# Technologie d'accès commuté : Techniques de dépannage

## Contenu



## Introduction

La connexion commutée est simplement l'application du réseau téléphonique public commuté (RTPC) qui transporte les données au nom de l'utilisateur final. Il s’agit d’un équipement client (CPE) qui envoie au commutateur téléphonique un numéro de téléphone vers lequel diriger une connexion. Les modèles Cisco3600, AS5200, AS5300 et AS5800 sont tous des exemples de routeurs capables d'exécuter un PRI avec des banques de modems numériques. L’AS2511, en revanche, est un exemple de routeur qui communique avec des modems externes.

## Conditions préalables

### Conditions requises

Les lecteurs de ce document doivent avoir une bonne connaissance de ce qui suit :

Le marché des opérateurs s'est considérablement développé et le marché exige désormais des densités de modems plus élevées. La réponse à ce besoin est un niveau plus élevé d'interopérabilité avec l'équipement de la compagnie de téléphone et le développement du modem numérique. Il s'agit d'un modem capable d'un accès numérique direct au RTPC. En conséquence, des modems CPE plus rapides ont été développés pour tirer parti de la clarté du signal dont jouissent les modems numériques. Le fait que les modems numériques se connectant au RTPC via un PRI ou un BRI puissent transmettre des données à plus de 53 000 en utilisant la norme de communication V.90 atteste du succès de l'idée.

Les premiers serveurs d'accès étaient les Cisco2509 et Cisco2511. L'AS2509 peut prendre en charge 8 connexions entrantes à l'aide de modems externes et l'AS2511 peut prendre en charge 16. L'AS5200 a été introduit avec 2 PRI et pourrait prendre en charge 48 utilisateurs utilisant des modems numériques, et représente un grand bond en avant en matière de technologie. Les densités de modems ont augmenté régulièrement avec l'AS5300 prenant en charge 4, puis 8 PRI. Enfin, l'AS5800 a été introduit pour répondre aux besoins des installations de classe opérateur qui doivent gérer des dizaines de T1 entrants et des centaines de connexions utilisateur.

Quelques technologies obsolètes méritent d'être mentionnées dans une discussion historique sur la technologie de numérotation. 56Kflex est une vieille norme de 56k (pré-V.90) proposée par Rockwell. Cisco prend en charge la version 1.1 de la norme 56Kflex sur ses modems internes, mais recommande de migrer les modems CPE vers V.90 dès que possible. Une autre technologie obsolète est l'AS5100. L'AS5100 était une coentreprise entre Cisco et un fabricant de modems. L'AS5100 a été créé pour augmenter la densité des modems grâce à l'utilisation de cartes quadruples. Il s'agissait d'un groupe d'AS2511 conçus comme des cartes insérées dans un fond de panier partagé par des cartes à quatre modems et une carte T1 double.

### Components Used

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

### Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Dépannage des appels entrants

Le dépannage d'un appel entrant commence en bas et s'accélère. Le raisonnement général tient compte des éléments suivants :

1. Voyons-nous l'appel arriver ? (Une réponse *oui* passe à la question suivante)
2. L'extrémité réceptrice répond-elle à l'appel ?
3. L'appel est-il terminé ?
4. Les données transitent-elles par la liaison ?
5. La session est-elle établie ? (PPP ou terminal)

Pour les connexions par modem, un appel de données ressemble à une session de terminal

entrant jusqu'à la fin où l'appel de données va négocier PPP.

Pour les appels entrants impliquant des modems numériques, assurez-vous d'abord que le RNIS ou le CAS sous-jacent reçoit l'appel. Si vous utilisez un modem externe, les sections RNIS et Groupe CAS peuvent être ignorées.

## Dépannage des appels RNIS entrants

Utilisez la commande **debug isdn q931**. Voici un exemple de sortie d'une connexion réussie :

```
Router# debug isdn q931
RX <- SETUP pd = 8 callref = 0x06
 Bearer Capability i = 0x8890
 Channel ID i = 0x89
 Calling Party Number i = 0x0083, `5551234'
TX -> CONNECT pd = 8 callref = 0x86
RX <- CONNECT_ACK pd = 8 callref = 0x06
```

Le message de configuration indique qu'une connexion est en cours d'établissement par l'extrémité distante. Les numéros de référence d'appel sont conservés en tant que paire. Dans ce cas, le numéro de référence d'appel pour le côté entrant de la connexion est 0x06 et le numéro de référence d'appel du côté sortant de la connexion est 0x86. La fonction de support (souvent appelée casque) indique au routeur le type d'appel entrant. Dans ce cas, la connexion est de type 0x8890. Cette valeur indique « RNIS Speed 64 Kb/s ». Si le casque d'antenne avait été 0x8090A2, il aurait indiqué « Allégement de la voix/voix ».

Si aucun message de configuration n'est entré, vous devez vérifier le numéro correct en l'appelant manuellement, s'il s'agit d'un appel vocal. Vous devez également vérifier l'état de l'interface RNIS (reportez-vous à Utilisation de la commande **show isdn status** pour le dépannage BRI). Si tout cela est vérifié, assurez-vous que l'initiateur de l'appel effectue l'appel correct. Pour ce faire, il suffit de contacter la compagnie de téléphone. L'initiateur de l'appel peut suivre l'appel pour voir où il est envoyé. Si la connexion est longue distance, essayez un autre opérateur longue distance en utilisant un code longue distance 1010.

Si l'appel entrant est un appel de modem asynchrone, assurez-vous que la ligne est provisionnée pour autoriser les appels vocaux.

**Remarque :** l'appel par modem asynchrone BRI est une fonctionnalité des routeurs 3600 exécutant 12.0(3)T ou version ultérieure. Il nécessite une révision matérielle récente du module de réseau d'interface BRI. Les modules WIC ne prennent pas en charge les appels de modem asynchrone.

Si l'appel est arrivé mais n'est pas terminé, recherchez un code de cause (voir le tableau 17-10). Une réussite est indiquée par la connexion.

S'il s'agit d'un appel de modem asynchrone, passez à la section « Dépannage des appels de modem entrant ».

Àce stade, l'appel RNIS est connecté, mais aucune donnée n'a été vue sur la liaison. Utilisez la commande **debug ppp negotiation** pour voir si un trafic PPP est en train de traverser la ligne. Si vous ne voyez pas de trafic, il peut y avoir une non-correspondance de vitesse. Pour déterminer si c'est le cas, utilisez la commande **show running-config en mode d'exécution privilégié** pour afficher la configuration du routeur. Vérifiez les entrées de commande de configuration d'interface **dialer**

**map** dans le routeur local et distant. Ces entrées doivent être similaires aux suivantes :

```
dialer map ip 131.108.2.5 speed 56 name C4000
```

Pour les profils de numérotation, une classe map doit être définie afin de définir la vitesse. Notez que, par défaut, les interfaces RNIS tentent d'utiliser des vitesses de communication de 64 K sur chaque canal.

Pour obtenir des informations détaillées sur la configuration des mappages et des profils de numérotation, reportez-vous au *Guide de configuration des solutions de numérotation Cisco IOS*, au *Guide de référence des commandes des solutions de numérotation* et au *Guide de configuration rapide des solutions de numérotation*.

Si vous recevez des paquets PPP valides, la liaison est active et fonctionne. Vous devez passer à la section Dépannage de PPP pour le moment.

## Dépannage des appels CAS entrants

Pour dépanner le groupe CAS servant la connectivité aux modems, utilisez les commandes **debug modem**, **debug modem csm** et **debug cas**.

**Remarque :** La commande **debug cas** est apparue pour la première fois dans 12.0(7)T pour les AS5200 et AS5300. Les versions antérieures de l'IOS utilisent la commande de configuration de niveau système service interne ainsi que la commande exec **modem-mgmt debug rbs**. Pour déboguer ces informations sur un AS5800, vous devez vous connecter à la carte réseau elle-même.

Tout d'abord, déterminez si le commutateur de la compagnie de téléphone a été décroché pour signaler l'appel entrant. Dans le cas contraire, vérifiez le numéro appelé. Pour ce faire, connectez un téléphone à la ligne téléphonique du côté d'origine et appelez le numéro. Si l'appel arrive correctement, le problème se trouve dans l'équipement d'abonné d'origine. Si l'appel ne s'affiche toujours pas sur le CAS, vérifiez le T1 (chapitre 15).Dans ce cas, utilisez la commande **debug serial interfaces**.

Les éléments suivants indiquent une bonne connexion à l'aide du **modem de débogage CSM** :

```
Router# debug modem csm
CSM_MODEM_ALLOCATE: slot 1 and port 0 is allocated.
MODEM_REPORT(0001): DEV_INCALL at slot 1 and port 0
CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 0
CSM_RING_INDICATION_PROC: RI is on
CSM_RING_INDICATION_PROC: RI is off
CSM_PROC_IC1_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 0
MODEM_REPORT(0001): DEV_CONNECTED at slot 1 and port 0
CSM_PROC_IC2_WAIT_FOR_CARRIER: CSM_EVENT_ISDN_CONNECTED at slot 1, port 0
```

Dans cet exemple, l'appel a été dirigé vers un modem. Si votre appel a été dirigé vers un modem, passez à la section « Dépannage des appels du modem entrant », ci-dessous.

## Dépannage des appels du modem entrant

Utilisez les commandes debug suivantes lors du dépannage des appels entrants de modem :

- **debug modem**
- **debug modem csm** (pour les modems numériques intégrés)

Utilisez les commandes debug suivantes conjointement pour indiquer le nouvel appel entrant :

- **debug isdn q931**
- **debug cas**

En supposant que l'appel atteigne le modem, celui-ci doit prendre l'appel.

## Conseils pour le débogage des modems externes

Pour faciliter le débogage sur un modem externe connecté à une ligne TTY, augmentez le volume du haut-parleur. Cela aide à rendre certains problèmes plus apparents.

Lorsque le modem d'origine appelle, le modem récepteur sonne-t-il ? Si ce n'est pas le cas, vérifiez le numéro et essayez un appel manuel à partir du site distant. Essayez également d'utiliser un téléphone normal sur l'extrémité de réception. Remplacer les câbles et le matériel selon les besoins.

## Interception d'appels du modem asynchrone

Si aucun modem externe ne répond, vérifiez le câblage entre le modem et le serveur d'accès ou le routeur. Vérifiez que le modem est connecté au port TTY ou auxiliaire du routeur avec un câble RJ-45 enroulé et un adaptateur MMOD DB-25. Cisco recommande et prend en charge cette configuration de câble pour les ports RJ-45. Notez que ces connecteurs sont généralement étiquetés : *Modem*.

Le câblage RJ-45 se décline en plusieurs types : droit, roulé et croisé. Vous pouvez déterminer le type de câblage en tenant côte à côte les deux extrémités d'un câble RJ-45. Vous verrez huit bandes colorées, ou épingles, à chaque extrémité.

- Si l´ordre des broches colorées est identique à chaque bout, le câble est direct.
- Si l´ordre des couleurs est inversé à chaque bout, le câble est roulé.
- Le câble est un câble croisé si les couleurs indiquent ce qui suit :

Câble croisé RJ45 à RJ45 :

```
RJ45                    RJ45
         5 ------------------ 2
         2 ------------------ 5
         4 ------------------ 1
         1 ------------------ 4
```

Pour vous assurer que la signalisation est correcte, utilisez la commande **show line** décrite au chapitre 16.

En dehors des problèmes de câblage, un modem externe doit être initialisé pour répondre automatiquement. Vérifiez le modem distant pour voir s'il est configuré sur réponse automatique. Généralement, un voyant AA est allumé lorsque la réponse automatique est définie. Définissez le modem distant sur réponse automatique s'il n'est pas déjà défini. Pour plus d'informations sur la vérification et la modification des paramètres du modem, reportez-vous à la documentation de votre modem. Utilisez une connexion Telnet inverse pour initialiser le modem (reportez-vous au chapitre 16).

## Interception d'appels par modem numérique (intégrée)

Sur un modem externe, il est clair si l'appel reçoit une réponse, mais les modems internes nécessitent un appel manuel vers le numéro de réception. Écoutez la tonalité de réponse (ABT). Si vous n'entendez pas d'ABT, vérifiez la configuration pour les deux éléments suivants :

1. Assurez-vous que la commande **isdn entrant-voice modem** existe sous toutes les interfaces RNIS gérant les connexions de modem entrantes.
2. Sous la configuration de ligne de l'ATS du modem, vérifiez que la commande **modem inout** existe.

Il est également possible que le module de commutation d'appels (CSM) n'ait pas affecté un modem interne pour traiter l'appel entrant. Ce problème peut être dû au fait que les pools de modems ou de ressources sont configurés pour trop peu de connexions entrantes. Cela peut également signifier que le serveur d'accès est peut-être simplement en dehors des modems. Vérifiez la disponibilité des modems et réglez les paramètres du pool de modems ou du gestionnaire de pools de ressources de manière appropriée. Si un modem a été attribué et que la configuration affiche **l'entrée du modem**, collectez des débogages et contactez Cisco pour obtenir de l'aide.

## Formation aux modems

Si le modem récepteur émet un DSR, la formation a réussi. Les échecs de formation peuvent indiquer un problème de circuit ou une incompatibilité de modem.

Pour accéder au bas d'un problème de modem individuel, accédez à l'invite AT au niveau du modem d'origine lorsqu'il est connecté à la ligne d'intérêt POTS. Si vous appelez dans un modem numérique d'un serveur d'accès Cisco, préparez-vous à enregistrer un fichier .wav de la musique de formation ou de la séquence d'apprentissage numérique pour personnes handicapées (DIL). Le DIL est la partition musicale (séquence PCM) que le modem analogique V.90 d'origine indique au modem numérique de réception de lire. La séquence permet au modem analogique de détecter toute déficience numérique dans le circuit ; comme plusieurs conversions D/A, une loi/u, des bits volés ou des pads numériques. Si vous n'entendez pas le DIL, les modems n'ont pas négocié V.90 dans V.8/V.8bis (c'est-à-dire un problème de compatibilité de modem). Si vous entendez le DIL et une formation à nouveau dans V.34, le modem analogique a décidé (sur la base de la lecture DIL) que V.90 était impossible.

La musique a-t-elle du bruit ? Si oui, nettoyez le circuit.

Le client abandonne-t-il rapidement, sans avoir suivi la formation V.34 ? Par exemple, il ne sait peut-être pas quoi faire lorsqu'il entend V.8bis. Dans ce cas, vous devez essayer de désactiver V.8bis (d'où K56Flex) sur le serveur (si acceptable). Vous devez obtenir un nouveau micrologiciel client ou remplacer le modem client. Vous pouvez également insérer cinq virgules à la fin de la chaîne de numérotation. Cela retarde l'écoute du modem appelant et entraînera le dépassement du délai d'attente de la tonalité V.8bis du serveur récepteur sans affecter le modem client. Cinq virgules dans la chaîne de numérotation sont une directive générale et peuvent nécessiter un ajustement pour tenir compte des conditions locales.

## Établissement de la session

Àce stade de la séquence, les modems sont connectés et formés. Il est maintenant temps de savoir si un trafic est correctement détecté.

Si la ligne qui reçoit l'appel est configurée avec **autoselect ppp** et que l'interface asynchrone est configurée avec le **mode asynchrone interactif**, utilisez la commande **debug modem** pour vérifier le processus de sélection automatique. Lorsque le trafic arrive sur la liaison asynchrone, le serveur d'accès examine le trafic pour déterminer s'il est basé sur des caractères ou sur des paquets. En fonction de la détermination, le serveur d'accès démarre ensuite une session PPP ou va au-delà d'une session exec sur la ligne.

Séquence d'autosélection normale avec paquets LCP PPP entrants :

```
*Mar  1 21:34:56.958: TTY1: DSR came up
*Mar  1 21:34:56.962: tty1: Modem: IDLE->READY
*Mar  1 21:34:56.970: TTY1: EXEC creation
*Mar  1 21:34:56.978: TTY1: set timer type 10, 30 seconds
*Mar  1 21:34:59.722: TTY1: Autoselect(2) sample 7E
 !--- The inbound traffic is displayed in hexadecimal format. This is based on the !--- bits
coming in over the line, regardless of whether the bits are ASCII !--- characters or elements of
a packet. The bits represented in this example are !--- correct for a LCP packet. Anything
different would be either a malformed packet !--- or character traffic. *Mar 1 21:34:59.726:
TTY1: Autoselect(2) sample 7EFF *Mar 1 21:34:59.730: TTY1: Autoselect(2) sample 7EFF7D *Mar 1
21:34:59.730: TTY1: Autoselect(2) sample 7EFF7D23 *Mar 1 21:34:59.734: TTY1 Autoselect cmd: ppp
negotiate !--- Having determined that the inbound traffic is actually an LCP packet, the access
!--- server triggers the PPP negotiation process. *Mar 1 21:34:59.746: TTY1: EXEC creation *Mar
1 21:34:59.746: TTY1: create timer type 1, 600 seconds *Mar 1 21:34:59.794: TTY1: destroy timer
type 1 (OK) *Mar 1 21:34:59.794: TTY1: destroy timer type 0 *Mar 1 21:35:01.798: %LINK-3-UPDOWN:
Interface Async1, changed state to up !--- The async interface changes state to up, and the PPP
negotiation (not shown) !--- commences.
```

Si l'appel est une session PPP et si le **mode asynchrone dédié** est configuré sur l'interface asynchrone, utilisez la commande **debug ppp negotiation** pour voir si des paquets de demande de configuration proviennent de l'extrémité distante. Les débogages affichent ces valeurs sous la forme CONFREQ. Si vous observez des paquets PPP entrants et sortants, passez à la section Dépannage de PPP. Sinon, connectez-vous à partir de l'extrémité d'origine de l'appel avec une session en mode caractère (ou « exec ») (c'est-à-dire une session non PPP).

**Remarque :** si l'extrémité réceptrice affiche **un modem asynchrone dédié** sous l'interface asynchrone, un numéro d'appel exec affiche uniquement ce qui semble être des déchets ASCII aléatoires. Pour autoriser une session de terminal et disposer toujours de la fonctionnalité PPP, utilisez la commande de configuration d'interface asynchrone **interactive mode asynchrone**. Sous la configuration de la ligne associée, utilisez la commande **autoselect ppp**.

## Le modem ne peut pas envoyer ou recevoir de données

Si les modems se connectent à une session de terminal et qu'aucune donnée n'apparaît, vérifiez les causes possibles suivantes et les actions suggérées :

- **Le paramètre de vitesse du modem n'est pas verrouillé**Utilisez la commande **show line** exec sur le serveur d'accès ou le routeur. Le résultat du port auxiliaire doit indiquer les vitesses Tx et Rx actuellement configurées.Pour une explication du résultat de la commande **show line**, reportez-vous à la section « Utilisation des commandes de débogage » du chapitre 15.Si la ligne n'est pas configurée à la vitesse correcte, utilisez la commande **speed** line configuration pour définir la vitesse de ligne sur le serveur d'accès ou la ligne du routeur. Définissez la valeur sur la vitesse la plus élevée en commun entre le modem et le port du serveur d'accès ou du routeur. Pour définir le débit en bauds du terminal, utilisez la commande de configuration de ligne de **vitesse**. Cette commande définit les vitesses de transmission (vers le

terminal) et de réception (depuis le terminal).Syntaxe:**vitesse** *bits/s*Description de la syntaxe:*bps* : débit en bauds par seconde (bps). La valeur par défaut est 9 600 bits/s.L'exemple suivant définit les lignes 1 et 2 sur un serveur d'accès Cisco 2509 sur 115 200 bits/s :

```
line 1 2
speed 115200
```

**Remarque :** si, pour une raison quelconque, vous ne pouvez pas utiliser le contrôle de flux, limitez la vitesse de ligne à 9 600 bits/s. Des vitesses plus rapides risquent de provoquer des pertes de données.Utilisez à nouveau la commande **show line** exec et confirmez que la vitesse de la ligne est définie sur la valeur souhaitée.Lorsque vous êtes certain que le serveur d'accès ou la ligne du routeur est configuré pour la vitesse souhaitée, lancez une session Telnet inverse vers le modem via cette ligne. Pour plus d'informations, reportez-vous à la section « Établissement d'une session Telnet inverse à un modem » du chapitre 16.Utilisez une chaîne de commande modem qui inclut la commande « lock DTE speed » pour votre modem. Reportez-vous à la documentation de votre modem pour connaître la syntaxe exacte des commandes de configuration.**Remarque :** La commande lock DTE speed, également appelée *port rate adjust* ou *buffered mode*, est souvent liée à la manière dont le modem gère la correction des erreurs. Cette commande varie considérablement d'un modem à l'autre.Le verrouillage de la vitesse du modem garantit que le modem communique toujours avec le serveur d'accès ou le routeur Cisco à la vitesse configurée sur le port auxiliaire Cisco. Si cette commande n'est pas utilisée, le modem revient à la vitesse de la liaison de données (la ligne téléphonique), au lieu de communiquer à la vitesse configurée sur le serveur d'accès.

- **Contrôle de flux matériel non configuré sur un modem ou un routeur local ou distant**Utilisez la commande d'exécution **show line** ***aux-line-number*** et recherchez les éléments suivants dans le champ Capacités :

  ```
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
  ```

  Pour plus d'informations, reportez-vous à Interprétation de la sortie de la ligne dans le chapitre 16.S'il n'est pas fait mention du contrôle de flux matériel dans ce champ, le contrôle de flux matériel n'est pas activé sur la ligne. Il est recommandé de contrôler le flux matériel pour les connexions serveur-modem d'accès.Pour une explication du résultat de la commande **show line**, reportez-vous à la section « Utilisation des commandes de débogage » du chapitre 15.Configurez le contrôle de flux matériel sur la ligne à l'aide de la commande de configuration de ligne de matériel de contrôle de flux.Pour définir la méthode de contrôle de flux de données entre le terminal ou un autre périphérique série et le routeur, utilisez la commande de configuration de ligne **flow** control. Utilisez la forme no de cette commande pour désactiver le contrôle de flux.Syntaxe:**contrôle de flux {aucun | logiciel [verrouiller] [dans | sortant] | matériel [dans | sortant]}**Description de la syntaxe:**none** - Désactive le contrôle de flux.**software** - Définit le contrôle de flux du logiciel. Un mot clé facultatif spécifie la direction : **in** entraîne le logiciel Cisco IOS à écouter le contrôle de flux à partir du périphérique connecté, et **out** fait que le logiciel envoie les informations de contrôle de flux au périphérique connecté. Si vous ne spécifiez pas de direction, les deux sont supposés.**lock** : empêche de désactiver le contrôle de flux à partir de l'hôte distant lorsque le périphérique connecté a besoin d'un contrôle de flux logiciel. Cette option s'applique aux connexions utilisant Telnet ou les protocoles de connexion.**hardware** - Définit le contrôle de flux matériel. Un mot clé facultatif spécifie la direction : **in** entraîne l'écoute du contrôle de flux par le logiciel du périphérique connecté et **out** l'envoi des informations de contrôle de flux au périphérique connecté. Si vous ne spécifiez pas de direction, les deux sont supposés. Pour plus d'informations sur le contrôle de flux matériel, reportez-vous au manuel matériel fourni avec votre routeur.Exemple

:L'exemple suivant définit le contrôle de flux matériel sur la ligne 7 :

```
line 7
flowcontrol hardware
```

**Remarque :** si, pour une raison quelconque, vous ne pouvez pas utiliser le contrôle de flux, limitez la vitesse de la ligne à 9 600 bits/s. Des vitesses plus rapides risquent de provoquer des pertes de données.Après avoir activé le contrôle de flux matériel sur le serveur d'accès ou la ligne du routeur, lancez une session Telnet inverse vers le modem via cette ligne. Pour plus d'informations, reportez-vous à la section « Établissement d'une session Telnet inverse à un modem » du chapitre 16.Utilisez une chaîne de commande modem qui inclut la commande **RTS/CTS Flow** pour votre modem. Cette commande garantit que le modem utilise la même méthode de contrôle de flux (c'est-à-dire le contrôle de flux matériel) que le serveur d'accès ou le routeur Cisco. Reportez-vous à la documentation de votre modem pour connaître la syntaxe exacte des commandes de configuration.

- **Commandes de mappage de numérotation mal configurées**Utilisez la commande **show running-config en** mode d'exécution **privilégié** pour afficher la configuration du routeur. Vérifiez les entrées de commande **dialer map** pour voir si le mot clé **broadcast** est spécifié.Si le mot clé est manquant, ajoutez-le à la configuration.Syntaxe:**dialer map *protocol next-hop-address* [name *hostname*] [broadcast] [*dial-string*]**Description de la syntaxe:*protocol* - Protocole sujet au mappage. Les options incluent IP, IPX, bridge et snapshot.*next-hop-address* : adresse de protocole de l'interface asynchrone du site opposé.**name *hostname*** - Paramètre requis utilisé dans l'authentification PPP. Il s'agit du nom du site distant pour lequel la carte de numérotation est créée. Le nom est sensible à la casse et doit correspondre au nom d'hôte du routeur distant.**broadcast** : mot-clé facultatif qui diffuse les paquets (par exemple, les mises à jour RIP ou RIP/SAP IPX) qui sont transférés à la destination distante. Dans les exemples de configuration de routage statique, les mises à jour de routage ne sont pas souhaitées et le mot clé **broadcast** est omis.*dial-string* : numéro de téléphone du site distant. Tous les codes d'accès (par exemple, 9 pour sortir d'un bureau, codes de numérotation internationaux, indicatifs régionaux) doivent être inclus.Assurez-vous que les commandes **dialer map** spécifient les adresses de tronçon suivant correctes.Si l'adresse de tronçon suivant est incorrecte, modifiez-la à l'aide de la commande **dialer map**.Assurez-vous que toutes les autres options des commandes dialer map sont correctement spécifiées pour le protocole que vous utilisez.Pour obtenir des informations détaillées sur la configuration des mappages de numérotation, reportez-vous au *Guide de configuration de la mise en réseau WAN de Cisco IOS* et au *Guide de référence des commandes de mise en réseau WAN*.
- **Problème avec le modem de numérotation**Assurez-vous que le modem de numérotation est opérationnel et qu'il est correctement connecté au port approprié. Déterminez si un autre modem fonctionne lorsqu'il est connecté au même port.

Le débogage d'une session d'exécution entrante se divise généralement en plusieurs catégories principales :

- Le client de numérotation ne reçoit aucune invite d'exécution
- La session commutée voit « Ordures »
- La session commutée s'ouvre dans une session existante
- Le Modem De Réception De Numérotation Ne Se Déconnecte Pas Correctement

## Le client de numérotation ne reçoit aucune invite d'exécution

- **La sélection automatique est activée sur la ligne**Essayez d'accéder au mode d'exécution en

appuyant sur Entrée.

- **La ligne est configurée avec la commande no exec**Utilisez la commande **show line** exec pour afficher l'état de la ligne appropriée.Cochez le champ Capacités pour voir s'il indique « exec suppressed ». Si c'est le cas, la commande de configuration de ligne **no exec** est activée.Configurez la commande de configuration de ligne **exec** sur la ligne pour autoriser l'ouverture de sessions exec. Cette commande n'a aucun argument ou mot clé.L'exemple suivant active l'exec à la ligne 7 :
```
line 7
exec
```
- **Le contrôle de flux n'est pas activé.ouLe contrôle de flux est activé uniquement sur un périphérique (ETTD ou ETCD).ouLe contrôle de flux est mal configuré.**Utilisez la commande d'exécution **show line** ***aux-line-number*** et recherchez les éléments suivants dans le champ Capacités :
```
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
```

  Pour plus d'informations, reportez-vous à Interprétation de la sortie de la ligne dans le chapitre 16.S'il n'est pas fait mention du contrôle de flux matériel dans ce champ, le contrôle de flux matériel n'est pas activé sur la ligne. Il est recommandé de contrôler le flux matériel pour les connexions serveur-modem d'accès.Pour obtenir une explication du résultat de la commande show line, reportez-vous à la section « Utilisation des commandes de débogage » du chapitre 15.Configurez le contrôle de flux matériel sur la ligne à l'aide de la commande de configuration de ligne **de contrôle de flux matériel**. L'exemple suivant définit le contrôle de flux matériel sur la ligne 7 :
```
line 7
flowcontrol hardware
```
  **Remarque :** si, pour une raison quelconque, vous ne pouvez pas utiliser le contrôle de flux, limitez la vitesse de la ligne à 9 600 bits/s. Des vitesses plus rapides risquent de provoquer des pertes de données.Après avoir activé le contrôle de flux matériel sur le serveur d'accès ou la ligne du routeur, lancez une session Telnet inverse vers le modem via cette ligne. Pour plus d'informations, reportez-vous à la section « Établissement d'une session Telnet inverse à un modem » du chapitre 16.Utilisez une chaîne de commande modem qui inclut la commande RTS/CTS Flow pour votre modem. Cette commande garantit que le modem utilise la même méthode de contrôle de flux (c'est-à-dire le contrôle de flux matériel) que le serveur d'accès ou le routeur Cisco. Reportez-vous à la documentation de votre modem pour connaître la syntaxe exacte des commandes de configuration.
- **Le paramètre de vitesse du modem n'est pas verrouillé**Utilisez la commande **show line** exec sur le serveur d'accès ou le routeur. Le résultat du port auxiliaire doit indiquer les vitesses Tx et Rx actuellement configurées.Pour une explication du résultat de la commande show line, reportez-vous à la section « Utilisation des commandes de débogage » du chapitre 15.Si la ligne n'est pas configurée à la vitesse correcte, utilisez la commande speed line configuration pour définir la vitesse de ligne sur la ligne du serveur d'accès ou du routeur. Définissez la valeur sur la vitesse la plus élevée en commun entre le modem et le port du serveur d'accès ou du routeur. Pour définir le débit en bauds du terminal, utilisez la commande speed line configuration. Cette commande définit les vitesses de transmission (vers le terminal) et de réception (depuis le terminal).Syntaxe:**vitesse** *bits/s*Description de la syntaxe:*bps* : débit en bauds par seconde (bps). La valeur par défaut est 9 600 bits/s.Exemple :L'exemple suivant définit les lignes 1 et 2 sur un serveur d'accès Cisco 2509 sur 115 200 bits/s :
```
line 1 2
speed 115200
```

**Remarque :** si, pour une raison quelconque, vous ne pouvez pas utiliser le contrôle de flux, limitez la vitesse de la ligne à 9 600 bits/s. Des vitesses plus rapides risquent de provoquer des pertes de données.Utilisez à nouveau la commande **show line** exec et confirmez que la vitesse de la ligne est définie sur la valeur souhaitée.Lorsque vous êtes certain que le serveur d'accès ou la ligne du routeur est configuré pour la vitesse souhaitée, lancez une session Telnet inverse vers le modem via cette ligne. Pour plus d'informations, reportez-vous à la section « Établissement d'une session Telnet inverse à un modem » du chapitre 16.Utilisez une chaîne de commande modem qui inclut la commande **lock** DTE speed pour votre modem. Reportez-vous à la documentation de votre modem pour connaître la syntaxe exacte des commandes de configuration.**Remarque :** La commande **lock** DTE speed, qui peut également être appelée mode d'ajustement du débit du port ou mode tampon, est souvent liée à la manière dont le modem gère la correction des erreurs. Cette commande varie considérablement d'un modem à l'autre.Le verrouillage de la vitesse du modem garantit que le modem communique toujours avec le serveur d'accès ou le routeur Cisco à la vitesse configurée sur le port auxiliaire Cisco. Si cette commande n'est pas utilisée, le modem revient à la vitesse de la liaison de données (la ligne téléphonique) au lieu de communiquer à la vitesse configurée sur le serveur d'accès.

## Les sessions commutées voient « ordures »

- **Le paramètre de vitesse du modem n'est pas verrouillé**Utilisez la commande **show line** exec sur le serveur d'accès ou le routeur. Le résultat du port auxiliaire doit indiquer les vitesses Tx et Rx actuellement configurées.Pour une explication du résultat de la commande **show line**, reportez-vous à la section « Utilisation des commandes de débogage » du chapitre 15.Si la ligne n'est pas configurée à la vitesse correcte, utilisez la commande **speed** line configuration pour définir la vitesse de ligne sur le serveur d'accès ou la ligne du routeur. Définissez la valeur sur la vitesse la plus élevée en commun entre le modem et le port du serveur d'accès ou du routeur.Pour définir le débit en bauds du terminal, utilisez la commande de configuration de ligne de **vitesse**. Cette commande définit les vitesses de transmission (vers le terminal) et de réception (depuis le terminal).Syntaxe:**vitesse** ***en bits/s***Description de la syntaxe:débit en bits/s en bits par seconde (bits/s). La valeur par défaut est 9 600 bits/s.Exemple :L'exemple suivant définit les lignes 1 et 2 sur un serveur d'accès Cisco 2509 sur 115 200 bits/s :ligne 1 2vitesse 115200**Remarque :** si, pour une raison quelconque, vous ne pouvez pas utiliser le contrôle de flux, limitez la vitesse de la ligne à 9 600 bits/s. Des vitesses plus rapides risquent de provoquer des pertes de données.Utilisez à nouveau la commande **show line** exec et confirmez que la vitesse de la ligne est définie sur la valeur souhaitée.Lorsque vous êtes certain que le serveur d'accès ou la ligne du routeur est configuré pour la vitesse souhaitée, lancez une session Telnet inverse vers le modem via cette ligne. Pour plus d'informations, reportez-vous à la section « Établissement d'une session Telnet inverse à un modem » du chapitre 16.Utilisez une chaîne de commande modem qui inclut la commande **lock** DTE speed pour votre modem. Reportez-vous à la documentation de votre modem pour connaître la syntaxe exacte des commandes de configuration.**Remarque :** La commande **lock** DTE speed, également appelée *port rate adjust* ou *buffered mode*, est souvent liée à la manière dont le modem gère la correction des erreurs. Cette commande varie considérablement d'un modem à l'autre.Le verrouillage de la vitesse du modem garantit que le modem communique toujours avec le serveur d'accès ou le routeur Cisco à la vitesse configurée sur le port auxiliaire Cisco. Si cette commande n'est pas utilisée, le modem revient

à la vitesse de la liaison de données (la ligne téléphonique) au lieu de communiquer à la vitesse configurée sur le serveur d'accès.

**Symptôme** : La session de numérotation à distance s'ouvre dans une session déjà existante initiée par un autre utilisateur. Autrement dit, au lieu d'obtenir une invite de connexion, un utilisateur de numérotation voit une session établie par un autre utilisateur (qui peut être une invite de commande UNIX, une session d'éditeur de texte, etc.).

## La session commutée s'ouvre dans une session existante

- **Modem configuré pour DCD toujours élevé**Le modem doit être reconfiguré pour que le DCD soit en hauteur uniquement sur le CD. Cela se fait généralement en utilisant la chaîne de commande **&C1** modem, mais vérifiez la syntaxe exacte de votre modem dans la documentation de votre modem.Vous devrez peut-être configurer la ligne du serveur d'accès à laquelle le modem est connecté à l'aide de la commande de configuration de ligne **no exec**. Effacez la ligne à l'aide de la commande **clear line en mode d'exécution privilégié**, lancez une session Telnet inverse avec le modem et reconfigurez le modem de sorte que le DCD soit élevé uniquement sur le CD.Terminez la session Telnet en entrant **disconnect** et reconfigurez la ligne du serveur d'accès à l'aide de la commande de configuration de ligne **exec**.
- **Le contrôle de modem n'est pas activé sur le serveur d'accès ou le routeur**Utilisez la commande **show line** exec sur le serveur d'accès ou le routeur. La sortie du port auxiliaire doit être show **inout** ou **RIisCD** dans la colonne Modem. Cela indique que le contrôle de modem est activé sur la ligne du serveur d'accès ou du routeur.Pour une explication de la sortie **show line**, reportez-vous à la section « Utilisation des commandes de débogage » du chapitre 15.Configurez la ligne pour le contrôle de modem à l'aide de la commande de configuration de ligne **modem inout**. Le contrôle de modem est maintenant activé sur le serveur d'accès.**Remarque :** assurez-vous d'utiliser la commande **modem inout** au lieu de la commande **modem dialin** lorsque la connectivité du modem est en question. Cette dernière commande permet à la ligne d'accepter uniquement les appels entrants. Les appels sortants seront refusés, ce qui rend impossible l'établissement d'une session Telnet avec le modem pour la configurer. Si vous voulez activer la commande **modem dialin**, ne le faites qu'après avoir vérifié que le modem fonctionne correctement.
- **Câblage incorrect**Vérifiez le câblage entre le modem et le serveur d'accès ou le routeur. Vérifiez que le modem est connecté au port auxiliaire du serveur d'accès ou du routeur avec un câble RJ-45 enroulé et un adaptateur MMOD DB-25. Cette configuration de câblage est recommandée et prise en charge par Cisco pour les ports RJ-45. Ces connecteurs sont généralement étiquetés : Modem.Il existe deux types de câblage RJ-45 : droit et roulé. Si vous tenez les deux extrémités d'un câble RJ-45 côte à côte, vous verrez huit bandes colorées, ou broches, à chaque extrémité. Si l'ordre des broches de couleur est le même à chaque extrémité, le câble est droit. Si l'ordre des couleurs est inversé à chaque extrémité, le câble est enroulé.Le câble enroulé (CAB-500RJ) est conforme à la norme Cisco 2500/CS500.Utilisez la commande **show line** exec pour vérifier que le câblage est correct. Reportez-vous à l'explication de la sortie de la commande **show line** dans la section « Utilisation des commandes de débogage » de ce chapitre 15.

## Le Modem De Réception De Numérotation Ne Se Déconnecte Pas Correctement

- **Le modem ne détecte pas DTR**Entrez la commande **Hangup DTR modem**. Cette commande

indique au modem d'abandonner le porteur lorsque le signal DTR n'est plus reçu.Sur un modem compatible Hayes, la chaîne **&D3** est couramment utilisée pour configurer **Hangup DTR** sur le modem. Pour connaître la syntaxe exacte de cette commande, reportez-vous à la documentation de votre modem.

- **Le contrôle de modem n'est pas activé sur le routeur ou le serveur d'accès**Utilisez la commande **show line** exec sur le serveur d'accès ou le routeur. Le résultat pour le port auxiliaire doit afficher **inout** ou **RlisCD** dans la colonne Modem. Cela indique que le contrôle de modem est activé sur la ligne du serveur d'accès ou du routeur.Pour obtenir une explication de la sortie de la ligne show, reportez-vous à la section « Utilisation des commandes de débogage » du chapitre 15.Configurez la ligne pour le contrôle du modem à l'aide de la commande de configuration de ligne d'entrée de modem. Le contrôle de modem est maintenant activé sur le serveur d'accès.**Remarque :** assurez-vous d'utiliser la commande **modem inout** au lieu de la commande **modem dialin** lorsque la connectivité du modem est en question. Cette dernière commande permet à la ligne d'accepter uniquement les appels entrants. Les appels sortants seront refusés, ce qui rend impossible l'établissement d'une session Telnet avec le modem pour la configurer. Si vous voulez activer la commande **modem dialin**, ne le faites qu'après avoir vérifié que le modem fonctionne correctement.

# Dépannage des appels sortants

Alors que l'approche de dépannage des appels entrants commence en bas, le dépannage d'une connexion sortante commence en haut. Le raisonnement général tient compte des éléments suivants :

1. Le routage à établissement de connexion à la demande (DDR) lance-t-il un appel ? (Une réponse oui passe à la question suivante)
2. S'il s'agit d'un modem asynchrone, les scripts de discussion émettent-ils les commandes attendues ?
3. L'appel est-il transmis au RTPC ?
4. L'extrémité distante répond-elle à l'appel ?
5. L'appel est-il terminé ?
6. Les données transitent-elles sur la liaison ?
7. La session est-elle établie ? (PPP ou terminal)

## Vérification du fonctionnement du numéroteur

Pour savoir si le numéroteur tente d'appeler sa destination distante, utilisez la commande **debug dialer events**. Des informations plus détaillées peuvent être obtenues à partir du **paquet debug dialer**, mais la commande **debug dialer packet** est gourmande en ressources et ne doit pas être utilisée sur un système occupé qui dispose de plusieurs interfaces de numérotation.

La ligne suivante de la sortie des événements de numérotation de débogage pour un paquet IP répertorie le nom de l'interface DDR et les adresses source et de destination du paquet :

```
Dialing cause: Async1: ip (s=172.16.1.111 d=172.16.2.22)
```

Si le trafic n'initie pas de tentative de numérotation, la raison la plus courante est une configuration incorrecte (soit l'une des définitions de trafic intéressantes, l'état de l'interface de numérotation, soit le routage).

## Le trafic n'initie pas de tentative de numérotation

- **Définitions de « trafic intéressant » manquantes ou incorrectes**À l'aide de la commande **show running-config**, assurez-vous que l'interface est configurée avec un **groupe de numérotation** et qu'il existe une **liste de numérotation** globale configurée avec un numéro correspondant.Assurez-vous que la commande **dialer-list** est configurée pour autoriser un protocole entier ou pour autoriser le trafic correspondant à une liste d'accèsVérifiez que la liste d'accès déclare intéressants les paquets circulant sur la liaison. Un test utile consiste à utiliser la commande d'exécution privilégiée **debug ip packet [list number]** en utilisant le numéro de la liste d'accès pertinente. Essayez ensuite d'envoyer une requête ping ou d'envoyer du trafic via la liaison. Si les filtres de trafic intéressants ont été correctement définis, vous verrez les paquets dans la sortie de débogage. S'il n'y a pas de résultat de débogage de ce test, alors la liste d'accès ne correspond pas aux paquets.
- **État de l'interface**Utilisez la commande **show interfaces [*interface name*]** pour vous assurer que l'interface est à l'état « up/up (spoofing)« .Interface en mode veilleUne autre interface (principale) du routeur a été configurée pour utiliser l'interface de numérotation comme interface de sauvegarde. En outre, l'interface principale n'est pas en état « down/down », ce qui est nécessaire pour sortir l'interface de numérotation du mode veille. En outre, un *délai de sauvegarde* doit être configuré sur l'interface principale, sinon la commande **d'interface de sauvegarde** ne sera jamais appliquée.Pour vérifier que l'interface de numérotation passe de « veille » à « up/up (spoofing)« , il est généralement nécessaire de retirer le câble de l'interface principale. Simplement arrêter l'interface principale avec la commande de configuration **shutdown** ne placera pas l'interface principale dans « down/down », mais la placera dans « administrativement down » - pas la même chose.En outre, si la connexion principale est via Frame Relay, la configuration Frame Relay doit être effectuée sur une sous-interface série point à point et la compagnie de téléphone doit passer le bit « Actif ». Cette pratique est également appelée « LMI de bout en bout ».L'interface est « administrativement désactivée »L'interface de numérotation a été configurée avec la commande **shutdown**. Il s'agit également de l'état par défaut de toute interface lorsqu'un routeur Cisco est amorcé pour la toute première fois. Utilisez la commande de configuration d'interface **no shutdown** pour supprimer cet obstacle.
- **Routage incorrect**Exécutez la commande exec **show ip route [*a.b.c.d*]**, où *a.b.c.d* est l'adresse de l'interface de numérotation du routeur distant. Si **ip unnumbered** est utilisé sur le routeur distant, utilisez l'adresse de l'interface répertoriée dans la commande **ip unnumbered**.Le résultat doit afficher une route vers l'adresse distante via l'interface de numérotation. S'il n'y a aucune route, assurez-vous que des routes statiques ou flottantes ont été configurées en examinant le résultat de la commande show running-config.S'il existe une route via une interface autre que l'interface de numérotation, cela signifie que DDR est utilisé comme sauvegarde. Examinez la configuration du routeur pour vous assurer que des routes statiques ou flottantes ont été configurées. La meilleure façon de tester le routage, dans ce cas, est de désactiver la connexion principale et d'exécuter la commande **show ip route [*a.b.c.d*]** pour vérifier que la route appropriée a été installée dans la table de routage.**Remarque :** si vous tentez de le faire lors d'opérations en direct sur le réseau, un événement de numérotation peut être déclenché. Ce type de test est le mieux effectué lors des cycles de maintenance programmés.

## Passer l'appel

Si le routage et les filtres de trafic intéressants sont corrects, un appel doit être lancé. Ceci peut être vu à l'aide des **événements de numérotation de débogage** :

```
Async1 DDR: Dialing cause ip (s=10.0.0.1, d=10.0.0.2)
Async1 DDR: Attempting to dial 5551212
```

Si la cause de numérotation est visible mais qu'aucune tentative de numérotation n'est effectuée, la raison habituelle est une carte de numérotation ou un profil de numérotation mal configuré.

### Appel non passé

Voici quelques problèmes possibles et des mesures suggérées :

- **Carte de numérotation mal configurée**Utilisez la commande **show running-config** pour vous assurer que l'interface de numérotation est configurée avec au moins une instruction *dialer map* qui pointe vers l'adresse de protocole et le numéro appelé du site distant.
- **Profil de numérotation mal configuré**Utilisez la commande **show running-config** pour vous assurer que l'interface de numérotation est configurée avec une commande **dialer pool X** et qu'une interface de numérotation sur le routeur est configurée avec un *membre de pool de numérotation X* correspondant. Si les profils de numérotation ne sont pas correctement configurés, un message de débogage peut s'afficher comme :
  ```
  Dialer1: Can't place call, no dialer pool set
  ```
  Vérifiez qu'une **chaîne de numérotation** est configurée.

## Appel sortant asynchrone - Vérifier le fonctionnement du script de conversation

Si l'appel sortant est un appel par modem, un script de conversation doit s'exécuter pour que l'appel puisse continuer. Pour le routage à établissement de connexion à la carte de numérotation, le script de conversation est appelé par le paramètre modem-script dans une commande dialer map. Si le DDR est basé sur le profil de numérotation, cela est accompli par la commande **script dialer**, configurée sur la ligne TTY. Les deux utilisations reposent sur un script de conversation existant dans la configuration globale du routeur, par exemple :

```
chat-script callout AT OK atdt\T TIMEOUT 60 CONNECT \c
```

Dans les deux cas, la commande permettant d'afficher l'activité du script de discussion est **debug chat**. Si la chaîne de numérotation (c'est-à-dire le numéro de téléphone) utilisée dans la commande **dialer map** ou **dialer string** était 5551212, la sortie de débogage ressemblerait à ceci :

```
CHAT1: Attempting async line dialer script

CHAT1: Dialing using Modem script: callout & System script: none
CHAT1: process started
CHAT1: Asserting DTR
CHAT1: Chat script callout started
CHAT1: Sending string: AT
CHAT1: Expecting string: OK
CHAT1: Completed match for expect: OK
CHAT1: Sending string: atdt5551212
CHAT1: Expecting string: CONNECT
CHAT1: Completed match for expect: CONNECT
CHAT1: Chat script callout finished, status = Success
```

Les problèmes de script de conversation peuvent être répartis en trois catégories :

- Erreur de configuration
- Défaillance du modem
- Échec de la connexion

### Échec du script de conversation

Cette liste affiche les sorties possibles des discussions de débogage et les actions suggérées :

- **aucun script de conversation correspondant trouvé pour [nombre]**Aucun script de conversation n'a été configuré. Ajoutez-en un.
- **Déconnexion du script de conversation terminée, état = Dépassement du délai de connexion ; hôte distant ne répondant pas**Le modem ne répond pas au script de conversation. Vérifiez la communication avec le modem (reportez-vous au tableau 16-2 du chapitre 16).
- **Délai d'attente : CONNECTER***Possibilité 1* : Le modem local ne passe pas l'appel. Vérifiez que le modem peut passer un appel en exécutant une connexion Telnet inverse vers le modem et en lançant manuellement une numérotation.*Possibilité 2* : Le modem distant ne répond pas. Testez-le en composant le modem distant avec un téléphone POTS ordinaire.*Possibilité 3* : Le numéro composé est incorrect. Vérifiez le numéro en le composant manuellement. Corrigez la configuration, si nécessaire.*Possibilité 4* : La formation du modem prend trop de temps ou la valeur TIMEOUT est trop faible. Si le modem local est externe, activez le volume du haut-parleur du modem et écoutez les tonalités de la formation. Si la formation est brusquement interrompue, essayez d'augmenter la valeur TIMEOUT dans la commande **chat-script**. Si le délai d'attente est déjà de 60 secondes ou plus, reportez-vous à la section Modem Trainup.

## Appel sortant RNIS

En cas de première suspicion de défaillance RNIS, que ce soit sur un BRI ou un PRI, vérifiez toujours le résultat de **show isdn status**. Les éléments clés à noter sont que la couche 1 doit être active et que la couche 2 doit être dans un état de *MULTIPLE_FRAME_ESTABLISHED*. Reportez-vous à la section « Interprétation de la sortie de l'état RNIS » du chapitre 16 pour obtenir des informations sur la lecture de cette sortie, ainsi que des mesures correctives.

Pour les appels RNIS sortants, **debug isdn q931** et **debug isdn events** sont les meilleurs outils à utiliser. Heureusement, le débogage des appels sortants est très similaire au débogage des appels entrants. Un appel normalement réussi peut ressembler à ceci :

```
*Mar 20 21:07:45.025: ISDN BR0: Event: Call to 5553759 at 64 Kb/s
*Mar 20 21:07:45.033: ISDN BR0: TX ->  SETUP pd = 8  callref = 0x2C
*Mar 20 21:07:45.037:         Bearer Capability i = 0x8890
*Mar 20 21:07:45.041:         Channel ID i = 0x83
*Mar 20 21:07:45.041:         Keypad Facility i = 0x35353533373539
*Mar 20 21:07:45.141: ISDN BR0: RX <-  CALL_PROC pd = 8  callref = 0xAC
*Mar 20 21:07:45.145:         Channel ID i = 0x89
*Mar 20 21:07:45.157: ISDN BR0: received HOST_PROCEEDING
        Channel ID i = 0x0101
*Mar 20 21:07:45.161:   -------------------
        Channel ID i = 0x89
*Mar 20 21:07:45.313: ISDN BR0: RX <-  CONNECT pd = 8  callref = 0xAC
```

```
*Mar 20 21:07:45.325: ISDN BR0: received HOST_CONNECT
 !--- The CONNECT message is the key indicator of success. If a CONNECT is not received, !---
you may see a DISCONNECT or a RELEASE_COMP (release complete) message followed by !--- a cause
code (see below) *Mar 20 22:11:03.212: ISDN BR0: RX <- RELEASE_COMP pd = 8 callref = 0x8F *Mar
20 22:11:03.216: Cause i = 0x8295 - Call rejected
```

La valeur de la cause indique deux choses.

- Le second octet de la valeur de 4 ou 6 octets indique à partir de quel emplacement dans le chemin d'appel de bout en bout a été reçu DISCONNECT ou RELEASE_COMP. Cela peut vous aider à localiser le problème.
- Les troisième et quatrième octets indiquent la raison réelle de l'échec. Reportez-vous aux tableaux qui suivent pour connaître la signification des différentes valeurs.

**Remarque :** L'impression suivante indique généralement une défaillance de protocole supérieur :

```
Cause i = 0x8090 - Normal call clearing
```

L'échec de l'authentification PPP est une raison typique. Activez **debug ppp negotiation** et **debug ppp authentication** avant de supposer que l'échec de connexion est nécessairement un problème RNIS

## Champs du code de cause

Le tableau 17-9 répertorie les champs de code de cause RNIS qui s'affichent au format suivant dans les commandes de débogage :

```
i=0x y1 y2 z1 z2 [a1 a2]
```

### Champs du code de cause RNIS

| Champ | Description de la valeur |
|---|---|
| 0x | Les valeurs suivantes sont au format hexadécimal. |
| *y1* | 8 : codage standard ITU-T. |
| *y2* | 0—Utilisateur 1—Réseau privé desservant l'utilisateur local 2—Réseau public desservant l'utilisateur local 3—Réseau de transit 4—Réseau public desservant l'utilisateur distant 5—Réseau privé desservant l'utilisateur distant 7—Réseau international A—Réseau au-delà du point d'interconnexion |
| *z1* | Classe (le nombre hexadécimal le plus significatif) de la valeur de cause. Reportez-vous au tableau suivant pour obtenir des informations détaillées sur les valeurs possibles. |
| *z2* | Valeur (nombre hexadécimal moins significatif) de la valeur de cause. Reportez-vous au tableau suivant pour obtenir des informations détaillées sur les valeurs possibles. |
| *a1* | (Facultatif) Champ de diagnostic qui est toujours 8. |

| | |
|---|---|
| *a2* | (Facultatif) Champ de diagnostic qui est l'une des valeurs suivantes : 0—Inconnu 1—Permanent 2—Transitionnel |

## Valeurs de cause RNIS

Le tableau suivant répertorie les descriptions de certaines des valeurs de cause les plus courantes de l'élément d'information de cause - les troisième et quatrième octets du code de cause. Pour plus d'informations sur les codes et les valeurs RNIS, référez-vous à Comprendre le débogage et les codes de cause de déconnexion q931.

| Valeur hexadécimale | Motif | Explication |
|---|---|---|
| 81 | Numéro non alloué (non affecté) | Le numéro RNIS a été envoyé au commutateur dans le format correct ; toutefois, le numéro n'est attribué à aucun équipement de destination. |
| 90 | Effacement d'appel normal | Un effacement d'appel normal s'est produit. |
| 91 | Utilisateur occupé | Le système appelé accuse réception de la demande de connexion mais ne peut pas accepter l'appel car tous les canaux B sont utilisés. |
| 92 | Aucun utilisateur ne répond | Impossible d'établir la connexion, car la destination ne répond pas à l'appel. |
| 93 | Aucune réponse de l'utilisateur (alerte de l'utilisateur) | La destination réagit à la requête de connexion mais ne complète pas la connexion dans le temps prescrit. Le problème est à l'extrémité distante de la connexion. |
| 95 | Appel rejeté | La destination peut accepter l'appel mais l'a rejeté pour une raison inconnue. |
| 9C | Format de numéro incorrect | La connexion n'a pas pu être établie car l'adresse de destination était présentée dans un format non reconnaissable ou parce que l'adresse de destination était incomplète. |
| 9F | Normal, | Signale l'occurrence d'un événement |

| | | |
|---|---|---|
| | non spécifié | normal lorsqu'aucune cause standard ne s'applique. Aucune action requise. |
| A2 | Aucun circuit/canal disponible | Impossible d'établir la connexion, car aucun canal approprié n'est disponible pour prendre l'appel. |
| A6 | Réseau en panne | La destination ne peut pas être atteinte car le réseau ne fonctionne pas correctement et la condition peut durer longtemps. Une tentative de reconnexion immédiate échouera probablement. |
| CA | Circuit/canal demandé non disponible | L'équipement distant ne peut pas fournir le canal demandé pour une raison inconnue. Il peut s'agir d'un problème temporaire. |
| B2 | Installation demandée non abonnée | L'équipement distant prend en charge le service supplémentaire demandé par abonnement uniquement. Il s'agit souvent d'une référence au service longue distance. |
| B9 | Capacité de support non autorisée | L'utilisateur a demandé une fonctionnalité de support que le réseau fournit, mais il n'est pas autorisé à l'utiliser. Il peut s'agir d'un problème d'abonnement. |
| D8 | Destination incompatible | Indique qu'une tentative de connexion à un équipement non RNIS a été effectuée. Par exemple, sur une ligne analogique. |
| E0 | L'élément d'information obligatoire est manquant | L'équipement récepteur a reçu un message qui ne contenait pas l'un des éléments d'information obligatoires. Ceci est généralement dû à une erreur de canal D. Si cette erreur se produit systématiquement, signalez-la à votre fournisseur de services RNIS. |
| E4 | Contenu d'élément d'information non valide | L'équipement distant a reçu un message qui inclut des informations non valides dans l'élément d'information. Ceci est généralement dû à une erreur de canal D. |

## Appel sortant CAS

Pour les appels sortants via CAS T1 ou E1 et les modems numériques intégrés, une grande partie du dépannage est similaire à d'autres dépannages DDR. Il en va de même pour les appels sortants par modem intégré sur une ligne PRI. Les fonctionnalités uniques impliquées dans un appel de cette manière nécessitent un débogage spécial en cas de défaillance d'un appel.

En ce qui concerne les autres situations DDR, vous devez vous assurer qu'une tentative d'appel est requise. Utilisez **les événements de numérotation de débogage** à cette fin. Reportez-vous à Vérification du fonctionnement du numéroteur.

Avant de pouvoir passer un appel, un modem doit être attribué à l'appel. Pour afficher ce processus et l'appel suivant, utilisez les commandes de débogage suivantes :

- **debug modem**
- **debug modem csm**
- **debug cas**

**Remarque :** La commande **debug cas** est apparue pour la première fois dans IOS version 12.0(7)T pour AS5200 et AS5300. Les versions antérieures d'IOS utilisent une commande de configuration système **service interne** avec la commande exec **modem-mgmt debug rbs** :

### Activation des débogages

```
router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#service internal
router(config)#^Z

router#modem-mgmt csm ?
  debug-rbs     enable rbs debugging
  no-debug-rbs  disable rbs debugging

router#modem-mgmt csm debug-rbs
router#
neat msg at slot 0: debug-rbs is on
neat msg at slot 0: special debug-rbs is on
```

### Désactivation des débogages

```
router#
router#modem-mgmt csm no-debug-rbs
neat msg at slot 0: debug-rbs is off
```

**Remarque :** le débogage de ces informations sur un AS5800 nécessite une connexion à la carte réseau. Voici un exemple d'appel sortant normal sur un serveur CAS T1 provisionné et configuré pour FXS-Ground-Start :

```
Mica Modem(1/0): Rcvd Dial String(5551111) [Modem receives digits from chat script]
CSM_PROC_IDLE: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 0
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_CHANNEL_LOCK at slot 1 and port 0
CSM_PROC_OC4_DIALING: CSM_EVENT_DSX0_BCHAN_ASSIGNED at slot 1, port 0
Mica Modem(1/0): Configure(0x1)
Mica Modem(1/0): Configure(0x2)
```

```
Mica Modem(1/0): Configure(0x5)
Mica Modem(1/0): Call Setup
neat msg at slot 0: (0/2): Tx RING_GROUND
Mica Modem(1/0): State Transition to Call Setup
neat msg at slot 0: (0/2): Rx TIP_GROUND_NORING [Telco switch goes OFFHOOK]
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_START_TX_TONE at slot 1 and port 0
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_DSX0_START_TX_TONE at slot 1, port 0
neat msg at slot 0: (0/2): Tx LOOP_CLOSURE [Now the router goes OFFHOOK]
Mica Modem(1/0): Rcvd Tone detected(2)
Mica Modem(1/0): Generate digits:called_party_num=5551111 len=8
Mica Modem(1/0): Rcvd Digits Generated
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_ADDR_INFO_COLLECTED at slot 1, port 0
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_CHANNEL_CONNECTED at slot 1 and port 0
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_DSX0_CONNECTED at slot 1, port 0
Mica Modem(1/0): Link Initiate
Mica Modem(1/0): State Transition to Connect
Mica Modem(1/0): State Transition to Link
Mica Modem(1/0): State Transition to Trainup
Mica Modem(1/0): State Transition to EC Negotiating
Mica Modem(1/0): State Transition to Steady State
Mica Modem(1/0): State Transition to Steady State Speedshifting
Mica Modem(1/0): State Transition to Steady State
```

Les débogages pour les T1 et E1 avec d'autres types de signalisation sont similaires.

Si vous arrivez à ce point dans le débogage, cela signifie que les modems d'appel et de réponse ont été formés et connectés, et que les protocoles de couche supérieure peuvent commencer à négocier. Si un modem est correctement alloué pour l'appel sortant mais que la connexion ne parvient pas à atteindre ce niveau, il faut examiner le T1. Reportez-vous au chapitre 15 pour obtenir des informations sur le dépannage de T1.

## Dépannage du protocole PPP

Le dépannage de la partie PPP d'une connexion commence lorsque vous savez que la connexion commutée, RNIS ou asynchrone, s'établit correctement.

Il est important de comprendre à quoi ressemble une séquence PPP de débogage réussie avant de dépanner la négociation PPP. De cette manière, la comparaison d'une session de débogage PPP défectueuse avec une séquence de débogage PPP terminée avec succès vous permet de gagner du temps et de l'effort.

Voici un exemple de séquence PPP réussie. Reportez-vous à Détails de négociation LCP PPP pour obtenir une description détaillée des champs de sortie.

```
Montecito#
Mar 13 10:57:13.415: %LINK-3-UPDOWN: Interface Async1, changed state to up
Mar 13 10:57:15.415: As1 LCP: O CONFREQ [ACKrcvd] id 2 len 25
Mar 13 10:57:15.415: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.415: As1 LCP:    AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.415: As1 LCP:    MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.415: As1 LCP:    PFC (0x0702)
Mar 13 10:57:15.415: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:15.543: As1 LCP: I CONFACK [REQsent] id 2 len 25
Mar 13 10:57:15.543: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.543: As1 LCP:    AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.543: As1 LCP:    MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.543: As1 LCP:    PFC (0x0702)
Mar 13 10:57:15.547: As1 LCP:    ACFC (0x0802)
```

```
Mar 13 10:57:16.919: As1 LCP: I CONFREQ [ACKrcvd] id 4 len 23
Mar 13 10:57:16.919: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:16.919: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:16.919: As1 LCP:    PFC (0x0702)
Mar 13 10:57:16.919: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP:    Callback 6  (0x0D0306)
Mar 13 10:57:16.919: As1 LCP: O CONFREJ [ACKrcvd] id 4 len 7
Mar 13 10:57:16.919: As1 LCP:    Callback 6  (0x0D0306)
Mar 13 10:57:17.047: As1 LCP: I CONFREQ [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP:    PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: O CONFACK [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP:    PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: State is Open
Mar 13 10:57:17.047: As1 PPP: Phase is AUTHENTICATING, by this end
Mar 13 10:57:17.047: As1 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
Mar 13 10:57:17.191: As1 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 10:57:17.191: As1 CHAP: O SUCCESS id 1 len 4
Mar 13 10:57:17.191: As1 PPP: Phase is UP
Mar 13 10:57:17.191: As1 IPCP: O CONFREQ [Closed] id 1 len 10
Mar 13 10:57:17.191: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:17.303: As1 IPCP: I CONFREQ [REQsent] id 1 len 40
Mar 13 10:57:17.303: As1 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
Mar 13 10:57:17.303: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:17.303: As1 IPCP: O CONFREJ [REQsent] id 1 len 22
Mar 13 10:57:17.303: As1 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:17.319: As1 CCP: I CONFREQ [Not negotiated] id 1 len 15
Mar 13 10:57:17.319: As1 CCP:    MS-PPC supported bits 0x00000001 (0x120600000001)
Mar 13 10:57:17.319: As1 CCP:    Stacker history 1 check mode EXTENDED (0x1105000104)
Mar 13 10:57:17.319: As1 LCP: O PROTREJ [Open] id 3 len 21 protocol CCP
Mar 13 10:57:17.319: As1 LCP:  (0x80FD0101000F12060000000111050001)
Mar 13 10:57:17.319: As1 LCP:  (0x04)
Mar 13 10:57:17.319: As1 IPCP: I CONFACK [REQsent] id 1 len 10
Mar 13 10:57:17.319: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:18.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
 changed state to up
Mar 13 10:57:19.191: As1 IPCP: TIMEout: State ACKrcvd
Mar 13 10:57:19.191: As1 IPCP: O CONFREQ [ACKrcvd] id 2 len 10
Mar 13 10:57:19.191: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:19.315: As1 IPCP: I CONFACK [REQsent] id 2 len 10
Mar 13 10:57:19.315: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:20.307: As1 IPCP: I CONFREQ [ACKrcvd] id 2 len 34
Mar 13 10:57:20.307: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:20.307: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:20.307: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:20.307: As1 IPCP: O CONFREJ [ACKrcvd] id 2 len 16
Mar 13 10:57:20.307: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:20.419: As1 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
```

```
Mar 13 10:57:20.419: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:20.419: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:20.419: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:20.419: As1 IPCP: O CONFNAK [ACKrcvd] id 3 len 22
Mar 13 10:57:20.419: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.419: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.419: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.543: As1 IPCP: I CONFREQ [ACKrcvd] id 4 len 22
Mar 13 10:57:20.543: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.547: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.547: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.547: As1 IPCP: O CONFACK [ACKrcvd] id 4 len 22
Mar 13 10:57:20.547: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.547: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.547: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.547: As1 IPCP: State is Open
Mar 13 10:57:20.551: As1 IPCP: Install route to 10.1.1.1
```

**Remarque :** Vos débogages peuvent apparaître dans un format différent. Cet exemple montre le nouveau format de sortie de débogage PPP qui a été modifié dans IOS version 11.2(8). Reportez-vous au chapitre 16 pour un exemple de débogage PPP avec les versions plus anciennes d'IOS.

## Détails de la négociation PPP LCP

| Horodatage | Description |
|---|---|
| 10:57:15.415 | Demande de configuration sortante (O CONFREQ). Le NAS envoie un paquet de demande de configuration PPP sortant au client. |
| 10:57:15.543 | Accusé de réception de configuration entrant (I CONFACK). Le client accuse réception de la requête PPP de Montecito. |
| 10:57:16.919 | Demande de configuration entrante (I CONFREQ). Le client souhaite négocier le protocole de rappel. |
| 10:57:16.919 | Rejet de configuration sortante (O CONFREJ). Le NAS rejette l'option de rappel. |
| 10:57:17.047 | Demande de configuration entrante (I CONFREQ). Le client demande un nouvel ensemble d'options. Notez que Microsoft Callback n'est pas demandé cette fois. |
| 10:57:17.047 | Accusé de réception de la configuration sortante (O CONFACK). Le NAS accepte le nouvel ensemble d'options. |
| 10:57:17.047 | La négociation LCP PPP est terminée. L'état LCP est « Open ». Les deux parties ont reconnu (CONFACK) la demande de configuration de l'autre partie (CONFREQ). |
| 10:57:17.047 jusqu'à | L'authentification PPP est terminée. Une fois que le protocole LCP a négocié, l'authentification commence. L'authentification doit avoir lieu avant que les protocoles réseau, tels que IP, ne soient livrés. Les deux parties s'authentifient avec la |

| | |
|---|---|
| 10:57:17.191 | méthode négociée lors du protocole LCP. Montecito authentifie le client à l'aide de CHAP. |
| 10:57:20.551 | L'état est ouvert pour le protocole IPCP (IP Control Protocol). Une route est négociée et installée pour l'homologue IPCP, auquel est attribuée l'adresse IP 1.1.1.1. |

## Protocole de contrôle de liaison

Deux types de problèmes sont généralement rencontrés lors de la négociation LCP.

La première se produit lorsqu'un homologue fait des demandes de configuration que l'autre homologue ne peut pas ou ne veut pas accepter. Bien qu'il s'agisse d'une occurrence fréquente, cela peut poser problème si le demandeur insiste sur le paramètre. Un exemple typique est lors de la négociation d'AUTHTYPE (également appelé « AuthProto »). Par exemple, de nombreux serveurs d'accès sont configurés pour accepter uniquement CHAP pour l'authentification. Si l'appelant est configuré pour effectuer uniquement l'authentification PAP, les CONFREQ et les CONFNAK seront échangés jusqu'à ce qu'un homologue ou l'autre abandonne la connexion.

```
BR0:1 LCP: I CONFREQ [ACKrcvd] id 66 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 66 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
BR0:1 LCP: I CONFREQ [ACKrcvd] id 67 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 67 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
BR0:1 LCP: I CONFREQ [ACKrcvd] id 68 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 68 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
...
...
```

Le deuxième type de problème dans LCP est quand seuls les CONFREQ sortants sont vus sur un ou les deux homologues comme dans l'exemple ci-dessous. Ceci est généralement le résultat de ce qu'on appelle une *incompatibilité de vitesse* au niveau de la couche inférieure. Cette condition peut se produire dans le DDR asynchrone ou RNIS.

```
Jun 10 19:57:59.768: As5 PPP: Phase is ESTABLISHING, Active Open
Jun 10 19:57:59.768: As5 LCP: O CONFREQ [Closed] id 64 len 25
Jun 10 19:57:59.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:57:59.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:57:59.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:57:59.768: As5 LCP: PFC (0x0702)
Jun 10 19:57:59.768: As5 LCP: ACFC (0x0802)
Jun 10 19:58:01.768: As5 LCP: TIMEout: State REQsent
Jun 10 19:58:01.768: As5 LCP: O CONFREQ [REQsent] id 65 len 25
Jun 10 19:58:01.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:58:01.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:58:01.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:58:01.768: As5 LCP: PFC (0x0702)
```

```
Jun 10 19:58:01.768: As5 LCP: ACFC (0x0802).
Jun 10 19:58:03.768: As5 LCP: TIMEout: State REQsent
Jun 10 19:58:03.768: As5 LCP: O CONFREQ [REQsent] id 66 len 25
Jun 10 19:58:03.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:58:03.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:58:03.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:58:03.768: As5 LCP: PFC (0x0702)
Jun 10 19:58:03.768: As5 LCP: ACF.C (0x0802)
Jun 10 19:58:05.768: As5 LCP: TIMEout: State REQsent
Jun 10 19:58:05.768: As5 LCP: O CONFREQ [REQsent] id 67 len 25
!--- This repeats every two seconds until: Jun 10 19:58:19.768: As5 LCP: O CONFREQ [REQsent] id
74 len 25 Jun 10 19:58:19.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000) Jun 10 19:58:19.768:
As5 LCP: AuthProto CHAP (0x0305C22305) Jun 10 19:58:19.768: As5 LCP: MagicNumber 0x5779D9D2
(0x05065779D9D2) Jun 10 19:58:19.768: As5 LCP: PFC (0x0702) Jun 10 19:58:19.768: As5 LCP: ACFC
(0x0802) Jun 10 19:58:21.768: As5 LCP: TIMEout: State REQsent Jun 10 19:58:21.768: TTY5: Async
Int reset: Dropping DTR
```

Si la connexion est asynchrone, la cause probable est une incompatibilité de vitesse entre le routeur et son modem. Ceci est généralement dû au fait que le débit ETTD du modem n'a pas été verrouillé sur la vitesse configurée de la ligne TTY. Le problème peut se trouver sur l'un ou l'autre ou sur les deux homologues, donc vérifiez les deux. Reportez-vous à Modem ne peut pas envoyer ou recevoir de données plus tôt dans ce chapitre.

Si les symptômes apparaissent lorsque la connexion est sur RNIS, le problème est probablement qu'un homologue se connecte à 56 K tandis que l'autre à 64 K. Bien que cette condition soit rare, elle se produit. Le problème peut être un ou les deux homologues, ou peut-être la compagnie de téléphone. Utilisez **debug isdn q931** et examinez les messages SETUP sur chacun des homologues. La capacité du porteur envoyée par un homologue doit correspondre à la capacité du porteur affichée dans le message SETUP reçu sur l'autre homologue. Comme remède possible, configurez la vitesse de numérotation, 56K ou 64K, soit dans la **carte de numérotation** de la commande interface level, soit dans la commande **dialer isdn speed** configurée sous une carte-class.

```
*Mar 20 21:07:45.033: ISDN BR0: TX ->  SETUP pd = 8  callref = 0x2C
*Mar 20 21:07:45.037:         Bearer Capability i = 0x8890
*Mar 20 21:07:45.041:         Channel ID i = 0x83
*Mar 20 21:07:45.041:         Keypad Facility i = 0x35353533373539
```

Cette situation peut justifier un appel au TAC Cisco. Recueillez les résultats suivants auprès des deux homologues avant d'appeler le centre d'assistance technique :

- **show running-config**
- **show version**
- **debug isdn q931**
- **debug isdn events**
- **debug ppp negotiation**

## Authentification

L'échec de l'authentification est la raison la plus courante d'une défaillance PPP. Des noms d'utilisateur et des mots de passe mal configurés ou mal concordants créent des messages d'erreur dans la sortie de débogage.

L'exemple suivant montre que le nom d'utilisateur Goleta n'est pas autorisé à se connecter au NAS, qui n'a pas de nom d'utilisateur local configuré pour cet utilisateur. Pour résoudre le problème, utilisez la commande **username** *name* **password** *password* pour ajouter le nom

d'utilisateur « Goleta » à la base de données AAA locale du NAS :

```
Mar 13 11:01:42.399: As2 LCP: State is Open
Mar 13 11:01:42.399: As2 PPP: Phase is AUTHENTICATING, by this end
Mar 13 11:01:42.399: As2 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
Mar 13 11:01:42.539: As2 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 11:01:42.539: As2 CHAP: Unable to validate Response.  Username Goleta not found
Mar 13 11:01:42.539: As2 CHAP: O FAILURE id 1 len 26 msg is "Authentication failure"
Mar 13 11:01:42.539: As2 PPP: Phase is TERMINATING
```

L'exemple suivant montre que le nom d'utilisateur « Goleta » est configuré sur le NAS. Cependant, la comparaison des mots de passe a échoué. Pour résoudre ce problème, utilisez la commande **username** ***name*** **password** ***password*** pour spécifier le mot de passe de connexion correct pour Goleta :

```
Mar 13 11:04:06.843: As3 LCP: State is Open
Mar 13 11:04:06.843: As3 PPP: Phase is AUTHENTICATING, by this end
Mar 13 11:04:06.843: As3 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
Mar 13 11:04:06.987: As3 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 11:04:06.987: As3 CHAP: O FAILURE id 1 len 25 msg is "MD/DES compare failed"
Mar 13 11:04:06.987: As3 PPP: Phase is TERMINATING
```

Pour plus d'informations sur l'authentification PAP, référez-vous à Configuration et dépannage du protocole PAP (PPP Password Authentication Protocol).

## Protocole de contrôle de réseau

Une fois que les homologues ont réussi l'authentification requise, la négociation passe à la phase NCP. Si les deux homologues sont correctement configurés, la négociation NCP peut ressembler à l'exemple suivant, qui montre un PC client entrant et négociant avec un NAS :

```
solvang# show debug
Generic IP:
IP peer address activity debugging is on
PPP:
PPP protocol negotiation debugging is on

*Mar  1 21:35:04.186: As4 PPP: Phase is UP
*Mar  1 21:35:04.190: As4 IPCP: O CONFREQ [Not negotiated] id 1 len 10
*Mar  1 21:35:04.194: As4 IPCP:    Address 10.1.2.1 (0x03060A010201)
*Mar  1 21:35:04.282: As4 IPCP: I CONFREQ [REQsent] id 1 len 28
*Mar  1 21:35:04.282: As4 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
*Mar  1 21:35:04.286: As4 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 21:35:04.290: As4 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 21:35:04.298: As4 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 21:35:04.306: As4 IPCP: O CONFREJ [REQsent] id 1 len 10
*Mar  1 21:35:04.310: As4 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
*Mar  1 21:35:04.314: As4 CCP: I CONFREQ [Not negotiated] id 1 len 15
*Mar  1 21:35:04.318: As4 CCP:    MS-PPC supported bits 0x00000001 (0x120600000001)
*Mar  1 21:35:04.318: As4 CCP:    Stacker history 1 check mode EXTENDED (0x1105000104)
*Mar  1 21:35:04.322: As4 LCP: O PROTREJ [Open] id 3 len 21 protocol CCP
*Mar  1 21:35:04.326: As4 LCP:  (0x80FD0101000F12060000000111050001)
*Mar  1 21:35:04.330: As4 LCP:  (0x04)
*Mar  1 21:35:04.334: As4 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar  1 21:35:04.338: As4 IPCP:    Address 10.1.2.1 (0x03060A010201)
*Mar  1 21:35:05.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async4,
```

```
 changed state to up
*Mar  1 21:35:07.274: As4 IPCP: I CONFREQ [ACKrcvd] id 2 len 22
*Mar  1 21:35:07.278: As4 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 21:35:07.282: As4 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 21:35:07.286: As4 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 21:35:07.294: As4 IPCP: O CONFNAK [ACKrcvd] id 2 len 22
*Mar  1 21:35:07.298: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.302: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.310: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar  1 21:35:07.426: As4 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
*Mar  1 21:35:07.430: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.434: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.442: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar  1 21:35:07.446: ip_get_pool: As4: validate address = 10.1.2.2
*Mar  1 21:35:07.450: ip_get_pool: As4: using pool default
*Mar  1 21:35:07.450: ip_get_pool: As4: returning address = 10.1.2.2
*Mar  1 21:35:07.454: set_ip_peer_addr: As4: address = 10.1.2.2 (3) is redundant
*Mar  1 21:35:07.458: As4 IPCP: O CONFACK [ACKrcvd] id 3 len 22
*Mar  1 21:35:07.462: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.466: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.474: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar  1 21:35:07.478: As4 IPCP: State is Open
*Mar  1 21:35:07.490: As4 IPCP: Install route to 10.1.2.2
```

Détails de la négociation PPP NCP

| Horodatage | Description |
|---|---|
| 21:35:04.190 | Demande de configuration sortante (O CONFREQ). Le NAS envoie un paquet de demande de configuration PPP sortant contenant son adresse IP à l'homologue. |
| 21:35:04.282 | CONFREQ entrant. L'homologue demande d'effectuer la compression d'en-tête VJ. Il a besoin d'une adresse IP pour lui-même, ainsi que des adresses des serveurs DNS principal et secondaire. |
| 21:35:04.306 | ConFREJ (Outbound Config-Reject). La compression d'en-tête VJ est rejetée. |
| 21:35:04.314 jusqu'à 21:35:04.330 | L'homologue envoie une requête pour exécuter le protocole de contrôle de compression ; le protocole entier est rejeté par le NAS au moyen d'un message PROTREJ. L'homologue ne doit pas (et ne tente pas) de réessayer CCP. |
| 21:35:04.334 | L'homologue accuse réception de l'adresse IP du NAS à l'aide d'un CONFACK. |
| 21:35:07.274 | CONFREQ entrant. L'homologue ne demande plus de compression d'en-tête VJ, mais a toujours besoin d'une adresse IP pour lui-même, ainsi que des adresses des serveurs DNS |

| | |
|---|---|
| | principal et secondaire. |
| 21:35:07.294 | Le NAS envoie une CONFNAK contenant l'adresse qu'il souhaite utiliser par l'homologue, ainsi que les adresses des serveurs DNS principal et secondaire. |
| 21:35:07.426 | L'homologue renvoie les adresses au NAS ; tentative de confirmation de la réception correcte des adresses. |
| 21:35:07.458 | Le NAS accuse réception des adresses à l'aide d'un CONFACK. |
| 21:35:07.478 | Chaque côté de la connexion ayant émis un CONFACK, la négociation se termine. La commande **show interfaces Async4** sur le NAS affiche « IPCP : Ouvert ». |
| 21:35:07.490 | Une route hôte vers l'homologue distant est installée dans la table de routage du NAS. |

Il est possible pour les homologues de négocier simultanément plusieurs protocoles de couche 3. Il n'est pas rare, par exemple, que les protocoles IP et IPX soient négociés. Il est également possible qu'un protocole réussisse à négocier, alors que l'autre ne le fait pas.

## Dépannage de NCP

Tous les problèmes survenant lors de la négociation NCP peuvent généralement être attribués aux configurations des homologues de négociation. Si la négociation PPP échoue pendant la phase NCP, reportez-vous aux étapes suivantes :

1. Vérifier la configuration du protocole d'interfaceExaminez le résultat de la commande d'exécution privilégiée **show running-config**. Vérifiez que l'interface est configurée pour prendre en charge le protocole que vous souhaitez exécuter sur la connexion.
2. Vérifier l'adresse de l'interfaceVérifiez que l'adresse de l'interface en question est configurée. Si vous utilisez **ip unnumbered [*interface-name*]** ou **ipx ppp-client loopback [*number*]**, assurez-vous que l'interface référencée est configurée avec une adresse.
3. Vérifier la disponibilité de l'adresse clientSi le NAS est censé émettre une adresse IP à l'appelant, assurez-vous qu'une telle adresse est disponible. L'adresse IP à transmettre à l'appelant peut être obtenue par l'une des méthodes suivantes :Configurez localement sur l'interface. Vérifiez la configuration de l'interface pour la commande **peer default ip address a.b.c.d**. En pratique, cette méthode ne doit être utilisée que sur les interfaces qui acceptent des connexions d'un seul appelant, par exemple sur une interface asynchrone (*pas* une interface groupe-asynchrone).Pool d'adresses configuré localement sur le NAS. L'interface doit avoir la commande **peer default ip address pool [*pool-name*]**. En outre, le pool doit être défini au niveau du système avec la commande **ip local pool [*pool-name*] [*first-address*] [*last-address*]**. La plage d'adresses définie dans le pool doit être suffisamment grande pour accueillir autant d'appelants connectés simultanément que le NAS.Serveur DHCP. L'interface NAS doit être configurée avec la commande **peer default ip address dhcp**. En outre, le NAS doit être configuré pour pointer vers un serveur DHCP avec la commande de configuration globale **ip dhcp-server [*address*]**.AAA. Si vous utilisez TACACS+ ou RADIUS

pour l'autorisation, le serveur AAA peut être configuré pour transmettre une adresse IP spécifique à un appelant donné chaque fois que l'appelant se connecte. Pour plus d'informations, reportez-vous au chapitre 16.

4. Vérifier la configuration de l’adresse du serveurPour renvoyer les adresses configurées des serveurs de noms de domaine ou des serveurs Windows NT en réponse aux requêtes BOOTP, assurez-vous que les commandes de niveau global **async-bootp dns-server [*address*]** et **async-bootp nbns-server [*address*]** sont configurées.**Remarque :** Bien que la commande **async-bootp subnet-mask [*mask*]** puisse être configurée sur le NAS, le masque de sous-réseau *ne sera pas* négocié entre le NAS et un PC client de connexion PPP. En raison de la nature des connexions point à point, le client utilise automatiquement l'adresse IP du NAS (apprise lors de la négociation IPCP) comme passerelle par défaut. Le masque de sous-réseau n'est pas nécessaire dans cet environnement point à point. Le PC sait que si l’adresse de destination ne correspond pas à l’adresse locale, le paquet doit être transféré à la passerelle par défaut (NAS) qui est toujours accessible via la liaison PPP.

## Avant d'appeler l'équipe TAC Cisco Systems

Avant d'appeler le centre d'assistance technique Cisco Systems (TAC), assurez-vous d'avoir lu ce chapitre et d'avoir suivi les actions suggérées pour résoudre le problème de votre système.

En outre, procédez comme suit et documentez les résultats afin que nous puissions mieux vous aider :

Pour tous les problèmes, collectez le résultat de **show running-config** et **show version**. Assurez-vous que la commande **service timestamps debug datetime msec** figure dans la configuration.

Pour les problèmes de DDR, collectez les éléments suivants :

- **show dialer map**
- **debug dialer**
- **debug ppp negotiation**
- **debug ppp authentication**

Si RNIS est impliqué, collectez :

- **show isdn status**
- **debug isdn q931**
- **debug isdn events**

Si des modems sont impliqués, collectez :

- **show lines**
- **show line [x]**
- **show modem** (si des modems intégrés sont impliqués)
- **show modem version** (si des modems intégrés sont impliqués)
- **debug modem**
- **debug modem** csm (si des modems intégrés sont impliqués)
- **debug chat** (si un scénario DDR)

Si des T1 ou des PRI sont impliqués, recueillir :

- show controller t1

## Informations connexes

- Page de dépannage T1/E1
- Guide des solutions de numérotation Cisco IOS
- Surveillance et maintenance de l'interface T1/E1
- Dépannage de la négociation PPP
- Dépannage de modems
- Commandes de débogage du modem
- Dépannage RNIS
- Dépannage de l'accès primaire (PRI) T1
- Support et documentation techniques - Cisco Systems