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

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Sfondo
TDM Voice Gateway e CUBE
Raccolta dei debug vocali Cisco IOS/IOS-XE
Come accedere a un router Cisco IOS/IOS-XE dall'interfaccia della riga di comando (CLI)
Come impostare Terminal Monitor per la raccolta dei comandi show o dei debug
Raccogli output di base del comando show dalla CLI
Raccogli output di debug dalla CLI
Controllo della memoria
Controllo CPU
Controllo chiamate attive correnti
Impostazioni buffer di registrazione
Configura impostazioni syslog
Raccolta di debug
Quali debug possono essere abilitati nei router voce?
Debug dell'API CCAPI (Internal Call Control API)
Flussi di chiamate SIP
Debug SIP base
Debug SIP avanzati
Flussi di chiamate digitali (PRI, BRI)
Debug digitale di base
Debug digitale avanzato
Flussi di chiamate analogiche
Flussi di chiamate MGCP
Debug di base
Debug di CCM-Manager
Debug avanzati MGCP
Flussi di chiamata H323
Debug base H323
Debug avanzati H323
Risorse multimediali SCCP
Debug SCCP di base
Debug SCCP avanzato
Traccia VoIP

Restrizioni
Come abilitare la traccia VoIP
Come disabilitare la traccia VoIP
Configura limite di memoria
Come visualizzare i dati di traccia VoIP
show voip trace all
show voip trace cover-buffer
show voip trace call-id
mostra statistiche traccia voip
Comandi show aggiuntivi

Introduzione

In questo documento vengono descritte alcune delle best practice da adottare per raccogliere i bug vocali in un router voce Cisco IOS/IOS-XE.

Prerequisiti

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.

Requisiti

- Conoscenze base di Cisco IOS/IOS-XE all'interno di ISR (Integrated Services Router).
- Accesso privilegiato per eseguire i comandi nei router ISR.
- Si desidera avere già esperienza con i protocolli VoIP (Voice-over-IP).
- Per la traccia VoIP è richiesto almeno Cisco IOS-XE 17.4.1 o 17.3.2.

Componenti usati

Ai fini del presente documento, i componenti utilizzati sono:

- Cisco ISR 3925
- Cisco ISR 4451
- PuTTY

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.

Sfondo

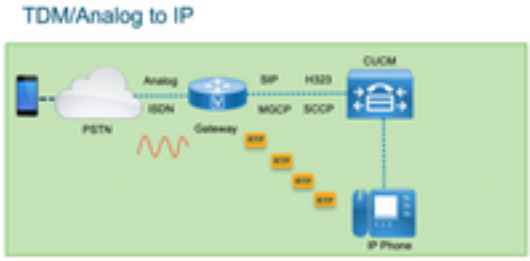
Il processo di raccolta di debug in queste piattaforme presenta problemi e potrebbe influire sulle prestazioni del dispositivo. Le sfide e i rischi aumentano quando vengono stabilite più chiamate

attive in un router voce. In alcuni scenari, se i debug non vengono raccolti correttamente, la CPU può essere elevata, il che potrebbe compromettere la capacità del router e causare un arresto anomalo del software. In questo documento viene descritta la differenza tra un CUBE (Cisco Unified Border Element) e un TDM/Analog Gateway.

TDM Voice Gateway e CUBE

I gateway voce TDM vengono utilizzati principalmente per interconnettere un sistema telefonico interno con un altro PBX (Private Branch Exchange) o PSTN (Public Switched Telephony Network). I tipi di connessione utilizzati nei gateway TDM sono i controller T1/E1 (ISDN o CAS) e i circuiti analogici come le porte FXS e FXO. Un DSP (Digital Signal Processor) converte l'audio dalla sua forma raw in pacchetti RTP. Analogamente, i pacchetti RTP vengono convertiti in audio raw dopo che il DSP ha elaborato i pacchetti RTP e invia l'audio sul circuito specifico. Questi gateway possono interagire con H323, MGCP o SCCP sul lato VoIP e, sul lato TDM, con i circuiti PRI ISDN o Analogici come le connessioni più comuni ai PSTN o agli endpoint.

Come mostrato nell'immagine, i gateway TDM fungono da ponte tra l'infrastruttura VoIP interna e i provider di servizi analogici o ISDN.



Con l'introduzione del VoIP, i clienti hanno iniziato a trasformare rapidamente i sistemi legacy in una moderna infrastruttura VoIP. Lo stesso si è verificato dal lato del provider di servizi, dove ora utilizzano le connessioni per interconnettere i servizi di telefonia locale con l'infrastruttura VoIP del provider di servizi ed espandere le loro funzionalità per fornire servizi migliori. Il protocollo VoIP più comune utilizzato attualmente è il SIP (Session Initiation Protocol), attualmente ampiamente utilizzato dai clienti e dai provider di servizi di telefonia Internet (ITSP) in tutto il mondo.

CUBE è stato introdotto per fornire un modo per interconnettere questi sistemi VoIP interni con il mondo esterno attraverso gli ITSP con SIP come protocollo VoIP primario. CUBE è semplicemente un gateway IP in cui non ha più bisogno di alcun tipo di connessione TDM come i controller T1/E1 o le porte analogiche. CUBE viene eseguito sulle stesse piattaforme dei gateway TDM.

Il protocollo VoIP più comune utilizzato è il SIP, per la definizione e la disinstallazione delle chiamate, e la RTP per il trasporto dei media. In CUBE non è necessario un DSP a meno che non sia richiesto un transcodificatore. I flussi di traffico RTP terminano dall'ITSP all'endpoint e CUBE funge da intermediario, nascondendo l'indirizzo come una delle numerose funzionalità offerte.

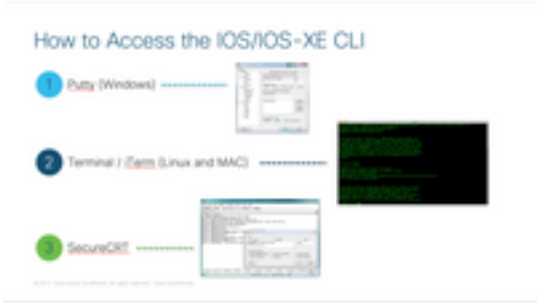
Come mostrato nell'immagine, CUBE fornisce una divisione tra l'infrastruttura VoIP interna e SIP ITSP:

Raccolta dei debug vocali Cisco IOS/IOS-XE

Le funzionalità vocali vengono eseguite su un elenco diverso di piattaforme, ad esempio ISR, ASR, CAT8K e altre ancora, tuttavia utilizzano un software comune che può essere Cisco IOS o Cisco IOS-XE (le differenze tra Cisco IOS e Cisco IOS-XE non sono illustrate in questo articolo). Iniziamo con le informazioni di base su come accedere al router Cisco IOS.

Come accedere a un router Cisco IOS/IOS-XE dall'interfaccia della riga di comando (CLI)

I router, come tutti gli altri dispositivi basati sulla CLI, richiedono un terminal monitor per accedere e eseguire i comandi tramite Secure Shell (SSH) o Telnet. SSH è il protocollo più comune utilizzato oggigiorno per accedere ai dispositivi, in quanto fornisce una connessione protetta e crittografata al dispositivo. Alcuni dei terminal monitor più comuni utilizzati per accedere alla CLI dei router sono:

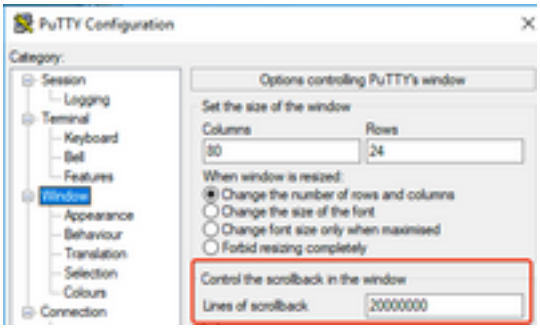


Come impostare Terminal Monitor per la raccolta dei comandi show o dei debug

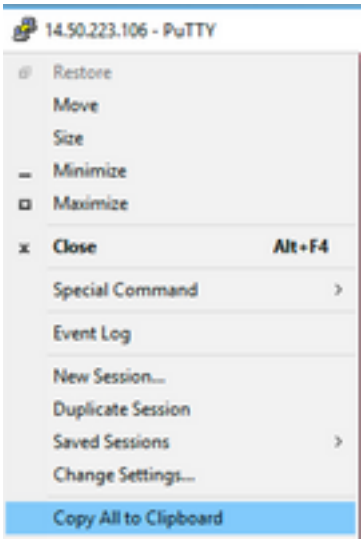
Ci sono diversi modi per raccogliere l'output dalla CLI. Si consiglia di esportare le informazioni dalla CLI del router in un file separato. Ciò semplifica la condivisione delle informazioni con terze parti.

Di seguito sono riportati due modi per raccogliere gli output dal dispositivo:

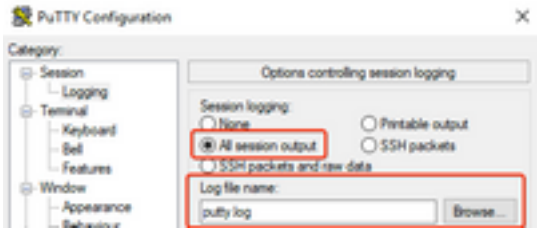
- Scaricare tutto l'output nel terminale, per questo è necessario assicurarsi che ci siano abbastanza linee di scrollback, altrimenti lo scrollback non prende le prime sezioni dell'output e i dati possono essere incompleti. Per aumentare le linee di scorrimento in Putty, selezionate Configurazione Putty > Finestra > Linee di scorrimento. Normalmente questo valore è impostato su un valore molto alto per avere un output di scorrimento sufficiente:



Successivamente, è possibile raccogliere le informazioni dal monitor del terminale con l'opzione **Copy All to Clipboard** (Copia tutto negli Appunti) e incollare l'output in un file di testo:



- Un'altra opzione consiste nel registrare l'output dell'intera sessione in un file .txt. Con questa opzione tutti i comandi immessi e gli output raccolti vengono immediatamente registrati nel file di testo. Questa è una procedura comune per registrare tutto l'output in una sessione. Per registrare l'output di tutte le sessioni in un file in Putty, selezionate **Configurazione Putty > Sessione > Log**, quindi selezionate Output di tutte le sessioni come segue:



> **Nota:** Se non viene specificato alcun altro nome, viene utilizzato il nome del file di registro predefinito. Fare clic sul pulsante Sfoglia per sapere esattamente dove è stato salvato il file e individuarlo in seguito. Assicurarsi inoltre di non sovrascrivere un altro file putty.log nello stesso percorso.

Raccogli output di base del comando show dalla CLI

I comandi show sono necessari per raccogliere informazioni di base dal router prima di qualsiasi raccolta di debug. I comandi show sono veloci da raccogliere e, nella maggior parte dei casi, non influiscono sulle prestazioni del router. L'isolamento del problema potrebbe iniziare immediatamente con un semplice output del comando show.

Una volta connesso al router, la lunghezza del terminale può essere impostata su 0. In questo modo, la raccolta può essere più veloce in modo da visualizzare tutto l'output contemporaneamente ed evitare l'uso della barra spaziatrice. L'unico comando che raccoglie informazioni dettagliate sul router è "show tech". In alternativa, è possibile raccogliere **show tech voice** che mostra dati più specifici delle funzionalità vocali abilitate sul router:

```
Router# terminal length 0
Router# show tech
!or
Router# show tech voice
Router# terminal default length !This cmd restores the terminal length to default
```

Raccogli output di debug dalla CLI

La raccolta degli output di debug in Cisco IOS/IOS-XE a volte può essere un problema, in quanto esiste il rischio di un arresto anomalo del router. Nelle sezioni seguenti vengono illustrate alcune delle procedure ottimali per evitare problemi.

Controllo della memoria

Prima di abilitare i debug, accertarsi che la memoria sia sufficiente per memorizzare l'output nel buffer.

Eseguire il comando **show process memory** per verificare la quantità di memoria che è possibile allocare per registrare tutto l'output nel buffer:

> **Suggerimento**: Usare il comando **terminal length default** o **terminal length <num_lines>** per tornare a una quantità limitata di linee visualizzate nel terminale.

```
Router# show process memory
Processor Pool Total: 8122836952 Used: 456568400 Free: 7666268552
lsmpi_io Pool Total: 6295128 Used: 6294296 Free: 832
```

Nell'esempio, il router può usare fino a 766268552 byte (7,6 GB). Questa memoria è condivisa dal router tra tutti i processi di sistema; ciò significa che non è possibile utilizzare l'intera memoria libera per registrare l'output nel buffer, ma è possibile utilizzare una buona quantità di memoria di sistema in base alle esigenze.

La maggior parte degli scenari richiede almeno 10 MB per raccogliere un output di debug sufficiente prima che l'output venga perso o sovrascritto. In rari casi è necessario raccogliere una quantità maggiore di dati, in questi scenari specifici è possibile ottenere un output di 50 MB-100 MB nel buffer o si può andare più in alto se c'è memoria disponibile.

Se la memoria disponibile è insufficiente, è possibile che si verifichi una perdita di memoria. In questo caso, rivolgersi al team TAC per rivedere la causa di tale perdita di memoria.

Controllo CPU

La CPU è influenzata dalla quantità di processi, funzionalità e chiamate attivi nel sistema. Maggiore è il numero di funzioni o chiamate attive nel sistema, maggiore è il traffico della CPU.

Un buon punto di riferimento è quello di garantire che la CPU del router sia al 30% o inferiore, il che significa che è possibile abilitare i debug da quelli di base a quelli avanzati (è necessario tenere sempre sotto controllo la CPU quando si utilizzano i debug avanzati). Se la CPU del router è al 50% circa, è possibile eseguire i debug di base e monitorare attentamente la CPU. Se la CPU raggiunge un valore superiore all'80%, interrompere immediatamente i debug (come mostrato più avanti in questo articolo) e chiedere assistenza al centro TAC.

Utilizzare il comando **show process cpu | exclude 0.00** per controllare i valori degli ultimi 5, 60 e 5 min della CPU insieme ai primi processi.

```
Router# show processes cpu sorted | exclude 0.00
CPU utilization for five seconds: 1%/0%; one minute: 0%; five minutes: 0%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
211 4852758 228862580 21 0.15% 0.06% 0.07% 0 IPAM Manager
84 3410372 32046994 106 0.07% 0.04% 0.05% 0 IOSD ipc task
202 3856334 114790390 33 0.07% 0.05% 0.05% 0 VRRS Main thread
```

Nell'output, il router non ha molta attività, la CPU è bassa e i debug possono essere abilitati senza problemi.

> **Attenzione:** Prestare particolare attenzione ai primi processi CPU attivi, se la CPU è al 50% o superiore e il processo superiore è un processo vocale, è possibile abilitare solo i debug di base. Monitorare continuamente la CPU con il comando per garantire che le prestazioni complessive del router non siano influenzate.

Controllo chiamate attive correnti

Ogni router ha soglie di capacità diverse. È importante controllare quante chiamate sono attive nel router per assicurarsi che non si avvicini alla capacità massima. Il Data Sheet degli elementi del bordo unificato Cisco versione 12 fornisce informazioni su ciascuna capacità della piattaforma come riferimento.

Utilizzare il comando **show call active total-call** per avere un'idea del numero di chiamate attive nel sistema:

```
Router# show call active total-calls
Total Number of Active Calls : 0
```

Utilizzare il comando **show call active voice summary** per ottenere informazioni più dettagliate sui tipi di chiamata specifici attivi:

```
Router# show call active voice summary
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
STCAPP call-legs: 0
Multicast call-legs: 0
Total call-legs: 0
```

Alcuni dei valori comuni sono:

- **Call-leg di telefonia**: Chiamate TDM Gateway, incluse le chiamate Analog e PRI/ISDN.

- **Call-leg SIP**: Totale chiamate SIP. Se si tratta di un router CUBE, verranno visualizzati 2 segmenti di chiamata per chiamata. Dividere per 2 il totale delle chiamate visualizzate per ottenere un numero preciso.
- **Call-leg H323**: Totale chiamate H323.
- **Call-leg SCCP**: Risorse multimediali controllate da CUCM utilizzate nel router, ad esempio trascodificatori e MTP.

Impostazioni buffer di registrazione

Per configurare il router in modo che memorizzi l'output di debug nel buffer, viene immessa la modalità di configurazione del terminale per regolare manualmente le impostazioni nella CLI. Questa configurazione non ha alcun impatto sul router, tuttavia, come mostrato nelle sezioni precedenti, il comando **show tech** o **show running-config** inviato dal router è necessario nel caso sia necessario eseguire il rollback della configurazione.

Di seguito è riportato un esempio di configurazione, ovvero una linea di base comune utilizzata dai tecnici TAC. Nell'esempio vengono allocati 10 MB di memoria buffer, ma è possibile aumentarli in base alle esigenze:

```
# configure terminal
service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year
service sequence-numbers
logging buffered 10000000
no logging console
no logging monitor
logging queue-limit 10000
logging rate-limit 10000
voice iec syslog
```

I comandi eseguono le seguenti attività:

- **debug o registro timestamp servizio**: Assicura che l'ora del router locale venga scritta su ogni messaggio registrato, con una precisione di millisecondi. Ciò è utile per trovare le chiamate in base alla durata. Gli indicatori di ora in millisecondi consentono di raggruppare le linee di debug in eventi correlati logici quando due linee si verificano nello stesso millisecondo.
- **numeri di sequenza del servizio:** Scrive il numero di sequenza del debug nella riga. Ciò è utile (essenzialmente obbligatorio) quando i registri vengono inoltrati a un server syslog. Questa opzione permette di verificare se alcuni messaggi di debug inviati al server syslog sono stati scartati dalla rete. Il numero di sequenza è il primo elemento del debug, prima dell'indicatore orario e del messaggio del log effettivo. Si noti che questo valore è diverso dal numero di timestamp/sequenza che i server syslog possono scrivere localmente nei propri file.
- **buffer di registrazione**: Comunica al router di inviare i debug alla memoria buffer locale. La dimensione del buffer è impostata in byte. Nella configurazione la dimensione del buffer è stata impostata su 10 MB.
- **nessuna console di registrazione** e **nessun monitor di registrazione:** Sul monitor della console o del terminale non viene stampato alcun messaggio log. Se questi comandi non sono configurati, potrebbero influire negativamente sulle prestazioni del router e sull'accuratezza dell'output del debug.
- **voice iec syslog:** Abilita i messaggi dei codici di errore interni voce per determinare i motivi della disconnessione.

Configura impostazioni syslog

A volte i problemi possono essere casuali e richiedere un modo continuo di raccogliere i debug fino al verificarsi dell'evento. Quando i debug vengono memorizzati nel buffer, vengono raccolti continuamente. Notare che è limitato alla quantità di memoria che è possibile allocare e una volta raggiunta tale quantità di memoria, il buffer cerchia e rilascia i messaggi più vecchi, il che porta a informazioni incomplete e preziose necessarie per isolare il problema.

Con Syslog, il router può inviare tutti i messaggi di debug a un server esterno, dove il software Syslog Server li memorizza in file di testo. Sebbene sia un metodo valido per raccogliere l'output di debug, non è il metodo preferito per la raccolta dei log. I server Syslog tendono a ignorare o a eliminare le linee dall'output ricevuto a causa della congestione del server, poiché l'output di debug può sovraccaricare il server o i pacchetti possono essere scartati a causa delle condizioni della rete. Tuttavia, in alcuni scenari Syslog è l'unico modo per fare progressi su un problema.

Se possibile, utilizzare un metodo di trasporto affidabile, come il protocollo TCP, per evitare la perdita di informazioni. Si consiglia di collegare il server Syslog allo stesso switch a cui è connesso il router o il più vicino possibile al router. Ciò non garantisce che tutti i dati siano memorizzati nei file, ma riduce le possibilità di perdita dei dati.

Per impostazione predefinita, i server syslog utilizzano UDP come protocollo di trasporto sulla porta 514.

```
#configure terminal
service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year
service sequence-numbers

!Optional in case you still want to store debug output in the buffer.
logging buffered 10000000

no logging console
no logging monitor

logging trap debugging

!Replace the 192.168.1.2 with the actual Syslog Server IP Address
logging host 192.168.1.2 transport [tcp|udp] port
```

Non appena i comandi sono configurati, il router inoltra immediatamente i messaggi all'indirizzo IP del server Syslog.

Raccolta di debug

Dopo aver abilitato i debug, è necessario cancellare il buffer prima di riprodurre il problema. Ciò viene fatto per garantire che l'output sia il più pulito possibile ed evitare dati aggiuntivi non necessari per l'analisi. Eseguire il comando **clear log** per assicurarsi che il buffer venga cancellato. Se sul router sono attive altre chiamate e i debug sono abilitati, l'output viene immediatamente stampato nel buffer.

```
Router# clear log
Clear logging buffer [confirm]
Router#
```

Una volta riprodotto il problema, disabilitare immediatamente i debug per arrestare l'output nel buffer. Raccogliere quindi i registri. È possibile eseguire il dump di tutto l'output nel terminale con i seguenti comandi:

```
Router# undebug all
Router# terminal length 0
Router# show log
```

A volte PuTTY si chiude in quanto non è in grado di gestire tutto l'output in una volta sola. Questa condizione è normale e non significa che si sia verificato un errore, se ciò si verifica, riaprire di nuovo la sessione e continuare normalmente. Se il buffer di registrazione è troppo grande o il monitor del terminale si blocca a causa della quantità di dati da stampare, copiare l'output del buffer su una periferica esterna direttamente con il comando **show log | reindirizzamento**:

```
Router# show log | redirect ftp://username:password@192.168.1.2/debugs.txt
```

Il comando copia l'intero output del buffer in un ftp con indirizzo IP 192.168.1.2 e nome file debug.txt. Specificare sempre il nome del file. Altre destinazioni disponibili per l'esportazione dei dati sono:

```
Router# sh log | redirect ?
bootflash: Uniform Resource Locator
flash: Uniform Resource Locator
ftp: Uniform Resource Locator
harddisk: Uniform Resource Locator
http: Uniform Resource Locator
https: Uniform Resource Locator
nvram: Uniform Resource Locator
tftp: Uniform Resource Locator
```

Quali debug possono essere abilitati nei router voce?

Ogni flusso di chiamata e tipo di funzionalità (TDM, CUBE o SCCP (Media Resources)) sono diversi ed è possibile abilitare debug specifici. Tutti i debug richiesti devono essere abilitati contemporaneamente. L'acquisizione simultanea di un solo debug non è efficace e genera maggiore confusione durante l'analisi dei dati.

i debug sono abilitati all'interno del **router n.** del prompt di CLI exec che richiede le autorizzazioni della modalità di esecuzione privilegiata.

Sono disponibili debug di base e avanzati. I debug di base vengono usati per raccogliere le informazioni di segnalazione in SIP, H323 o MGCP, per mostrare le conversazioni tra il router e i dispositivi peer.

I debug avanzati sono molto dettagliati e vengono in genere utilizzati per raccogliere più informazioni in caso di errori interni dello stack che i debug di base non sono in grado di visualizzare. In genere, questi debug richiedono un utilizzo intensivo della CPU.

> **Suggerimento**: Dopo aver abilitato i debug, eseguire il comando **clear logging**. Questo comando assicura che il buffer venga cancellato per un'acquisizione più pulita dei debug.

Debug dell'API CCAPI (Internal Call Control API)

All'interno di ciascun router Cisco IOS/IOS-XE è presente un'API di controllo delle chiamate responsabile della comunicazione tra diverse applicazioni o protocolli VoIP e i componenti Data Plane, ad esempio RTP, DSP, schede voce e altri. Per acquisire i dati da questo livello, è possibile usare un debug specifico:

```
debug voip ccapi inout
```

Per questo debug sono disponibili altre opzioni, tuttavia il comando **debug voip ccapi inout** copre tutte le informazioni di base relative alla connessione a dial-plan e alla chiamata, informazioni in genere più che sufficienti per comprendere quali sono gli stati di questo livello.

> **Suggerimento**: **il comando debug voip capi inout** ha in genere un impatto minimo sulla CPU del router e si consiglia di abilitarlo insieme ai debug delle segnalazioni in modo da fornire un set completo di registri con le informazioni sulle chiamate e i relativi stati.

Flussi di chiamate SIP

Questi debug sono i più comunemente utilizzati per i flussi di chiamate SIP e possono essere abilitati all'interno dei gateway CUBE e TDM con una linea SIP tra il router e CUCM o qualsiasi altro server/proxy SIP.

Debug SIP base

```
debug ccsip messages
debug ccsip error
debug ccsip non-call !Optional, applies for SIP OPTIONS and SIP REGISTER Messages.
```

Debug SIP avanzati

```
debug ccsip all
debug ccsip verbose
debug voice ccapi inout
```

Flussi di chiamate digitali (PRI, BRI)

Questi debug si applicano alle interfacce di frequenza primaria (PRI) T1/E1 o alle interfacce di velocità base (BRI):

Debug digitale di base

```
debug isdn q931
```

Debug digitale avanzato

```
debug isdn q921
```

Flussi di chiamate analogiche

Questi debug vengono usati quando sono coinvolti circuiti analogici come le porte Foreigh eXchange Subscriber (FXS) o Foreign eXchange Office (FXO):

```
debug vpm signal
debug voip vtsp all
```

Flussi di chiamate MGCP

Questi debug vengono usati quando il protocollo MGCP viene usato come protocollo vocale tra un Voice Gateway e CUCM.

Debug di base

```
debug mgcp packets
debug mgcp errors
```

Debug di CCM-Manager

Il comando **debug cm-manager** viene usato per tenere traccia dei messaggi di backhaul MoH e PRI/BRI tra CUCM e Voice Gateway. Questi debug vengono utilizzati in base alle necessità e dipendono dallo scenario di errore.

```
debug ccm-manager backhaul !For PRI and BRI Deployments
debug ccm-manager errors
debug ccm-manager events
debug ccm-manager config-download !Troubleshoot Configuration download issues from CUCM TFTP
debug ccm-mananger music-on-hold !Troubleshoot internal MoH Process
```

Debug avanzati MGCP

```
debug mgcp all
```

Flussi di chiamata H323

Sebbene H323 non sia ampiamente utilizzato, vi sono ancora alcune implementazioni con H323 configurato:

Debug base H323

```
debug h225 asn1
debug h245 asn1
debug h225 events
debug h245 events
```

Debug avanzati H323

```
debug cch323 h225
debug cch323 h245
debug cch323 all
```

Risorse multimediali SCCP

Questi debug vengono utilizzati per risolvere i problemi relativi alle risorse multimediali SCCP (Skinny Call Control Protocol) che coinvolgono MTP (Media Termination Point) o Transcoder registrati su un server Cisco Unified Communications Manager (CUCM):

Debug SCCP di base

```
debug sccp messages
debug sccp events
debug sccp errors
```

Debug SCCP avanzato

```
debug sccp all
```

Traccia VoIP

Con l'introduzione di Cisco IOS-XE 17.4.1 e 17.3.2, è disponibile una nuova opzione per acquisire i log vocali all'interno del CUBE (Cisco Unified Border Element). Questa nuova funzionalità è denominata Traccia VoIP. Si tratta di una nuova struttura di servizi creata per registrare i segnali SIP e gli eventi senza la necessità di abilitare debug.

La traccia VoIP è abilitata per impostazione predefinita e può essere disabilitata in qualsiasi momento. VoIP Trace acquisisce informazioni specifiche solo per le chiamate SIP:

- Messaggi SIP per chiamate da trunk SIP a trunk
- Eventi e chiamate API dal livello SIP ad altri livelli nel CUBE
- Errori SIP
- Controllo delle chiamate (flussi di chiamate Unified Communications elaborati da CUBE)
- Stati ed eventi di macchine a stato finito (FSM)
- Dial Peer corrispondente
- Porte RTP allocate
- Correlazione degli errori IEC con la segnalazione SIP

Restrizioni

- La traccia VoIP non registra le informazioni correlate ai messaggi SIP fuori dialogo: REGISTRATIOPZIONIISCRIVITI/NOTIFICAINFORMAZIONI
- La traccia VoIP in HA è supportata, tuttavia si applicano le seguenti avvertenze: Per impostazione predefinita, per il router in standby la traccia VoIP è abilitata. Vengono presentate solo le tracce applicabili per il processo di standby fino a quando non diventa attivoQuando lo standby è attivo, **NON** contiene le tracce complete delle chiamate a checkpoint e solo le nuove chiamate**show voip trace <key>** funziona ancora sul router di standby e visualizza il buffer di copertura e i dati del flusso multimediale per le chiamate

Come abilitare la traccia VoIP

Come accennato in precedenza, questa funzione è abilitata per impostazione predefinita. Il comando per abilitare questa funzione è:

```
Router# configuration terminal
Router(config)# voice service voip
Router(conf-voi-serv)# trace
Router(conf-serv-trace)#
```

Come disabilitare la traccia VoIP

Per disabilitare questa funzione, i comandi sono:

```
Router(conf-serv-trace)# no trace
!or
Router(conf-serv-trace)# shutdown
```

> **Attenzione:** Dopo aver disattivato la traccia VoIP, tutta la memoria viene cancellata e le informazioni vengono perse.

I comandi disponibili nella modalità di configurazione traccia sono:

```
Router(conf-serv-trace)# ?
default       Set a command to its defaults
 exit          Exit from voice service voip trace mode
 memory-limit  Set limit based on memory used
 no            Negate a command or set its defaults
 shutdown      Shut Voip Trace debugging
```

Configura limite di memoria

Il limite di memoria determina la quantità di memoria utilizzata dalla traccia VoIP per archiviare i dati. Per impostazione predefinita, è il 10% della memoria disponibile nella piattaforma, ma può essere modificato in un massimo di 1 GB e un minimo di 10 MB. La memoria allocata in modo dinamico, ovvero la funzionalità utilizza la memoria solo in base alle esigenze e dipende dal volume di chiamata. Una volta raggiunta la quantità massima di memoria disponibile, la macro esegue un cerchio ed elimina le voci meno recenti.

Quando il limite di memoria viene modificato in modo che sia maggiore del 10% della memoria disponibile, viene visualizzato un messaggio nell'interfaccia della riga di comando:

```
Router(conf-serv-trace)# memory-limit 1000
Warning: Setting memory limit more than 10% of available platform memory (166 MB) will affect
system performance.
```

Per impostare l'utilizzo predefinito della memoria al 10%, è possibile utilizzare il comando **memory-limit platform**:

```
Router(conf-serv-trace)# memory-limit platform
 Reducing the memory-limit clears all VoIP Trace statistics and data.
 If you wish to copy this data first, enter 'no' to cancel,
 otherwise enter 'yes' to proceed. Continue? [no]:
```

> **Attenzione:** Quando si riduce il limite di memoria, tutti i dati di traccia VoIP vengono persi. Prima di ridurre la memoria è necessario raccogliere un backup dei dati.

Come visualizzare i dati di traccia VoIP

Per visualizzare i dati da VoIP Trace, è necessario utilizzare comandi show specifici. I dati possono essere visualizzati nella stessa sessione del terminale o inviati tramite Syslog a un server syslog esterno.

> **Nota:** Le tracce vengono scaricate dopo 32 secondi dalla ricezione di un BYE per una chiamata.

> **Nota:** Il segnale SIP viene visualizzato per tappa e non è combinato come un normale debug. I debug regolari, come i **messaggi debug ccsip** visualizzano la segnalazione SIP di una chiamata nell'ordine esatto in cui si sono verificati gli eventi. Nella traccia VoIP ogni segmento è separato. Per determinare l'ordine corretto, vengono utilizzati i timestamp.

Per visualizzare i dati, sono disponibili i seguenti comandi:

```
Router# show voip trace ?
 all            Display all VoIP Traces
 call-id        Filter traces based on Internal Call Id
 correlator     Filter traces based on FPI Correlator
 cover-buffers  Display the summary of all cover buffers
 session-id     Filter traces based on SIP Session ID
 sip-call-id    Filter traces based on SIP Call Id
 statistics     Display statistics for VoIP Trace
```

show voip trace all

Con questo comando vengono visualizzati tutti i dati di traccia VoIP disponibili nel buffer. L'uso di questo comando influisce sulle prestazioni del router. Una volta immesso il comando, viene visualizzato un messaggio di avvertenza per avvisare del rischio e confermare per continuare:

```
Router# show voip trace all
 Displaying 11858 cover buffers
 This may severely impact system performance.
 Continue? [yes/no] no
```

show voip trace cover-buffer

Questo comando visualizza una panoramica dei dettagli delle chiamate per tutte le chiamate segnalate in Traccia VoIP. Ogni tappa della chiamata dispone di un buffer di copertura che contiene un riepilogo della chiamata registrata.

```
Router# show voip trace cover-buffers
------------------ Cover Buffer ---------------
Search-key = 8845:3002:659
Timestamp = *Sep 30 01:17:33.615
Buffer-Id = 1
CallID = 659
Peer-CallID = 661
Correlator = 4
Called-Number = 3002
Calling-Number = 8845
```

```
SIP CallID = 20857880-1ec12085-13b930-411b300a@10.48.27.65
SIP Session ID = 2b1289c400105000a0002c3ecf872659
GUID = 208578800000
-----------------------------------------------

------------------ Cover Buffer ---------------
Search-key = 8845:3002:661
Timestamp = *Sep 30 01:17:33.634
Buffer-Id = 2
CallID = 661
Peer-CallID = 659
Correlator = 4
Called-Number = 3002
Calling-Number = 8845
SIP CallID = 8D6DEC28-1F111EB-829FD797-1B22F6DB@10.48.55.11
SIP Session ID = 0927767800105000a0005006ab805584
GUID = 208578800000
-----------------------------------------------
```

Per ulteriori informazioni su ciascun campo, consultare la tabella seguente:

Campo	Descrizione
Chiave di ricerca	Contiene una combinazione di chiamata, chiamata numero e call-id
Timestamp	Ora di creazione del buffer di copertura
Buffer-ID	ID buffer del buffer di copertura
Call-id	Call-id del segmento di chiamata corrispondente del buffer di copertura
Peer-CallID	ID chiamata della gamba peer
Correlatore	Correlatore FPI della chiamata
Numero chiamato	Numero richiamato della gamba di richiamo del buffer di copertura
Calling-number	Numero chiamante del segmento di chiamata corrispondente del buffer di copertura
Sip Call-ID	Call-id SIP del segmento di chiamata corrispondente del buffer di copertura
ID sessione SIP	ID sessione SIP della rispettiva parte di chiamata del buffer di copertura
GUID	GUID della chiamata corrispondente del buffer di copertura
Gamba di ancoraggio	La gamba di ancoraggio è impostata su yes se la gamba di richiamo corrispondente è una gamba di ancoraggio nel flusso di richiamo o distribuzione del proxy di supporto
Gamba biforcata	Gamba biforcata è impostata su yes se la gamba di richiamo corrispondente è una gamba di ancoraggio nel flusso di richiamo o nella distribuzione del proxy multimediale
ID Call associati	Call-id delle gambe biforcate associate

Per filtrare i buffer di copertura, è possibile utilizzare i comandi **include** e **section**:

```
Router# show voip trace cover-buffers | include Search-key | 8845 | 3002
Search-key = 8845:3002:661
!or
Router# show voip trace cover-buffers | section Search-key | 8845 | 3002
Search-key = 8845:3002:661
```

show voip trace call-id

In combinazione con il comando precedente, è possibile utilizzare **show voip trace call-id** per trovare le chiamate. Dopo aver identificato l'id della chiamata, è possibile utilizzare questo comando per visualizzare tutte le informazioni relative alla coda di chiamata specifica:

```
Router# show voip trace cover-buffers | include Search-key | 8845 | 3002
Search-key = 8845:3002:661
```

```
Router# show voip trace call-id 661
```

mostra statistiche traccia voip

Questo comando show visualizza un output dettagliato su stato, consumo di memoria, chiamate errate o non riuscite, chiamate riuscite, timestamp delle voci più recenti e meno recenti e altro ancora.

```
Router# show voip trace statistics
VoIP Trace Statistics
Tracing status             : ENABLED at *Sep 12 06:44:02.349
Memory limit configured    : 803209216 bytes
Memory consumed            : 254550928 bytes (31%)
Total call legs dumped     : 2
Oldest trace dumped        : *Sep 12 07:29:21.077 Search-key: 9898:30000:64
Latest trace dumped        : *Sep 12 07:29:21.010 Search-key: 9898:30000:63
Total call legs captured   : 11858
Total call legs available  : 11858
Oldest trace available     : *Sep 12 06:57:23.923, Search-key: 5250001:4720001:11
Latest trace available     : *Sep 13 05:08:25.353, Search-key: 19074502232:30000:13177
Total traces missed        : 0
```

Per ulteriori informazioni su ciascun campo, fare riferimento alla tabella seguente:

Campo	Descrizione
Stato traccia	Visualizza lo stato di traccia, inclusa la data e l'ora in cui è stata abilitata la traccia VoIP.
Limite di memoria configurato	Visualizza il limite di memoria configurato. 10% delle dimensioni della memoria del pool di processori
Memoria utilizzata	Visualizza la quantità di memoria utilizzata in modo dinamico per la traccia VoIP
Totale gambe chiamate scaricate	Visualizza il numero di segmenti di chiamata non riusciti scaricati nel buffer di registrazione. Le chiamate di tipo dump si riferiscono a co di chiamata associati a errori IEC
Traccia meno recente di cui è stato eseguito il dump	Visualizza i timestamp e la chiave di ricerca della chiamata non riuscita meno recente dall'abilitazione della traccia VoIP
Ultima traccia di cui è stato eseguito il dump	Visualizza i timestamp e la chiave di ricerca dell'ultima chiamata non riuscita dall'abilitazione della traccia VoIP
Totale gambe chiamate acquisite	Visualizza il totale dei segmenti acquisiti dopo l'abilitazione della traccia VoIP
Totale gambe chiamate disponibili	Visualizza il totale delle parti di chiamata disponibili nella cronologia. Può essere ugu diverso rispetto al totale delle code di chiamata acquisite, a seconda del limite di mer
Traccia meno recente disponibile	Visualizza l'indicatore orario e la chiave di ricerca del buffer di copertura più vecchio disponibile in memoria
Traccia più recente disponibile	Visualizza l'indicatore orario e la chiave di ricerca dell'ultimo buffer di copertura dispo nella memoria
Tracce mancanti totali	Visualizza il numero di segmenti di chiamata non riusciti a causa del limite di memori

Comandi show aggiuntivi

Campo	Utilizzo	
show voip trace correlator <correlatore>	show voip trace correator 4	Filtra e visualizza la traccia VOIP per un ID chiamata specifi
show voip trace session-id <id-sessione>	show voip trace session-id 87003120822b5dbd8fd80f62d8e57c48	Filtra e visualizza la traccia VOIP per utilizzare l'UUID locale o remoto prese per visualizzare entrambi i component
show voip trace sip-call-id <id-chiamata>	show voip trace sip-call-id 01e60dfa9d8442848336d79e3155a8a1	Filtra e visualizza la traccia VOIP in ba

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).