timeout a intercifre su una porta voce. Gli amministratori possono interrompere il timeout tra le cifre usando il simbolo # sul tastierino numerico. Questo è modificabile tramite il terminatore dial-peer configurato globalmente.</p> <p>T fa riferimento anche al timer T302.</p>	9011T
-	Utilizzato tra parentesi per definire l'intervallo.	[5-9]1234

Output dal gateway che visualizza i possibili input delle espressioni regolari.

```
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?(\$)?$`

## Stati Dial-Peer

I peer di composizione possono trovarsi in uno dei due stati operativi.

1. Su
2. Giù

Per essere in uno stato operativo valido e utilizzabile con il routing delle chiamate, un dial-peer deve essere nello stato UP. Per i dial-peer VOIP in uscita, ciò significa che possono esistere un meccanismo di corrispondenza in uscita valido e una destinazione di sessione valida per instradare la chiamata verso. Per i dial-peer POTS in uscita, è possibile configurare un meccanismo di corrispondenza in uscita valido e una porta vocale valida. Solo con i dial-peer in ingresso, è necessario configurare un meccanismo di corrispondenza in ingresso valido.

Lo stato busyout viene visualizzato quando un dial-peer è configurato con un meccanismo keepalive e la destinazione remota non ha soddisfatto i parametri di tale meccanismo keepalive. Il gateway quindi sposta il dial-peer in uno stato busyout in modo che non venga più utilizzato per le decisioni di routing delle chiamate e, quando il meccanismo keepalive viene nuovamente soddisfatto, il gateway reimposta il dial-peer in uno stato attivo. Se si seleziona un dial-peer come dial-peer in uscita e questo dial-peer si trova in uno stato busyout, la chiamata del gateway ha esito negativo con un codice causa 188.

Insieme agli stati operativi ci sono stati amministrativi.

1. Su
2. Giù

Un amministratore può disabilitare un dial-peer senza rimuoverlo dalla configurazione immettendo il comando shutdown sul dial-peer. Per riattivare la connessione remota, immettere no shutdown.

---

Nota: un dial-peer con una porta voce inattiva, spenta o non operativa rimane nello stato di operatività Attivo anche se lo stato di Uscita è Inattivo.

---

## Verifica

```
Gateway# show dial-peer voice summary
dial-peer hunt 0
```

TAG	TYPE	AD MIN	OPER	PREFIX	DEST-PATTERN	PRE FER	PASS THRU	SESS-TARGET	OUT 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) e Dial-Peer Hunting

### Corrispondenza Dial-Peer in entrata con VRF

A partire da IOS 15.6(3)M e IOS-XE 16.3.1, i gateway Cisco possono associare i dial-peer in entrata utilizzando gli ID VRF. Per sfruttare questo vantaggio, l'amministratore deve associare il dial-peer in entrata a un'interfaccia che a sua volta associa il dial-peer all'ID VRF sull'interfaccia specificata. Al termine del binding, le chiamate in entrata vengono filtrate dal gateway Cisco in modo da includere solo i dial-peer in entrata idonei che corrispondono all'ID VRF dell'interfaccia su cui è stato ricevuto il pacchetto. Da qui viene eseguita la corrispondenza del dial-peer in ingresso in base all'ordine di corrispondenza delle operazioni del dial-peer normale.

Prima delle versioni IOS / IOS-XE, il gateway Cisco effettuava una selezione in entrata in base alla normale corrispondenza dial-peer in entrata, senza alcun filtro. Questo significa che una chiamata VRF1 può essere associata da un dial-peer VRF2. Inoltre, poiché H323 e SIP supportavano un solo VRF prima di queste versioni, si verificano altri problemi quando si cerca di utilizzare le funzioni multi VRF. L'utilizzo di un singolo VRF per le applicazioni vocali era noto come configurazione compatibile con VRF.

Documentazione completa compatibile con VRF: [H.323 e SIP compatibili con VRF per gateway voce](#)

Documentazione completa relativa a Multi-VRF: [guida alla configurazione degli elementi di frontiera unificati Cisco - Cisco IOS XE versione 17.6 e successive](#)

### Corrispondenza Dial-Peer in uscita con VRF

I gateway Cisco sono in grado di collegare le chiamate attraverso i VRF senza che sia necessario configurare le perdite di routing. Ciò significa che una chiamata in entrata sul VRF1 può essere indirizzata in uscita su un dial-peer per VRF2 se viene soddisfatta la normale selezione di corrispondenza dial-peer in uscita. È possibile utilizzare i gruppi Dial-Peer per forzare il gateway Cisco a mantenere la chiamata all'interno dello stesso VRF.

### Esempio di configurazione di VRF e Dial-Peer Group

Questo esempio di configurazione ha VRF1 e VRF2 con due intervalli IP sovrapposti e due intervalli di numeri telefonici sovrapposti.

Utilizzare il binding VRF per verificare che il dial-peer in entrata corretto corrisponda e i gruppi di dial-peer per verificare che il dial-peer in uscita corretto sia corrispondente. Se un pacchetto SIP per una chiamata a 8675309 arriva in data gig0/0/1.2, il gateway filtra tutti i dial-peer in entrata disponibili in base all'ID VRF2. Ciò significa che non è possibile trovare una corrispondenza con dial-peer 10. Ora, quando si controlla la stringa di cifre, è possibile trovare la corrispondenza dial-peer 20. Dial-peer 20 dispone di un gruppo dial-peer che indica al gateway che l'unico dial-peer in uscita a cui è possibile trovare una corrispondenza è anche dial-peer 20. Questo gruppo di peer di composizione consente di evitare la corrispondenza del peer di composizione 10 e

l'attraversamento di una chiamata proveniente dal VRF1 nel VRF2. Da qui la chiamata può procedere come normale.

```
!  
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  
!
```

Verifica

```
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

## Tecniche avanzate di routing delle chiamate

Con l'aumentare delle esigenze aziendali, l'azienda si espande e necessita di un numero maggiore di DID e gli amministratori aziendali possono rilevare che le connessioni di base non sono in grado di soddisfare adeguatamente le esigenze di scalabilità. Possono esserci situazioni da affrontare, o forse ci sono troppi dial-peer in generale. La disponibilità di migliaia di connessioni peer non semplifica l'amministrazione e la risoluzione dei problemi. La presenza di un dial-peer per ogni server CUCM o agente di chiamata specifico inizia a complicare il problema di troppi dial-peer perché ora un amministratore deve configurare un dial-peer per ogni stringa di cifre. Se esistono più provider SIP che si connettono a un gateway o poche persone diverse che utilizzano lo stesso CUBE, l'isolamento di un tenant specifico è molto difficile.

Cisco ha raccolto questo feedback e ha creato una serie di elementi in grado di risolvere questi problemi e altro ancora. I gruppi Dial-Peer, i tenant della classe vocale, i gruppi di server di destinazione, le mappe e164-pattern e i gruppi di trunk POTS consentono a un amministratore di risolvere tutti i problemi elencati e molti altri non elencati.

## Dial-Peer Group

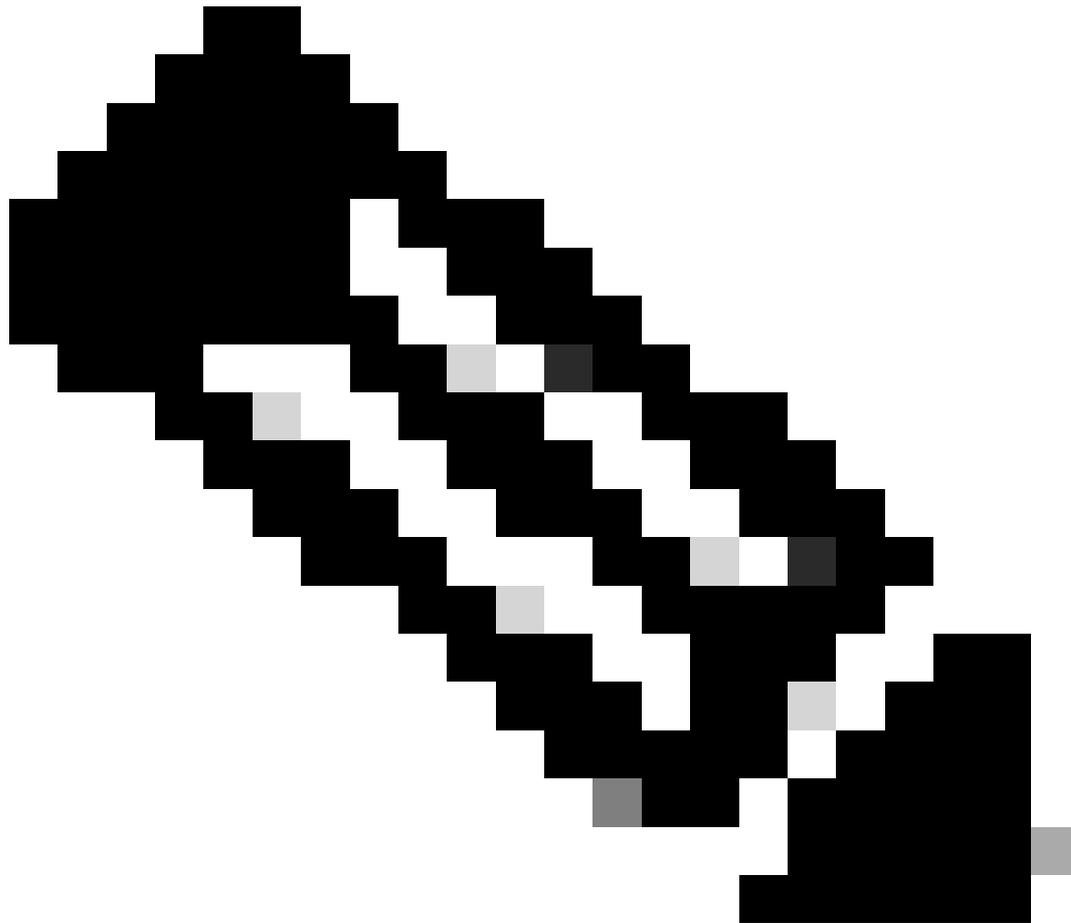
I gruppi di peer di composizione sono stati aggiunti in IOS 15.4(1)T e IOS-XE 3.11S e i peer di composizione POTS sono stati aggiunti come opzione in IOS 15.5(1)T e IOS-XE 3.14S. Un gruppo dial-peer consente agli amministratori di specificare un dial-peer esatto per il routing in uscita in base alla corrispondenza del dial-peer in entrata. Una volta trovata una corrispondenza tra un dial-peer in entrata e un gruppo dial-peer configurato, la chiamata utilizzerà il dial-peer definito nel gruppo dial-peer anche se il modello di destinazione non corrisponde. L'unico prerequisito è che il dial-peer in uscita sia attivo, pertanto è necessario configurare un metodo di corrispondenza in uscita, che tuttavia non viene effettivamente utilizzato per instradare la chiamata.

Il modo migliore per descrivere i gruppi dial-peer è paragonarli al concetto di route statiche in una tabella di routing. Si tratta di decisioni statiche di routing in entrata verso l'uscita che eliminano alcune incertezze relative al gateway in quanto indicano esattamente come instradare la chiamata.

Documentazione completa: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

### Esempio di configurazione

In questo esempio, il numero chiamato è 8675309. Corrisponde a dial-peer 1234 in base all'istruzione call-number in arrivo. Questo dial-peer è configurato con un gruppo dial-peer che indica che la chiamata può ora instradare i dial-peer 2, 3 e infine 1 se il dial-peer 2 ha esito negativo. Il gateway tenta ora di indirizzare la chiamata in uscita dial-peer 2, come è stato esplicitamente detto tramite il gruppo dial-peer che è quello che può fare.



Nota: il modello di destinazione sul dial-peer 1, 2 e 3, non è il numero chiamato 8675309. La procedura è corretta e la chiamata continua a funzionare senza problemi.

---

Tenere presente che, come illustrato nella sezione stati dial-peer, è necessario un elemento configurato come istruzione di abbinamento in uscita. In questo caso, il modello di destinazione prevede solo di portare il dial-peer in uno stato operativo Su e la stringa di cifre di tale comando non viene mai valutata. Si consiglia di configurare un modello come il modello di destinazione AAAA, poiché si tratta di un modello di destinazione valido. Poiché tecnicamente si tratta di un dial-peer valido, è possibile che altre chiamate corrispondano. Pertanto, la stringa di cifre AAAA indica che non può essere utilizzata per scopi diversi da uno scenario specifico che coinvolge un gruppo di dial-peer, in quanto la probabilità di una chiamata in arrivo per AAAA è molto, molto bassa.

```
!  
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
!

```

## Verifica

```

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

## Mappe modello E164

Questa funzionalità consente agli amministratori di ridurre il numero totale di peer di chiamata combinando molte possibili corrispondenze numeriche (modelli di destinazione, numero chiamato in ingresso e così via) in un'unica mappa di schema. Il supporto dial-peer in uscita e164-pattern-map è stato aggiunto in IOS 15.2(4)M e IOS-XE 3.7S, mentre il supporto dial-peer in entrata e164-pattern-map è stato aggiunto in IOS 15.4(1)T e IOS-XE 3.11S.

Un modello e164-map può essere configurato tramite la CLI o preconfigurato e salvato come file .cfg. Il file con estensione cfg viene quindi aggiunto alla memoria flash del gateway e vi viene fatto riferimento durante la configurazione del resto del comando. Il file .cfg può utilizzare 5000 voci.

Le voci in entrambi i metodi di configurazione possono utilizzare tutti i normali caratteri jolly dial-

peer per un'ulteriore aggregazione!

Documentazione completa: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

### Esempio di configurazione CLI - Chiamata di numeri

```
!  
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  
!
```

### Esempio di configurazione CLI - Numero chiamato

```
!  
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  
!
```

### Esempio di configurazione Flash

```
!  
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>
```

## Verifica

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

```
e164-pattern-map 1
```

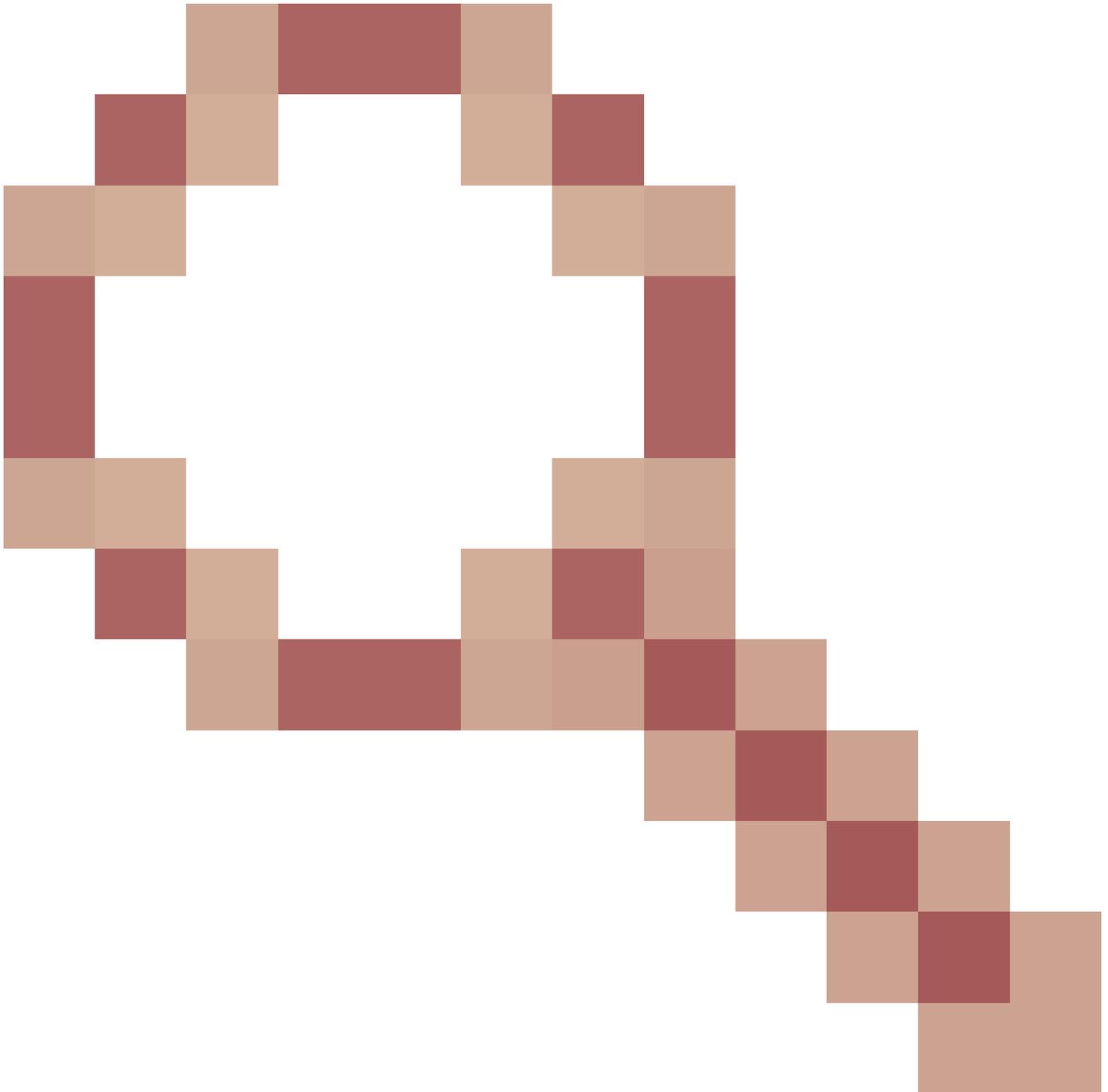
```
-----  
  Description: CUCM phones  
  It has 3 entries  
  It is not populated from a file.  
  Map is valid.
```

```
E164 pattern
```

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

## Difetti rilevanti

L'ID bug Cisco [CSCva64393](https://www.cisco.com/cisco/webbugtool/show_bug.do?bugID=CSCva64393)



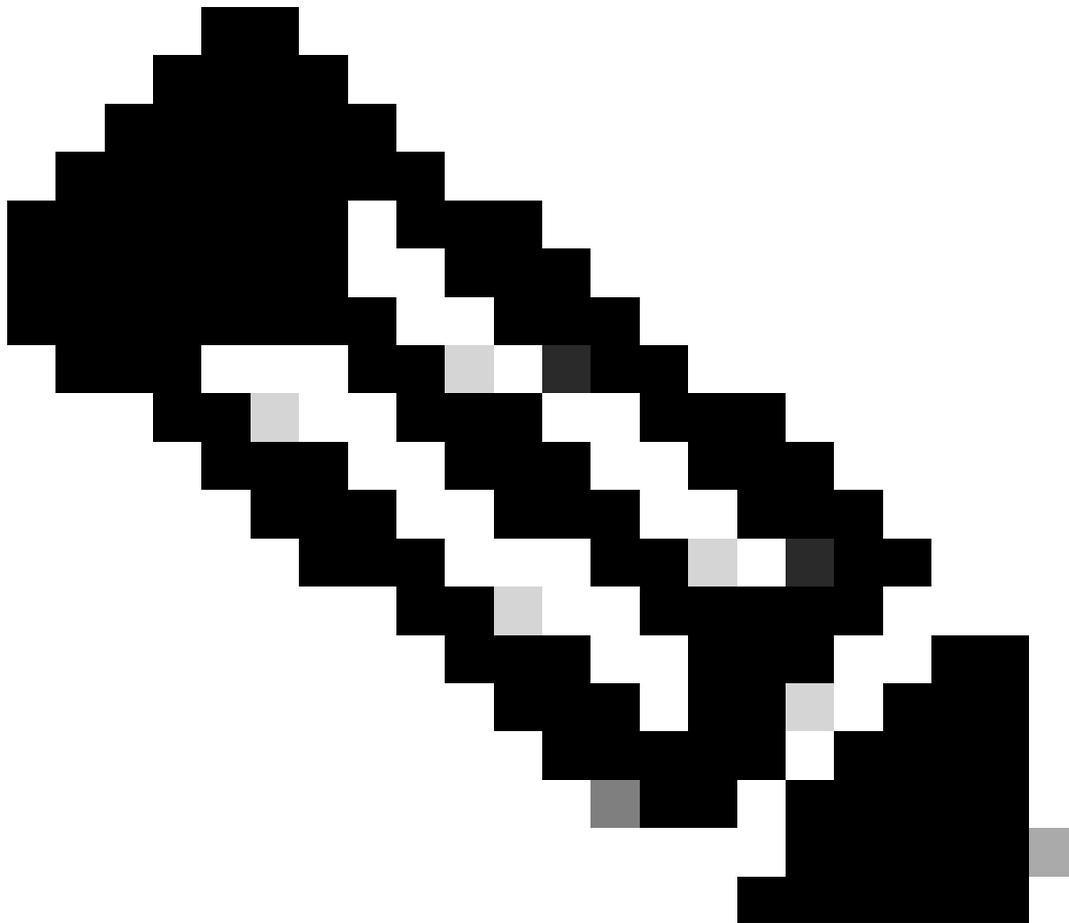
e164-pattern-map non analizza l'ultima riga del file di configurazione.

## Gruppi-server di destinazione

I gruppi di server consentono agli amministratori di configurare più destinazioni (destinazioni sessione) sullo stesso dial-peer VOIP. Per impostazione predefinita, il tipo di ordinamento è quello definito nelle voci relative ai gruppi di server. La caccia round robin può essere utilizzata quando si utilizza il comando hunt-scheme round robin. I gruppi di server sono stati aggiunti in Cisco IOS 15.4(1)T e Cisco IOS XE 3.11S. In Cisco IOS XE 17.4.1a i codici di errore huntstop configurabili sono stati aggiunti alle configurazioni dei gruppi voce-classe server. In altre parole, è possibile configurare un singolo codice di errore, ad esempio 404 Non trovato, e l'errore SIP normalmente attiva il dispositivo per provare l'opzione successiva nel gruppo di server. Con la configurazione huntstop 1 resp-code 404 in posizione all'interno del gruppo di server, la caccia può essere

interrotta. Questi possono anche essere configurati per un intervallo come: huntstop 1 codice di risposta da 401 a 599.

---



Nota: il numero massimo di voci è 5 per gruppo di server.

---

Documentazione completa: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

Esempio di configurazione - Normale

```
!  
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
!
```

## Verifica

```
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..]
```

## Gruppo server di destinazione e OPZIONI attive

Tenere presente che i gruppi di server non seguono i normali meccanismi OUT-OF-DIALOG OPTIONS Keepalive. Utilizzano una feature denominata profilo option-keepalive. In questo modo il gateway può monitorare ogni agente di chiamata definito nello specifico gruppo di server.

Esempio di opzione-keepalive con il gruppo di server

```
!
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
!
```

## Verifica

<#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
```

## Proxy in uscita

La configurazione del proxy in uscita SIP può essere aggiunta alle configurazioni voip del servizio vocale, del tenant della classe vocale o del dial-peer per specificare la destinazione di un pacchetto SIP di layer 3.

In altre parole, la destinazione della sessione su un dial-peer può essere utilizzata per creare il pacchetto SIP, ma il proxy in uscita può essere il luogo in cui il pacchetto viene inviato al layer 3.

```
!  
voice service voip  
  sip  
    outbound-proxy dns:1a01.sipconnect-us10.cisco-bc1d.com  
!  
voice class tenant 100  
  outbound-proxy dns:1a01.sipconnect-us10.cisco-bc1d.com  
!  
dial-peer voice 100 voip  
  session target ipv4:192.168.1.1  
  voice-class sip outbound-proxy dns:1a01.sipconnect-us10.cisco-bc1d.com  
!
```

È possibile notare che la configurazione predefinita per un dial-peer è il sistema proxy sip in uscita di classe vocale che può far sì che un dial-peer utilizzi la configurazione voip > sip del servizio vocale globale.

Questo comportamento può essere disattivato e forzare un dial-peer a eseguire il fallback e utilizzare la destinazione della sessione come destinazione di layer 3 per dial-peer con questa configurazione:

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

## Gruppi trunk POTS

Trunk Group è un insieme di porte vocali fisiche con funzionalità di segnalazione simili. Questa funzionalità può essere utilizzata per ridurre il numero totale di dial-peer POTS da configurare. I gruppi trunk sono stati introdotti in IOS nella versione 12.1(3)T e sono presenti in tutte le versioni di Cisco IOS XE.

Documentazione completa: [miglioramenti di Gateway Trunk e Carrier Based Routing](#)

### Esempio di configurazione

```
!
trunk group PSTN
  description PSTN voice-ports
!
trunk group FX0
  description FX0 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 FX0 1
!
voice-port 0/2/3
  trunk-group FX0 2
!
dial-peer voice 1234 pots
  trunkgroup PSTN 1
  trunkgroup FX0 2
!
```

## Tenant classe voce

Cisco IOS 15.6(2)T e Cisco IOS XE 16.3.1 hanno introdotto i tenant di classe vocale che consentono a ciascun tenant di avere le proprie configurazioni individuali. Un tenant può essere un provider di telefonia, Cisco Unified Communications Manager (CUCM) o qualsiasi altro agente

di chiamata di terze parti per il quale un amministratore desidera disporre di impostazioni globali specifiche. In primo luogo, un amministratore crea un tenant della classe vocale e definisce i parametri. Il tenant della classe vocale viene quindi applicato allo specifico dial-peer o alla scelta. Questa nuova configurazione offre agli amministratori un altro livello di controllo sulle chiamate oltre ai dial-peer e alla configurazione globale.

Con la versione 17.8.1a, le configurazioni Voice Class Tenant possono essere configurate con un comando sip-Listen (insieme al comando SIP control binding appropriato) per definire la porta non protetta o protetta del tenant. Ciò significa che il tenant 1 può ascoltare il SIP non sicuro su UDP 5060 + VRF Red mentre il tenant 2 ascolta il SIP su TCP TLS 5070 + VRF Blue. Dopo aver stabilito una corrispondenza con il tenant in base alla porta di ascolto + bind + vrf opzionale, i dial-peer in ingresso vengono filtrati in base a quelli a cui è applicato il tenant.

Documentazione completa: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

Ordine di preferenza dei comandi normale senza tenant

1. Comando Dial-peer
2. Comando globale (voice service voip e sip-ua)

Ordine di preferenza comando con tenant

1. comando Dial-peer
2. Tenant, comando
3. Comando globale (voice service voip e sip-ua)

Esempio di configurazione multi-tenant

Hai due affittuari, 777 e 999. Sono state configurate con configurazioni leggermente diverse e applicate ai dial-peer. Ciò significa che le chiamate che utilizzano i diversi dial-peer dispongono delle configurazioni basate sul dial-peer e delle configurazioni specifiche del tenant. Le opzioni elencate sono solo un frammento della potenza dei tenant della classe vocale. Fare riferimento alla documentazione per vedere cosa può essere configurato su un tenant. È consigliabile utilizzare meccanismi di corrispondenza rigidi, ad esempio l'URI della classe vocale o l'assegnazione di tag ai numeri con determinate stringhe di numero, per separare la corrispondenza dial-peer del tenant oppure configurare i VRF in modo che il tenant A non si sovrapponga mai al tenant B e che corrisponda involontariamente a un dial-peer che non è in grado di individuare.

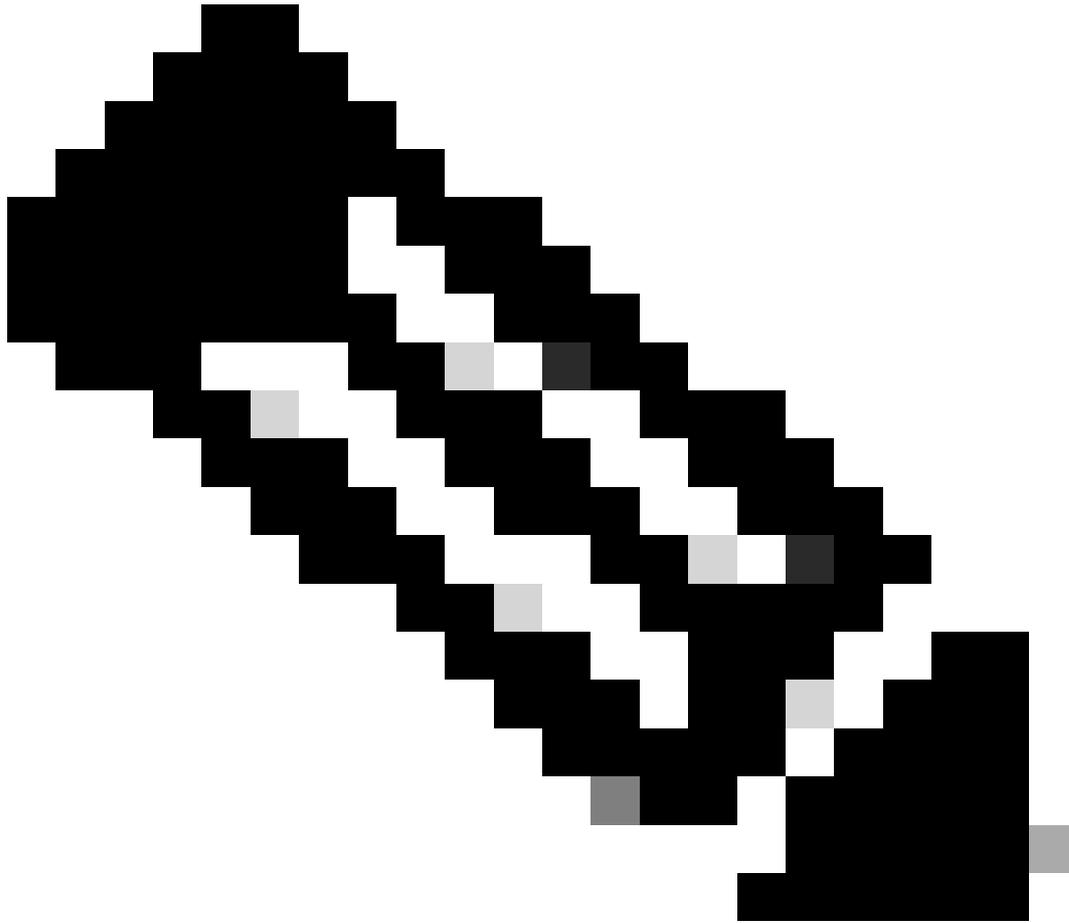
```
!  
voice class tenant 999  
  asymmetric payload full  
  bind control source-interface GigabitEthernet0/0/0.228  
  bind media source-interface GigabitEthernet0/0/0.228  
  g729 annexb-all  
!  
voice class tenant 777  
  sip-server ipv4:192.168.1.2  
  bind control source-interface Loopback0
```

```
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
!
```

## Verifica

Al momento non sono disponibili comandi singoli per visualizzare le configurazioni del tenant della classe vocale. Questo comando può essere sufficiente per filtrare la configurazione in esecuzione in base alle sole informazioni sul tenant.

```
show run | sec tenant
```



Nota: l'ID bug Cisco [CSCvf28730](#) è questo: il comando show sip-ua register status non riflette lo stato della registrazione trunk SIP su un tenant di classe voce.

---

## Chiamate URI ILS a CUBE (Voice Class Route-String)

Le stringhe di route vengono utilizzate con il servizio di ricerca intercluster (ILS) CUCM e possono essere configurate in modo da consentire ai gateway Cisco di instradare le chiamate VoIP tramite la stringa di instradamento inclusa nell'invito SIP ricevuto da un CUCM 9.5+ che esegue il servizio ILS. Questa funzione è stata aggiunta in Cisco IOS 15.3(3)M e Cisco IOS XE 3.10S. La maggior parte delle connessioni ILS è CUCM a CUCM e gli amministratori non si preoccupano di utilizzare un CUBE per il trunking intercluster. Tuttavia, se è necessario eseguire la funzione con CUBE al centro, le opzioni sono disponibili. Per inviare l'intestazione X-cisco-dest-route-string a CUBE, CUCM deve avere l'impostazione Send ILS Learned Destination Route String abilitata sul profilo SIP applicato al trunk SIP

Documentazione completa: [Guida alla configurazione dell'interoperabilità delle applicazioni aziendali per H.323-to-SIP e SIP-to-SIP, Cisco IOS release 15M&T](#)

## Esempio di configurazione 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-passthru-list 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  
!
```

### Verifica

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

## Tecniche di routing delle chiamate legacy

Gli elementi trattati in questa sezione sono considerati tecniche precedenti. Anche se la capacità di configurare questi comandi è ancora presente in un Cisco Gateway, si consiglia di non utilizzarli nelle configurazioni moderne. Nel documento vengono illustrati solo i problemi riscontrati durante l'utilizzo di configurazioni legacy o durante l'esecuzione di aggiornamenti.

### Mappa DNIS

Le mappe DNIS potrebbero essere considerate il precursore di quella che ora sarebbe una mappa modello E164. Le mappe DNIS sono state aggiunte a Cisco IOS nella versione 12.2(2)XB e sono sempre esistite in Cisco IOS XE.

Se sono state configurate mappe DNIS, sarebbe opportuno convertirle nella più affidabile funzionalità mappa modello e164.

Sintassi dei comandi: [Cisco IOS Voice Command Reference - Da D a I](#)

Esempio di configurazione

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

## Etichette gruppi trunk

Le etichette dei gruppi di trunk sono state aggiunte in Cisco IOS versione 12.2(11)T ed esistono in tutte le versioni di Cisco IOS XE. Lo scopo di un'etichetta trunk-group-label è simile a un Carrier-ID nel senso che può essere utilizzato per aumentare la corrispondenza dei peer di composizione. Questa opzione è disponibile per la configurazione nei gruppi di trunk POTS, nei dial-peer VOIP e POTS e nei gruppi di origini voce. L'uso delle etichette dei gruppi di trunk è raramente visibile nelle moderne configurazioni di Cisco Gateway.

Sintassi dei comandi: [Cisco IOS Voice Command Reference - Da T a Z](#)

Esempio di configurazione

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

## Tipo di numerazione

Le integrazioni ISDN Q.931 consentono di individuare un dial-peer in base al numero chiamante o chiamato e al tipo di numero ITU specifico del messaggio Q.931 SETUP. Questa operazione è configurabile tramite il comando number-type su un dial-peer VOIP o POTS. Il tipo di numerazione non può essere utilizzato da solo e deve essere utilizzato insieme al modello di destinazione, all'indirizzo di risposta o al numero chiamato in ingresso. Ciò significa che la condizione dell'istruzione di corrispondenza in entrata/in uscita e il tipo di numero devono corrispondere affinché il dial-peer venga considerato per il routing delle chiamate in entrata e in uscita.

La numerazione può essere considerata come un meccanismo di filtro dial-peer piuttosto che

come un meccanismo di corrispondenza. Ciò è dovuto al fatto che un dial-peer con e senza un comando di numerazione applicato è considerato lo stesso peso predefinito delle preferenze se non viene applicata alcuna preferenza dell'amministratore. Ciò è diverso da carrier-id che, se applicato a un dial-peer insieme ad altri meccanismi di corrispondenza, aggiunge la preferenza a quel dial-peer rispetto ad altri se entrambe le condizioni sono vere.

La corrispondenza del tipo di numerazione è stata aggiunta in Cisco IOS 12.0(7)XR1 ed è presente in tutte le versioni di Cisco IOS XE. Con il declino delle linee ISDN POTS tradizionali implementate nelle reti di collaborazione, l'uso della numerazione è raramente visto nelle implementazioni moderne.

Sintassi dei comandi: [Cisco IOS Voice Command Reference - Da K a R](#)

### Esempio di configurazione

Questo dial-peer può corrispondere da 4085150000 a 4085159999 solo se il tipo di numero ISDN è National.

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

Tipi di numero possibili:

Abbreviato	Rappresentazione abbreviata del numero completo supportato dalla rete
Internazionale	Numero chiamato per raggiungere un sottoscrittore in un altro paese
Nazionale	Numero chiamato per raggiungere un utente nello stesso paese, ma all'esterno della rete locale
Rete	Numero amministrativo o di servizio specifico della rete servita
Reserved	Riservato per estensione
Sottoscrittore	Numero chiamato per raggiungere un sottoscrittore nella stessa rete locale

Sconosciuto	Tipo di numero sconosciuto dalla rete
-------------	---------------------------------------

## Dial-Peer Data

I peer di connessione dati sono stati introdotti in Cisco IOS versione 12.2(13)T e l'uso di tali peer di connessione è stato previsto per le chiamate di modem dati in ingresso su un gateway Cisco. Questo dial-peer deve essere utilizzato solo nella direzione in entrata e raramente nelle distribuzioni moderne.

Sintassi dei comandi: [Cisco IOS Voice Command Reference - Da D a I](#)

### Esempio di configurazione

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

## Voice Source-Group

Questa funzionalità è stata aggiunta nella versione 15.1(2)T ma non è implementata in molte distribuzioni moderne. In genere vengono distribuiti altri metodi di protezione per IOS/CUBE.

La panoramica sulla sicurezza delle applicazioni CUBE è disponibile in questo white paper a partire dalla sezione 4.2.

[Specifiche di gestione e gestibilità CUBE \(Cisco Unified Border Element\)](#)

Sintassi dei comandi: [Voice Source-Group Feature](#)

## Autorizzazioni Dial-Peer

Questa configurazione consente a un amministratore di limitare un dial-peer per consentire solo le connessioni in entrata (termine / terminazione) o in uscita (origine / origine). È possibile configurare in modo esplicito un dial-peer in entrata da utilizzare solo per le chiamate in entrata e un dial-peer in uscita per le chiamate in uscita. L'impostazione predefinita per qualsiasi dial-peer prevede sia la connessione in entrata che quella in uscita. Questa CLI non viene spesso implementata nelle implementazioni moderne.

```
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
```

## Manipolazione dell'URI e della cifra

In un determinato momento di un'implementazione di tipo collaborativo può essere necessario che un amministratore modifichi le cifre o un'intestazione URI/SIP. I gateway Cisco dispongono di numerosi metodi per la manipolazione delle cifre che consentono a un amministratore di avere un controllo completo su come e quando una cifra può essere manipolata. Tuttavia, non è sempre facile e alcune persone si trovano sopraffatte dalle diverse opzioni o l'amministratore non sa che un'opzione esiste.

## Manipolazione della cifra tramite Dial-Peer POTS

I dial-peer POTS dispongono di alcune tecniche di manipolazione delle cifre esclusive che i dial-peer VOIP non possiedono.

Il primo è lo stripping di cifre giustificate a sinistra definite in modo esplicito in un modello di destinazione. È possibile disabilitare questa funzione usando il comando no digit-strip sul dial-peer POTS.

Esempio:

Nell'esempio, 9011T viene definito come la stringa per il modello di destinazione.

Con questa configurazione è possibile ricevere una chiamata per 90113227045555. In questo modo viene trovata una corrispondenza con il dial-peer per il routing delle chiamate in uscita e le cifre 9011 definite in modo esplicito vengono eliminate prima che la chiamata venga instradata alla porta vocale.

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

Nell'esempio viene mostrata una configurazione senza digit-strip.

Se si chiama lo stesso numero, viene inviato il 9011 .

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

```
no digit-strip
```

```
!
```

Il secondo consiste nella possibilità di specificare il numero di cifre che si desidera inoltrare sul dial-peer POTS.

Si prenda questo esempio dove si riceve una chiamata per 918005532447 da CUCM. In questo caso, rimuovere il 9, ma inviare il resto del numero a partire dal 1.

Se si configura il comando forward-digits sul dial-peer POTS, è possibile specificare esattamente il numero di cifre inviate.

```
!
```

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

```
!
```

Infine, i dial-peer POTS possono usare il comando prefix per aggiungere cifre a una chiamata prima di indirizzare la porta voce. In questo esempio viene eliminato il prefisso 91 e 007 dal numero definito in modo esplicito prima di inviare la chiamata alla porta vocale.

```
!
```

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

```
!
```

## Manipolazione della cifra tramite regole e profili di conversione vocale

Le regole di conversione vocale sono espressioni regolari (regex) utilizzate per trasformare le cifre. Le regole di conversione e i profili sono stati aggiunti a Cisco IOS nella versione 12.0(7)XR1. Una regola di conversione viene applicata ai profili di traduzione vocale che vengono quindi applicati a un dial-peer o a una porta vocale. Le regole di conversione contengono un input di corrispondenza e un output di modifica. Insieme all'input di corrispondenza sul numero, c'è una corrispondenza e un input di modifica per il piano e il tipo ISDN. La combinazione di stringa numerica, piano e tipo è considerata una corrispondenza. Ciò significa che tutti gli input corrispondenti definiti devono essere veri affinché la traduzione abbia luogo.

Le regole di conversione possono modificare le chiamate, le chiamate, le chiamate di reindirizzamento, le destinazioni di reindirizzamento e i numeri di richiamata nei protocolli di segnalazione ISDN, SIP e H323. Le regole di conversione corrispondono in base a una ricerca

top-down, pertanto l'ordine delle regole è della massima importanza. Se viene trovata una corrispondenza in una regola superiore, il gateway interrompe immediatamente la ricerca ed elabora la traduzione. Le regole di conversione non possono modificare intestazioni SIP non numeriche, ad esempio testuser@10.10.10.10. Per questa manipolazione, utilizzare un profilo SIP.

Le regole di transizione possono essere utilizzate per bloccare le chiamate sui gateway Cisco.

#### Preferenza di selezione profilo di traduzione

1. Profilo di conversione vocale in ingresso sulla porta vocale
2. Profilo di conversione della voce in arrivo sul gruppo trunk applicato all'interfaccia seriale
3. Profilo di conversione vocale in ingresso nel dial-peer in ingresso
4. Profilo di traduzione vocale in entrata definito tramite porte del servizio vocale
5. Profilo di traduzione vocale in ingresso definito tramite 'voip-incoming translation-profile' globale
6. Profilo di traduzione vocale in uscita definito tramite porte per servizi vocali
7. Profilo di conversione vocale in uscita o translate-outbound sul dial-peer in uscita
8. Profilo di conversione vocale in uscita su gruppo trunk applicato all'interfaccia seriale
9. Profilo di conversione vocale in uscita sulla porta voce

Oltre alla composizione peer, regex e wilcards translation-rules hanno i propri caratteri regex.

Carattere	Definizione
*	Se utilizzato nelle regole di conversione, si tratta di regex per 0 o più caratteri precedenti.  Per ottenere una corrispondenza con un valore letterale * utilizzare un carattere di escape: \ *
\	Utilizzato comunemente per l'escape dei set nella regola di conversione \( \)
&	La E commerciale viene utilizzata per trasferire qualsiasi elemento corrispondente nel set di corrispondenze iniziale per il set di modifiche
()	Gli elementi racchiusi tra parentesi sono considerati un insieme.
^	Definisce l'inizio esplicito di una stringa.  A differenza dei dial-peer, le regole di conversione non definiscono l'inizio della stringa.  Ciò significa che la definizione di una stringa senza una ^ può corrispondere in qualsiasi punto della stringa di input, il che può portare a traduzioni indesiderate nel mezzo di un

numero.
---------

## Set di modifiche

- I set vengono specificati come \0, \1, \2 e così via.
- \0 corrisponde a qualsiasi elemento compreso tra il primo insieme di corrispondenze. Questa operazione può essere effettuata anche con il carattere commerciale: &.
- \1 corrisponde al primo insieme di ( ) nel set di corrispondenze
- \2 corrisponde al secondo insieme di ( ) nel set di corrispondenze
- E così via.

## Esempio di regola di conversione con due set

In questo esempio è possibile esaminare il numero 000111000222.

Si desidera rimuovere gli 0 dal numero e ottenere il numero finale 111222.

A tale scopo, si configura il set 1 e 2 per catturare rispettivamente il 111 e il 222 mentre si rilasciano gli 0.

```
!  
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
```

## Esempio per rimuovere il motivo di composizione a 9 da un numero chiamato

```
!  
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
```

## Tronca il numero chiamato a 4 cifre

```
!
voice translation-rule 4
 rule 1 /.*\(...\) / \1/
!
voice translation-profile STRIP-T0-4
 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
```

## Eliminazione di più + dal numero chiamato

```
!
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
```

Le regole di conversione possono inoltre essere applicate direttamente a un dial-peer senza prima essere applicate a un translation-profile.

```
!
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  
!
```

## Profilo di conversione nel gruppo trunk

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

## Debug delle regole e dei profili di conversione vocale

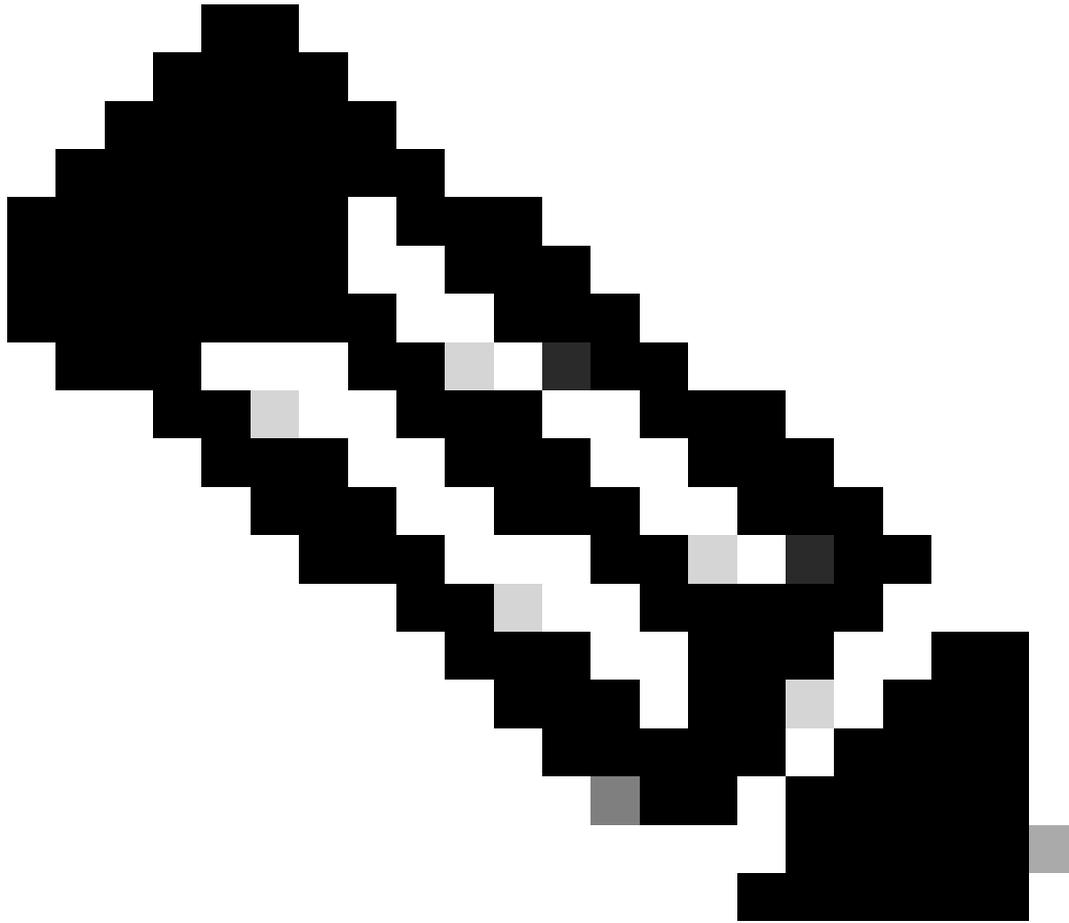
```
debug voip ccapi inout  
debug voice translation  
debug dialpeer  
test voice translation-rule <number> <string> type <type> plan <plan>
```

## Traduzione della classe voce e164

La funzionalità di conversione della classe voce e164 è una nuova funzionalità di Cisco IOS XE che consente a un amministratore di creare un elenco di istruzioni match e di modificare le istruzioni da caricare tramite un file di configurazione dalla memoria flash o da una directory di rete. Questo concetto è simile a quello della funzione e164-pattern-map discussa in questo documento. Questo consente all'amministratore di configurare fino a 100 traduzioni all'interno di un file di configurazione e di applicarle in un unico profilo di traduzione. Per ulteriori informazioni, consultare la [guida di riferimento dei comandi vocali di Cisco IOS](#)

Seguire questa sintassi per il file .cfg:

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



Nota: lo spazio finale è molto importante e l'importazione può avere esito negativo senza questo passaggio di formattazione aggiuntivo.

---

### Esempio.cfg

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

Il file fa quindi riferimento come tale:

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

A questo punto si applica normalmente a un profilo di traduzione e quindi ai dial-peer che utilizzano la normale sintassi del profilo di traduzione.

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

Il comando `show voice class e164-translation-e164-translation-number` può essere usato per visualizzare il contenuto del profilo di traduzione.

## Manipolazione della cifra tramite mappe ISDN

Le mappe ISDN sono una tecnica meno recente per la modifica delle cifre. Questa funzionalità è stata aggiunta in Cisco IOS 12.0(6)T e la maggior parte delle nuove configurazioni non la utilizza in quanto non sono affidabili come le regole di conversione vocale e i profili. Le mappe ISDN sono definite nell'interfaccia seriale.

### Esempio di configurazione

```
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
```

## Manipolazione della cifra tramite espansione del numero (num-exp)

Come le mappe ISDN, l'espansione del numero è una tecnica meno recente aggiunta in Cisco IOS versione 11.3(1)T e non molto utilizzata nelle nuove reti. Questa funzione è stata aggiunta prima dell'esistenza di regole per la traduzione vocale e profili. L'espansione del numero è una modifica globale delle cifre applicata a tutti i peer di connessione su un gateway Cisco. La modifica viene applicata al numero chiamato dopo la corrispondenza del dial-peer e subito prima dell'invio della chiamata al call-agent successivo.

### Esempio di configurazione

```
num-exp 4... 18005554...
```

## Profili SIP in entrata/in uscita

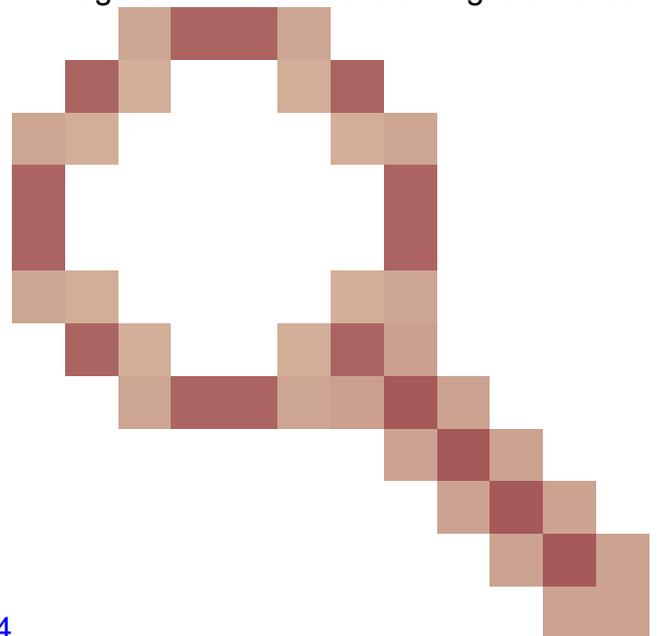
I profili SIP sono affidabili istruzioni Regex (Regular Expression) Match che consentono a un amministratore di modificare qualsiasi aspetto di un messaggio SIP che include intestazioni SDP e SIP. Questi possono essere abilitati a livello globale, per dial-peer o per tenant. I profili SIP sono disponibili per le modifiche in entrata a partire da Cisco IOS 15.4(2)T e Cisco IOS XE 3.12S. Poiché i profili SIP sono così affidabili, questo documento offre solo alcuni esempi specifici. I profili SIP consentono anche di modificare o aggiungere intestazioni SIP personalizzate in IOS 15.5(2)T e IOS-XE 3.13S.

### Punti chiave sui profili SIP in entrata e in uscita

- I profili SIP in entrata modificano il messaggio PRIMA che il CUBE elabori il messaggio per il routing delle chiamate.
- I profili SIP in uscita modificano il messaggio DOPO che il CUBE ha elaborato il routing delle chiamate e prima che il messaggio venga inviato all'hop successivo.

### Altre note sulla configurazione del profilo sip:

- I profili SIP non possono modificare gli attributi m=image SDP. La funzione di miglioramento



è stata archiviata nell'ID bug Cisco [CSCsr20474](#)

Inoltre, i profili SIP non possono rimuovere o aggiungere valori a SDP. Solo l'utente può modificare questi valori. Tuttavia, è possibile modificare un valore SDP in un valore null specificando l'intero valore e quindi impostando l'output su un set di virgolette vuote senza uno spazio.

- Non vengono eseguiti controlli per verificare se il comando corrente immesso esiste già o se esiste già una versione di tale comando quando si immettono comandi nella classe vocale sip-profile. Se un amministratore incolla una linea 7 volte in un profilo sip, la linea verrà visualizzata 7 volte nella configurazione corrente. Si consiglia di rimuovere il comando da modificare e quindi immettere il nuovo comando quando si modificano i profili sip per evitare

la presenza di più comandi.

Documentazione completa: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

Strumento di test del profilo SIP: [strumento di test del profilo SIP](#)

Sintassi di esempio del profilo SIP in entrata/in uscita

```
!  
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  
!
```

Esempio di profilo SIP in entrata/in uscita con numeri

```
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"
```

Metodi di applicazione profilo SIP in uscita

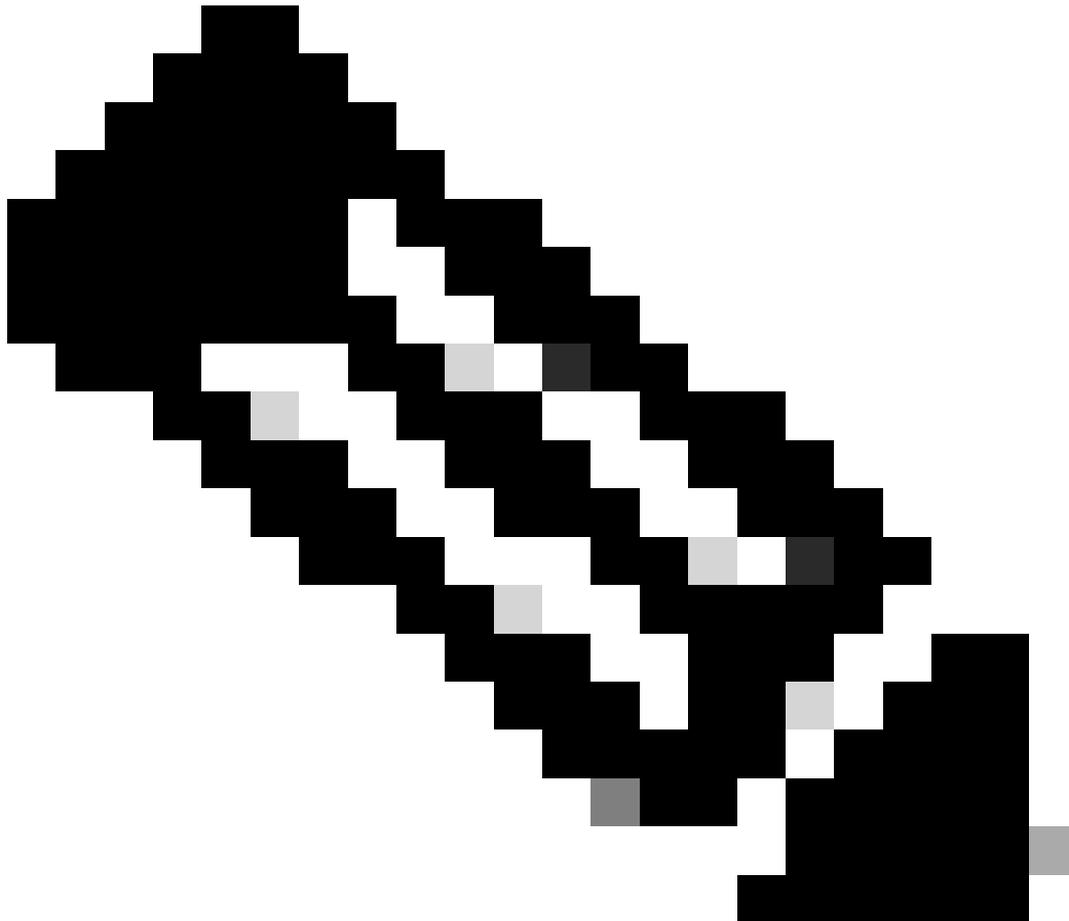
```
<#root>  
  
! Global Application  
  
voice service voip  
  sip  
    sip-profiles <number>  
!  
  
! Tenant Application  
  
voice class tenant <tag>  
  sip-profiles <tag>  
!
```

```
! Dial-peer Application
```

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

## Metodi di applicazione profilo SIP in entrata

---



Nota: è necessario abilitare il profilo sip in entrata nel servizio vocale voip sip indipendentemente dal fatto che venga utilizzata l'applicazione globale, il tenant o l'applicazione dial-peer.

---

```
<#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
!
```

Esempio di profilo SIP per modificare i messaggi OPTIONS keepalive.

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

Profilo SIP di esempio per modificare Host, Dominio o entrambe le parti di un URI.

<#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>"
!

```

Esempio di profilo SIP per aggiungere, modificare o rimuovere intestazioni di deviazione.

```

<#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
!

```

Esempio di profilo SIP per modificare la parte relativa al nome dell'ID chiamante delle intestazioni SIP.

```

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

```

Esempio di profilo SIP per modificare una sessione 183 in corso in un ring 180.

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

Esempio di profilo SIP per l'interoperabilità audio unidirezionale o non direzionale con un provider.

```
<#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
```

Esempio di profilo SIP per rimuovere il metodo UPDATE per problemi di interoperabilità.

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

Esempio di profilo SIP che mostra l'uso di SET all'interno del profilo SIP. Si tratta dello stesso concetto di set descritto nella sezione regola di conversione vocale.

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

Configurazione della logica IF e delle interruzioni di riga con un profilo SIP.

Le interruzioni di nuova riga sono supportate nei profili SIP, tuttavia esiste solo un caso di utilizzo molto specifico per questi profili. Poiché i profili SIP non dispongono di alcuna logica If, Then, Else, è ora disponibile un modo per apportare modifiche a un'intestazione in base a un input da un'altra intestazione. Ad esempio, un amministratore desidera modificare un'intestazione per la deviazione solo se l'intestazione FROM contiene 1234@cisco.com. Utilizzando l'interruzione di riga è possibile contraffare l'istruzione IF all'interno di un profilo SIP. Vedere la configurazione di esempio: Si ottiene una corrispondenza con 1234 in qualsiasi dominio nell'intestazione From. Quindi, portate sopra il primo gruppo e aggiungete una nuova interruzione di riga \x0D\x0AD. Infine, aggiungere l'intestazione desiderata. Si noti che questo metodo consente solo di

AGGIUNGERE un'intestazione. Impossibile modificare un'altra intestazione. Ciò soddisfa solo in parte i requisiti che un amministratore intendeva soddisfare in precedenza.

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

Esempio di profilo SIP con logica OR.

```
!  
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"  
!
```

Esempio di ispezione SIP di layer 7 tramite profilo SIP.

<#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
!
```

## Copylist SIP

Gli elenchi di copie SIP sono un'estensione dei profili SIP che consente al gateway di COPIARE un'intestazione dal lato interno di una chiamata e quindi di INCOLLARLA in un altro punto del messaggio SIP in uscita. Il supporto di copylist SIP è stato aggiunto in Cisco IOS 15.1(3)T e Cisco IOS XE 3.6S. Questo è un modo molto potente di creare intestazioni dinamiche basate su altre intestazioni dall'inizio della chiamata.

Il caso di utilizzo più comune è la copia dinamica di un'intestazione FROM in un'intestazione diversa, ad esempio diversion o p-asserted-id, in modo che il valore della parte utente sia l'utente di origine. Questa operazione viene eseguita principalmente per scopi di autenticazione e ID chiamante.

Documentazione completa: [Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 o versioni successive](#)

Esempio di elenco di copie SIP

```
<#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 to
!
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>
!

```

## Debug dei profili SIP e dell'elenco di copie

```

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

```

## Output di debug dell'elenco di copie SIP di esempio

### 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~cdf43-5020-4e79-a10b-99d406971010-36470319

Contact: <sip:5001@10.50.244.3:5060;transport=tcp>

### Copylist Details

00440: 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\_i

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\_i

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>

# Note speciali

## Segnalazione protocollo e associazione supporti

Tutti i protocolli di segnalazione consentono agli amministratori di associare la segnalazione a un'interfaccia specifica. Per impostazione predefinita, in un gateway senza un binding statico definito il gateway invia la segnalazione per una chiamata dall'interfaccia fisica attraversata dal pacchetto. Con il binding su un dial-peer, il pacchetto include intestazioni di origine, messaggi e pacchetti dall'interfaccia specificata, ma il pacchetto effettivo continua a instradare sull'interfaccia fisica. L'associazione Dial-Peer sostituisce sempre il tenant della classe vocale e l'associazione VOIP del servizio vocale globale con il protocollo SIP (Session Initiation Protocol).

Molte volte gli amministratori associano la segnalazione a un loopback. Trattandosi di un'interfaccia logica, nessun pacchetto attraversa questa interfaccia. Per eseguire le acquisizioni dei pacchetti, occorre eseguire l'acquisizione su un'interfaccia fisica. Il comando `show ip cef <ip remoto>` visualizza l'interfaccia fisica usata dal pacchetto per indirizzare all'IP di destinazione/remoto anche se la configurazione è associata a un'interfaccia virtuale.

Non è sempre necessario che il binding di supporti e segnali sia lo stesso IP. Se un amministratore deve collegarsi a un'interfaccia specifica per la segnalazione da/verso un CUCM ma l'audio / supporto tra il telefono e il gateway può dover collegarsi a un'altra interfaccia.

### Esempio di configurazione

Nell'esempio viene mostrato un dial-peer associato al loopback 1 che riceve una chiamata da CUCM.

Anche se i media e il segnale (controllo) sono associati al loopback 1, il comando `show ip cef` mostra che i pacchetti inviati a CUCM partono dall'interfaccia fisica Gigabit Ethernet0/0/1.

```
!  
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  
!
```

### Ordine delle operazioni per l'associazione delle applicazioni di layer 7

1. In base all'istruzione `bind` sul dial-peer in entrata/in uscita corrispondente.
2. In base ai binding nel tenant della classe voce assegnato al dial-peer in entrata/in uscita corrispondente.
3. Secondo l'istruzione di binding globale.

4. In base all'interfaccia fisica di layer 3, il pacchetto deve uscire da sulla base della tabella di routing.

### Comandi di binding SIP

```
<#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>
!
```

### Comandi di binding MGCP

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

### Comandi binding SCCP

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

### Comandi binding H323

```
<#root>
```

```
!
```

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

## DNS e VoIP Dial-Peer

Il DNS con VOIP viene utilizzato come qualsiasi altra soluzione DNS. Una configurazione comune prevede l'utilizzo del dns:FQDN.com di destinazione della sessione.

Un gateway Cisco esegue una risoluzione DNS anche quando non è configurata alcuna ricerca di dominio ip a livello globale sul gateway. Ciò significa che, anche se si disabilita il DNS, i dial-peer VOIP continuano a risolvere la voce DNS. Tuttavia, di recente in Cisco IOS XE 3.16S sono state apportate alcune modifiche alla funzionalità DNS complessiva nelle piattaforme Cisco IOS XE.

Dopo questa modifica, i peer di composizione configurati con la destinazione della sessione dns:FQDN.com ora obbediscono al fatto che DNS è disabilitato senza ricerca di dominio ip. Per evitare questo problema, è consigliabile verificare sempre che il comando "ip domain lookup" sia configurato quando si utilizza DNS.

Per le connessioni SIP in uscita, CUBE esegue questo ordine di operazioni per la risoluzione DNS.

1. Ricerca query SRV
2. Ricerca record
3. Ricerca record AAAA

Per informazioni su come creare l'SRV o ignorare l'SRV ed eseguire una query su un record A su una destinazione sessione, consultare la documentazione completa: [Cisco Unified Border Element Configuration Guide - Cisco IOS XE 17.6 On](#)

Per le connessioni SIP in entrata in cui un gateway IOS deve risolvere un'intestazione per rispondere a un messaggio, il gateway può utilizzare questo ordine di operazioni per la risoluzione DNS

1. Ricerca record
2. Ricerca record AAAA

In Cisco IOS XE 17.9.1, CUBE può controllare la raggiungibilità delle destinazioni di sessione DNS tramite le opzioni del meccanismo keepalive. Vedere la documentazione completa:

[Guida alla configurazione di Cisco Unified Border Element - Cisco IOS XE 17.6 in avanti](#)

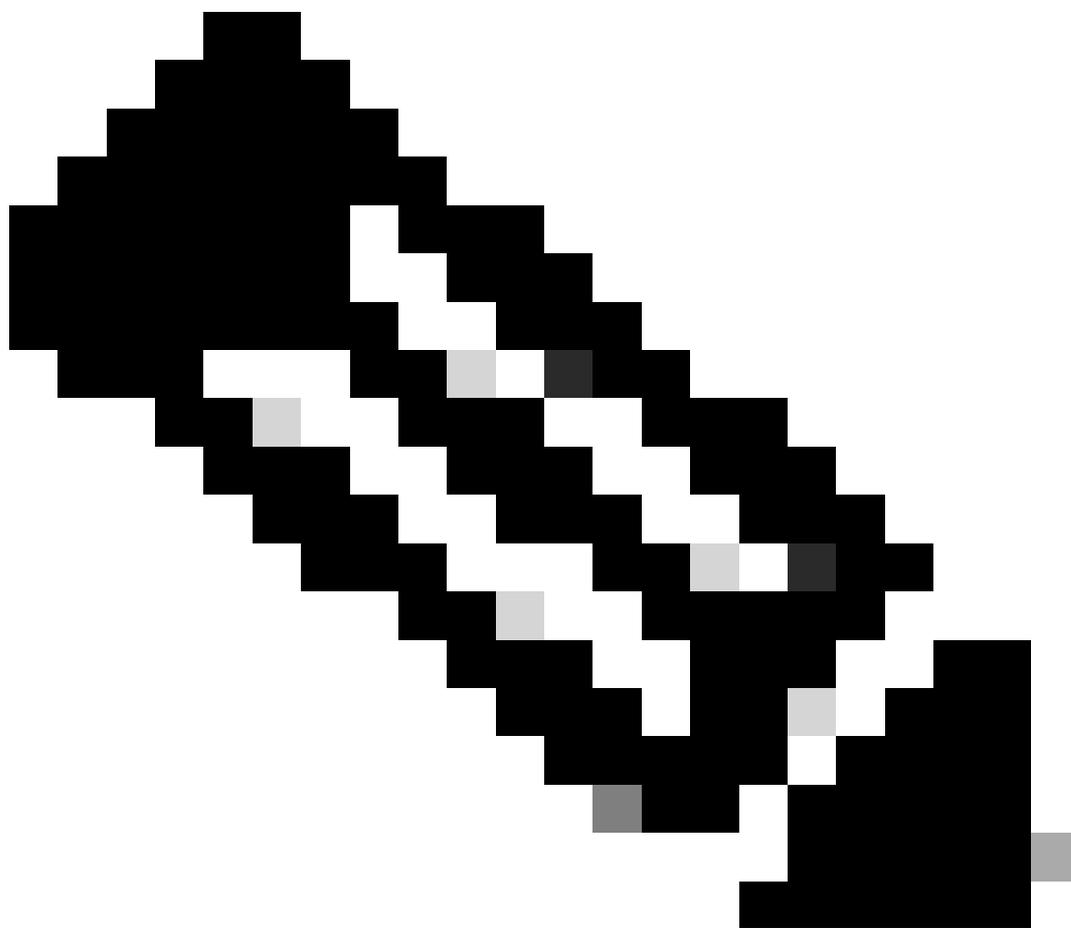
## Esempi di configurazione DNS IOS

```
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
```

---



Nota: il supporto DNS SRV su Cisco IOS XE è supportato sulle versioni 15.6(1)S / 3.17.00.S e successive.

---

<#root>

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

Test DNS 3.15S e versioni successive

<#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.
```

Test DNS versione 3.16S e successive.

<#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.
```

## Connessioni e larghezza di banda massime

Per impostazione predefinita, i dial-peer VOIP e POTS consentono connessioni (chiamate) e larghezza di banda illimitate (solo dial-peer VOIP). Per i trunk che hanno un limite al numero di

chiamate o alla larghezza di banda che possono essere utilizzate, può essere utile usare i comandi max-conn o max-bandwidth. max-conn è stato aggiunto in Cisco IOS 11.3(1)T ed è presente in tutte le versioni di Cisco IOS XE, mentre max-bandwidth è stato aggiunto in 15.2(2)T e IOS-XE 3.7S.

Esempio di configurazione:

Qui si dice al gateway di limitare le chiamate dial-peer da 1 a 30 utilizzando "max-conn 30". Dial-peer 2 limita la larghezza di banda per il dial-peer in modo da non superare il limite allocato.

```
!  
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  
!
```

Errore di esempio quando viene superata la soglia max-conn.

```
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
```

## Direct Inward Dial (DID)

### Composizione in una fase

Se la funzionalità Direct Inward Dial è abilitata sui peer di connessione POTS, la messaggistica in ingresso può contenere tutte le cifre necessarie per indirizzare la chiamata. Cisco Gateway non può eseguire la raccolta di cifre successive. Quando il router o il gateway cerca un dial-peer in uscita, il dispositivo usa l'intera stringa di composizione in arrivo. Questa corrispondenza è di lunghezza variabile per impostazione predefinita. Questa corrispondenza non viene eseguita cifra per cifra perché per definizione DID sono state ricevute tutte le cifre. Questa è la configurazione predefinita per i dial-peer POTS.

Documentazione completa: [Informazioni su Direct-Inward-Dial \(DID\) su interfacce IOS Voice Digital \(T1/E1\)](#)

### Esempio di configurazione

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

### Composizione in due fasi

Se il dial-peer POTS in arrivo è configurato senza la connessione diretta verso l'interno, il router o il gateway entra nella modalità di raccolta delle cifre (le cifre vengono raccolte in banda). La corrispondenza dial-peer in uscita viene eseguita cifra per cifra. Il router o il gateway verifica la presenza di corrispondenze dial-peer dopo che il dispositivo ha ricevuto ciascuna cifra, quindi instrada la chiamata quando viene effettuata una corrispondenza completa.

### Esempio di configurazione

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

## Blocco delle chiamate

Ogni protocollo gestisce il blocco delle chiamate in modo leggermente diverso. La maggior parte dei protocolli può utilizzare il modello di rifiuto basato su regole di conversione, ovvero blocchi basati su una stringa di cifre. Se un amministratore desidera ancora applicare un profilo di traduzione in entrata per la normale manipolazione delle cifre, ma non blocca alcun numero all'interno, è possibile implementare un blocco di chiamata utilizzando il comando `call-block translation-profile`.

```
!  
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
```

In E1 R2 esiste la possibilità per un amministratore di bloccare le chiamate di raccolta. Questo è principalmente visto e impiegato nelle distribuzioni in Brasile, ma può essere configurato tramite qualsiasi gruppo personalizzato di caso.

Le due opzioni sono:

1. Bloccare la chiamata a carico del destinatario sulla base della categoria II-8 ricevuta dallo switch telco. Questo è il meccanismo predefinito e tutti i gateway Cisco eseguono questa operazione senza alcuna configurazione. Questo metodo di blocco richiede un commutatore telco più recente che supporti il contrassegno basato sulle categorie. Per disabilitare questo metodo, utilizzare il comando `collect-call-enable` sul gruppo `cas-customer`.
2. Utilizzare la funzionalità a doppia risposta in un gruppo personalizzato di case R2-digital E1 R2. La configurazione a doppia risposta disattiva il blocco basato sulle categorie e lo sostituisce con la funzione a doppia risposta. Questa operazione viene eseguita rispondendo prima alla chiamata in arrivo e avviando un timer di 1 secondo. Dopo 1 secondo, il gateway invia una versione sotto forma di comando `CLEAR BWD`. La Telco può quindi inviare un messaggio `CLEAR FWD` al gateway e la chiamata può disconnettersi. Un timer inizia dopo che il gateway invia il messaggio `CLEAR BWD` e, se il timer scade, il gateway invia un altro segnale `ANSWER`, presupponendo che la chiamata non sia una chiamata a carico del destinatario e che la chiamata proceda normalmente. Questo timer può essere configurato

usando il comando cc-reanswer-to all'interno del gruppo personalizzato cas.

## Messaggio di blocco categoria II-8 (segnale vpm di debug)

<#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\_RE

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 IDLEvm\_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

## Esempio di configurazione a risposta doppia

```
!  
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  
!
```

## Debug a doppia risposta (segnale debug vpm)

<#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
```

## Ricezione sovrapposizione ISDN

Esistono implicazioni per la corrispondenza dial-peer in entrata quando il comando isdn overlap-receiver è configurato sulle interfacce ISDN. Dopo la ricezione di ogni cifra sul layer ISDN, i dial-peer vengono controllati per verificare la presenza di corrispondenze. Se viene effettuata una corrispondenza completa, la chiamata viene instradata immediatamente (all'app della sessione in questo caso) senza attendere cifre aggiuntive. Il terminatore T può essere usato per sospendere la corrispondenza cifra per cifra e forzare il router o il gateway ad attendere finché tutte le cifre non vengono ricevute. Il T si riferisce al timer internumerico T302 a livello ISDN, configurabile tramite l'interfaccia seriale associata all'interfaccia ISDN. ISDN fornisce anche altri meccanismi per indicare la fine delle cifre, ad esempio l'impostazione dell'elemento di informazione completo (IE, Sending Complete Information Element) nei messaggi informativi Q.931.

## Numero chiamato vuoto

Il messaggio di avviso visualizzato viene visualizzato quando il dial-peer è configurato con il numero chiamato T in ingresso.

### Output di esempio

```
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
```

Note speciali sulla corrispondenza dial-peer in ingresso con un numero chiamato vuoto.

- Un numero chiamato nullo è considerato meno qualificato rispetto a una porta voce e/o in alcuni casi a un indirizzo di risposta. Pertanto, una corrispondenza basata su un numero null chiamato può verificarsi solo se non esiste alcuna corrispondenza basata su indirizzo-risposta o numero-porta.

- In caso di composizione sovrapposta, un numero null chiamato non corrisponde al numero chiamato in ingresso T perché non si è verificato il timeout.
- Un numero chiamato nullo può corrispondere al numero chiamato in ingresso T solo in caso di ENBLOCK e non esiste alcuna corrispondenza a causa di indirizzo-risposta e numero-porta. L'avviso visualizzato quando un amministratore configura il numero chiamato in ingresso T fa riferimento a questo caso specifico.

## Classe di restrizione

Class of Restriction (COR) consente di limitare le chiamate a un gateway Cisco. Il CdR viene spesso descritto come un meccanismo di blocco e di chiave. I blocchi vengono assegnati ai peer di composizione con un elenco COR in uscita. I tasti vengono assegnati ai peer della connessione remota con un elenco COR in ingresso. Quando si applicano gli elenchi COR, i dial-peer in uscita disponibili sono quelli che la chiave può sbloccare. Questo filtro viene applicato prima del controllo degli altri metodi di corrispondenza dial-peer in uscita.

Due regole importanti con la classe di restrizione:

1. Se non è applicato alcun elenco COR in uscita, la chiamata viene sempre instradata.
2. Se non è presente alcun elenco COR in ingresso, la chiamata viene sempre instradata.

La configurazione di Class of Restriction (COR), Logical Partitioning Class of Restriction (LPCOR) e LPCOR con Codici di autorizzazione forzati (FAC) esula dall'ambito di questo documento, ma è possibile fare riferimento a questi documenti per ulteriori letture.

COR	<a href="#">Configurazione della classe di limitazioni (COR)</a>
LPCOR con CME	<a href="#">Esempio di configurazione di CME con LPCOR</a>
LPCOR con CME e FAC	<a href="#">Guida per l'amministratore di sistema di Cisco Unified Communications Manager Express</a>

## Peer di connessione remota Cisco Unified Communications Manager Express (CUCME)

CME crea dial-peer di sistema per telefoni e pool di registrazioni vocali. Non sono visibili nella configurazione in esecuzione. Per apportare modifiche ai dial-peer CME, è necessario apportare le modifiche sul pool di chiamate o di registri vocali effettivi. Quando si visualizzano gli output del riepilogo della voce del dial-peer, i dial-peer che iniziano con 2000 sono telefoni SCCP e i dial-peer che iniziano con 4000 sono pool di registrazione voce SIP. Questo dial-peer viene visualizzato come dial-peer in entrata per le chiamate dai telefoni registrati CME e come dial-peer in uscita nei debug per le chiamate ai telefoni registrati CME.

Output di esempio per show dial-peer voice summary con 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

```

Output di esempio per show voice register dial-peer con 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 kpm1
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 kpm1
codec g711ulaw bytes 160
no vad
after-hours-exempt FALSE

```

## MGCP e SCCP con Dial-Peer

MGCP e SCCP seguono le loro regole per i dial-peer. L'unico concetto che utilizzano è che devono essere configurati con la porta voce desiderata per la chiamata. Il resto viene gestito dai processi STCAPP e MGCPAPP. Quando si esamina la configurazione di questi peer della connessione remota, è possibile che dispongano del servizio comandi mgcpapp o service stcapp. Questi abilitano il dial-peer per l'applicazione scelta, oltre a indicare all'applicazione quale dial-peer può gestire.

Durante il debug di questi protocolli, l'output non visualizza mai una corrispondenza dial-peer in ingresso. Può sempre essere visualizzato come dial-peer 0. Perché non esiste. L'agente di chiamata che gestisce l'applicazione ha già scelto la porta a cui inviare la chiamata e la corrispondenza dial-peer in ingresso è inutile poiché il gateway non ha alcun controllo su quella parte della chiamata. Tuttavia, è possibile osservare una corrispondenza dial-peer in uscita. Questo è solo per mostrare come in ultima analisi l'agente di chiamata che gestisce il processo ha il controllo anche su quel lato della chiamata.

Tenere presente che il dial-peer indica solo all'applicazione di scelta quale porta vocale fisica controllare. Dal momento che la maggior parte di questo è controllata da un agente di chiamata esterno e il gateway fa solo quello che è detto. La procedura sottostante per questa sezione verrà ignorata e verranno fornite alcune configurazioni per iniziare.

Esempio di configurazione MGCP [con configurazione automatica CUCM\*]

```
!  
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  
!
```

Documentazione completa relativa a MGCP: [Cisco Unified Communications Manager and Interoperability Configuration Guide, Cisco IOS release 15M&T](#)

Configurazione SCCP/STCAPP di esempio [con configurazione automatica CUCM\*]

```
!  
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
!

```

Se un amministratore non desidera che CUCM configuri il gateway, è sufficiente rimuovere i comandi ccm-manager. La configurazione dial-peer è inclusa per portare a casa il punto su come funziona il concetto. Con le configurazioni di gestione della porta, CUCM crea questi dial-peer in base alla configurazione della porta in CUCM, quindi non è necessario definire realmente il dial-peer. I peer di composizione creati da CUCM in genere iniziano con 999 e sono quindi costituiti da altre tre cifre.

## SIP DSAPP con Dial-Peer

SIP DSAPP è stato aggiunto in Cisco IOS XE 16.12.1+ e CUCM 12.5.1SU+

Grazie a questa funzione, le porte vocali analogiche come FXS possono essere registrate e gestite da CUCM. Il routing delle chiamate con DSAPP è leggermente diverso da MGCP o SCCP in quanto i peer di chiamata vengono ancora abbinati normalmente. In altre parole, il gateway può raccogliere cifre dalla porta FXS ed eseguire una ricerca dial-peer sui dial-peer VOIP. Una volta trovata una corrispondenza, l'istruzione INVITE viene inviata a CUCM enblock affinché CUCM esegua un'ulteriore analisi delle cifre.

Esempio di configurazione SIP DSAPP [con configurazione automatica CUCM\*] | IOS-XE 16.12.1+ e 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
!

```

Documentazione completa relativa a SIP DSAPP: [guida alla configurazione del software Cisco VG450 Voice Gateway](#)

## Risoluzione dei problemi e verifica del routing delle chiamate

Per informazioni più dettagliate, consultare questo documento.

[Configurazione della raccolta di debug per i gateway CUBE \(Unified Border Element\) e TDM \(Time-Division Multiplexing\)](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).