Configurer la collecte de débogage pour les passerelles CUBE (Unified Border Element) et TDM (Time-Division Multiplexing)

Contenu

Introduction

Ce document décrit certaines des meilleures pratiques afin de collecter des débogages vocaux dans un routeur vocal Cisco IOS/IOS-XE.

Conditions préalables

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Conditions requises

- Connaissances de base de Cisco IOS/IOS-XE dans les routeurs à services intégrés (ISR).
- Accès privilégié afin d'exécuter des commandes dans les routeurs ISR.
- Une expérience préalable des protocoles VoIP (Voice-over-IP) est souhaitée.
- Pour VoIP Trace, Cisco IOS-XE 17.4.1 ou 17.3.2 minimum est requis.

Components Used

Aux fins du présent document, les composants utilisés sont les suivants :

- 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

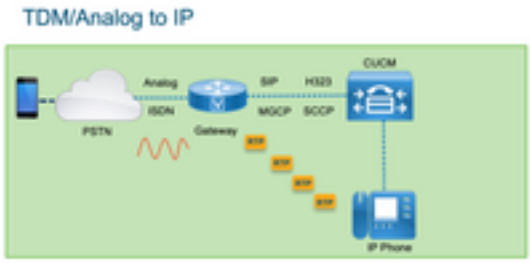
Le processus de collecte de débogage dans ces plates-formes présente des défis et peut potentiellement affecter les performances du périphérique. Les défis et les risques augmentent

lorsque plusieurs appels actifs sont établis dans un routeur vocal. Dans certains scénarios, si les débogages ne sont pas collectés correctement, cela peut conduire à une CPU élevée qui pourrait nuire à la capacité du routeur et même provoquer une panne logicielle. Ce document traite de la différence entre un CUBE (Cisco Unified Border Element) et une passerelle TDM/analogique.

Passerelles vocales TDM et CUBE

Les passerelles vocales TDM sont principalement utilisées pour interconnecter un système téléphonique interne avec un autre autocommutateur privé (PBX) ou le réseau téléphonique public commuté (RTPC). Les types de connexions utilisés dans les passerelles TDM sont les contrôleurs T1/E1 (RNIS ou CAS) et les circuits analogiques tels que les ports FXS et FXO. Un processeur de signal numérique (DSP) convertit l'audio de sa forme brute en paquets RTP. De la même manière, les paquets RTP sont convertis en audio brut après que le DSP a traité les paquets RTP et envoyé l'audio sur le circuit spécifique. Ces passerelles peuvent interagir avec H323, MGCP ou SCCP du côté VoIP et du côté TDM avec ses circuits RNIS PRI ou analogiques comme connexions les plus courantes au RTPC ou aux points d'extrémité.

Comme l'illustre l'image, les passerelles TDM fournissent un pont entre votre infrastructure VoIP interne et les fournisseurs de services analogiques ou RNIS.



Avec l'introduction de la VoIP, les clients ont commencé à transformer rapidement leurs systèmes existants en une infrastructure VoIP moderne. La même chose s'est produite du côté des fournisseurs de services, où ils utilisent désormais des connexions pour interconnecter les services de téléphonie sur site avec l'infrastructure VoIP des fournisseurs de services et étendre leurs capacités afin de fournir de meilleurs services. Le protocole VoIP le plus couramment utilisé aujourd'hui est le protocole SIP (Session Initiation Protocol) et est actuellement largement utilisé par les clients et les fournisseurs de services de téléphonie Internet (ITSP) dans le monde entier.

CUBE a été introduit pour fournir un moyen d'interconnecter ces systèmes VoIP internes avec le monde extérieur par le biais des ITSP avec SIP comme protocole VoIP principal. CUBE est simplement une passerelle IP-IP qui n'a plus besoin d'aucun type de connexion TDM, comme les contrôleurs T1/E1 ou les ports analogiques. CUBE fonctionne sur les mêmes plates-formes que les passerelles TDM.

Le protocole VoIP le plus couramment utilisé est le protocole SIP, pour l'établissement et le démontage des appels, et le protocole RTP pour le transport multimédia. Dans CUBE, un DSP n'est pas nécessaire, sauf si un transcodeur est requis. Le trafic RTP circule de bout en bout du fournisseur de services Internet au point d'extrémité, et CUBE agit comme intermédiaire avec une adresse cachée comme l'une des nombreuses fonctionnalités qu'il offre.

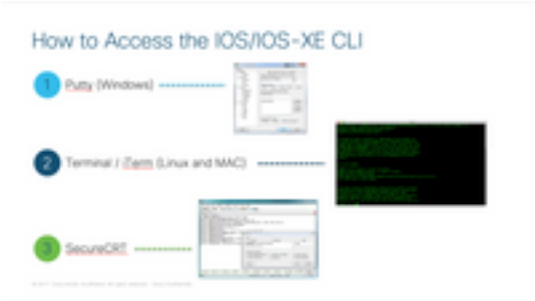
Comme l'illustre l'image, CUBE permet de distinguer votre infrastructure VoIP interne de l'ITSP SIP :

Collection de débogages vocaux Cisco IOS/IOS-XE

Les fonctionnalités vocales s'exécutent sur une liste différente de plates-formes, comme ISR, ASR, CAT8K, entre autres, mais elles utilisent un logiciel commun qui est soit Cisco IOS, soit Cisco IOS-XE (les différences entre Cisco IOS et Cisco IOS-XE ne sont pas couvertes dans cet article). Commençons par les bases de l'accès au routeur Cisco IOS.

Comment accéder à un routeur Cisco IOS/IOS-XE via l'interface de ligne de commande (CLI)

Les routeurs, comme tout autre périphérique basé sur l'interface de ligne de commande, nécessitent un moniteur de terminal pour accéder à l'exécution des commandes via Secure Shell (SSH) ou Telnet. SSH est le protocole le plus utilisé de nos jours pour accéder aux périphériques, car il fournit une connexion sécurisée et chiffrée au périphérique. Voici quelques-uns des moniteurs de terminal couramment utilisés pour accéder à l'interface de ligne de commande des routeurs :

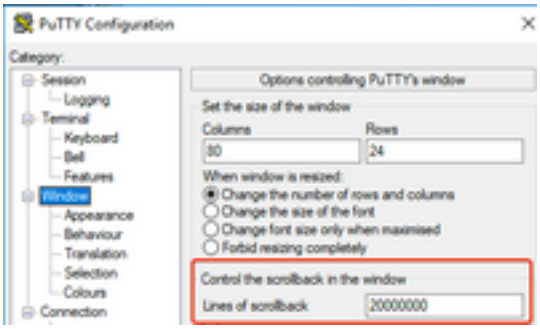


Comment configurer le Moniteur de terminal pour collecter les commandes show ou les débogages

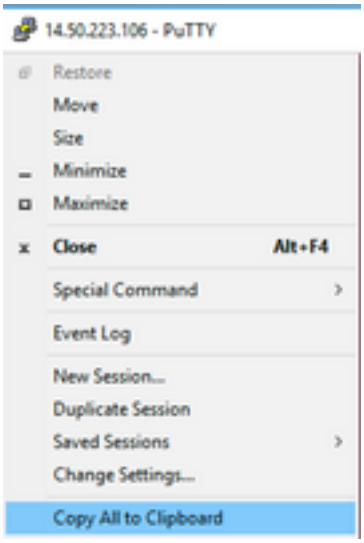
Il existe différentes manières de collecter les résultats de l'interface de ligne de commande. Il est recommandé d'exporter les informations de la CLI du routeur vers un fichier distinct. Cela facilite le partage de l'information avec des parties externes.

Voici quelques façons de collecter les sorties du périphérique :

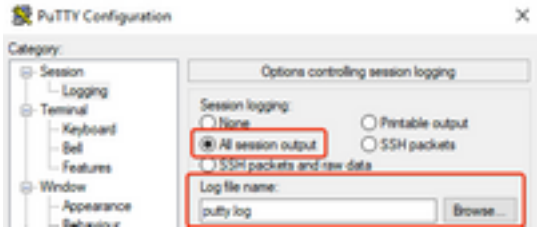
- Videz toute la sortie dans le terminal, pour cela vous devez vous assurer qu'il y a assez de lignes de défilement, sinon le défilement manque les premières sections de la sortie et les données peuvent être incomplètes. Afin d'augmenter les lignes de défilement dans Putty, naviguez vers Putty Configuration > Window > Lines of Scrollback. Normalement, cette valeur est très élevée afin d'avoir assez de résultats de défilement :



Vous pouvez ensuite collecter les informations du moniteur de terminal avec l'option **Copier tout dans le Presse-papiers** et coller le résultat dans un fichier texte :



- Une autre option consiste à consigner l'intégralité du résultat de la session dans un fichier .txt. Avec cette option, toutes les commandes entrées et les résultats collectés sont immédiatement consignés dans le fichier texte. Il s'agit d'une pratique courante pour consigner tous les résultats dans une session. Afin de consigner toutes les sorties de session dans un fichier dans Putty, naviguez à **Putty Configuration > Session > Logging** puis sélectionnez All Session Output comme suit :



> **Note**: Le nom de fichier journal par défaut est utilisé si aucun autre nom n'est spécifié. Cliquez sur le bouton Parcourir pour savoir exactement où le fichier est enregistré et le retrouver ultérieurement. Veillez également à ne pas écraser un autre fichier putty.log dans le même chemin d'accès.

Collecter le résultat de la commande show de base à partir de la CLI

Les commandes show sont nécessaires pour collecter les informations de base du routeur avant toute collecte de débogage. Les commandes show sont rapides à collecter et, pour la plupart, n'ont aucun impact sur les performances du routeur. L'isolation du problème peut commencer immédiatement avec une simple sortie de commande show.

Une fois connecté au routeur, la longueur du terminal peut être définie sur 0. Cela peut accélérer la collecte afin d'afficher toutes les sorties à la fois et éviter l'utilisation de la barre d'espace. La seule commande qui collecte des informations détaillées sur le routeur est « show tech », et vous pouvez également collecter **show tech voice** qui affiche des données plus spécifiques aux fonctionnalités vocales activées dans le routeur :

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

Collecter les résultats du débogage à partir de la CLI

La collecte des résultats de débogage dans Cisco IOS/IOS-XE peut parfois être un défi, car il existe un risque de panne du routeur. Certaines des meilleures pratiques sont expliquées dans les sections suivantes pour éviter tout problème.

Vérification de la mémoire

Avant d'activer des débogages, vous devez vous assurer qu'il y a suffisamment de mémoire pour stocker la sortie dans la mémoire tampon.

Exécutez la commande **show process memory** pour savoir combien de mémoire vous pouvez allouer afin de consigner toutes les sorties dans la mémoire tampon :

> **Astuce** : Utilisez la commande **terminal length default** ou **terminal length <num_lines>** pour revenir à une quantité limitée de lignes affichées dans le terminal.

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

Dans l'exemple, 7666268552 octets (7,6 Go) peuvent être utilisés par le routeur. Cette mémoire est partagée par le routeur entre tous les processus système, ce qui signifie que vous ne pouvez pas utiliser toute la mémoire libre pour enregistrer le résultat dans la mémoire tampon, mais que vous pouvez utiliser une bonne quantité de mémoire système si nécessaire.

La plupart des scénarios nécessitent au moins 10 Mo pour collecter suffisamment de sortie de débogage avant que la sortie soit perdue ou écrasée. Dans de rares cas, une plus grande quantité de données doit être collectée, dans ces scénarios spécifiques, vous pouvez obtenir 50 Mo à 100 Mo de sortie dans la mémoire tampon ou vous pouvez aller plus haut tant qu'il y a de la mémoire disponible.

Si la mémoire libre est insuffisante, il y a un problème de fuite de mémoire, dans ce cas, contactez l'équipe du TAC d'architecture pour réviser la cause de cette mémoire insuffisante.

Vérification de l'unité centrale (UC)

Le processeur est affecté par la quantité de processus, de fonctionnalités et d'appels actifs dans le système. Plus le nombre de fonctions ou d'appels actifs dans le système est élevé, plus le

processeur est occupé.

Un bon test consiste à s'assurer que le routeur dispose d'un processeur à 30 % ou moins, ce qui signifie que vous pouvez activer en toute sécurité les débogages de base à avancé (gardez toujours un oeil sur le processeur lorsque des débogages avancés sont utilisés). Si le processeur du routeur est à environ 50 %, les débogages de base peuvent être exécutés et surveiller attentivement le processeur. Si le processeur atteint plus de 80 %, arrêtez immédiatement les débogages (voir plus loin dans cet article) et demandez de l'aide au TAC.

Utilisez la commande **show process cpu sorted | exclude 0.00** pour vérifier les 5 dernières valeurs CPU, 60 dernières et 5 minutes ainsi que les Processus supérieurs.

```
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
```

Dans le résultat, le routeur n'a pas beaucoup d'activité, le processeur est faible et les débogages peuvent être activés en toute sécurité.

> **Attention** : Soyez particulièrement attentif aux processus CPU actifs, si le CPU est à 50 % ou plus et que le processus supérieur est un processus vocal, seuls les débogages de base peuvent être activés. Surveillez en permanence le processeur à l'aide de la commande pour vous assurer que les performances globales du routeur ne sont pas affectées.

Vérification des appels actifs actuels

Chaque routeur a des seuils de capacité différents. Il est important de vérifier combien d'appels sont actifs dans le routeur pour s'assurer qu'il n'est pas proche de la capacité maximale. La fiche technique Cisco Unified Border Element Version 12 fournit des informations de référence sur la capacité de chaque plate-forme.

Utilisez la commande **show call active total-calls** pour avoir une idée du nombre d'appels actifs dans le système :

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

Utilisez la commande **show call active voice summary** pour obtenir des informations plus détaillées sur les types d'appels spécifiques qui sont actifs :

```
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
```

Voici quelques-unes des valeurs communes :

- **Branchements d'appels téléphoniques** : Appels de la passerelle TDM, y compris les appels analogiques et PRI/RNIS.
- **Tronçons d'appel SIP** : Total des appels SIP. S'il s'agit d'un routeur CUBE, cela indique 2 tronçons d'appel par appel. Divisez le total des appels affichés ici par 2 pour obtenir un nombre précis.
- **Tronçons d'appel H323** : Total des appels H323.
- **Tronçons d'appel SCCP** : Ressources média contrôlées CUCM utilisées dans le routeur, telles que les transcodeurs et les MTP.

Paramètres du tampon de journalisation

Pour configurer le routeur de manière à stocker la sortie de débogage dans la mémoire tampon, le mode terminal configure est activé pour modifier manuellement les paramètres de l'interface de ligne de commande. Cette configuration n'a pas d'impact sur le routeur. Cependant, comme indiqué dans les sections précédentes, la commande **show tech** ou **show running-config** du routeur est nécessaire dans le cas où la configuration doit être restaurée.

Vous trouverez ci-dessous un exemple de configuration, qui est une référence commune utilisée par les ingénieurs du TAC. L'exemple alloue 10 Mo de mémoire tampon, mais peut être augmenté si nécessaire :

```
# 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
```

Les commandes permettent d'effectuer les tâches suivantes :

- **service timestamps debug or log** : Garantit que l'heure du routeur local est écrite sur chaque message enregistré, avec une précision de quelques millisecondes. Cela est utile pour rechercher des appels en fonction de l'heure. Les horodatages en millisecondes vous permettent de regrouper des lignes de débogage en événements logiques connexes lorsque deux lignes se produisent au cours de la même milliseconde.
- **numéro d'ordre du service :** Écrit le numéro de séquence du débogage dans la ligne. Ceci est utile (essentiellement requis) lorsque les journaux sont transférés à un serveur Syslog. Ceci est très utile afin d'identifier si des messages de débogage au serveur Syslog ont été abandonnés dans le réseau. Le numéro d'ordre est le premier élément du débogage, avant l'horodatage et le message de journal réel. Notez que ceci est différent de l'horodatage/numéro de séquence que les serveurs syslog peuvent écrire localement dans leurs fichiers.
- **tampon de journalisation** : Indique au routeur d'envoyer des débogages à sa mémoire tampon locale. La taille de la mémoire tampon est définie en octets. Dans la configuration, la taille de la mémoire tampon était définie sur 10 Mo.
- **pas de console de journalisation** et **pas de moniteur de journalisation :** Aucun message de journal n'est imprimé dans la console ou le moniteur de terminal. Si ces commandes ne sont

pas configurées, elles peuvent nuire aux performances du routeur et à la précision des résultats de débogage.
- **voice iec syslog :** Active les messages de codes d'erreur internes vocaux pour déterminer les raisons de déconnexion.

Configuration des paramètres Syslog

Parfois, les problèmes peuvent être aléatoires et nécessitent un moyen de collecter continuellement des débogages jusqu'à ce que l'événement se produise. Lorsque vous stockez les débogages dans la mémoire tampon, elle les collecte en continu. Notez qu'il est limité à la quantité de mémoire que vous pouvez allouer et une fois qu'il atteint cette quantité de mémoire, la mémoire tampon entoure et abandonne les messages les plus anciens, ce qui conduit à des informations précieuses incomplètes nécessaires pour isoler le problème.

Avec Syslog, le routeur peut envoyer tous les messages de débogage à un serveur externe, où le logiciel Syslog Server les stocke dans des fichiers texte. Bien que ce soit un bon moyen de collecter la sortie de débogage, n'est pas la méthode préférée pour la collecte de journaux. Les serveurs Syslog ont tendance à ignorer ou à supprimer des lignes du résultat reçu en raison d'un encombrement du serveur, car le résultat du débogage peut submerger le serveur ou des paquets peuvent être supprimés en raison de conditions réseau. Cependant, dans certains cas, Syslog est le seul moyen de progresser sur un problème.

Si possible, utilisez une méthode de transport fiable telle que TCP pour éviter toute perte d'informations et, comme suggestion, connectez le serveur Syslog au même commutateur où le routeur est connecté ou aussi près que possible du routeur. Il ne garantit toujours pas que toutes les données sont stockées dans les fichiers, mais réduit les risques de perte de données.

Par défaut, les serveurs syslog utilisent UDP comme protocole de transport sur le port 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
```

Dès que les commandes sont configurées, le routeur transmet immédiatement les messages à l'adresse IP du serveur Syslog.

Debug Collection

Une fois les débogages activés, la mémoire tampon doit être effacée avant que le problème ne soit reproduit. Cela permet de s'assurer que le résultat est aussi propre que possible et d'éviter toute donnée supplémentaire qui n'est pas nécessaire pour l'analyse. Exécutez la commande **clear log**, ce qui garantit que la mémoire tampon est effacée. Si d'autres appels sont actifs dans le routeur et que les débogages sont activés, le résultat s'imprime immédiatement dans la mémoire tampon.

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

Une fois le problème reproduit, désactivez les débogages immédiatement pour arrêter d'autres sorties dans la mémoire tampon. Ensuite, collectez les journaux. Vous pouvez vider tous les résultats du terminal avec les commandes suivantes :

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

Parfois, PuTTY se ferme parce qu'il ne gère pas toutes les sorties à la fois, c'est normal et cela ne signifie pas qu'un échec s'est produit, si cela se produit rouvrir la session et continuer normalement. Dans les scénarios où la mémoire tampon de journalisation est trop grande ou le moniteur de terminal tombe en panne en raison de la quantité de données qui doit être imprimée, copiez la sortie de la mémoire tampon sur un périphérique externe directement avec la commande **show log | redirection** :

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

La commande copie l'intégralité de la sortie de la mémoire tampon dans un FTP avec l'adresse IP 192.168.1.2 et le nom de fichier debug.txt. Le nom de fichier doit toujours être spécifié. Les autres destinations disponibles pour exporter ces données sont les suivantes :

```
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
```

Quels débogages peuvent être activés dans les routeurs vocaux ?

Chaque flux d'appels et type de fonctionnalités (TDM, CUBE ou SCCP (Media Resources)) sont différents et il existe des débogages spécifiques que vous pouvez activer. Tous les débogages requis doivent être activés en même temps. Lorsqu'un seul débogage est capturé à la fois, cela est inefficace et crée plus de confusion lors de l'analyse des données.

Les débogages sont activés dans le niveau d'invite **Router#** du mode d'exécution CLI, ce qui nécessite que vous ayez des autorisations en mode d'exécution privilégié.

Il existe des débogages de base et avancés. Les débogages de base sont utilisés pour collecter

des informations de signalisation dans SIP, H323 ou MGCP, qui montre les conversations du routeur avec ses périphériques homologues.

Les débogages avancés sont très détaillés et sont généralement utilisés pour collecter davantage d'informations en cas d'erreurs internes de pile que les débogages de base ne peuvent pas afficher. Ces débogages sollicitent généralement le processeur.

> **Astuce** : Une fois les débogages activés, n'oubliez pas d'exécuter la commande **clear logging**. Cette commande garantit que la mémoire tampon est effacée pour une capture plus nette des débogages.

Débogage de l'API de contrôle d'appel interne (CCAPI)

Àl'intérieur de chaque routeur Cisco IOS/IOS-XE se trouve une API de contrôle d'appel qui est chargée de la communication entre les différentes applications ou protocoles VoIP et les composants du plan de données, tels que RTP, DSP, cartes vocales, entre autres. Afin de capturer les données de cette couche, il y a un débogage spécifique qui peut être utilisé :

```
debug voip ccapi inout
```

Il existe d'autres options pour ce débogage, cependant **debug voip ccapi inout** couvre toutes les informations de base du plan de numérotation et de l'établissement d'appel qui sont normalement plus que suffisantes pour comprendre quels sont les états de cette couche.

> **Astuce** : **debug voip ccapi inout** a généralement un impact minimal sur le CPU du routeur et il est recommandé de l'activer avec tout débogage de signalisation afin de fournir un ensemble complet de journaux avec des informations sur le ou les appels et ses différents états.

Flux d'appels SIP

Ces débogages sont les plus couramment utilisés pour les flux d'appels SIP et peuvent être activés à l'intérieur des passerelles CUBE et TDM avec une branche SIP entre le routeur et CUCM ou tout autre serveur/proxy SIP.

Débogages SIP de base

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

Débogages SIP avancés

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

Flux d'appels numériques (PRI, BRI)

Ces débogages s'appliquent aux interfaces PRI T1/E1 ou BRI (Basic Rate Interfaces) :

Débogage numérique de base

```
debug isdn q931
```

Débogage numérique avancé

```
debug isdn q921
```

Flux d'appels analogiques

Ces débogages sont utilisés lorsqu'il y a des circuits analogiques impliqués comme Foreigh eXchange Subscriber (FXS) ou Foreign eXchange Office (FXO) ports :

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

Flux d'appels MGCP

Ces débogages sont utilisés lorsque MGCP est utilisé comme protocole vocal entre une passerelle vocale et CUCM.

Débogages de base

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

Débogages de CCM-Manager

Le **debugs ccm-manager** est utilisé pour suivre le téléchargement de la configuration, la musique d'attente et les messages de liaison PRI/BRI entre CUCM et la passerelle vocale. Ces débogages sont utilisés en fonction des besoins et dépendent du scénario de défaillance.

```
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
```

Débogages MGCP avancés

```
debug mgcp all
```

Flux d'appels H323

Bien que H323 ne soit pas très répandu, il existe encore des déploiements avec H323 configuré :

Débogages H323 de base

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

Débogages H323 avancés

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

Ressources média SCCP

Ces débogages sont utilisés pour dépanner les problèmes de ressources multimédias SCCP (Skinny Call Control Protocol) impliquant un point de terminaison multimédias (MTP) ou des transcodeurs enregistrés sur un serveur Cisco Unified Communications Manager (CUCM) :

Débogages SCCP de base

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

Débogage SCCP avancé

```
debug sccp all
```

Suivi VoIP

Avec l'introduction de Cisco IOS-XE 17.4.1 et 17.3.2, il existe une nouvelle option pour capturer les journaux vocaux à l'intérieur de Cisco Unified Border Element (CUBE). Cette nouvelle fonctionnalité est appelée VoIP Trace. Il s'agit d'un nouveau cadre de facilité de maintenance créé pour consigner la signalisation et les événements SIP sans avoir à activer de débogages.

VoIP Trace est activé par défaut et peut être désactivé à tout moment si nécessaire. VoIP Trace capture des informations spécifiques pour les appels SIP uniquement :

- Messages SIP pour les appels de liaison SIP à liaison
- Événements et appels API de la couche SIP vers d'autres couches dans CUBE
- Erreurs SIP
- Contrôle des appels (flux d'appels de communications unifiées traités par CUBE)
- États et événements FSM (Finite State Machines)
- Homologue de numérotation correspondant
- Ports RTP alloués
- Corrélation des erreurs IEC avec la signalisation SIP

Restrictions

- VoIP Trace n'enregistre pas les informations relatives aux messages SIP hors dialogue : REGISTREOPTIONSABONNEMENT/NOTIFICATIONINFORMATIONS
- VoIP Trace dans HA est pris en charge, mais les mises en garde suivantes s'appliquent : Par

défaut, le suivi VoIP est activé sur le routeur de secours. Seules les traces applicables au processus de veille sont présentées jusqu'à ce qu'il devienne actifUne fois que la veille est active, elle ne contient **PAS** de traces complètes d'appels avec points de contrôle et seulement de nouveaux appels**show voip trace <key>** fonctionne toujours sur le routeur de secours et affiche les données du tampon de couverture et du flux multimédia pour les appels

Activation de la trace VoIP

Comme indiqué, cette fonctionnalité est activée par défaut. La commande permettant d'activer cette fonctionnalité est la suivante :

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

Désactivation du suivi VoIP

Pour désactiver cette fonctionnalité, les commandes sont les suivantes :

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

> **Attention** : Une fois la fonction VoIP Trace désactivée, toute la mémoire est effacée et les informations perdues.

Les commandes disponibles dans le mode de configuration trace sont les suivantes :

```
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
```

Configurer la limite de mémoire

La limite de mémoire détermine la quantité de mémoire utilisée par VoIP Trace pour stocker les données. Par défaut, cette valeur représente 10 % de la mémoire disponible sur la plate-forme, mais elle peut être modifiée pour atteindre un maximum de 1 Go et un minimum de 10 Mo. La mémoire est allouée dynamiquement, ce qui signifie que la fonctionnalité utilise uniquement la mémoire nécessaire et dépend du volume d'appels. Une fois qu'il atteint la mémoire maximale disponible, il tourne autour et supprime les entrées plus anciennes.

Lorsque la limite de mémoire est modifiée pour être supérieure à 10 % de mémoire disponible, un message s'affiche dans l'interface de ligne de commande :

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

Pour définir la valeur par défaut de 10% d'utilisation de la mémoire, la commande **memory-limit platform** peut être utilisée :

```
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]:
```

> **Attention** : Lorsque la limite de mémoire est réduite, toutes les données VoIP Trace sont perdues. Une sauvegarde des données doit être collectée avant que la mémoire ne soit réduite.

Affichage des données de suivi VoIP

Pour afficher les données de VoIP Trace, nous devons utiliser des commandes show spécifiques. Les données peuvent être affichées dans la même session de terminal ou peuvent également être envoyées via Syslog à un serveur syslog hors boîte.

> **Note**: Les traces sont vidées 32 secondes après la réception d'un BYE pour un appel.

> **Note**: La signalisation SIP est affichée par segment et n'est pas combinée comme des débogages standard. Les débogages réguliers tels que les **messages debug ccsip** affichent la signalisation SIP d'un appel dans l'ordre exact des événements survenus. Dans VoIP Trace, chaque branche est distincte. Pour déterminer le bon ordre, les horodatages sont utilisés.

Les commandes disponibles pour afficher les données sont les suivantes :

```
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

Cette commande affiche toutes les données de trace VoIP disponibles dans la mémoire tampon. L'utilisation de cette commande a un impact sur les performances du routeur. Une fois la commande entrée, un message d'avertissement s'affiche pour alerter sur le risque et confirmer la poursuite de l'opération :

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

show voip trace cover-buffers

Cette commande affiche une vue d'ensemble des détails de tous les appels signalés sous VoIP Trace. Chaque tronçon d'appel est doté d'une mémoire tampon de couverture qui contient un résumé de l'appel enregistré.

```
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
-------------------------------------------
```

Pour plus d'informations sur chaque champ, reportez-vous au tableau suivant :

Champ	Description
Search-Key	Contient une combinaison d'appel, de numéro appelé et d'ID d'appel
Horodatage	Heure de création du tampon de couverture
ID de tampon	ID tampon du tampon de couverture
ID d'appel	ID d'appel de la branche d'appel respective vers la mémoire tampon de couverture
Peer-CallID	ID d'appel de la branche homologue
Corrélateur	corrélateur FPI de l'appel
Numéro appelé	Numéro appelé de la branche d'appel respective du tampon de couverture
Numéro-appelant	Numéro d'appel de la branche d'appel respective du tampon de couverture
ID d'appel Sip	Sip call-id de la branche d'appel respective du tampon de couverture
ID de session Sip	ID de session SIP de la branche d'appel respective du tampon de couverture
GUIDE	GUID de l'appel respectif de la mémoire tampon de couverture
Jambe D'Ancrage	La branche d'ancrage est définie sur yes si la branche d'appel respective est une branche d'ancrage dans le flux de transfert d'appel ou déploiement de proxy multimédia
Jambe Fourchue	Le segment bifurqué est défini sur oui si le segment d'appel respectif est un segment d'ancrage dans le flux de bifurcation d'appel ou le déploiement de proxy multimédia
ID d'appel associés	ID d'appel des branches fourchues associées

Afin de filtrer les tampons de couverture, nous pouvons utiliser les commandes **include** et **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 combinaison avec la commande précédente, **show voip trace call-id** peut être utilisé pour trouver les appels. Une fois que l'ID d'appel a été identifié, cette commande peut être utilisée pour afficher toutes les informations relatives à la branche d'appel spécifique :

```
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

Cette commande show affiche des informations détaillées sur l'état, la consommation de mémoire, les appels en erreur ou en panne, les appels réussis, les horodatages des entrées les plus récentes et les plus anciennes, etc.

```
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
```

Pour plus d'informations sur chaque champ, reportez-vous au tableau suivant :

Champ	Description
État de suivi	Affiche l'état du suivi, y compris l'heure et la date d'activation du suivi VoIP.
Limite de mémoire configurée	Affiche la limite de mémoire configurée. Cela représente 10 % de la taille de la mémoire du pool de processeurs
Mémoire consommée	Affiche la quantité de mémoire consommée dynamiquement pour la trace VoIP
Total des tronçons d'appel abandonnés	Affiche le nombre de tronçons d'appel ayant échoué dans la mémoire tampon de journalisation. Les appels ignorés correspondent aux t d'appel associés aux erreurs IEC
Trace la plus ancienne abandonnée	Affiche les horodatages et la clé de recherche de l'appel ayant échoué le plus ancien depuis l'activation de VoIP Trace
Dernière trace vidée	Affiche les horodatages et la clé de recherche du dernier appel ayant échoué depuis l'activation de la trace VoIP
Total des tronçons d'appel capturés	Affiche le nombre total de tronçons capturés après l'activation de VoIP Trace
Nombre total de tronçons d'appel disponibles	Affiche le nombre total de tronçons d'appel disponibles dans l'historique. Ce nombre être identique ou différent du nombre total de tronçons d'appel capturés, selon la limi mémoire.
Trace la plus ancienne disponible	Affiche l'horodatage et la clé de recherche du tampon de couverture le plus ancien disponible dans la mémoire
Dernière trace disponible	Affiche l'horodatage et la clé de recherche de la dernière mémoire tampon de couver disponible dans la mémoire
Total des traces manquées	Affiche le nombre de tronçons d'appel manqués en raison d'une limite de mémoire.

Commandes show supplémentaires

Champ	Utilisation	
show voip trace correlator <correlator>	show voip trace correlator 4	Filtre et affiche le suivi VOIP pour un ID d'appel spécifique à
show voip trace session-id <session-id>	show voip trace session-id 87003120822b5dbd8fd80f62d8e57c48	Filtre et affiche le suivi VOIP d'un app de l'en-tête de l'ID de session du mes l'appel.
show voip trace sip-call-id <call-id>	show voip trace sip-call-id 01e60dfa9d8442848336d79e3155a8a1	Filtre et affiche le suivi VOIP en foncti

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.