

# Informations importantes sur les commandes debug

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Avertissements](#)

[Conventions](#)

[Avant de déboguer](#)

[Obtenir des résultats du débogage](#)

[D'autres tâches de prédébogage](#)

[Pour cesser de déboguer](#)

[Utilisation de la commande debug ip packet](#)

[Débogages conditionnellement déclenchés](#)

[Informations connexes](#)

## [Introduction](#)

Cette page fournit quelques lignes directrices générales sur l'utilisation des débogages disponibles sur des plates-formes Cisco IOS®, aussi bien que des exemples pour utiliser correctement la commande **debug ip packet** et le débogage conditionnel.

**Remarque:** Ce document n'explique pas comment utiliser et interpréter les commandes spécifiques **debug** et les résultats. Reportez-vous à la documentation de référence appropriée sur les commandes de débogage de Cisco pour les informations sur les commandes **debug** spécifiques.

La sortie de **mettent au point les** commandes de privileged exec fournit les informations de diagnostic qui incluent un grand choix d'événements d'interconnexion de réseaux concernant l'état du protocole et l'activité réseau en général.

## [Conditions préalables](#)

### [Conditions requises](#)

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connexion au routeur à l'aide de la console ainsi que des ports aux et vty
- Questions générales de configuration 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.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Avertissements

Utilisez les commandes **debug** avec prudence. D'une manière générale, il est recommandé que ces commandes soient seulement utilisées sous les orientations de l'agent d'assistance technique de votre routeur pour le dépannage de problèmes spécifiques.

Permettre le débogage peut perturber le fonctionnement du routeur quand les interréseaux connaissent des conditions de charge élevée. Par conséquent, si se connecter est activé, le serveur d'accès peut par intermittence geler dès que le port de console obtiendra surchargé avec des messages de log.

Avant que vous commenciez une commande de **débogage**, considérez toujours la sortie que cette commande générera et la durée ceci peut prendre. Par exemple, si vous avez un routeur avec un accès de base (BRI), le **debug isdn q931** ne nuira pas probablement au système. Mais, en faisant la même chose mettez au point sur un AS5800 avec la pleine configuration d'E1 peut générer probablement tellement l'entrée qu'elle peut s'arrêter et cesser de répondre.

Avant le débogage, regardez votre chargement CPU avec la commande de **show processes cpu**. Vérifiez que vous avez la CPU suffisante disponible avant que vous commenciez mettre au point. Référez-vous à l'[utilisation du CPU élevé de dépannage sur des Routeurs de Cisco](#) pour plus d'informations sur la façon manipuler les chargements élevés CPU. Par exemple, si vous avez un routeur de Cisco 7200 avec une interface ATM faisant la transition alors, selon la quantité de sous-interfaces configurées, redémarrant le routeur pourrait utiliser beaucoup de sa CPU. La raison à cela est que, pour chaque circuit virtuel (VC), un paquet Bridge Protocol Data Unit (BPDU) doit être généré. Initier des débogages à ce moment critique peut provoquer l'augmentation excessive de l'utilisation du CPU et résulter en une suspension et en une perte de connectivité du réseau.

**Remarque:** Quand met au point s'exécutent, vous ne voient pas habituellement la demande de routeur, particulièrement quand le débogage est intensif. Mais, dans la plupart des cas, vous pouvez employer les **commande no debug all ou undebg all** afin d'arrêter met au point. Reportez-vous à la section [Obtenir des résultats du débogage](#) pour plus d'informations sur la façon d'utiliser prudemment les débogages

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Avant de déboguer

En plus des points mentionnés ci-dessus, assurez-vous de comprendre l'incidence des débogages sur la stabilité de la plate-forme. Vous devriez également considérer sur quelle interface du routeur vous devriez vous connecter. Cette section a quelques instructions.

## [Obtenir des résultats du débogage](#)

Les routeurs peuvent afficher des résultats du débogage sur diverses interfaces, y compris la console ainsi que les ports aux et vty. Les routeurs peuvent également consigner des messages vers un tampon interne vers un serveur syslog unix externe. Les instructions et les mises en garde pour chaque méthode sont discutées ci-dessous :

### Port de console

Si vous êtes connecté sur la console, sous des configurations normales, aucun travail supplémentaire doit être fait. Le résultat du débogage devrait être automatiquement affiché. Mais, assurez-vous que le **niveau de la console de journalisation** est placé comme désiré et cela se connectant n'a pas été désactivé avec la commande de **no logging console**. Reportez-vous à [Utiliser les commandes de débogage](#) pour plus d'informations.

**Avertissement** : Les débogages excessifs du port de console d'un routeur peuvent causer sa suspension. Ceci se doit au fait que le routeur donne automatiquement la priorité à la sortie de console vis-à-vis d'autres fonctions du routeur. Par conséquent, si le routeur traite d'un grand résultat de débogage au port de console, il peut être suspendu. Par conséquent, si le résultat du débogage est excessif, utilisez les ports vty (telnet) ou les mémoires tampon de journal pour obtenir vos débogages. Plus d'informations sont fournies ci-dessous.

**Remarque:** Par défaut, la journalisation est activée sur le port de console. Par conséquent, le port de console traite toujours du résultat de débogage même si vous employez réellement un autre port ou méthode (tel qu'Aux, vty ou mémoire tampon) pour saisir le résultat. Par conséquent, Cisco recommande que, en fonctionnement normal, vous ont la commande enabled de **no logging console** à tout moment et emploient d'autres méthodes pour les capturer met au point. Dans les situations où vous devez utiliser la console, activez temporairement de nouveau **logging console**.

### Port AUX

Si vous êtes connecté par l'intermédiaire d'un port auxiliaire, introduisez la commande de **terminal monitor**. Vérifiez également que la commande **no logging on** n'a pas été activée sur le routeur.

**Remarque:** Si vous utilisez le port aux pour contrôler le routeur, gardez présent à l'esprit que, quand le routeur redémarre, le port Aux n'affiche pas la séquence de démarrage. Connectez au port de console afin de visualiser la séquence de démarrage.

### Ports VTY

Si vous êtes connecté par l'intermédiaire d'un port auxiliaire ou par l'intermédiaire du telnet, introduisez la commande de **terminal monitor**. Vérifiez également que la commande **no logging on** n'a pas été utilisée.

### Messages de journalisation à un tampon interne

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

Aux messages du journal à un tampon interne, utilisez la commande de configuration du routeur de journalisation bufférisé. C'est la syntaxe complète de cette commande :

```
logging buffered no logging buffered
```

La commande **logging buffered** copie les messages du journal des copies vers un tampon interne au lieu de les écrire sur la console. La mémoire tampon est de nature circulaire, donc les messages les plus récents écrasent les messages plus anciens. Pour afficher les messages qui sont consignés dans la mémoire tampon, utilisez la commande privilégiée EXEC **show logging**. Le premier message affiché est le message le plus ancien dans la mémoire tampon. Vous pouvez spécifier la taille de la mémoire tampon ainsi que le niveau de gravité des messages à consigner.

**Conseil** : Assurez-vous que suffisamment de mémoire est disponible dans la boîte avant d'introduire la taille du tampon. Employez la commande de **mem de show proc de** Cisco IOS afin de voir la mémoire disponible.

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

## Messages de journalisation vers un serveur Syslog UNIX

Aux messages du journal à l'hôte du serveur syslog, utilisez la commande de configuration du routeur de journalisation. La syntaxe complète de cette commande suit :

```
logging <ip-address> no logging <ip-address>
```

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

La commande **no logging** ne supprime pas le serveur syslog avec l'adresse spécifiée de la liste de Syslog.

Pour plus d'informations sur l'installation d'un serveur syslog, reportez-vous à [Utilisation des commandes de débogage](#).

## [D'autres tâches de prédébugage](#)

1. Installez votre logiciel émulateur de terminal (par exemple, HyperTerminal) de sorte qu'il puisse saisir le résultat du débogage dans un fichier. Par exemple, dans l'HyperTerminal, cliquez sur **Transfer**, puis cliquez sur **Capture Text** et choisissez les options appropriées. Pour plus d'informations, reportez-vous à [Saisir un résultat de texte de l'hyperterminal](#). Pour l'autre logiciel émulateur de terminal, reportez-vous à la documentation du logiciel.

2. Activez les horodatages en millisecondes (msec) à l'aide de la commande **service**

```
timestamps : router(config)#service timestamps debug datetime msec router(config)#service timestamps log datetime msec
```

Ces commandes ajoutent des horodatages aux débogages sous le format MMM JJ HH :

Millimètre : SS, indiquant la date et l'heure selon l'horloge système. Si l'horloge système n'a pas

été réglée, la date et l'heure sont précédées par un astérisque (\*) pour indiquer que la date et l'heure ne sont probablement pas correctes.

Il est généralement recommandé de configurer des horodatages en millisecondes dans la mesure où cela confère un haut niveau de clarté aux résultats du débogage. Les horodatages en millisecondes fournissent une meilleure indication de la temporisation des divers événements de débogages les uns envers les autres. Cependant, notez que, quand le port de console émet beaucoup de messages, ceux-ci pourraient ne pas correspondre à la véritable temporisation de l'événement. Par exemple, si vous activez le **debug x25** tout sur une case qui a 200 VCs, et la sortie est enregistré à la mémoire tampon (utilisant le **no logging console** et les commandes de **logging buffered**), l'horodateur affiché dans la sortie de débogage (dans la mémoire tampon) ne pourrait pas être l'heure exacte où le paquet traverse l'interface. Par conséquent, n'utilisez pas les horodatages en millisecondes pour justifier des problèmes de performances, mais pour obtenir une information relative sur le moment où les événements se produisent.

## Pour cesser de déboguer

Pour arrêter un débogage, utilisez la commande **no debug all** ou **undebug all**. Vérifiez que les débogages ont été désactivés à l'aide de la commande **showdebug** .

Souvenez-vous que les commandes **no logging console** et **terminal no monitor** empêchent seulement le résultat d'être émis sur la console ainsi que les ports aux ou vty, respectivement. Elle n'arrête pas le débogage et utilise donc des ressources du routeur.

## Utilisation de la commande debug ip packet

La commande **debug ip packet** produit les informations sur les paquets qui ne sont pas rapides commutés par le routeur. Cependant, puisqu'il génère un résultat pour chaque paquet, le résultat peut être étendu et causer ainsi la suspension du routeur. Pour cette raison, utilisez seulement **debug ip packet** sous les contrôles les plus stricts, comme décrit dans cette section.

La meilleure façon de limiter le résultat de **debug ip packet** est de créer une liste d'accès liée au débogage. Seulement les paquets qui correspondent aux critères de la liste d'accès seront sujets à **debug ip packet**. Cette liste d'accès n'a pas besoin d'être appliquée sur aucune interface, mais est plutôt appliquée à l'opération de débogage.

Avant d'utiliser **debugging ip packet**, notez que le routeur fait une commutation rapide par défaut ou peut faire une commutation CEF s'il est configuré de la sorte. Ceci signifie que, une fois que ces techniques sont en place, le paquet n'est pas fourni au processeur, par conséquent, le débogage ne montre rien. Pour que ceci fonctionne, vous devez désactiver la commutation rapide sur le routeur avec **no ip route-cache** (pour des paquets monodestinataires) ou **no ip mroute-cache** (pour des paquets de multidiffusion). Ceci devrait être appliqué sur les interfaces où le trafic est censé s'écouler. Vérifiez ceci avec la commande **show ip route**.

### Avertissements :

- Désactiver la commutation rapide sur un routeur qui prend en charge un grand nombre de paquets peut causer un pic d'utilisation du CPU de sorte que le boîtier se suspende ou perde sa connexion avec ses pairs.
- Ne désactivez pas la commutation rapide sur un routeur exécutant une commutation

multiprotocole par étiquette (MPLS). MPLS est utilisé en conjonction avec CEF. Par conséquent, désactiver la commutation rapide sur l'interface peut avoir un effet désastreux. Considérons un exemple de scénario :

La liste d'accès configurée sur router\_122 est :

```
access-list 105 permit icmp host 10.10.10.2 host 13.1.1.1 access-list 105 permit icmp host 13.1.1.1 host 10.10.10.2
```

Cette liste d'accès permet à n'importe quel paquet d'Internet Control Message Protocol (ICMP) de l'hôte router\_121 (avec l'adresse IP 10.10.10.2) pour héberger router\_123 (avec l'adresse IP 13.1.1.1) aussi bien que dans l'autre direction. Il est important que vous permettiez les paquets dans les deux directions, faute de quoi le routeur peut abandonner le paquet ICMP de renvoi.

Enlevez la commutation rapide sur seulement une interface sur router\_122. Ceci signifie que vous pouvez seulement voir ce qui se passe pour les paquets qui sont destinés à cette interface, comme vu de la perspective de l'IOS interceptant le paquet. Du point de vue de tels paquets apparaissent avec le « d= ». Puisque vous n'avez pas encore arrêté la commutation rapide sur l'autre interface, le paquet de retour n'est pas sujet au **debug ip packet**. Cette sortie affiche comment vous pouvez désactiver la commutation rapide :

```
router_122(config)#interface virtual-template 1 router_122(config-if)#no ip route-cache
router_122(config-if)#end
```

Vous devez maintenant lancer le **debug ip packet** avec la liste d'accès définie plus tôt (liste d'accès 105).

```
router_122#debug ip packet detail 105 IP packet debugging is on (detailed) for access list 105
router_122# 00:10:01: IP: s=13.1.1.1 (Serial3/0), d=10.10.10.2 (Virtual-Access1), g=10.10.10.2,
len 100, forward 00:10:01: ICMP type=0, code=0 ! -- ICMP packet from 13.1.1.1 to 10.10.10.2. ! -
- This packet is displayed because it matches the ! -- source and destination requirements in
access list 105 00:10:01: IP: s=13.1.1.1 (Serial3/0), d=10.10.10.2 (Virtual-Access1),
g=10.10.10.2, len 100, forward 00:10:01: ICMP type=0, code=0 00:10:01: IP: s=13.1.1.1
(Serial3/0), d=10.10.10.2 (Virtual-Access1), g=10.10.10.2, len 100, forward 00:10:01: ICMP
type=0, code=0
```

Maintenant, supprimons la commutation rapide sur l'autre interface (sur le router\_122). Ceci signifie que tous les paquets à travers ces deux interfaces ont maintenant commuté de paquets (ce qui est une condition requise pour **debug ip packet**) :

```
router_122(config)#interface serial 3/0 router_122(config-if)#no ip route-cache
router_122(config-if)#end router_122# 00:11:57: IP: s=10.10.10.2 (Virtual-Access1), d=13.1.1.1
(Serial3/0), g=172.16.1.6, len 100, forward 00:11:57: ICMP type=8, code=0 ! -- ICMP packet
(echo) from 10.10.10.2 to 13.1.1.1 00:11:57: IP: s=13.1.1.1 (Serial3/0), d=10.10.10.2 (Virtual-
Access1), g=10.10.10.2, len 100, forward 00:11:57: ICMP type=0, code=0 ! -- ICMP return packet
(echo-reply) from 13.1.1.1 to 10.10.10.2 00:11:57: IP: s=10.10.10.2 (Virtual-Access1),
d=13.1.1.1 (Serial3/0), g=172.16.1.6, len 100, forward 00:11:57: ICMP type=8, code=0 00:11:57:
IP: s=13.1.1.1 (Serial3/0), d=10.10.10.2 (Virtual-Access1), g=10.10.10.2, len 100, forward
00:11:57: ICMP type=0, code=0
```

Notez que le résultat **debug ip packet** ne montre aucun paquet qui ne correspond pas aux critères de la liste d'accès. Pour des informations supplémentaires sur cette procédure, reportez-vous à [Comprendre les commandes ping et traceroute](#).

Pour plus d'informations sur la façon d'établir des listes d'accès, reportez-vous à [Journalisation de la liste d'accès IP standard](#).

## [Débogages conditionnellement déclenchés](#)

Quand la fonction de débogage conditionnellement déclenchée est activée, le routeur génère des messages de débogage pour des paquets entrant ou sortant du routeur sur une interface spécifiée ; le routeur ne génère pas le résultat du débogage pour des paquets entrant ou sortant par une interface différente. Pour les informations concernant les utilisations pour des débogages conditionnels, reportez-vous au [Débogage conditionnellement déclenché](#).

Regardez une implémentation simple de conditionnel met au point. Considérez ce scénario : le routeur affiché ci-dessous (traxbol) a deux interfaces (interface série 0 et interface série 3) les deux encapsulation d'exécution HDLC.

Vous pouvez utiliser la normale **mettez au point la** commande d'**interface série** afin d'observer le Keepalives HDLC reçu sur toutes les interfaces. Vous pouvez observer le Keepalives sur les deux interfaces.

```
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 keepalive on
interface Serial 0 *Mar 8 09:42:34.855: Serial3: HDLC myseq 26, mineseen 26*, yourseen 27, line
up ! -- HDLC keepalive 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
```

L'enable conditionnel met au point pour l'interface série 3. d'interface. Ceci signifie que seuls les débogages pour l'interface de série 3 sont affichés. Utilisez l'*interface\_number* > la commande de <*interface\_type* de debug interface.

```
traxbol#debug interface serial 3 Condition 1 set
```

Employez la commande de **show debug condition** afin de vérifier que le conditionnel met au point est en activité. Notez qu'une condition pour l'interface de la série 3 est active.

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

Notez que maintenant seuls les débogages pour l'interface de la série 3 sont affichés

```
*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
```

Utilisez l'*interface\_number* > la commande de <*interface\_type* d'interface d'undebug afin de retirer le conditionnel met au point. Il est recommandé que vous arrêtez met au point (par exemple, utilisant undebug all) avant que vous retiriez le déclencheur conditionnel. Ceci permet d'éviter un déluge de résultats de débogage quand la condition est supprimée.

```
traxbol#undebug interface serial 3 This condition is the last interface condition set. Removing
all conditions may 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 maintenant observer que pour lequel mettez au point l'interface série 0 d'interface aussi bien que l'interface série 3 sont affichées.

```
*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 :** Quelques opérations de débogage sont conditionnelles en elles-mêmes. Un exemple réside en le débogage atm. Avec le débogage ATM, vous devriez explicitement spécifier l'interface pour laquelle des débogages devraient être activés plutôt qu'activer des débogages sur toutes les interfaces atm et spécifiant une condition.

Cette section affiche la manière correcte de limiter le paquet ATM met au point à une sous-interface :

```
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 10:16:51.895: 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 **atm debugging** sur toutes les interfaces (avec une condition appliquée), le routeur peut se suspendre s'il a un grand nombre de sous-interfaces ATM. Un exemple de la méthode incorrecte pour le débogage atm est montré.

Dans ce cas, vous pouvez voir qu'une condition est appliquée, mais vous voyez également que ceci n'a aucun effet. Vous pouvez encore voir le paquet de l'autre interface. Dans ce scénario de laboratoire vous avez seulement deux interfaces et très peu de trafic. Si le nombre d'interfaces est élevé, alors la sortie de débogage pour toutes les interfaces sont extrêmement élevée et elle peut faire arrêter le routeur.

```

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: 11 *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 *Dec 21
10:22:13.931: 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 *Dec 21
10:22:13.931: 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

```

## [Informations connexes](#)

- [Numérotation et accès de l'assistance technique](#)
- [Support et documentation techniques - Cisco Systems](#)