Comprendre les informations importantes sur les commandes de débogage

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Avertissements
- Avant le débogage
  - Obtention des résultats du débogage
    - Port de console
    - Port auxiliaire
    - Ports VTY
    - Consignation des messages dans une mémoire tampon interne
    - Consignation des messages sur un serveur Syslog UNIX
  - Autres tâches de pré-débogage
  - Arrêter le débogage
- Utilisation de la commande debug ip packet
- Débogages déclenchés conditionnellement
- Informations connexes

Introduction

Ce document décrit les directives générales sur l'utilisation des commandes de débogage, y compris la commande de débogage ip packet disponible sur les plateformes Cisco IOS®.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connexion au routeur à l'aide des ports de console, aux et vty.

- Problèmes généraux de configuration de Cisco IOS.
- Interprétation des sorties de débogage de Cisco IOS.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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

Ce document fournit des directives générales pour l'utilisation des commandes debug sur les plates-formes Cisco IOS®. Il inclut également des exemples et une présentation du débogage conditionnel.

Les commandes du mode d’exécution privilégié debug fournissent des informations de diagnostic sur les événements réseau, l’état du protocole, le traitement des paquets et l’activité générale du réseau. Ces commandes permettent d'identifier la cause de problèmes spécifiques lors du dépannage.

Cependant, les commandes debug peuvent générer une grande quantité d'informations de sortie et peuvent affecter les performances du périphérique, en particulier sur les routeurs qui gèrent déjà un trafic élevé ou une utilisation CPU élevée. Pour cette raison, exécutez les commandes debug avec précaution et uniquement lorsque cela est nécessaire pour le dépannage.



Remarque : Ce document n'explique pas comment utiliser ou interpréter des commandes de débogage spécifiques et leur résultat. Pour plus d'informations sur les commandes de débogage individuelles, reportez-vous à la documentation de référence des commandes de débogage Cisco appropriée.

Avertissements

Exécutez les commandes debug avec précaution. En règle générale, utilisez ces commandes uniquement sous la direction de votre représentant du support technique lors du dépannage de

problèmes spécifiques.

L’activation du débogage peut perturber le fonctionnement du routeur, en particulier lorsque le réseau est soumis à une charge importante. Si la journalisation est activée, le serveur d'accès peut se bloquer par intermittence lorsque le port de console est surchargé de messages de journalisation.

Avant d'exécuter une commande debug, tenez compte de la quantité de sortie que la commande peut générer et de la durée pendant laquelle la session de débogage peut s'exécuter.

Par exemple, sur un routeur avec une interface Basic Rate, debug isdn q931 est peu susceptible d'affecter le système. Cependant, l'exécution de la même commande debug sur un AS5800 avec une configuration E1 complète peut générer suffisamment de résultats pour que le périphérique se bloque ou cesse de répondre.

Avant le débogage, vérifiez la charge du processeur en exécutant la commande show processes cpu. Vérifiez qu'une capacité de processeur suffisante est disponible avant d'activer le débogage, c'est ainsi.

Par exemple, si un routeur Cisco 7200 avec une interface ATM exécute le pontage, le redémarrage du routeur peut consommer des ressources CPU importantes, selon le nombre de sous-interfaces configurées. Pour chaque circuit virtuel (VC), un paquet BPDU (Bridge Protocol Data Unit) doit être généré. L'activation du débogage pendant cette période critique peut entraîner une augmentation considérable de l'utilisation du processeur, ce qui peut entraîner un blocage du périphérique ou une perte de connectivité réseau.



Remarque : Lorsque des débogages sont en cours d'exécution, vous ne voyez généralement pas l'invite du routeur, en particulier lorsque le débogage est intensif. Cependant, dans la plupart des cas, vous pouvez exécuter les commandes no debug all ou undebug all pour arrêter les débogages.

Avant le débogage

En plus des points mentionnés ci-dessus, assurez-vous de comprendre l'impact des débogages sur la stabilité de la plate-forme. Avant d’activer une commande debug, vous devez également déterminer l’interface du routeur à connecter.

Obtention des résultats du débogage

Les routeurs peuvent afficher les résultats du débogage sur diverses interfaces, notamment les ports de console, aux et vty. Les routeurs peuvent également consigner les messages dans une mémoire tampon interne vers un serveur syslog unix externe.

Port de console

Si vous êtes connecté à la console dans des configurations normales, aucune tâche supplémentaire n'est nécessaire. Le résultat du débogage doit être affiché automatiquement. Cependant, assurez-vous que le niveau de la console de journalisation est défini comme souhaité et que la journalisation n'a pas été désactivée avec la commande no logging console.



Avertissement : Un nombre excessif de débogages sur le port de console d’un routeur peut entraîner son blocage. En effet, le routeur donne automatiquement la priorité aux résultats de la console avant les autres fonctions du routeur. Si le routeur traite une sortie de débogage importante vers le port de console, il peut se bloquer. Si le résultat du débogage est excessif, utilisez les ports vty (telnet) ou les tampons du journal pour obtenir vos débogages.



Remarque : Par défaut, la journalisation est activée sur le port de console. Le port de console traite toujours la sortie de débogage même si vous utilisez un autre port ou une autre méthode (comme aux, vty ou buffer) pour capturer la sortie. Cisco recommande, dans des conditions de fonctionnement normales, d'exécuter la commande no logging console, qui est activée à tout moment et d'utiliser d'autres méthodes pour capturer les débogages. Dans les cas où vous devez utiliser la console, réactivez temporairement la console de journalisation.

Port auxiliaire

Si vous êtes connecté via un port auxiliaire, exécutez la commande terminal monitor. Vérifiez également que la commande no logging on n'est pas activée sur le routeur.



Remarque : Si vous utilisez le port aux pour surveiller le routeur, gardez à l'esprit que lorsque le routeur redémarre, le port aux n'affiche pas la sortie de la séquence de démarrage. Connectez-vous au port de console pour afficher la séquence de démarrage.

Ports VTY

Si vous êtes connecté via un port auxiliaire ou via telnet, tapez la commande terminal monitor. Vérifiez également que la commande no logging on n'est pas utilisée.

Consignation des messages dans une mémoire tampon interne

Le périphérique de journalisation par défaut est la console ; tous les messages sont affichés sur la console, sauf indication contraire.

Pour consigner les messages dans une mémoire tampon interne, exécutez la commande de configuration de routeur logging buffered. Voici la syntaxe complète de cette commande :

<#root>

```
logging buffered
no logging buffered
```

La commande logging buffered copie les messages de journal dans une mémoire tampon interne au lieu de les écrire dans la console. La mémoire tampon est de nature circulaire, de sorte que les messages plus récents remplacent les messages plus anciens.

Pour afficher les messages consignés dans la mémoire tampon, utilisez la commande d'exécution privilégiée show logging. Le premier message affiché est le plus ancien message de la mémoire tampon. Vous pouvez spécifier la taille de la mémoire tampon et le niveau de gravité des messages à consigner.



Remarque : Assurez-vous que la mémoire disponible est suffisante avant d'entrer la taille du tampon. Utilisez la commande show proc mem pour voir votre mémoire disponible.

La commande no logging buffered annule l'utilisation de la mémoire tampon et écrit des messages sur la console (valeur par défaut).

Consignation des messages sur un serveur Syslog UNIX

Pour consigner les messages sur l'hôte du serveur syslog, exécutez la commande de

configuration logging router. Affichez la syntaxe complète de cette commande :

<#root>

logging

no logging

La commande logging identifie un hôte serveur syslog pour recevoir des messages de journalisation. L'argument **<**ip-address**>** est l'adresse IP de l'hôte. En exécutant cette commande plusieurs fois, vous créez une liste de serveurs syslog qui reçoivent des messages de journalisation.

La commande no logging supprime le serveur syslog avec l'adresse spécifiée de la liste des syslogs.

Autres tâches de pré-débogage

1. Configurez le logiciel émulateur de terminal de sorte qu'il capture la sortie de débogage dans un fichier. Reportez-vous à la documentation de votre émulateur de terminal logiciel.
2. Activez les horodatages en millisecondes (ms) en exécutant la commande service timestamps :

   <#root>

   router(config)#

   service timestamps debug datetime msec

   router(config)#

   service timestamps log datetime msec

Ces commandes ajoutent des horodatages aux débogages au format MMM DD HH:MM:SS, indiquant la date et l'heure en fonction de l'horloge système. Si l'horloge système n'a pas été réglée, la date et l'heure sont précédées d'un astérisque (*) pour indiquer que la date et l'heure

sont probablement incorrectes.

Il est généralement conseillé de configurer des horodatages en millisecondes, car cela fournit un haut niveau de clarté lors de l'examen des sorties de débogage. Les horodatages en millisecondes fournissent une meilleure indication de la synchronisation des divers événements de débogage les uns par rapport aux autres. Cependant, lorsque le port de console émet un grand nombre de messages, ils ne peuvent pas être mis en corrélation avec la synchronisation réelle de l'événement.

Par exemple, si vous activez debug x25all sur une boîte qui a 200 VC, et que la sortie est consignée dans la mémoire tampon (en exécutant les commandes no logging console et logging buffered), l'horodatage affiché dans la sortie de débogage (dans la mémoire tampon) ne peut pas être l'heure exacte à laquelle le paquet passe par l'interface. Par conséquent, n'utilisez pas les horodatages msec pour prouver les problèmes de performances, mais pour obtenir des informations relatives au moment où les événements se produisent.

Arrêter le débogage

Pour arrêter un débogage, utilisez les commandes no debug all ou undebug all. Vérifiez que les débogages ont été désactivés en utilisant la commande show debug.

N'oubliez pas que les commandes no logging console et terminal no monitor empêchent uniquement la sortie sur la console, respectivement aux ou vty. Il n’arrête pas le débogage et utilise les ressources du routeur.

Utilisation de la commande debug ip packet

Sur les routeurs Cisco IOS® classiques, le paquet debug ip voit principalement le trafic commuté par processus. Le trafic transféré via la commutation rapide ou CEF n'apparaît pas à moins que le transfert ne soit forcé dans le chemin de commutation de processus. Cependant, comme il génère une sortie pour chaque paquet, la sortie peut être étendue et le routeur se bloque. Pour cette raison, exécutez uniquement le paquet debug ip sous les contrôles les plus stricts comme décrit dans cette section.

La meilleure façon de limiter la sortie de debug ip packet est de créer une liste d'accès qui est liée au débogage. Seuls les paquets qui correspondent aux critères de la liste d'accès peuvent être soumis au paquet debug ip. Cette liste d'accès n'a pas besoin d'être appliquée sur une interface, mais est plutôt appliquée à l'opération de débogage.

Avant d'exécuter le paquet ip de débogage, notez que le routeur utilise la commutation rapide par défaut, ou peut utiliser la commutation CEF s'il est configuré pour le faire. Cela signifie que, une fois que ces techniques sont en place, le paquet n'est pas fourni au processeur, le débogage ne montre rien. Pour que cela fonctionne, vous devez désactiver la commutation rapide sur le routeur sans ip route-cache (pour les paquets de monodiffusion) ou sans ip mroute-cache (pour les paquets de multidiffusion). Cela doit être appliqué sur les interfaces où le trafic est censé circuler. Vérifiez ceci avec la commande show ip route.



Remarque : Sur les plates-formes plus récentes, le transfert est généralement géré par CEF ou par une commutation matérielle, de sorte que la désactivation de la commutation rapide n'est plus applicable ou recommandée. Par conséquent, debug ip packet peut échouer à montrer de manière fiable le trafic de transit, et le dépannage moderne se base généralement sur la capture spécifique à la plate-forme ou des outils matériels à la place.

Débogages déclenchés conditionnellement

Lorsque la fonctionnalité Débogage conditionnellement déclenché est activée, le routeur génère des messages de débogage pour les paquets entrant ou sortant du routeur sur une interface spécifiée ; le routeur ne génère pas de sortie de débogage pour les paquets entrant ou sortant par une autre interface.

Examinez une implémentation simple de débogages conditionnels. Considérez ce scénario : le routeur suivant (trabol) comporte deux interfaces (série 0 et série 3) qui exécutent toutes deux l’encapsulation HDLC.

Vous pouvez exécuter la commande normaldebug serial interface pour observer les keepalives HDLC reçus sur toutes les interfaces. Vous pouvez observer les keepalives sur les deux interfaces :

<#root>

```
traxbol#

debug serial interface


Serial network interface debugging is on
traxbol#
*Mar  8 09:42:34.851:

Serial0: HDLC
```

```
 myseq 28, mineseen 28*, yourseen 41, line up

! -- HDLC keeplaive on interface Serial 0

*Mar  8 09:42:34.855:

Serial3: HDLC

 myseq 26, mineseen 26*, yourseen 27, line up

! -- HDLC keeplaive on interface Serial 3

*Mar  8 09:42:44.851: Serial0: HDLC myseq 29, mineseen 29*, yourseen 42, line up
*Mar  8 09:42:44.855: Serial3: HDLC myseq 27, mineseen 27*, yourseen 28, line up
```

Activez les débogages conditionnels pour l'interface série 3, ce qui signifie que seuls les débogages de l'interface série 3 sont affichés. Exécutez la commande debug interface <interface_type interface_number >:

<#root>

```
traxbol#

debug interface serial 3


Condition 1 set
```

Exécutez la commande show debug condition pour vérifier que le débogage conditionnel est actif (une condition pour l'interface série 3 est active) :

<#root>

```
traxbol#

show debug condition



Condition 1: interface Se3 (1 flags triggered)
Flags: Se3
traxbol#
```

Maintenant, seuls les débogages de l'interface Serial 3 sont affichés :

<#root>

```
*Mar  8 09:43:04.855:

Serial3: HDLC

 myseq 29, mineseen 29*, yourseen 30, line up
*Mar  8 09:43:14.855:

Serial3: HDLC

 myseq 30, mineseen 30*, yourseen 31, line up
```

Exécutez la commande undebug interface <interface_type interface_number> pour supprimer le débogage conditionnel. Il est recommandé de désactiver les débogages (par exemple, en utilisant undebug all) avant de supprimer le déclencheur conditionnel. Cela permet d'éviter un déluge de sorties de débogage lorsque la condition est supprimée.

<#root>

```
traxbol#

undebug interface serial 3

This condition is the last interface condition set.
Removing all conditions can cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.
Proceed with removal? [yes/no]:

y


Condition 1 has been removed
traxbol
```

Vous pouvez observer le débogage à la fois pour l'interface Serial 0 et pour l'interface Serial 3 :

<#root>

```
*Mar  8 09:43:34.927:

Serial3: HDLC

 myseq 32, mineseen 32*, yourseen 33, line up
*Mar  8 09:43:44.923:

Serial0: HDLC

 myseq 35, mineseen 35*, yourseen 48, line up
```

Avertissement : Certaines opérations de débogage sont conditionnelles par elles-mêmes. Un exemple est le débogage ATM. Avec le débogage ATM, vous devez spécifier explicitement l'interface pour laquelle les débogages doivent être activés plutôt que d'activer les débogages sur toutes les interfaces ATM et de spécifier une condition.

Cette section montre la manière correcte de limiter le débogage des paquets ATM à une sous-interface :

<#root>

```
arielle-nrp2#

debug atm packet interface atm 0/0/0.1


!--- Note that you explicitly specify the sub-interface to be used for debugging

ATM packets debugging is on

Displaying packets on interface ATM0/0/0.1 only


arielle-nrp2#
*Dec 21 10:16:51.891: ATM0/0/0.1(O):
VCD:0x1 VPI:0x1 VCI:0x21 DM:0x100 SAP:AAAA CTL:03 OUI:0080C2 TYPE:0007
Length:0x278
*Dec 21 10:16:51.891: 0000 FFFF FFFF FFFF 0010 7BB9 BDC4 0800 4500 025C 01FE
0000 FF11 61C8 0A30
*Dec 21 10:16:51.891: 4B9B FFFF FFFF 0044 0043 0248 0000 0101 0600 0015 23B7
0000 8000 0000 0000
*Dec 21 10:16:51.891: 0000 0000 0000 0000 0000 0000 0010 7BB9 BDC3 0000 0000
0000 0000 0000 0000
*Dec 21 10:16:51.891: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000
*Dec 21 10:16:51.891: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000
*Dec 21 10:16:51.891: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000
*Dec 21 10:16:51.891: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000
*Dec 21 10:16:51.895: 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000
*Dec 21 10:16:51.895:
arielle-nrp2#
```

Si vous essayez d'activer le débogage ATM sur toutes les interfaces (avec une condition appliquée), le routeur peut se bloquer s'il a un grand nombre de sous-interfaces ATM. Un exemple de méthode incorrecte pour le débogage ATM est montré.

Dans ce cas, vous pouvez voir qu'une condition est appliquée, mais vous voyez également que cela n'a aucun effet. Vous pouvez toujours voir le paquet de l’autre interface.

Dans ce scénario de travaux pratiques, vous n’avez que deux interfaces et très peu de trafic. Si le nombre d'interfaces est élevé, le résultat du débogage pour toutes les interfaces est également extrêmement élevé et peut entraîner le blocage du routeur :

<#root>

```
arielle-nrp2#

show debugging condition



Condition 1: interface AT0/0/0.1


 (1 flags triggered)
Flags: AT0/0/0.1

! -- A condition for a specific interface.


arielle-nrp2#

debug atm packet


ATM packets debugging is on
Displaying all ATM packets
arielle-nrp2#
*Dec 21 10:22:06.727:

ATM0/0/0.2

(O):

! -- You see debugs from interface ATM0/0/0/.2, even though the condition
! -- specified ONLY AT0/0/0.1


  VCD:0x2 VPI:0x5 VCI:0x37 DM:0x100 SAP:AAAA CTL:03 OUI:0080C2
TYPE:000E Length:0x2F
*Dec 21 10:22:06.727: 0000 0000 0180 0000 107B B9BD C400 0000 0080
0000 107B B9BD C480 0800 0014
*Dec 21 10:22:06.727: 0002 000F 0000
*Dec 21 10:22:06.727: un a
*Dec 21 10:22:08.727: ATM0/0/0.2(O):
  VCD:0x2 VPI:0x5 VCI:0x37 DM:0x100 SAP:AAAA CTL:03 OUI:0080C2
TYPE:000E Length:0x2F
*Dec 21 10:22:08.727: 0000 0000 0180 0000 107B B9BD C400 0000 0080
0000 107B B9BD C480 0800 0014
*Dec 21 10:22:08.727: 0002 000F 0000
*Dec 21 10:22:08.727: ll
```

```
*Dec 21 10:22:10.727: ATM0/0/0.2(O):
  VCD:0x2 VPI:0x5 VCI:0x37 DM:0x100 SAP:AAAA CTL:03 OUI:0080C2
TYPE:000E Length:0x2F
*Dec 21 10:22:10.727: 0000 0000 0080 0000 107B B9BD C400 0000 0080
0000 107B B9BD C480 0800 0014
*Dec 21 10:22:10.727: 0002 000F 0000
*Dec 21 10:22:10.727:
*Dec 21 10:22:12.727: ATM0/0/0.2(O):
  VCD:0x2 VPI:0x5 VCI:0x37 DM:0x100 SAP:AAAA CTL:03 OUI:0080C2
TYPE:000E Length:0x2F
*Dec 21 10:22:12.727: 0000 0000 0080 0000 107B B9BD C400 0000 0080
0000 107B B9BD C480 0800 0014
*Dec 21 10:22:12.727: 0002 000F 0000
*Dec 21 10:22:12.727:
*Dec 21 10:22:13.931:
```

ATM0/0/0.1

```
(O):

!--- You also see debugs for interface ATM0/0/0.1 as you wanted.

VCD:0x1 VPI:0x1 VCI:0x21 DM:0x100 SAP:AAAA CTL:03 OUI:0080C2
TYPE:0007 Length:0x278
*Dec 21 10:22:13.931: 0000 FFFF FFFF FFFF 0010 7BB9 BDC4 0800 4500
025C 027F 0000 FF11 6147 0A30
*Dec 21 10:22:13.931: 4B9B FFFF FFFF 0044 0043 0248 0000 0101 0600
001A 4481 0000 8000 0000 0000
*Dec 21 10:22:13.931: 0000 0000 0000 0000 0000 0000 0010 7BB9 BDC3
0000 0000 0000 0000 0000 0000
*Dec 21 10:22:13.931: 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000
*Dec 21 10:22:13.931: 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000
*Dec 21 10:22:13.931: 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000
*Dec 21 10:22:13.931: 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000
*Dec 21 10:22:13.935: 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000
```

Informations connexes

- Assistance technologique pour la numérotation et l'accès
- Assistance technique de Cisco et téléchargements

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.