Configurar a Coleta de Depuração para Gateways Unified Border Element (CUBE) e Time-Division Multiplexing (TDM)

Contents

Introduction

Este documento descreve algumas das melhores práticas para coletar depurações de voz em um roteador de voz Cisco IOS/IOS-XE.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Requirements

- Conhecimento básico no Cisco IOS/IOS-XE dentro dos Integrated Services Routers (ISR).
- Acesso privilegiado para executar comandos nos roteadores ISR.
- Édesejável ter experiência prévia com protocolos VoIP (Voice-over-IP).
- Para rastreamento de VoIP, é necessário o Cisco IOS-XE 17.4.1 ou 17.3.2 no mínimo.

Componentes Utilizados

Para os fins deste documento, os componentes usados são:

- 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

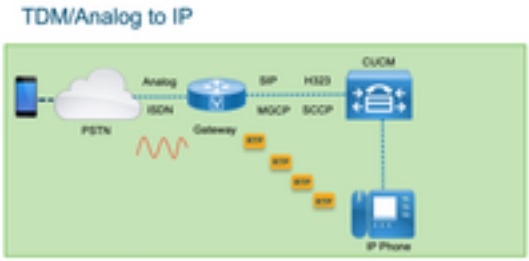
O processo de coleta de depuração nessas plataformas apresenta desafios e pode afetar potencialmente o desempenho do dispositivo. Os desafios e riscos aumentam quando há várias chamadas ativas estabelecidas em um roteador de voz. Em alguns cenários, se as depurações não forem coletadas corretamente, isso pode levar a uma alta utilização da CPU, o que poderia

prejudicar a capacidade do Roteador e até mesmo causar um travamento do software. Este documento fala sobre a diferença entre um Cisco Unified Border Element (CUBE) e um Gateway TDM/Analógico.

Gateways de voz TDM x CUBE

Os gateways de voz TDM são usados principalmente para interconectar um sistema telefônico interno com outro PBX ou PSTN. Os tipos de conexões que são usados em gateways TDM são controladores T1/E1 (ISDN ou CAS) e circuitos analógicos como portas FXS e FXO. Um Processador de Sinal Digital (DSP - Digital Signal Processor) converte o áudio de sua forma bruta em pacotes RTP. Da mesma forma, os pacotes RTP são convertidos em áudio bruto depois que o DSP processa os pacotes RTP e envia o áudio no circuito específico. Esses gateways podem interoperar com H323, MGCP ou SCCP no lado VoIP e, no lado TDM, seus circuitos ISDN PRI ou analógicos como as conexões mais comuns com a PSTN ou endpoints.

Como mostrado na imagem, os gateways TDM fornecem uma ponte entre sua infraestrutura VoIP interna e os provedores de serviços analógicos ou ISDN.



Com a introdução do VoIP, os clientes começaram a mudar rapidamente seus sistemas antigos para uma infraestrutura VoIP moderna. O mesmo ocorreu no lado do provedor de serviços, onde agora usam conexões para interconectar serviços de telefonia no local com a infraestrutura de VoIP do provedor de serviços e expandir seus recursos para fornecer melhores serviços. O protocolo VoIP mais comum usado atualmente é o Session Initiation Protocol (SIP) e é amplamente usado atualmente por clientes e provedores de serviços de telefonia Internet (ITSP) em todo o mundo.

O CUBE foi introduzido para fornecer uma maneira de interconectar esses sistemas VoIP internos com o mundo externo através dos ITSPs com SIP como o protocolo VoIP primário. O CUBE é simplesmente um gateway IP em que não precisa mais de nenhum tipo de conexão TDM, como controladores T1/E1 ou portas analógicas. O CUBE é executado nas mesmas plataformas que os gateways TDM.

O protocolo VoIP mais comum usado é o SIP, para o estabelecimento e a desativação de chamadas, e o RTP para o transporte de mídia. No CUBE não há necessidade de um DSP, a menos que um transcodificador seja necessário. O tráfego RTP flui de ponta a ponta do ITSP para o endpoint, e o CUBE atua como o intermediário com endereço oculto como um dos muitos recursos que oferece.

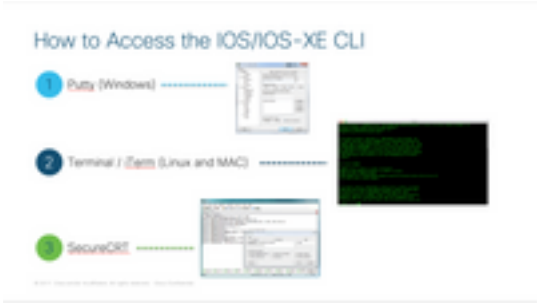
Como mostrado na imagem, o CUBE oferece uma divisão entre sua infraestrutura VoIP interna e o SIP ITSP:

Coleção de depurações de voz do Cisco IOS/IOS-XE

Os recursos de voz são executados em uma lista diferente de plataformas, como ISR, ASRs, CAT8Ks, entre outros, no entanto, eles usam um software comum que é o Cisco IOS ou o Cisco IOS-XE (as diferenças entre o Cisco IOS e o Cisco IOS-XE não são abordadas neste artigo). Vamos começar com os fundamentos de como acessar o Cisco IOS Router.

Como acessar um roteador Cisco IOS/IOS-XE através da interface de linha de comando (CLI)

Os roteadores, como qualquer outro dispositivo baseado em CLI, exigem um monitor de terminal para obter acesso para executar os comandos através do Secure Shell (SSH) ou Telnet. O SSH é o protocolo mais comum usado atualmente para acessar os dispositivos, uma vez que fornece uma conexão segura e criptografada para o dispositivo. Alguns dos monitores de terminal comuns usados para acessar o CLI dos Roteadores são:

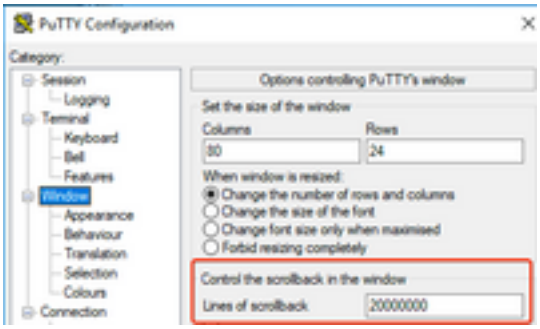


Como configurar o Monitor de Terminal para Coletar comandos show ou depurações

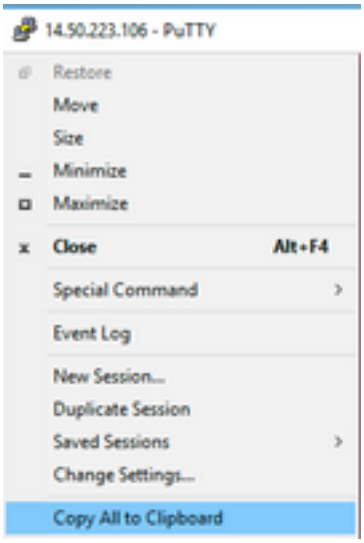
Há diferentes maneiras de coletar a saída do CLI. A recomendação é exportar as informações da CLI do Roteador para um arquivo separado. Isso facilita o compartilhamento das informações para terceiros.

Algumas maneiras de coletar as saídas do dispositivo são:

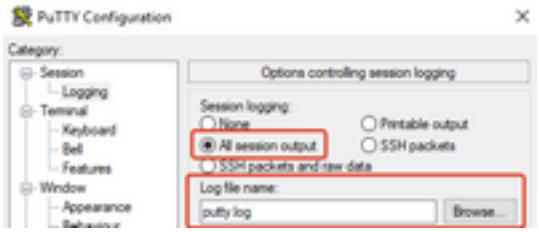
- Descarte toda a saída no terminal, para isso você precisa garantir que haja linhas de rolagem suficientes, caso contrário, a rolagem perde as primeiras seções da saída e os dados podem estar incompletos. Para aumentar as linhas de rolagem de volta em Putty, navegue até Putty Configuration > Window > Lines of Scrollback. Normalmente, é definido como um valor muito alto para ter saída de rollback suficiente:



Posteriormente, você poderá coletar as informações do monitor de terminal com a opção **Copiar Tudo para a Área de Transferência** e colar a saída em um arquivo de texto:



- Outra opção é registrar toda a saída da sessão em um arquivo .txt. Com essa opção, todos os comandos inseridos e saídas coletadas são imediatamente registrados no arquivo de texto. Esta é uma prática comum para registrar todas as saídas em uma sessão. Para registrar toda a saída da sessão em um arquivo no Putty, navegue para **Putty Configuration > Session > Logging** e selecione All Session Output da seguinte maneira:



> **Note**: O nome do arquivo de log padrão será usado se nenhum outro nome for especificado. Clique no botão Procurar para saber exatamente onde o arquivo foi salvo e localizá-lo posteriormente. Certifique-se também de não substituir outro arquivo putty.log no mesmo caminho de arquivo.

Coletar saída básica do comando show da CLI

Comandos show são necessários para coletar informações básicas do Roteador antes de qualquer coleta de depuração. Os comandos show são rápidos de coletar e, na maioria das vezes, não têm nenhum impacto no desempenho do Roteador. O isolamento do problema pode começar imediatamente com apenas uma saída do comando show.

Uma vez conectado ao Roteador, o comprimento do terminal pode ser definido como 0. Isso pode tornar a coleta mais rápida para exibir toda a saída de uma vez e evitar o uso da barra de espaço. O único comando que coleta informações detalhadas sobre o Roteador é 'show tech' e, como alternativa, você pode coletar **show tech voice** que mostra dados mais específicos para os recursos de voz habilitados no Roteador:

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

Coletar saída de depuração do CLI

Às vezes, a coleta de saída de depuração no Cisco IOS/IOS-XE pode ser um desafio, pois há risco de travamento do roteador. Algumas das práticas recomendadas são explicadas nas próximas seções para evitar problemas.

Verificação de memória

Antes de habilitar qualquer depuração, você precisa garantir que haja memória suficiente para armazenar a saída no buffer.

Execute o comando **show process memory** para descobrir quanta memória você pode alocar para registrar toda a saída no buffer:

> **Tip**: Use o comando **terminal length default** ou **terminal length <num_lines>** para voltar a uma quantidade limitada de linhas exibidas no terminal.

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

No exemplo, há 7666268552 bytes (7,6 GB) livres para serem usados pelo Roteador. Essa memória é compartilhada pelo Roteador entre todos os Processos do Sistema. Isso significa que você não pode usar toda a memória livre para registrar a saída no buffer, mas pode usar uma boa quantidade de memória do sistema conforme necessário.

A maioria dos cenários exige pelo menos 10 MB para coletar saída de depuração suficiente antes que a saída seja perdida ou substituída. Em raras ocasiões, uma quantidade maior de dados é necessária para ser coletada. Nesses cenários específicos, você pode obter um valor de saída de 50 MB a 100 MB no buffer ou pode aumentar, desde que haja memória disponível.

Se a memória livre estiver baixa, há um possível problema de vazamento de memória. Se esse for o caso, solicite à equipe do TAC de arquitetura que revise a causa dessa memória baixa.

Verificação da Unidade Central de Processamento (CPU)

A CPU é afetada pela quantidade de Processos, recursos e chamadas ativos no sistema. Quanto mais recursos ou chamadas estiverem ativas no sistema, mais ocupada será a CPU.

Uma boa referência de desempenho é garantir que o Roteador tenha a CPU em 30% ou menos, o que significa que você pode habilitar depurações com segurança, do básico ao avançado (sempre fique de olho na CPU quando depurações avançadas forem usadas). Se a CPU do roteador estiver em cerca de 50%, as depurações básicas poderão ser executadas e monitoradas cuidadosamente a CPU. Se a CPU atingir mais de 80%, pare imediatamente as depurações (mostradas mais adiante neste artigo) e acione o TAC para obter assistência.

Use o comando **show process cpu sorted | exclude 0.00** para verificar os últimos valores de CPU de 5, 60 e 5 minutos junto com os principais processos.

```
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
```

Na saída, o Roteador não tem muita atividade, a CPU está baixa e as depurações podem ser ativadas com segurança.

> **Caution**: Preste atenção extra aos principais processos da CPU ativos, se a CPU estiver com 50% ou mais e o processo superior for um processo de voz, apenas depurações básicas poderão ser habilitadas. Monitore continuamente a CPU com o comando para garantir que o desempenho geral do Roteador não seja afetado.

Verificação de Chamadas Ativas Atuais

Cada Roteador tem limites de capacidade diferentes. É importante verificar quantas chamadas estão ativas no Roteador para garantir que ele não esteja próximo da capacidade máxima. A Folha de Dados do Cisco Unified Border Element Versão 12 fornece informações sobre a capacidade de cada plataforma para referência.

Use o comando **show call ative total-calls** para ter uma ideia de quantas chamadas estão ativas no sistema:

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

Use o comando **show call ative voice summary** para obter informações mais detalhadas dos tipos de chamada específicos que estão ativos:

```
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
```

Alguns dos valores comuns são:

- **Segmentos de chamada de telefonia**: Chamadas de Gateway TDM, isso inclui chamadas

analógicas e PRI/ISDN.
- **Trechos de chamada SIP**: Total de chamadas SIP. Se este for um roteador CUBE, ele mostrará 2 segmentos de chamada por chamada. Divida o total de chamadas mostrado aqui por 2 para obter um número preciso.
- **Trechos de chamada H323**: Total de chamadas H323.
- **Trechos de chamada SCCP**: Recursos de mídia controlados pelo CUCM usados no roteador, como o transcodificador e os MTPs.

Configurações do buffer de registro

Para configurar o Roteador para armazenar a saída de depuração no buffer, o modo configure terminal é inserido para ajustar manualmente as configurações na CLI. Essa configuração não tem nenhum impacto no Roteador, no entanto, como mostrado nas seções anteriores, o comando **show tech** ou **show running-config** do Roteador é necessário caso a configuração precise ser revertida.

Um exemplo de configuração pode ser visto a seguir, que é uma linha de base comum usada pelos engenheiros do TAC. O exemplo aloca 10 MB de memória de buffer, mas pode ser aumentado conforme necessário:

```
# 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
```

Os comandos realizam estas tarefas:

- **log ou depuração de service timestamps**: Garante que o horário local do roteador seja gravado em cada mensagem registrada, com precisão de milissegundos. Isso é útil para localizar chamadas com base no tempo. Os timestamps de milissegundos permitem que você agrupe linhas de depuração em eventos lógicos relacionados quando duas linhas ocorrem no mesmo milissegundo.
- **service sequence-numbers:** Grava o número de sequência da depuração na linha. Isso é útil (essencialmente necessário) quando os logs são encaminhados a um Servidor syslog. Isso é muito útil para identificar se alguma mensagem de depuração para o Servidor syslog foi eliminada na rede. O número de sequência é o primeiro item na depuração, antes do carimbo de data/hora e da mensagem de log real. Observe que isso é diferente do número de sequência/timestamp que os servidores syslog podem gravar localmente em seus arquivos.
- **buffer de registro**: Instrui o Roteador a enviar depurações para sua memória de buffer local. O tamanho do buffer é definido em bytes. Na configuração, o tamanho do buffer foi definido como 10MB.
- **no logging console** e **no logging monitor:** Nenhuma mensagem de registro é impressa no console ou no monitor de terminal. Se esses comandos não forem configurados, poderão prejudicar o desempenho do Roteador e a precisão da saída de depuração.
- **syslog de voz iec:** Habilita mensagens de Códigos de Erro Interno de Voz para determinar os

motivos da desconexão.

Definir Configurações de Syslog

Às vezes, os problemas podem ser aleatórios e exigem uma maneira de coletar continuamente depurações até que o evento aconteça. Quando você armazena as depurações no buffer, ele as coleta continuamente. Observe que ele é limitado à quantidade de memória que você pode alocar e, uma vez que atinja essa quantidade de memória, o buffer circula e elimina as mensagens mais antigas, o que leva a informações valiosas incompletas necessárias para isolar o problema.

Com o Syslog, o Roteador pode enviar todas as mensagens de depuração para um servidor externo, onde o software Servidor Syslog as armazena em arquivos de texto. Embora seja uma boa maneira de coletar a saída de depuração, não é o método preferido para a coleta de logs. Os servidores de syslog tendem a ignorar ou descartar linhas da saída recebida devido ao congestionamento no servidor, já que a saída de depuração pode sobrecarregar o servidor ou os pacotes podem ser descartados devido às condições da rede. No entanto, em alguns cenários, o Syslog é a única maneira de fazer progresso em um problema.

Se possível, use um método de transporte confiável, como o TCP, para evitar qualquer perda de informações e, como sugestão, conecte o servidor Syslog ao mesmo switch onde o Roteador está conectado ou o mais próximo possível do Roteador. Ele ainda não garante que todos os dados sejam armazenados nos arquivos, mas reduz as chances de perda de dados.

Por padrão, os servidores syslog usam UDP como o protocolo de transporte na 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
```

Assim que os comandos são configurados, o Roteador encaminha imediatamente as mensagens para o endereço IP do servidor Syslog.

Depurar Coleção

Depois que as depurações forem habilitadas, o buffer deverá ser limpo antes que o problema seja reproduzido. Isso é feito para garantir que a saída esteja o mais limpa possível e evitar dados extras que não sejam necessários para a análise. Execute o comando **clear log**, que garante que o buffer seja limpo. Se houver outras chamadas ativas no Roteador e as depurações estiverem

ativadas, a saída imediatamente será impressa no buffer.

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

Depois que o problema for reproduzido, desative as depurações imediatamente para parar mais saída no buffer. Em seguida, colete os logs. Você pode despejar toda a saída no terminal com os comandos:

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

Às vezes o PuTTY fecha, já que não precisa processar toda a saída de uma vez, isso é normal e não significa que ocorreu uma falha, se isso acontecer, reabra a sessão novamente e continue normalmente. Em cenários onde o buffer de registro é muito grande ou o monitor do terminal trava devido à quantidade de dados que precisa ser impressa, copie a saída do buffer para um dispositivo externo diretamente com o comando **show log | redirecionamento**:

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

O comando copia toda a saída do buffer para um ftp com endereço IP 192.168.1.2 com o nome de arquivo debug.txt. O nome do arquivo sempre deve ser especificado. Outros destinos disponíveis para exportar esses dados são:

```
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
```

Quais depurações podem ser ativadas nos roteadores de voz?

Cada fluxo de chamada e tipo de recurso (TDM, CUBE ou SCCP (Recursos de mídia)) são diferentes e há depurações específicas que podem ser habilitadas. Todas as depurações necessárias devem ser habilitadas ao mesmo tempo. Quando apenas uma depuração é capturada por vez, isso é ineficaz e gera mais confusão quando os dados são analisados.

As depurações são ativadas dentro do prompt exec da CLI no nível **Router#**, que exige que você tenha permissões do modo de execução privilegiado.

Existem depurações básicas e avançadas. As depurações básicas são usadas para coletar informações de sinalização em SIP, H323 ou MGCP, que mostra as conversas que o Roteador tem com seus dispositivos pares.

As depurações avançadas são muito detalhadas e normalmente são usadas para coletar mais informações no caso de erros de pilha interna que as depurações básicas não possam mostrar. Essas depurações normalmente exigem muito da CPU.

> **Tip**: Depois que as depurações estiverem ativadas, lembre-se de executar o comando **clear logging**. Este comando garante que o buffer seja limpo para uma captura mais limpa das depurações.

Depuração de CCAPI (Internal Call Control API)

Dentro de cada Roteador Cisco IOS/IOS-XE há uma API de controle de chamadas que é responsável pela comunicação entre diferentes aplicativos VoIP, ou protocolos, e os componentes do Plano de Dados, como RTP, DSP, Placas de Voz, entre outros. Para capturar dados dessa camada, há uma depuração específica que pode ser usada:

```
debug voip ccapi inout
```

Há outras opções para essa depuração, no entanto, **debug voip ccapi inout** abrange todas as informações básicas de plano de discagem e estabelecimento de chamada que normalmente são mais do que suficientes para entender quais são os estados dessa camada.

> **Tip**: **debug voip ccapi inout** geralmente tem impacto mínimo na CPU do Roteador e é recomendável que seja habilitado juntamente com quaisquer depurações de sinalização para fornecer um conjunto completo de logs com informações das chamadas e seus diferentes estados.

Fluxos de chamada SIP

Essas depurações são as mais comumente usadas para fluxos de chamada SIP e podem ser habilitadas dentro dos gateways CUBE e TDM com um segmento SIP entre o Roteador e o CUCM ou qualquer outro servidor/proxy SIP.

Depurações SIP básicas

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

Depurações SIP avançadas

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

Fluxos de chamadas digitais (PRI, BRI)

Estas depurações se aplicam a Interfaces de taxa primária (PRI - Primary Rate Interfaces) T1/E1 ou Interfaces de taxa básica (BRI - Basic Rate Interfaces):

Depuração digital básica

```
debug isdn q931
```

Depuração digital avançada

```
debug isdn q921
```

Fluxos de chamada analógica

Essas depurações são usadas quando há circuitos analógicos envolvidos, como as portas FXS (Foreigh eXchange Subscriber) ou FXO (Foreign eXchange Office):

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

Fluxos de chamada MGCP

Essas depurações são usadas quando o MGCP é usado como o protocolo de voz entre um gateway de voz e o CUCM.

Depurações básicas

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

Depurações do CCM-Manager

O comando **debugs ccm-manager** é usado para rastrear o download de configuração e as mensagens de backhaul do MoH e PRI/BRI entre o CUCM e o gateway de voz. Essas depurações são usadas conforme necessário e dependem do cenário de falha.

```
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
```

Depurações avançadas de MGCP

```
debug mgcp all
```

Fluxos de chamada H323

Embora o H323 não seja amplamente usado, ainda há algumas implantações com o H323 configurado:

Depurações H323 básicas

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

Depurações H323 avançadas

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

Recursos de mídia SCCP

Essas depurações são usadas para solucionar problemas de recursos de mídia do Skinny Call Control Protocol (SCCP) que envolvem Media Termination Point (MTP) ou transcodificadores registrados em um servidor Cisco Unified Communications Manager (CUCM):

Depurações básicas de SCCP

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

Depuração SCCP avançada

```
debug sccp all
```

Rastreamento de VoIP

Com a introdução do Cisco IOS-XE 17.4.1 e 17.3.2, há uma nova opção para capturar registros de voz dentro do Cisco Unified Border Element (CUBE). Esse novo recurso é chamado Rastreamento de VoIP. Esta é uma nova estrutura de manutenção criada para registrar eventos e sinalização SIP sem a necessidade de habilitar depurações.

O rastreamento de VoIP é ativado por padrão e pode ser desativado a qualquer momento, conforme necessário. O Rastreamento de VoIP captura informações específicas somente para chamadas SIP:

- Mensagens SIP para chamadas de Tronco SIP para Tronco
- Eventos e chamadas de API da camada SIP para outras camadas no CUBE
- Erros SIP
- Controle de chamadas (fluxos de chamadas de Comunicações Unificadas processados pelo CUBE)
- Estados e eventos de Máquinas de Estado Finito (FSM)
- Ponto de discagem correspondente
- Portas RTP Alocadas
- Correlação de erros IEC com sinalização SIP

Restrições

- O Rastreamento de VoIP não registra informações relacionadas a Mensagens SIP Fora do Diálogo: REGISTROOPÇÕESASSINAR/NOTIFICARINFORMAÇÕES
- O rastreamento de VoIP em HA é suportado, no entanto, estas advertências se aplicam: O Rastreamento VoIP do Roteador em Standby está habilitado por padrão. Somente os rastreamentos aplicáveis para o processo em Standby são apresentados até que se torne ativoQuando o Standby está ativo, ele **NÃO** contém rastreamentos completos de chamadas com ponto de verificação e apenas novas chamadas**show voip trace <key>** ainda funciona no

roteador em standby e exibe dados de buffer de cobertura e fluxo de mídia para chamadas

Como ativar o rastreamento de VoIP

Como mencionado, esse recurso é ativado por padrão. O comando para ativar esse recurso é:

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

Como desativar o rastreamento de VoIP

Para desativar esse recurso, os comandos são:

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

> **Caution**: Depois que o rastreamento de VoIP é desativado, toda a memória é limpa e as informações são perdidas.

Os comandos disponíveis dentro do modo de configuração de rastreamento são:

```
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 limite de memória

O limite de memória determina quanta memória é usada pelo Rastreamento VoIP para armazenar os dados. Por padrão, é 10% da memória disponível na plataforma, mas isso pode ser alterado para um máximo de 1 GB e um mínimo de 10 MB. A memória é alocada dinamicamente, o que significa que o recurso usa apenas a memória conforme necessário e depende do volume da chamada. Quando atinge a memória máxima disponível, ele circula e exclui entradas mais antigas.

Quando o limite de memória é modificado para ser maior que os 10% de memória disponível, uma mensagem é mostrada na Interface de linha de 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.
```

Para definir o padrão de 10% de uso de memória, o comando **memory-limit platform** pode ser usado:

```
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]:
```

> **Caution**: Quando o limite de memória é reduzido, todos os dados de rastreamento VoIP são perdidos. Um backup dos dados precisa ser coletado antes que a memória seja reduzida.

Como exibir dados de rastreamento de VoIP

Para exibir os dados do rastreamento de VoIP, precisamos usar comandos show específicos. Os dados podem ser exibidos na mesma sessão de terminal ou também podem ser enviados via Syslog para um Servidor syslog fora da caixa.

> **Note**: Os rastreamentos são despejados após 32 segundos a partir do momento em que um BYE é recebido para uma chamada.

> **Note**: A sinalização SIP é exibida por trecho e não é combinada como depurações regulares. As depurações regulares, como **debug ccsip messages**, exibem a sinalização SIP de uma chamada na ordem exata em que os eventos ocorreram. No rastreamento VoIP, cada trecho é separado. Para determinar a ordem correta, os timestamps são usados.

Os comandos disponíveis para mostrar os dados são:

```
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 exibe todos os dados de rastreamento VoIP disponíveis no buffer. O uso desse comando afeta o desempenho do Roteador. Depois que o comando é inserido, uma mensagem de aviso é exibida para alertar sobre o risco e confirmar para continuar:

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

show voip trace cover-buffers

Esse comando exibe uma visão geral dos detalhes de chamadas para todas as chamadas relatadas em Rastreamento de VoIP. Cada perna da chamada tem um buffer de cobertura criado que contém um resumo da chamada 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 = 0927767800105000a0005006ab805584
GUID = 208578800000
-----------------------------------------------
```

Para obter mais informações sobre cada campo, consulte a próxima tabela:

Campo	Descrição
Chave de Pesquisa	Contém uma combinação de chamada, número chamado e ID de chamada
Carimbo de data/hora	Tempo de criação do buffer de cobertura
ID do buffer	ID do buffer de cobertura
Call-id	Call-id do respectivo segmento de chamada do buffer de cobertura
Peer-CallID	Call-id do leg do peer
Correlator	Correlacionador FPI da chamada
Número chamado	Número chamado do respectivo call-leg do buffer de cobertura
Calling-number	Número de chamada do trecho de chamada respectivo do buffer de cobertura
Sip Call-ID	Sip call-id do trecho de chamada respectivo do buffer de cobertura
ID da sessão Sip	ID da sessão SIP do respectivo segmento de chamada do buffer de cobertura
GUID	GUID da chamada respectiva do buffer de cobertura
Perna Âncora	O leg da âncora será definido como sim se o leg da chamada respectivo for um leg da âncora no fluxo de bifurcação de chamadas ou n implantação do proxy de mídia
Perna bifurcada	O trecho bifurcado é definido como sim se o respectivo trecho da chamada for um trecho âncora no fluxo de bifurcação de chamadas o implantação do proxy de mídia
IDs de Call associadas	Call-id das pernas bifurcadas associadas

Para filtrar os buffers de cobertura, podemos usar os comandos **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

Em combinação com o comando anterior, **show voip trace call-id** pode ser usado para localizar as

chamadas. Após a identificação do call-id, este comando pode ser usado para exibir todas as informações sobre o leg da chamada 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

Esse comando show exibe saída detalhada sobre status, consumo de memória, chamadas com erros ou falhas, chamadas bem-sucedidas, carimbos de data/hora das entradas mais recentes e mais antigas e muito mais.

```
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 obter mais informações sobre cada campo, consulte a próxima tabela:

Campo	Descrição
Status de Rastreamento	Exibe o status do rastreamento, incluindo a hora e a data em que o rastreamento VoIP foi habilitado.
Limite de memória configurado	Exibe o limite de memória configurado. Isso representa 10% do tamanho da memória do pool de processadores
Memória consumida	Exibe a quantidade de memória consumida dinamicamente para rastreamento de VoIP
Total de pernas de chamada despejadas	Exibe o número de trechos de chamada com falha despejados no buffer de registro. Chamadas despejadas se referem a trechos de ch associados a erros do IEC
Rastreamento mais antigo despejado	Exibe carimbos de data/hora e a chave de pesquisa da chamada com falha mais antiga desde que o Rastreamento VoIP foi habilitado
Último rastreamento despejado	Exibe carimbos de data/hora e a chave de pesquisa da última chamada com falha desde que o Rastreamento VoIP foi habilitado
Total de trechos de chamada capturados	Exibe o total de trechos capturados após a ativação do rastreamento VoIP
Total de trechos de chamada disponíveis	Exibe o total de trechos de chamada disponíveis no histórico. Pode ser igual ou difer em comparação com o Total de trechos de chamada capturados, dependendo do lim de memória.
Rastreamento mais antigo disponível	Exibe o timestamp e a chave de pesquisa do buffer de cobertura mais antigo disponí na memória
Último rastreamento disponível	Exibe o carimbo de data/hora e a chave de pesquisa do buffer de cobertura mais rec disponível na memória
Total de rastreamentos perdidos	Exibe o número de segmentos de chamada perdidos devido ao limite de memória.

Comandos show adicionais

Campo	Uso	
show voip trace correlator <correlator>	show voip trace correlator 4	Filtra e exibe o rastreamento VOIP de uma ID de chamada e
show voip trace session-id <session-id>	show voip trace session-id 87003120822b5dbd8fd80f62d8e57c48	Filtra e exibe o rastreamento VOIP de

		local ou remoto do cabeçalho de ID de dois segmentos da chamada.
show voip trace sip-call-id <call-id>	show voip trace sip-call-id 01e60dfa9d8442848336d79e3155a8a1	Filtra e exibe o rastreamento VOIP co

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.