Configurer la collecte de débogage pour les passerelles CUBE et TDM

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Passerelles vocales TDM et CUBE
- Collection de débogages vocaux Cisco IOS/IOS XE
  - Comment accéder à un routeur Cisco IOS/IOS XE via l'interface de ligne de commande (CLI)
  - Comment configurer le moniteur de terminal pour collecter des commandes show ou des débogages
  - Collecter les résultats de la commande show de base à partir de la CLI
  - Collecter les résultats du débogage à partir de la CLI
    - Vérification de la mémoire
    - Vérification de l'unité centrale (UC)
    - Vérification des appels actifs actuels
    - Paramètres du tampon de journalisation
    - Configuration des paramètres Syslog
    - Debug Collection
- Quels débogages peuvent être activés dans les routeurs vocaux
  - Débogage de l'API de contrôle d'appel interne (CCAPI)
  - Flux d'appels SIP
    - Débogages SIP de base
    - Débogages SIP avancés
  - Flux d'appels numériques (PRI, BRI)
    - Débogage numérique de base
    - Débogage numérique avancé
  - Flux d'appels analogiques
  - Flux d'appels MGCP
    - Débogages de base
    - Débogages de CCM-Manager
    - Débogages MGCP avancés
  - Flux d'appels H323
    - Débogages H323 de base
    - Débogages H323 avancés
  - Ressources multimédias SCCP
    - Débogages SCCP de base
    - Débogage SCCP avancé
- Suivi VoIP
  - Restrictions
  - Activation de la trace VoIP

Désactivation de la trace VoIP
Configurer la limite de mémoire
Affichage des données de suivi VoIP
Show VoIP Trace All
Show VoIP Trace Cover-Buffers
Show VoIP Trace Call-Id
Afficher les statistiques de suivi VoIP
Commandes show supplémentaires

Introduction

Ce document décrit certaines des meilleures pratiques pour collecter des débogages vocaux dans le routeur vocal Cisco IOS®/IOS XE®.

Conditions préalables

Exigences

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

Composants utilisés

Pour les besoins de ce document, les composants utilisés sont :

- PuTTY
- Cisco ISR 3925
- Cisco ISR 4451

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.

Informations générales

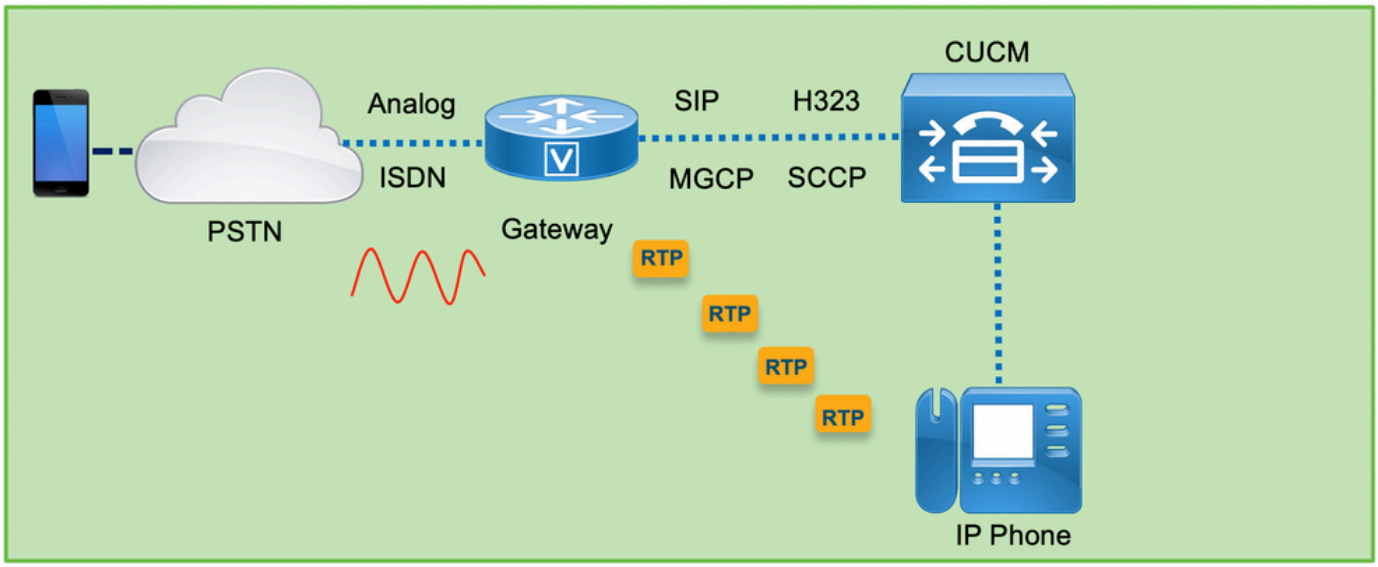
Le processus de collecte de débogage dans ces plates-formes présente des défis et peut potentiellement affecter les performances du périphérique. Les défis et les risques augmentent lorsque plusieurs appels actifs sont établis dans un routeur vocal. Dans certains scénarios, si les débogages ne sont pas collectés correctement, cela peut conduire à une CPU élevée qui peut endommager la capacité du routeur et même déclencher une panne logicielle. Ce document traite des différences entre un CUBE (Cisco Unified Border Element) et une passerelle analogique/multiplexage temporel (TDM).

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 DSP a traité les paquets RTP et envoyé l'audio au circuit spécifique. Ces passerelles interagissent avec H323, MGCP ou Skinny Call Control Protocol (SCCP) du côté VoIP et du côté TDM. Ses circuits RNIS PRI ou analogiques sont les 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 :

TDM/Analog to IP

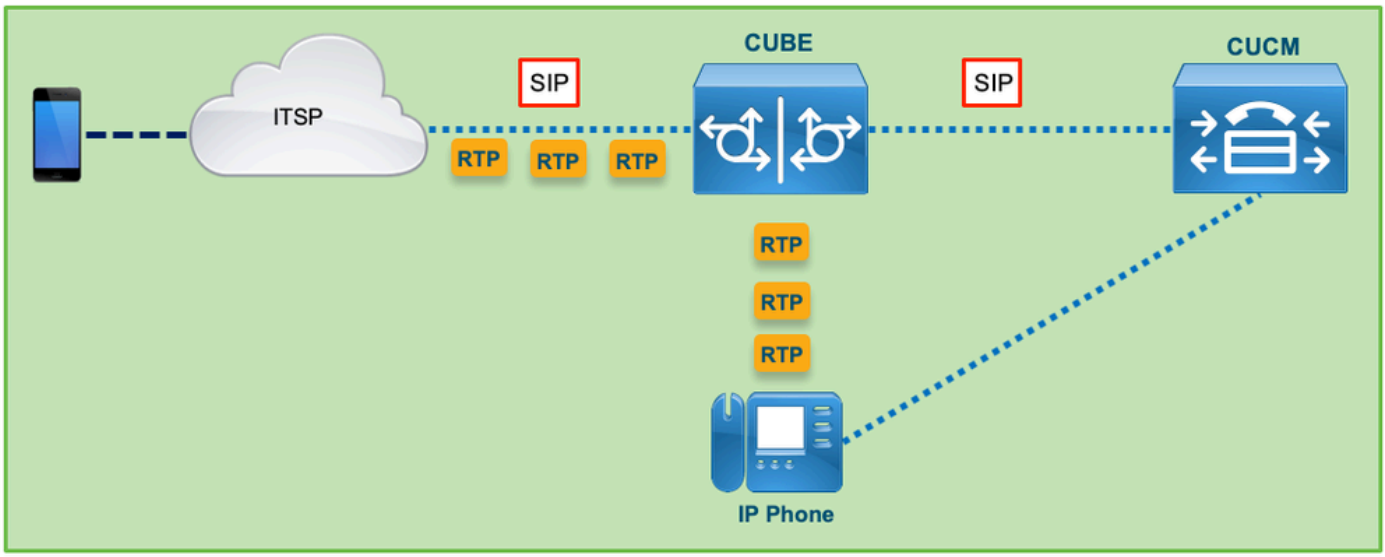


Avec l'introduction de la VoIP, les clients ont rapidement changé leurs systèmes hérités pour adopter une infrastructure VoIP moderne. La même chose s'est produite du côté des fournisseurs de services, où ils utilisent désormais des connexions pour interconnecter les services de téléphonie sur site avec l'infrastructure VoIP des fournisseurs de services et étendre leurs capacités pour 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 ne nécessite plus de 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 :

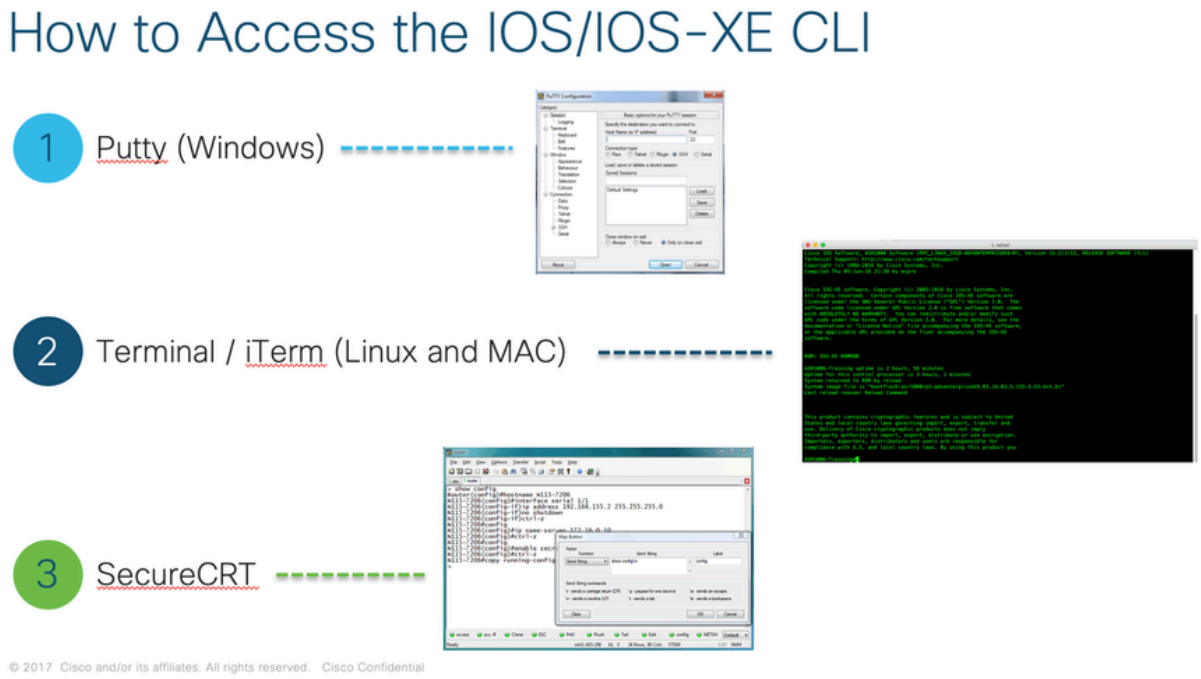


Collection de débogages vocaux Cisco IOS/IOS XE

Les fonctions vocales sont exécutées sur une liste différente de plates-formes, telles que ISR, ASR, CAT8K, entre autres ; cependant, ils utilisent un logiciel commun qui est soit Cisco IOS ou Cisco IOS XE (les différences entre Cisco IOS et Cisco IOS XE ne sont pas couvertes dans cet article). Voici 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 tous les autres périphériques basés 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 couramment utilisé de nos jours pour accéder aux périphériques donnés. 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 :

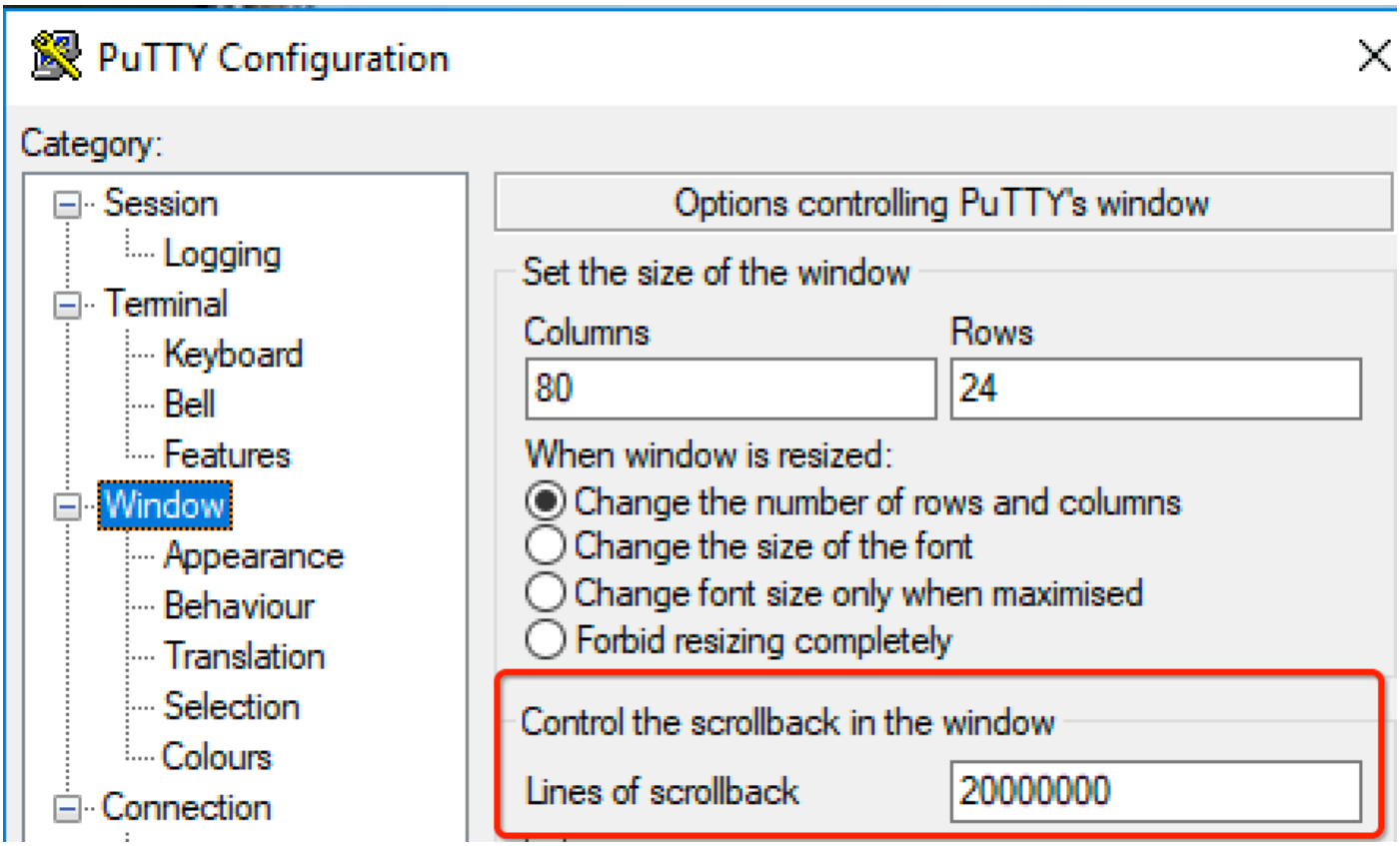


Comment configurer le moniteur de terminal pour collecter des commandes show ou des débogages

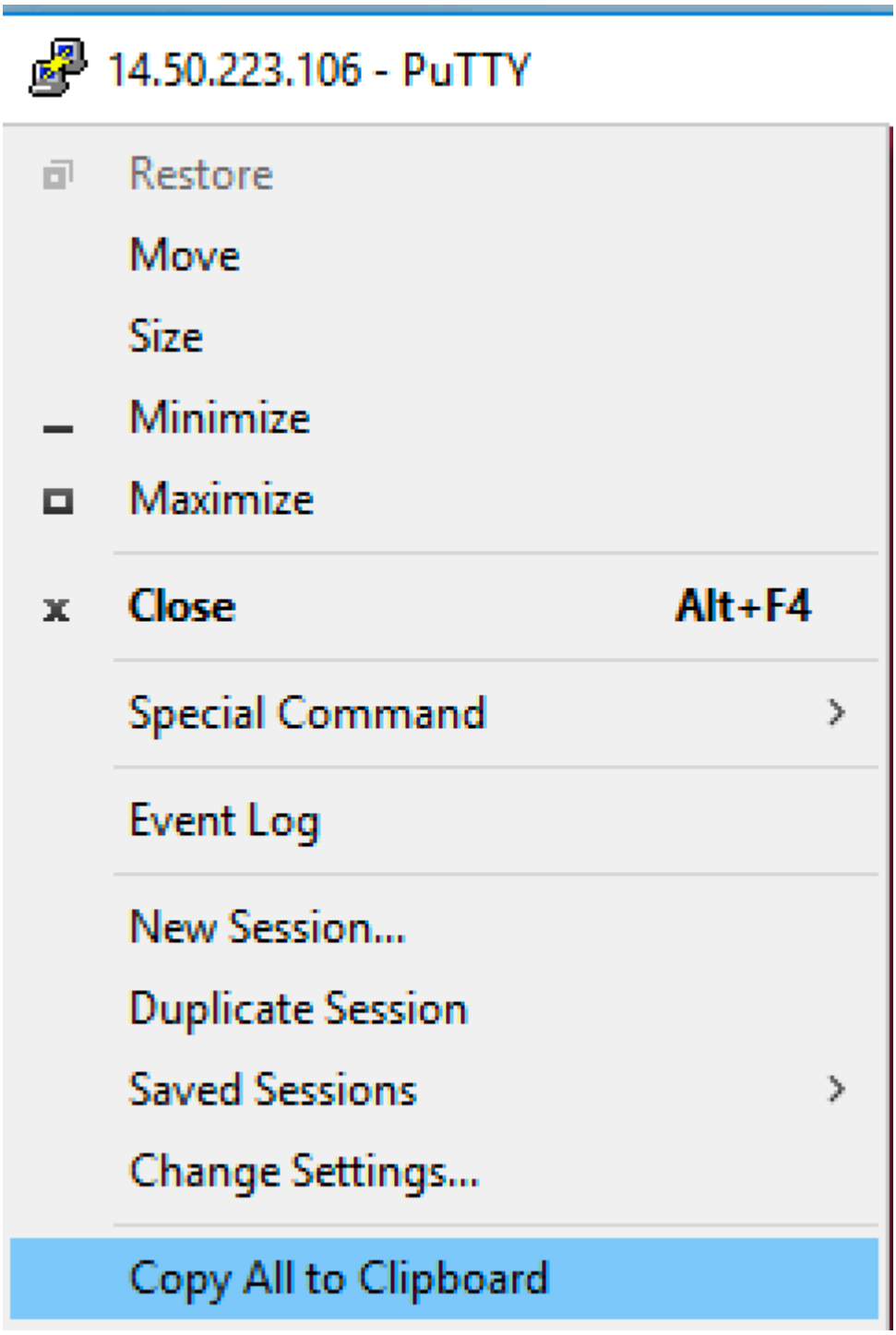
Il existe différentes manières de collecter les résultats de l'interface de ligne de commande. Il est recommandé d'exporter les informations de l'interface de ligne de commande du routeur vers un fichier distinct. Cela facilite le partage de l'information avec des parties externes.

Voici quelques façons de collecter les sorties du périphérique :

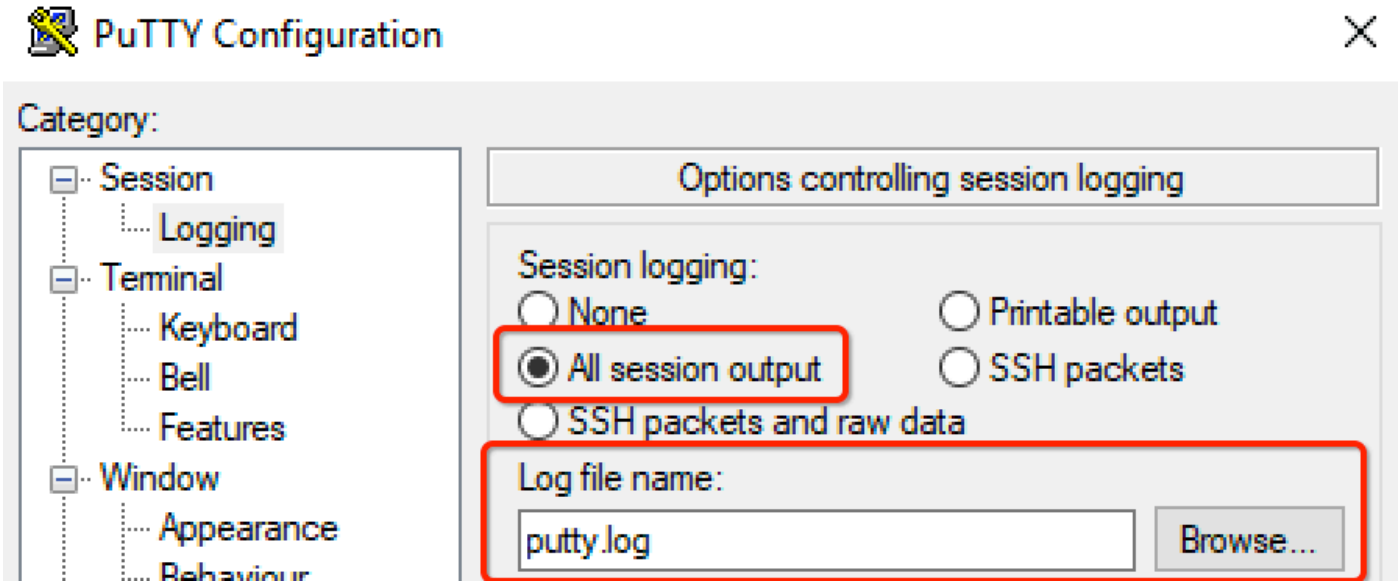
- Videz tous les résultats dans le terminal. Vous devez vous assurer qu'il y a suffisamment de lignes de défilement, sinon, le défilement manque les premières sections de la sortie et les données peuvent être incomplètes. Afin d'augmenter les lignes de défilement dans Putty, naviguez à Putty Configuration > 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 à l'aide de l'option Copier tout dans le Presse-papiers et coller le résultat dans un fichier texte :



- Une autre option consiste à consigner la sortie de session entière dans un fichier .txt. Avec cette option, toutes les commandes entrées et toutes les sorties collectées sont immédiatement consignées dans le fichier texte. Il s'agit d'une pratique courante afin de 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 :



Remarque : Le nom de fichier journal par défaut est utilisé si aucun autre nom n'est spécifié. Cliquez sur le bouton Parcourir afin de savoir exactement où le fichier est enregistré afin de le retrouver plus tard. Assurez-vous également de ne pas écraser un autre fichier putty.log dans le même chemin d'accès.

Collecter les résultats de la commande show de base à partir de la CLI

Les commandes show sont nécessaires pour collecter des informations de base à partir 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 en exécutant une commande show.

Une fois connecté au routeur, la longueur du terminal peut être définie sur 0. Cela permet une collecte plus rapide pour afficher toutes les sorties à la fois et éviter l'utilisation de la barre d'espace. La commande show tech permet de collecter des informations détaillées sur le routeur. Vous pouvez également collecter la commande show tech voice, qui affiche des données plus spécifiques aux fonctionnalités vocales activées sur le routeur :

<#root>

```
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 y a un risque de panne du routeur. Certaines des meilleures pratiques sont expliquées dans les sections suivantes pour éviter certains de ces problèmes.

Vérification de la mémoire

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

Exécutez la commande show process memory pour déterminer la quantité de mémoire que vous pouvez allouer pour consigner toutes les sorties dans la mémoire tampon :



Conseil : Utilisez la commande terminal length default ou terminal length pour revenir à un nombre limité de lignes affichées dans le terminal.

<#root>

```
Router#

show process memory


Processor Pool Total: 8122836952 Used: 456568400

Free: 7666268552
```

```
lsmpi_io Pool Total: 6295128 Used: 6294296 Free: 832
```

Dans cet exemple, 7666268552 octets (7,6 Go) peuvent être utilisés par le routeur. Cette mémoire est partagée par le routeur entre tous les processus système. Cela signifie que vous ne pouvez pas utiliser toute la mémoire disponible pour enregistrer les résultats dans la mémoire tampon, mais 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 ne soit perdue ou écrasée. Dans de rares cas, une plus grande quantité de données est requise pour la collecte. Dans ces scénarios, vous pouvez recevoir de 50 Mo à 100 Mo de sortie dans la mémoire tampon, ou vous pouvez aller plus haut si la mémoire est disponible.

Si la mémoire disponible est insuffisante, il peut y avoir un problème de fuite de mémoire. Si tel est le cas, demandez à l'équipe du TAC de l'architecture de réviser la cause de la mémoire insuffisante.

Vérification de l'unité centrale (UC)

Le processeur est affecté par le nombre 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 basique à avancé (gardez toujours un oeil sur le processeur lorsque des débogages avancés sont utilisés). Si le processeur du routeur est d'environ 50 %, des débogages de base peuvent être exécutés, mais surveillez toujours le processeur. Si le processeur atteint plus de 80 %, arrêtez immédiatement les débogages (voir plus loin dans cet article) et demandez l'aide du centre d'assistance technique.

Exécutez la commande show process cpu sorted | exclude 0.00 pour passer en revue les 5 dernières secondes, 60 secondes et 5 minutes des valeurs de CPU avec les processus supérieurs.

<#root>

```
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.

⚠ Mise en garde : Soyez particulièrement attentif aux principaux processus CPU actifs. Si le processeur est à 50 % ou plus et que le processus supérieur est un processus vocal uniquement, 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 sur la capacité de chaque plate-forme à titre de référence.

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

<#root>

```
Router#

show call active total-calls


Total Number of Active Calls : 0
```

Exécutez la commande show call active voice summary pour recevoir des informations plus détaillées sur les types d'appels qui sont actifs :

<#root>

```
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 valeurs courantes :

- Tronçons d'appel de téléphonie : Appels TDM Gateway, y compris les appels analogiques et PRI/RNIS.
- Pieds d'appel SIP : Total des appels SIP ; s'il s'agit d'un routeur CUBE, cela indique deux tronçons d'appel par appel. Divisez le nombre total d'appels par deux pour obtenir un numéro précis.
- Tronçons d'appel H323 : Total des appels H323.
- Tronçons d'appel SCCP : Ressources multimédias contrôlées par Cisco Unified Communications Manager (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 configure terminal 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, les commandes show tech ou show running-config du routeur sont requises si l'événement de la configuration doit être restauré.

Il s'agit d'un exemple de configuration, qui est une ligne de base commune utilisée par les

ingénieurs du TAC. Cela alloue 10 Mo de mémoire tampon, mais peut être augmenté si nécessaire :

<#root>

#

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

Ces commandes permettent d'effectuer les tâches suivantes :

- service timestamps debug ou log : Garantit que les heures locales du routeur sont écrites sur chaque message enregistré avec une précision de millisecondes. Cette fonction est utile pour rechercher des appels en fonction de l'heure. horodatage en millisecondes, qui vous permet 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 (obligatoire) lorsque les journaux sont transférés à un serveur Syslog. Ceci est très utile pour identifier si un message de débogage au serveur Syslog a été abandonné dans le réseau. Le numéro d'ordre est le premier élément du débogage avant l'horodatage et le message du journal. 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 la mémoire tampon locale. La taille du tampon est définie en octets. Dans la configuration, la taille de la mémoire tampon a été définie sur 10 Mo.
- no logging console et no logging monitor : 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 de la sortie de débogage.
- voice iec syslog : Active les messages de code d'erreur interne vocal 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 des débogages dans la mémoire tampon, elle les collecte en continu. Elle est limitée à la quantité de mémoire que vous pouvez allouer et une fois qu'elle atteint cette quantité de mémoire, la mémoire tampon entoure et abandonne les messages les plus anciens, ce qui conduit à des informations précieuses incomplètes requises pour isoler le problème.

Avec Syslog, le routeur peut envoyer tous les messages de débogage à un serveur externe où le logiciel serveur Syslog les stocke dans des fichiers texte. Bien qu'il s'agisse d'un bon moyen de collecter les résultats du débogage, il ne s'agit pas de la méthode préférée pour la collecte des journaux. Les serveurs Syslog ont tendance à ignorer ou à supprimer des lignes dans le résultat reçu en raison d'un encombrement du serveur. Comme les sorties de débogage peuvent submerger le serveur ou que les paquets peuvent tomber en raison des conditions du réseau. Cependant, dans certains scénarios, les syslogs sont 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. Cela ne garantit pas que toutes les

données sont stockées dans les fichiers, mais réduit le risque de perte de données.

Par défaut, les serveurs syslog utilisent le protocole UDP comme protocole de transport sur le port 514 :

```
<#root>
#
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 <port>
```

Une fois les commandes configurées, le routeur transfère 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 des données supplémentaires qui ne sont pas nécessaires à l'analyse. Exécutez la commande clear log , car cela 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 :

<#root>

```
Router#

clear log


Clear logging buffer [confirm]
Router#
```

Une fois le problème reproduit, désactivez les débogages immédiatement pour arrêter les sorties supplémentaires dans la mémoire tampon, puis collectez les journaux. Vous pouvez vider tous les résultats dans le terminal avec ces commandes :

<#root>

```
Router#

undebug all


Router#

terminal length 0


Router#

show log
```

Parfois, PuTTY se ferme car il ne gère pas toutes les sorties à la fois. Cela est normal et ne signifie pas qu'une défaillance s'est produite. Dans ce cas, rouvrez la session et continuez 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 doivent être imprimées, copiez la sortie de la mémoire tampon sur un périphérique externe directement avec show log | commande redirect :

<#root>

```
Router#

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

Cette commande copie l'intégralité de la sortie du tampon vers une adresse IP FTP de : 192.168.1.2 avec le nom de fichier debug.txt. Le nom de fichier doit toujours être spécifié. Les autres destinations disponibles pour l'exportation des données sont :

<#root>

```
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 ressources multimédias SCCP) est différent et des débogages spécifiques doivent être activés. Tous les débogages requis doivent être activés simultanément. Lorsqu'un seul débogage est capturé à la fois, il est inefficace et accroît la confusion lors de l'analyse des données.

Les débogages sont activés au niveau de l’invite d’exécution de l’interface de ligne de commande Router#, ce qui nécessite que vous disposiez d’autorisations en mode d’exécution privilégié.

Il existe des débogages de base et avancés et des débogages de base sont utilisés pour collecter des informations de signalisation dans SIP, H323 ou MGCP. Ceci montre les conversations que le routeur a avec ses périphériques homologues.

Les débogages avancés sont très détaillés et sont utilisés pour collecter des informations supplémentaires si les erreurs de pile internes ne peuvent pas afficher les débogages de base. Ces débogages sollicitent généralement beaucoup le processeur.

 Conseil : Une fois les débogages activés, n'oubliez pas d'exécuter la commande clear logging. Cette commande efface la mémoire tampon pour une sortie de débogage plus propre.

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

À l'intérieur de chaque routeur Cisco IOS/IOS XE, il y a une API de contrôle d'appel qui est responsable de la communication entre les différentes applications ou protocoles VoIP. Les composants du plan de données tels que RTP, DSP, cartes vocales, entre autres, capturent les données de cette couche. Il y a un débogage spécifique qui peut être utilisé :

<#root>

```
debug voip ccapi inout
```

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

 Conseil : debug voip ccapi inout a généralement un impact minimal sur le CPU du routeur et il est recommandé d'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 couramment utilisés pour les flux d'appels SIP et peuvent être activés à l'intérieur des passerelles CUBE et TDM avec un segment SIP entre le routeur et CUCM ou tout autre serveur ou proxy SIP.

Débogages SIP de base

<#root>

debug ccsip messages

debug ccsip error

debug ccsip non-call

!Optional, applies for SIP OPTIONS and SIP REGISTER Messages.

Débogages SIP avancés

<#root>

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

<#root>

debug isdn q931

Débogage numérique avancé

<#root>

debug isdn q921

Flux d'appels analogiques

Ces débogages sont utilisés lorsque des circuits analogiques impliquent des ports Foreign eXchange Subscriber (FXS) ou Foreign eXchange Office (FXO) :

<#root>

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

<#root>

debug mgcp packets

debug mgcp errors

Débogages de CCM-Manager

Les débogages ccm-manager sont utilisés pour suivre le téléchargement de la configuration, et les messages de liaison MoH et PRI/BRI entre CUCM et la passerelle vocale. Ces débogages sont utilisés en fonction des besoins et dépendent du scénario de défaillance :

<#root>

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

<#root>

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

<#root>

```
debug h225 asn1
```

```
debug h245 asn1
```

```
debug h225 events
```

```
debug h245 events
```

Débogages H323 avancés

<#root>

```
debug cch323 h225
```

```
debug cch323 h245
```

```
debug cch323 all
```

Ressources multimédias SCCP

Ces débogages sont utilisés pour dépanner les problèmes de ressources multimédias SCCP qui impliquent un point de terminaison multimédias (MTP) ou des transcodeurs enregistrés sur un serveur CUCM :

Débogages SCCP de base

<#root>

debug sccp messages

debug sccp events

debug sccp errors

Débogage SCCP avancé

<#root>

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 :

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

Restrictions

VoIP Trace n'enregistre pas les informations relatives aux messages SIP hors dialogue :

- ENREGISTRER
- OPTIONS
- ABONNEMENT/NOTIFICATION
- INFOS

VoIP Trace in HA est pris en charge, mais les mises en garde suivantes s'appliquent :

- Par défaut, VoIP Trace est activé sur le routeur de secours. Seules les traces applicables au processus de veille sont présentées jusqu'à ce qu'il devienne actif.
- Une fois la veille active, elle ne contient PAS les traces complètes des appels avec points de contrôle, mais uniquement les 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. Pour activer cette fonction, exécutez les commandes suivantes :

<#root>

```
Router#
```

configuration terminal

```
Router(config)#
```

```
voice service voip


Router(conf-voi-serv)#

trace

Router(conf-serv-trace)#
```

Désactivation de la trace VoIP

Pour désactiver cette fonction, exécutez les commandes suivantes :

<#root>

```
Router(conf-serv-trace)#

no trace


!or
Router(conf-serv-trace)#

shutdown
```

⚠ Mise en garde : Une fois la fonction VoIP Trace désactivée, toute la mémoire est effacée et les informations sont perdues.

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

<#root>

```
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 des données. Par défaut, elle représente 10 % de la mémoire disponible sur la plate-forme. Toutefois, elle peut être ajustée à un maximum de 1 Go et à un minimum de 10 Mo. La mémoire est allouée de manière dynamique, car la fonction utilise uniquement la mémoire nécessaire et dépend du volume d'appels. Une fois qu'il a 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 sur l'interface de ligne de commande :

<#root>

```
Router(conf-serv-trace)#

memory-limit 1000


Warning: Setting memory limit more than 10% of available platform memory (166 MB) will affect system pe
```

Pour définir la valeur par défaut sur 10 % d'utilisation de la mémoire, exécutez la commande memory-limit platform :

<#root>

```
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]:
```

⚠ Mise en garde : 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, vous devez utiliser des commandes show spécifiques. Les données peuvent être affichées dans la même session de terminal ou peuvent être envoyées via syslog à un serveur syslog hors-box.



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

La signalisation SIP est affichée par segment et n'est pas combinée comme des débogages standard. Les débogages réguliers, tels que les messages de débogage CCSIP, affichent la signalisation SIP d'un appel dans l'ordre exact des événements. Dans VoIP Trace, chaque segment est séparé, pour déterminer le bon ordre, les horodatages sont utilisés.

Pour afficher les données disponibles, exécutez ces commandes :

<#root>

```
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 vous avertir des risques si vous continuez :

<#root>

```
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 comporte une mémoire tampon de couverture créée qui contient un résumé des appels consignés :

<#root>

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

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

Champ	Description
Clé De Recherche	Contient une combinaison d'appel, de numéro appelé et d'ID d'appel
Horodatage	Heure de création du tampon de couverture
Buffer-ID	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-Call-ID	ID d'appel de la branche homologue
Corrélateur	corrélateur FPI de l'appel
Numéro appelé	Numéro appelé de la branche d'appel respective de la mémoire tampon de couverture
Numéro-Appelant	Numéro d'appel de la branche d'appel respective du tampon de couverture
ID d'appel SIP	ID d'appel SIP de la branche d'appel respective de la mémoire 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 « Oui » si la branche d'appel correspondante est une branche d'ancrage dans le flux de transfert d'appel ou le déploiement de proxy multimédia
Jambe Fourchue	Le segment bifurqué est défini sur « Oui » si le segment d'appel correspondant

	est un segment d'ancrage dans le flux de bifurcation d'appel ou le déploiement de proxy multimédia
ID d'appels associés	ID d'appel des branches fourchues associées

---

Pour filtrer les tampons de couverture, exécutez les commandes include et section :

<#root>

```
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 rechercher des appels. Une fois l'ID d'appel identifié, la commande suivante peut être exécutée pour afficher toutes les informations sur le tronçon d'appel spécifique :

<#root>

```
Router#

show voip trace cover-buffers | include Search-key | 8845 | 3002


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

Afficher les statistiques de suivi VoIP

Cette commande show affiche des informations détaillées sur l'état, la consommation de mémoire, les erreurs/échecs d'appel, les appels réussis, les horodatages des entrées les plus récentes et les plus anciennes, etc. :

<#root>

```
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, qui inclut l'heure et la date d'activation du suivi VoIP.
Limite de mémoire configurée	Affiche la limite de mémoire configurée. Il s'agit de 10 % de la taille de la mémoire du pool de processeurs.
Mémoire consommée	Affiche la quantité de mémoire consommée dynamiquement pour la trace VoIP.
Nombre total de segments d'appel vidés	Affiche le nombre de tronçons d'appel ayant échoué dans la mémoire tampon de journalisation. Les appels ignorés font référence aux tronçons 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.
Nombre total de segments d'appel capturés	Affiche le nombre total de tronçons capturés après l'activation de VoIP Trace.
Nombre total de segments d'appel disponibles	Affiche le nombre total de tronçons d'appel disponibles dans l'historique. Cela peut être identique ou différent par rapport au nombre total de tronçons d'appel capturés, cela dépend de la limite de mémoire.
Plus ancienne trace 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 disponible dans la mémoire.
Total des traces manquantes	Affiche le nombre de tronçons d'appel manqués en raison d'une limite de mémoire.

Commandes show supplémentaires

Champ	Utilisation	Description
show voip trace correlator <correlator>	show voip trace correlator 4	Filtre et affiche le suivi VOIP pour un ID d'appel spécifique à partir de la mémoire tampon de couverture.
show voip trace session-id <session-id>	show voip trace session-id 87003120822b5dbd8fd80f62d8e57c48	Filtre et affiche le suivi VOIP d'un appel en fonction de l'ID de session SIP. L'UUID local ou distant de l'en-tête session-ID du message SIP peut être utilisé pour afficher les deux tronçons

		de l'appel.
show voip trace sip-call-id <call-id>	show voip trace sip-call-id 01e60dfa9d8442848336d79e3155a8a1	Filtre et affiche le suivi VOIP en fonction de l'ID d'appel SIP.

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.