Configuración de la recopilación de depuración para gateways de Unified Border Element (CUBE) y de multiplexación por división de tiempo (TDM)

Contenido

Introducción

Este documento describe algunas de las prácticas recomendadas para recopilar los debugs de voz en un router de voz IOS/IOS-XE de Cisco.

Prerequisites

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Requirements

- Conocimientos básicos de Cisco IOS/IOS-XE en routers de servicios integrados (ISR).
- Acceso privilegiado para ejecutar comandos en los routers ISR.
- Se requiere experiencia previa con protocolos de voz sobre IP (VoIP).
- Para VoIP Trace se requiere un mínimo de Cisco IOS-XE 17.4.1 o 17.3.2.

Componentes Utilizados

A efectos del presente documento, los componentes utilizados son:

- Cisco ISR 3925
- Cisco ISR 4451
- PuTTY

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

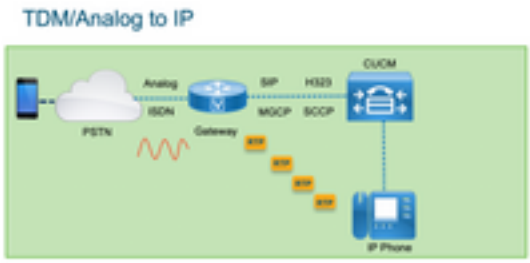
El proceso de recolección de depuración en estas plataformas tiene desafíos y podría afectar

potencialmente el rendimiento del dispositivo. Los retos y riesgos aumentan cuando se establecen varias llamadas activas en un router de voz. En algunos escenarios, si los debugs no se recolectan correctamente, puede conducir a una CPU alta que podría perjudicar la capacidad del router e incluso causar una caída del software. Este documento trata sobre la diferencia entre un Cisco Unified Border Element (CUBE) y un TDM/Analog Gateway.

Gateways de voz TDM frente a CUBE

Los gateways de voz TDM se utilizan principalmente para interconectar un sistema telefónico interno con otra centralita privada (PBX) o la red pública de telefonía conmutada (PSTN). El tipo de conexiones que se utilizan en las puertas de enlace TDM son los controladores T1/E1 (ISDN o CAS) y los circuitos analógicos como los puertos FXS y FXO. Un procesador de señales digitales (DSP) convierte el audio de su forma original en paquetes RTP. De manera similar, los paquetes RTP se convierten en audio sin procesar después de que el DSP haya procesado los paquetes RTP y envíe el audio en el circuito específico. Estas puertas de enlace pueden interoperar con H323, MGCP o SCCP en el lado de VoIP, y en el lado de TDM sus circuitos ISDN PRI o analógico como las conexiones más comunes a PSTN o terminales.

Como se muestra en la imagen, las puertas de enlace TDM proporcionan un puente entre su infraestructura VoIP interna y los proveedores de servicios analógicos o ISDN.



Con la introducción de VoIP, los clientes comenzaron a cambiar rápidamente sus sistemas heredados a una infraestructura VoIP moderna. Lo mismo ocurrió en el lado del proveedor de servicios, donde ahora utilizan conexiones para interconectar los servicios de telefonía en las instalaciones con la infraestructura VoIP del proveedor de servicios y ampliar sus capacidades para proporcionar mejores servicios. El protocolo VoIP más habitual que se utiliza actualmente es el protocolo de inicio de sesión (SIP), que en la actualidad utilizan habitualmente los clientes y los proveedores de servicios de telefonía por Internet (ITSP) de todo el mundo.

CUBE se introdujo para proporcionar una forma de interconectar esos sistemas VoIP internos con el mundo externo a través de los ITSP con SIP como el protocolo VoIP principal. CUBE es simplemente un gateway IP-IP en el que ya no necesita ningún tipo de conexión TDM, como controladores T1/E1 o puertos analógicos. CUBE se ejecuta en las mismas plataformas que los gateways TDM.

El protocolo VoIP más utilizado es SIP, para el establecimiento y el cierre de llamadas, y RTP para el transporte de medios. En CUBE no se necesita un DSP a menos que se requiera un transcodificador. El tráfico RTP fluye de extremo a extremo desde el ITSP al terminal, y CUBE actúa como intermediario con la ocultación de direcciones como una de las muchas funciones que ofrece.

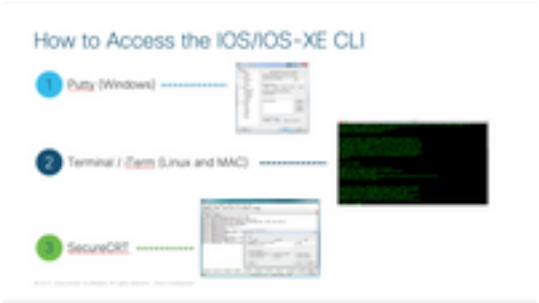
Como se muestra en la imagen, CUBE proporciona una división entre su infraestructura VoIP interna y SIP ITSP:

Colección de Cisco IOS/IOS-XE Voice Debugs

Las funciones de voz se ejecutan en una lista diferente de plataformas, como ISR, ASR, CAT8K, entre otras, sin embargo, utilizan un software común que es Cisco IOS o Cisco IOS-XE (las diferencias entre Cisco IOS y Cisco IOS-XE no se tratan en este artículo). Comencemos con los conceptos básicos sobre cómo acceder al router Cisco IOS.

Cómo acceder a un router Cisco IOS/IOS-XE a través de la interfaz de línea de comandos (CLI)

Los routers, como cualquier otro dispositivo basado en CLI, requieren un monitor de terminal para obtener acceso y ejecutar los comandos a través de Secure Shell (SSH) o Telnet. SSH es el protocolo más utilizado actualmente para acceder a los dispositivos, ya que proporciona una conexión segura y cifrada con el dispositivo. Algunos de los monitores de terminal comunes utilizados para acceder a la CLI de los routers son:

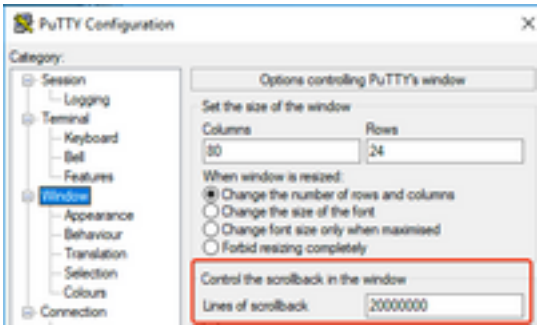


Cómo configurar Terminal Monitor para recopilar comandos show o depuraciones

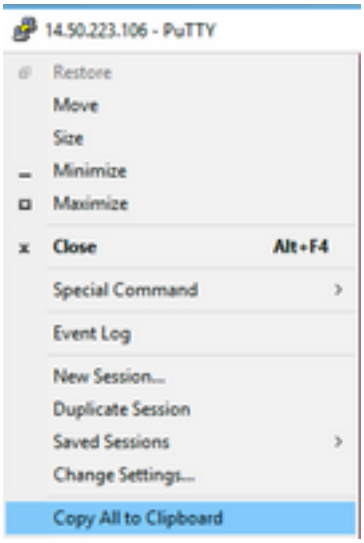
Hay diferentes maneras de recopilar el resultado de la CLI. Se recomienda exportar la información de la CLI del router a un archivo independiente. Esto facilita el intercambio de información con terceros.

Algunas formas de recopilar las salidas del dispositivo son:

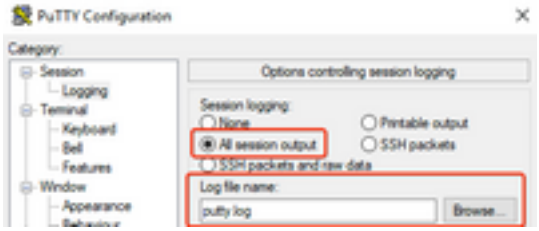
- Vuelca toda la salida en el terminal, para esto debe asegurarse de que hay suficientes líneas de desplazamiento hacia atrás, de lo contrario el desplazamiento hacia atrás pierde las primeras secciones de la salida y los datos pueden estar incompletos. Para aumentar las líneas de desplazamiento en masilla, navegue hasta Configuración de masilla > Ventana > Líneas de desplazamiento. Normalmente, se establece en un valor muy alto para tener suficiente salida de desplazamiento:



Más adelante puede recopilar la información desde el monitor de terminal con la opción **Copiar todo en el Portapapeles** y pegar el resultado en un archivo de texto:



- Otra opción es registrar el resultado de toda la sesión en un archivo .txt. Con esta opción, todos los comandos introducidos y las salidas recopiladas se registran inmediatamente en el archivo de texto. Esta es una práctica común para registrar todos los resultados en una sesión. Para registrar toda la salida de sesión en un archivo en masilla, navegue hasta **Configuración de masilla > Sesión > Registro** y luego seleccione Toda la salida de sesión de la siguiente manera:



> **Nota:** Si no se especifica otro nombre, se utiliza el nombre del archivo de registro predeterminado. Haga clic en el botón Browse (Examinar) para saber exactamente dónde se guarda el archivo y poder encontrarlo más adelante. Asegúrese también de no sobrescribir otro archivo putty.log en la misma ruta de acceso.

Recopile el resultado básico del comando show desde la CLI

Los comandos Show son necesarios para recopilar información básica del router antes de que tenga lugar cualquier recopilación de depuración. Los comandos Show se recopilan rápidamente y, en general, no afectan al rendimiento del router. El aislamiento del problema podría comenzar inmediatamente con solo un resultado del comando show.

Una vez conectado al router, la longitud del terminal se puede establecer en 0. Esto puede hacer que la recopilación sea más rápida para mostrar toda la salida a la vez y evitar el uso de la barra espaciadora. El único comando que recopila información detallada sobre el router es 'show tech' y, alternativamente, puede recopilar **show tech voice**, que muestra datos más específicos de las funciones de voz habilitadas en el 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
```

Recopile la salida de depuración de la CLI

La recopilación de salida de depuración en Cisco IOS/IOS-XE puede ser a veces un desafío, ya que existe el riesgo de una caída del router. Sin embargo, algunas de las prácticas recomendadas se explican en las siguientes secciones para evitar problemas.

Comprobación de memoria

Antes de habilitar cualquier depuración, debe asegurarse de que haya suficiente memoria para almacenar el resultado en el búfer.

Ejecute el comando **show process memory** para averiguar cuánta memoria puede asignar para registrar todos los resultados en el buffer:

> **Consejo:** Utilice el comando **terminal length default** o **terminal length <num_lines>** para volver a una cantidad limitada de líneas que se muestran en el terminal.

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

En el ejemplo, hay 7666268552 bytes (7,6 GB) libres para ser utilizados por el router. El router comparte esta memoria entre todos los procesos del sistema, lo que significa que no puede utilizar toda la memoria libre para registrar la salida en el búfer, pero puede utilizar una buena cantidad de memoria del sistema según sea necesario.

La mayoría de los escenarios requieren al menos 10 MB para recopilar suficiente salida de depuración antes de que la salida se pierda o se sobrescriba. En raras ocasiones se requiere una mayor cantidad de datos para ser recolectados, en esos escenarios específicos puede obtener un valor de salida de 50MB a 100MB en el buffer o puede ir más alto siempre que haya memoria disponible.

Si la memoria libre es baja, entonces hay un problema de pérdida de memoria potencial; si este es el caso, por favor contacte al equipo del TAC de arquitectura para revisar cuál podría ser la causa de tal memoria baja.

Comprobación de la unidad central de procesamiento (CPU)

La CPU se ve afectada por la cantidad de procesos, funciones y llamadas activas en el sistema.

Cuantas más funciones o llamadas estén activas en el sistema, más ocupada estará la CPU.

Un buen punto de referencia es asegurarse de que el router tiene la CPU al 30% o menos, lo que significa que puede habilitar de forma segura depuraciones de básicas a avanzadas (esté siempre atento a la CPU cuando se utilicen depuraciones avanzadas). Si la CPU del router está en alrededor del 50%, se pueden ejecutar depuraciones básicas y supervisar cuidadosamente la CPU. Si la CPU supera el 80%, detenga inmediatamente las depuraciones (que se muestran más adelante en este artículo) y solicite ayuda al TAC.

Utilice el comando **show process cpu sorted | exclude 0.00** para verificar los últimos 5 s, 60 s y 5 min valores de CPU junto con los procesos principales.

```
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
```

En el resultado, el router no tiene mucha actividad, la CPU es baja y las depuraciones se pueden habilitar de forma segura.

> **Precaución:** Preste especial atención a los principales procesos de CPU activos, si la CPU está al 50% o más y el proceso superior es un proceso de voz, solo se pueden habilitar las depuraciones básicas. Supervise continuamente la CPU con el comando para asegurarse de que el rendimiento general del router no se vea afectado.

Comprobación de llamadas activas actuales

Cada router tiene umbrales de capacidad diferentes. Es importante comprobar cuántas llamadas hay activas en el router para asegurarse de que no se aproxima a la capacidad máxima. La hoja de datos de Cisco Unified Border Element versión 12 proporciona información sobre la capacidad de cada plataforma para referencia.

Utilice el comando **show call active total-calls** para hacerse una idea de cuántas llamadas hay activas en el sistema:

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

Utilice el comando **show call active voice summary** para obtener información más detallada de los tipos de llamada específicos que están activos:

```
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
```

Algunos de los valores comunes son:

- **Tramos de llamadas de telefonía**: Llamadas de gateway TDM, incluidas las llamadas analógicas y PRI/ISDN.
- **Tramos de llamada SIP**: Total de llamadas SIP. Si se trata de un router CUBE, muestra dos tramos de llamada por llamada. Divida el total de llamadas mostradas aquí por 2 para obtener un número exacto.
- **Tramos de llamada H323**: Total de llamadas H323.
- **Tramos de llamada SCCP**: Recursos de medios controlados de CUCM utilizados en el router como transcodificador y MTP.

Configuración del búfer de registro

Para configurar el router para almacenar la salida de depuración en el búfer, se ingresa el modo de terminal de configuración para ajustar manualmente los ajustes en la CLI. Esta configuración no tiene impacto en el router; sin embargo, como se muestra en las secciones anteriores, se necesita el comando **show tech** o el comando **show running-config** del router en caso de que sea necesario revertir la configuración.

A continuación se puede ver un ejemplo de configuración, que es una línea de base común utilizada por los ingenieros del TAC. El ejemplo asigna 10 MB de memoria intermedia, pero se puede aumentar según sea necesario:

```
# 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
```

Los comandos realizan estas tareas:

- **service timestamps debug or log**: Asegura que la hora del router local se escribe en cada mensaje registrado, con precisión de milisegundos. Esto es útil para encontrar llamadas basadas en la hora. Las marcas de tiempo en milisegundos permiten agrupar líneas de depuración en eventos lógicos relacionados cuando dos líneas se producen en el mismo milisegundo.
- **números de secuencia de servicio:** Escribe el número de secuencia de la depuración en la línea. Esto es útil (esencialmente necesario) cuando los registros se reenvían a un servidor syslog. Esto es muy útil para identificar si cualquier mensaje de depuración al servidor syslog se ha descartado en la red. El número de secuencia es el primer elemento de la depuración, antes de la marca de tiempo y del mensaje de registro real. Tenga en cuenta que esto es diferente de la marca de tiempo/número de secuencia que los servidores syslog pueden escribir localmente en sus archivos.
- **búfer de registro**: Indica al router que envíe depuraciones a su memoria intermedia local. El tamaño del búfer se establece en bytes. En la configuración, el tamaño del búfer se estableció en 10 MB.
- **no logging console** y **no logging monitor:** No se imprimen mensajes de registro en la consola o en el monitor de terminal. Si estos comandos no se configuran, podrían ser perjudiciales

para el rendimiento del router y la precisión de la salida de depuración.
- **voice iec syslog:** Habilita mensajes de códigos de error internos de voz para determinar las razones de desconexión.

Configuración de Syslog

A veces, los problemas pueden ser aleatorios y requieren una manera de recopilar continuamente las depuraciones hasta que ocurre el evento. Cuando almacena las depuraciones en el búfer, las recopila continuamente. Tenga en cuenta que está limitado a la cantidad de memoria que puede asignar y una vez que alcanza esa cantidad de memoria, el búfer da vueltas y descarta los mensajes más antiguos, lo que da lugar a información valiosa incompleta que se requiere para aislar el problema.

Con Syslog, el router puede enviar todos los mensajes de depuración a un servidor externo, donde el software del servidor Syslog los almacena en archivos de texto. Aunque es una buena manera de recopilar el resultado de la depuración, no es el método preferido para la recopilación de registros. Los servidores de Syslog tienden a saltar o descartar líneas de la salida recibida debido a la congestión en el servidor, ya que la salida de depuración puede abrumar al servidor, o los paquetes pueden descartarse debido a las condiciones de la red. Sin embargo, en algunos escenarios Syslog es la única manera de avanzar en un problema.

Si es posible, utilice un método de transporte confiable como TCP para evitar cualquier pérdida de información y, como sugerencia, conecte el servidor Syslog al mismo switch donde está conectado el router o lo más cerca posible del router. Todavía no garantiza que todos los datos se almacenen en los archivos, pero reduce las posibilidades de pérdida de datos.

De forma predeterminada, los servidores syslog utilizan UDP como protocolo de transporte en el puerto 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
```

Tan pronto como se configuran los comandos, el router reenvía inmediatamente los mensajes a la dirección IP del servidor Syslog.

Colección Debug

Una vez que se han habilitado los debugs, el buffer debe ser borrado antes de que se reproduzca el problema. Esto se hace para garantizar que el resultado sea lo más limpio posible y evitar cualquier dato adicional que no sea necesario para el análisis. Ejecute el comando **clear log**, esto garantiza que se borre el buffer. Si hay otras llamadas activas en el router y las depuraciones están activadas, el resultado se imprime inmediatamente en el búfer.

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

Después de reproducir el problema, inhabilite las depuraciones inmediatamente para detener más salida en el buffer. A continuación, recopile los registros. Puede volcar toda la salida en el terminal con los comandos:

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

A veces PuTTY se cierra, ya que no es capaz de manejar toda la salida a la vez, esto es normal y no significa que haya ocurrido una falla, si esto sucede reabra la sesión de nuevo y continúe normalmente. En escenarios donde el buffer de registro es demasiado grande o el monitor de terminal falla debido a la cantidad de datos que se deben imprimir, copie la salida del buffer a un dispositivo externo directamente con el comando **show log | redirigir**:

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

El comando copia el resultado completo del búfer en un ftp con la dirección IP 192.168.1.2 con el nombre de archivo debug.txt. El nombre de archivo siempre debe especificarse. Otros destinos disponibles para exportar esos datos son:

```
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
```

¿Qué depuraciones se pueden habilitar en los routers de voz?

Cada flujo de llamada y tipo de funciones (TDM, CUBE o SCCP (recursos multimedia)) son diferentes y hay depuraciones específicas que puede habilitar. Todas las depuraciones necesarias deben estar habilitadas al mismo tiempo. Cuando solo se captura una depuración a la vez es ineficaz y proporciona más confusión cuando se analizan los datos.

Las depuraciones están habilitadas dentro del comando CLI exec prompt level **Router#**, que requiere que tenga permisos de modo de ejecución con privilegios.

Hay depuraciones básicas y avanzadas. Las depuraciones básicas se utilizan para recopilar información de señalización en SIP, H323 o MGCP, que muestra las conversaciones del router con sus dispositivos pares.

Las depuraciones avanzadas son muy detalladas y normalmente se utilizan para recopilar más información en caso de errores de pila internos que las depuraciones básicas no pueden mostrar. Estos debugs son normalmente intensivos en CPU.

> **Consejo:** Una vez que se habiliten las depuraciones, recuerde ejecutar el comando **clear logging**. Este comando garantiza que el buffer esté despejado para una captura más limpia de los debugs.

Depuración de API de control de llamadas interno (CCAPI)

Dentro de cada router IOS/IOS-XE de Cisco hay una API de control de llamadas que se encarga de la comunicación entre diferentes aplicaciones VoIP, o protocolos, y los componentes del plano de datos, como RTP, DSP, tarjetas de voz, entre otros. Para capturar los datos de esta capa hay una depuración específica que se puede utilizar:

```
debug voip ccapi inout
```

Hay otras opciones para esta depuración, sin embargo, **debug voip ccapi inout** cubre toda la información básica de plan de marcado y establecimiento de llamadas que normalmente es más que suficiente para entender cuáles son los estados de esta capa.

> **Consejo: debug voip ccapi inout** suele tener un impacto mínimo en la CPU del router y se recomienda habilitarlo junto con cualquier depuración de señalización para proporcionar un conjunto completo de registros con información de las llamadas y sus diferentes estados.

Flujos de llamadas SIP

Estas depuraciones son las más utilizadas para flujos de llamadas SIP y se pueden habilitar dentro de gateways CUBE y TDM con un tramo SIP entre el router y CUCM o cualquier otro servidor/proxy SIP.

Depuraciones SIP básicas

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

Depuraciones SIP avanzadas

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

Flujos de llamadas digitales (PRI, BRI)

Estas depuraciones se aplican a Interfaces de velocidad primaria (PRI) T1/E1 o Interfaces de velocidad básica (BRI):

Depuración digital básica

```
debug isdn q931
```

Depuración digital avanzada

```
debug isdn q921
```

Flujos de llamadas analógicas

Estas depuraciones se utilizan cuando hay circuitos analógicos involucrados, como los puertos del suscriptor de Foreigh eXchange (FXS) o del Foreign eXchange Office (FXO):

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

Flujos de llamadas MGCP

Estas depuraciones se utilizan cuando se utiliza MGCP como protocolo de voz entre una puerta de enlace de voz y CUCM.

Depuraciones básicas

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

Depuraciones de CCM-Manager

El **debug ccm-manager** se utiliza para realizar un seguimiento de los mensajes de descarga de configuración, MoH y retorno PRI/BRI entre CUCM y la gateway de voz. Estos debugs se utilizan según sea necesario y dependen del escenario de falla.

```
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
```

Depuraciones MGCP avanzadas

```
debug mgcp all
```

Flujos de llamadas H323

Aunque H323 no se utiliza ampliamente, todavía hay algunas implementaciones con H323 configurado:

Depuraciones básicas de H323

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

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

Depuraciones avanzadas de H323

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

Recursos de medios SCCP

Estas depuraciones se utilizan para solucionar problemas de recursos multimedia del Protocolo ligero de control de llamadas (SCCP) que afectan al punto de terminación de medios (MTP) o a los transcodificadores registrados en un servidor de Cisco Unified Communications Manager (CUCM):

Depuraciones SCCP básicas

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

Depuración SCCP avanzada

```
debug sccp all
```

Seguimiento de VoIP

Con la introducción de Cisco IOS-XE 17.4.1 y 17.3.2 existe una nueva opción para capturar registros de voz dentro de Cisco Unified Border Element (CUBE). Esta nueva función se llama VoIP Trace. Se trata de un nuevo marco de mantenimiento creado para registrar la señalización SIP y los eventos sin necesidad de habilitar ninguna depuración.

VoIP Trace está activado de forma predeterminada y se puede desactivar en cualquier momento según sea necesario. VoIP Trace captura información específica solo para llamadas SIP:

- Mensajes SIP para llamadas de troncal SIP a troncal SIP
- Eventos y llamadas a API desde la capa SIP a otras capas de CUBE
- Errores SIP
- Control de llamadas (flujos de llamadas de Unified Communication procesados por CUBE)
- Estados y eventos de máquinas de estado finito (FSM)
- Dial Peer match
- Puertos RTP asignados
- Correlación de errores IEC con señalización SIP

Restricciones

- VoIP Trace no registra información relacionada con los mensajes SIP fuera de diálogo: REGISTROOPCIONESSUSCRIBIRSE/NOTIFICARINFO
- Se admite el seguimiento VoIP en HA; sin embargo, se aplican estas advertencias: El router en espera tiene activado VoIP Trace de forma predeterminada. Solo se muestran los

seguimientos aplicables para el proceso en espera hasta que se activaUna vez que el modo en espera está activo, **NO** contiene seguimientos completos de llamadas verificadas y solo llamadas nuevas**show voip trace <key>** aún funciona en el router en espera y muestra los datos del búfer de cobertura y del flujo de medios para las llamadas

Cómo Habilitar el Seguimiento VoIP

Como se ha mencionado, esta función está activada de forma predeterminada. El comando para habilitar esta función es:

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

Cómo Inhabilitar VoIP Trace

Para desactivar esta función, los comandos son:

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

Precaución: Una vez que se inhabilita el seguimiento VoIP, se borra toda la memoria y se pierde la información.

Los comandos disponibles dentro del modo de configuración trace son:

```
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
```

Configurar límite de memoria

El límite de memoria determina cuánta memoria utiliza VoIP Trace para almacenar los datos. De forma predeterminada es el 10% de la memoria disponible en la plataforma, pero puede cambiarse a un máximo de 1 GB y un mínimo de 10 MB. La memoria que se asigna dinámicamente, lo que significa que la función solo utiliza memoria según sea necesario y depende del volumen de la llamada. Una vez que alcanza la memoria máxima disponible, da vueltas y elimina las entradas más antiguas.

Cuando el límite de memoria se modifica para ser mayor que el 10% de memoria disponible, se muestra un mensaje en la Interfaz de línea de comandos:

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

Para establecer el valor predeterminado del 10% de uso de memoria, se puede utilizar el

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]:
```

> **Precaución:** Cuando se reduce el límite de memoria, se pierden todos los datos de VoIP Trace. Se debe recopilar una copia de seguridad de los datos antes de reducir la memoria.

Cómo Mostrar Datos de Rastreo VoIP

Para mostrar los datos de VoIP Trace necesitamos utilizar comandos show específicos. Los datos se pueden mostrar en la misma sesión de terminal o también se pueden enviar a través de Syslog a un servidor syslog externo.

> **Nota:** Los seguimientos se descartan transcurridos 32 segundos desde el momento en que se recibe un BYE para una llamada.

> **Nota:** La señalización SIP se muestra por tramo y no se combina como depuraciones regulares. Los debugs regulares como **debug ccsip messages** muestran la señalización SIP de una llamada en el orden exacto en que ocurrieron los eventos. En VoIP Trace cada tramo es independiente. Para determinar el orden correcto, se utilizan las marcas de tiempo.

Los comandos disponibles para mostrar los datos son:

```
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

Este comando muestra todos los datos de rastreo VoIP disponibles en el buffer. El uso de este comando afecta al rendimiento del router. Una vez que se ingresa el comando, se muestra un mensaje de advertencia para alertar sobre el riesgo y confirmar que se continúe:

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

show voip trace cover-buffers

Este comando muestra una descripción general de los detalles de llamada para todas las llamadas notificadas bajo Seguimiento VoIP. Cada segmento de llamada tiene un búfer de cobertura creado que contiene un resumen de la llamada registrada.

```
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 = 09277678001050000a0005006ab805584
GUID = 208578800000
-------------------------------------------
```

Para obtener más información sobre cada campo, consulte la siguiente tabla:

Campo	Descripción
Search-Key	Contiene una combinación de call, called number y call-id
Grupo fecha/hora	Tiempo de creación del búfer de cobertura
Buffer-ID	ID del búfer de cobertura
ID de llamada	ID de llamada del tramo de llamada respectivo de a la memoria intermedia de la cubierta
Peer-CallID	ID de llamada del tramo de peer
Correlador	Correlator FPI de la llamada
Called-number	Número llamado del tramo de llamada respectivo del búfer de cobertura
Calling-number	Número de llamada del tramo de llamada respectivo del búfer de cobertura
Sip Call-ID	Sip call-id del tramo de llamada respectivo del buffer de cobertura
ID de sesión Sip	ID de sesión SIP del tramo de llamada respectivo del búfer de cobertura
GUID	GUID de la llamada respectiva del búfer de cubierta
Pierna de anclaje	El tramo de anclaje se establece en sí si el tramo de llamada respectivo es un tramo de anclaje en el flujo de bifurcación de llamada o e implementación de proxy de medios
Tronco bifurcado	El tramo bifurcado se establece en sí si el tramo de llamada respectivo es un tramo de anclaje en el flujo de bifurcación de llamada o en implementación de proxy de medios
ID de llamadas asociadas	ID de llamada de los tramos bifurcados asociados

Para filtrar los buffers de cubierta podemos utilizar los comandos **include** y **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

En combinación con el comando anterior, **show voip trace call-id** se puede utilizar para encontrar las llamadas. Una vez identificado el call-id, este comando se puede utilizar para mostrar toda la información sobre el tramo de llamada específico:

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

show voip trace statistics

Este comando show muestra información detallada sobre el estado, el consumo de memoria, las llamadas con errores o con errores, las llamadas exitosas, las marcas de tiempo de las entradas más recientes y más antiguas y más.

```
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
```

Para obtener más información sobre cada campo, consulte la siguiente tabla:

Campo	Descripción
Estado de seguimiento	Muestra el estado de seguimiento, incluida la hora y la fecha en que se activó el seguimiento VoIP.
Límite de memoria configurado	Muestra el límite de memoria configurado. Esto representa el 10% del tamaño de la memoria del conjunto de procesadores
Memoria consumida	Muestra la cantidad de memoria consumida dinámicamente para el rastreo VoIP
Tramos de llamadas totales descartados	Muestra el número de tramos de llamadas fallidas volcados en el búfer de registro. Las llamadas volcadas se refieren a tramos de llam asociados con errores IEC
Rastreo más antiguo volcado	Muestra las marcas de tiempo y la clave de búsqueda de la llamada fallida más antigua desde que se habilitó el seguimiento VoIP
Último seguimiento descargado	Muestra las marcas de tiempo y la clave de búsqueda de la última llamada fallida desde que se habilitó el seguimiento VoIP
Tramos de llamadas totales capturados	Muestra los tramos totales capturados después de habilitar el seguimiento VoIP
Tramos de llamadas totales disponibles	Muestra los tramos de llamadas totales disponibles en el historial. Puede ser igual o diferente en comparación con el tramo de llamada total capturado, dependiendo del de memoria.
Rastreo más antiguo disponible	Muestra la marca de tiempo y la clave de búsqueda del búfer de cubierta más antigu disponible en la memoria
Último seguimiento disponible	Muestra la marca de tiempo y la clave de búsqueda del último búfer de cubierta disp en la memoria
Total de seguimientos perdidos	Muestra el número de tramos de llamada perdidos debido al límite de memoria.

Comandos show adicionales

Campo	Uso	
show voip trace correlator <correlator>	show voip trace correlator 4	Filtra y muestra el seguimiento de VOIP para una identificaci
show voip trace session-id <session-id>	show voip trace session-id 87003120822b5dbd8fd80f62d8e57c48	Filtra y muestra el seguimiento de VO UUID local o remoto del encabezado mostrar ambos tramos de la llamada.
show voip trace sip-call-id <call-id>	show voip trace sip-call-id 01e60dfa9d8442848336d79e3155a8a1	Filtra y muestra el seguimiento de VO

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).