Technologie d'accès commuté : Présentation et explications

Contenu

Introduction

Ce chapitre présente et explique certaines des technologies utilisées dans les réseaux commutés. Vous trouverez des conseils de configuration et des interprétations de certaines commandes **show**, utiles pour vérifier le bon fonctionnement du réseau. Les procédures de dépannage ne relèvent pas de ce document et se trouvent dans le document intitulé *Dépannage de la connexion commutée*.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

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.

Fonctionnement du modem

Cette section explique les problèmes liés spécifiquement à la configuration, à la vérification et à l'utilisation des modems avec les routeurs Cisco.

Utilisation de la commande Modem Autoconfigure

Si vous utilisez Cisco Internetwork Operating System (Cisco IOS) version 11.1 ou ultérieure, vous pouvez configurer votre routeur Cisco pour communiquer avec votre modem et le configurer automatiquement.

Procédez comme suit pour configurer un routeur Cisco afin de tenter automatiquement de découvrir quel type de modem est connecté à la ligne, puis pour configurer le modem :

1. Pour découvrir le type de modem connecté à votre routeur, utilisez la commande de configuration de ligne **modem autoconfigure discovery**.
2. Une fois le modem détecté, configurez-le automatiquement à l'aide de la commande de configuration de ligne **modem autoconfigure type** ***modem-name***.

Si vous voulez afficher la liste des modems pour lesquels le routeur a des entrées, utilisez la commande **show modemcap** ***modem-name*** . Si vous souhaitez modifier une valeur de modem renvoyée à partir de la commande **show modemcap**, utilisez la commande de configuration de ligne **modemcap edit** ***modem-name attribute value***.

Pour obtenir des informations complètes sur l'utilisation de ces commandes, reportez-vous au *Guide de configuration des solutions de numérotation et au Guide de référence des commandes des solutions de numérotation de la documentation Cisco IOS*.

Remarque : Ne *pas* entrer **&W** dans l'entrée modemcap utilisée pour la configuration automatique. Cela entraîne la réécriture de la mémoire NVRAM à chaque fois qu'un modem est configuré automatiquement et détruit le modem.

Établissement d'une session Reverse Telnet sur un modem

Pour des raisons de diagnostic ou pour configurer initialement le modem si vous utilisez Cisco IOS version 11.0 ou antérieure, vous devez établir une session Telnet inverse pour configurer un modem afin qu'il communique avec un périphérique Cisco. Tant que vous verrouillez la vitesse du modem côté ETTD (Data Terminal Equipment), le modem communique toujours avec le serveur d'accès ou le routeur à la vitesse souhaitée. Reportez-vous au tableau 16-5 pour obtenir des informations sur le verrouillage de la vitesse du modem. Assurez-vous que la vitesse du périphérique Cisco est configurée avant d'émettre des commandes au modem via une session Telnet inverse. Reportez-vous à nouveau au tableau 16-5 pour obtenir des informations sur la configuration de la vitesse du serveur d'accès ou du routeur.

Pour configurer le modem pour une session Telnet inverse, utilisez la commande de configuration de ligne **transport input telnet**. Pour configurer un groupe rotatif (dans ce cas, sur le port 1), entrez la commande de configuration de ligne **rotatif 1**. En plaçant ces commandes sous la configuration de ligne, IOS attribue des écouteurs IP pour les connexions entrantes aux plages de ports commençant par les numéros de base suivants :

2000	protocole Telnet
3000	Protocole Telnet avec protocole rotatif
4000	Protocole TCP brut
5000	Protocole TCP brut avec rotation
6000	Protocole Telnet, mode binaire
7000	Protocole Telnet, mode binaire avec rotation
9000	Protocole XRemote
10 000	Protocole XRemote avec rotative

Pour initier une session Telnet inversée sur votre modem, procédez comme suit :

1. Àpartir de votre terminal, utilisez la commande **telnet ip-address 20yy** où *ip-address* est l'adresse IP de toute interface active et connectée sur le périphérique Cisco, et yy est le numéro de ligne auquel le modem est connecté.Par exemple, la commande suivante vous connecte au port auxiliaire d'un routeur Cisco 2501 avec l'adresse IP 192.169.53.52 : **telnet 192.169.53.52 2001**. En règle générale, une commande Telnet de ce type peut être exécutée à partir de n'importe quel endroit du réseau, s'il peut **envoyer une requête ping** à l'adresse IP en question.**Remarque :** Sur la plupart des routeurs Cisco, le port 01 est le port auxiliaire. Sur un serveur d'accès Cisco, le port auxiliaire est le dernier ATS +1. Par exemple, le port auxiliaire d'un 2511 est le port 17 (16 ports TTY + 1). Utilisez toujours la commande **show line** exec pour trouver le numéro de port auxiliaire, en particulier sur les gammes 2600 et 3600, qui utilisent des numéros de port non contigus pour prendre en charge des tailles de modules asynchrones variables.
2. Si la connexion est refusée, elle peut indiquer qu'il n'y a pas d'écouteur à l'adresse et au port spécifiés, ou qu'une personne est déjà connectée à ce port. Vérifiez l'adresse de connexion et le numéro de port. Assurez-vous également que la commande **modem inout** ou **modem DTR-active**, ainsi que **transport input all**, figurent sous la configuration de ligne pour les lignes à atteindre.Si vous utilisez la fonction de rotation, assurez-vous que la commande *rotative n* apparaît également dans la configuration de ligne où n représente le numéro du groupe rotative. Pour vérifier si une personne est déjà connectée, établissez une connexion Telnet avec le routeur et utilisez la commande **show line *n*** . Recherchez un astérisque pour indiquer que la ligne est utilisée. Assurez-vous que le CTS est élevé et que le DSR ne l'est

pas. Utilisez la commande **clear line *n*** pour déconnecter la session en cours sur le numéro de port n. Si la connexion est toujours refusée, il se peut que le modem proclame le service Carrier Detect (CD) en permanence. Déconnectez le modem de la ligne, établissez une session Telnet inverse, puis connectez le modem.

3. Après avoir réussi la connexion Telnet, entrez AT et assurez-vous que le modem répond par OK.
4. Si le modem ne répond pas, reportez-vous au tableau suivant.

Le tableau 16-1 ci-dessous présente les causes possibles des symptômes de problème de connectivité modem-routeur et décrit les solutions à ces problèmes.

Tableau 16-1 : Aucune connectivité entre le modem et le routeur

Causes possibles	Actions suggérées

Le contrôle de modem n'est pas activé sur le serveur d'accès ou le routeur	1. Utilisez la commande **show line** exec sur le serveur d'accès ou le routeur. Le résultat pour le port auxiliaire doit afficher **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.
	2. 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.
	Exemple : L'exemple suivant illustre comment configurer une ligne pour les appels entrants et sortants :
	`line 5`
	`modem inout`
	Remarque : assurez-vous d'utiliser la commande **modem inout**, et non 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 et il sera impossible d'établir une session Telnet avec le modem afin de le configurer. Si vous voulez utiliser la commande **modem dialin**, ne le faites qu'après avoir vérifié que le modem fonctionne correctement.

Le modem	Entrez **AT&FE1Q0** pour rétablir les paramètres d'usine et assurez-vous que le modem est défini sur les caractères d'écho et renvoie la sortie. Le

peut être mal configuré ou avoir une session interrompue.	modem peut avoir une session suspendue. Utilisez "^**U**" pour effacer la ligne et "^**Q**" pour ouvrir le contrôle de flux (XON). Vérifiez les paramètres de parité.
Câblage incorrect	1. 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.) 2. 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 intitulée « Utilisation des commandes de débogage » au chapitre 15.
Problème matériel	1. Vérifiez que vous utilisez le câblage approprié et que toutes les connexions sont correctes. 2. Vérifiez que tout le matériel est endommagé, y compris le câblage (câbles cassés), les adaptateurs (broches desserrées), les ports du serveur d'accès et le modem. 3. Pour plus d'informations sur le dépannage matériel, reportez-vous au chapitre 3, « Dépannage matériel et problèmes de démarrage ».

Utilisation des groupes de rotation

Pour certaines applications, les modems d'un routeur donné doivent être partagés par un groupe d'utilisateurs. Cisco Dialout Utility est un exemple de ce type d'application. En gros, les utilisateurs se connectent à un port qui les connecte à un modem disponible. Pour ajouter une ligne asynchrone à un groupe rotatif, entrez simplement **rotative *n*** où *n* est le numéro du groupe rotatif dans la configuration de la ligne asynchrone. Reportez-vous à l'exemple ci-dessous .

```
line 1 16
 modem InOut
 transport input all
 rotary 1
 speed 115200
 flowcontrol hardware
```

La configuration de ligne ci-dessus permettrait aux utilisateurs de se connecter au groupe rotatif en entrant **telnet 192.169.53.52 3001** pour telnet normal. Les alternatives incluent les ports 5001 pour le protocole Raw TCP, 7001 pour le protocole Telnet binaire (que l'utilitaire Cisco Dialout utilise) et 10001 pour les connexions Xremote.

Remarque : pour vérifier la configuration de l'utilitaire de numérotation Cisco, double-cliquez sur l'icône de l'utilitaire de numérotation en bas à droite de l'écran et appuyez sur le bouton Autres>. Appuyez ensuite sur le bouton Configurer les ports>. Assurez-vous que le port se trouve dans la plage 7000, si vous utilisez des groupes rotatifs, et dans la plage 6000, si l'utilitaire Dialout cible un modem individuel. Vous devez également activer la journalisation par modem sur le PC. Pour ce faire, sélectionnez la séquence suivante : **Démarrer->Panneau de configuration-> modems->**(choisissez votre modem Cisco Dialout)**->Propriétés->Connexion->Avancé**.**->Enregistrer un fichier journal**.

Interprétation de la sortie de la ligne show

Le résultat de la commande **show line** *line-number* exec est utile lors du dépannage d'une connexion modem-serveur ou routeur d'accès. Voici le résultat de la commande **show line**.

```
as5200-1#show line 1
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
   1 TTY 115200/115200-    -      -    -    -      0       0     0/0       -

Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
Status: No Exit Banner
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
Modem state: Hanging up
  modem(slot/port)=1/0, state=IDLE
  dsx1(slot/unit/channel)=NONE, status=VDEV_STATUS_UNLOCKED
Group codes:    0
Modem hardware state: CTS noDSR  noDTR RTS
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                      none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are lat pad telnet rlogin udptn v120 lapb-ta.
```

```
Preferred is l
at pad telnet rlogin udptn v120 lapb-ta.
No output characters are padded
No special data dispatching characters
as5200-1#
```

Lorsque des problèmes de connectivité surviennent, des informations importantes s'affichent dans les champs Modem et Modem Hardware State.

Remarque : Le champ d'état matériel du modem n'apparaît pas dans la sortie **show line** pour chaque plate-forme. Dans certains cas, les indications relatives à l'état du signal s'affichent dans le champ État du modem.

Le tableau 16-2 présente les chaînes d'état du modem et de l'état du matériel du modem à partir du résultat de la commande **show line**. Il explique également le sens de chaque état.

Tableau 16-2 : États matériels du modem et du modem dans la sortie de la ligne show

État du modem	État du matériel du modem	Signification
Inactif	CTS no DSR DTR RTS	Il s'agit des états de modem appropriés pour les connexions entre un serveur d'accès ou un routeur et un modem (en l'absence d'appel entrant). Les résultats de toute autre nature indiquent généralement un problème.
Prêt	-	Si l'état du modem est Prêt, au lieu d'Inactif, tenez compte des points suivants : 1. Le contrôle de modem n'est pas configuré sur le serveur d'accès ou le routeur. Configurez le serveur d'accès ou le routeur à l'aide de la commande de configuration de ligne **modem inout**. 2. Une session existe sur la ligne. Utilisez la commande **show users** exec et la commande **clear line** en mode privilégié pour arrêter la session si vous le souhaitez. 3. DSR est élevé. Il y a deux raisons possibles à cela : Problèmes de câblage. Si votre connecteur utilise la broche DB-25 6 et n'a pas de broche 8, vous devez

		déplacer la broche de 6 à 8 ou obtenir le connecteur approprié.Le modem configuré pour DCD est toujours élevé. Le modem doit être reconfiguré pour que DCD ne soit élevé que sur un CD(1). Cela se fait généralement avec la commande modem **&C1**, mais vérifiez la syntaxe exacte de votre modem dans la documentation de votre modem. Si votre logiciel ne prend pas en charge le contrôle de modem, vous devez configurer la ligne de 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.
Prêt	noCTS noDSR DTR RTS(2)	La chaîne noCTS apparaît dans le champ d'état matériel du modem pour l'une des quatre raisons suivantes : 1. Le modem est désactivé. 2. Le modem n'est pas correctement connecté au serveur d'accès. Vérifiez les connexions de câblage du modem au serveur d'accès. 3. Câblage incorrect (MDCE enroulé ou MDTE droit, mais sans déplacement des broches). La configuration de câblage recommandée est indiquée plus haut dans ce tableau. 4. Le modem n'est pas configuré pour le contrôle de flux matériel. Utilisez la commande de configuration de ligne **no flow control hardware** pour désactiver le contrôle de flux matériel sur le serveur d'accès. Activez ensuite le contrôle de flux matériel sur le modem via une session Telnet inverse. (Consultez la documentation de votre modem et reportez-vous à la section « Établissement d'une session Telnet

		inversée à un modem », plus haut dans ce chapitre.) Réactivez le contrôle de flux matériel sur le serveur d'accès à l'aide de la commande de configuration de ligne de **matériel de contrôle de flux**.
Prêt	DSR DTR CTS RTS(2)	La chaîne DSR (au lieu de la chaîne noDSR) apparaît dans le champ d'état matériel du modem pour l'une des raisons suivantes : 1. Câblage incorrect (MDCE enroulé ou MDTE droit, mais sans déplacement des broches). La configuration de câblage recommandée est indiquée plus haut dans ce tableau. 2. Le modem est configuré pour DCD toujours élevé. Reconfigurez le modem de sorte que le DCD ne soit qu'élevé sur le CD. Cela se fait généralement avec la commande modem **&C1**, mais vérifiez la syntaxe exacte de votre modem dans la documentation de votre modem. Configurez 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**. Reconfigurer la ligne du serveur d'accès à l'aide de la commande de configuration de ligne exec.
Prêt	CTS* DSR* DTR RTS(2)	Si cette chaîne apparaît dans le champ État matériel du modem, le contrôle de modem n'est probablement pas activé sur le serveur d'accès. Utilisez la commande de configuration de ligne **modem inout** pour activer le contrôle de modem sur la ligne. Des informations supplémentaires sur la configuration du contrôle de modem sur un serveur d'accès ou une ligne de routeur sont fournies précédemment dans ce tableau.

(1) CD = Détection de porteuse

(2) Un * à côté d'un signal indique l'une des deux choses suivantes : Le signal a changé au cours des dernières secondes ou le signal n'est pas utilisé par la méthode de contrôle de modem sélectionnée.

Collecte des informations sur les performances des modems

Cette section explique les méthodes de collecte de données de performances sur les modems numériques MICA de la gamme de serveurs d'accès Cisco AS5x00. Les données de performances peuvent être utilisées pour l'analyse des tendances et sont utiles pour le dépannage des problèmes de performances susceptibles d'être rencontrés. En regardant les chiffres présentés ci-dessous, gardez à l'esprit que la perfection n'est pas possible dans le monde réel. Le taux de succès d'appel du modem (CSR) est fonction de la qualité des circuits, de la base d'utilisateurs du modem client et de l'ensemble de modules utilisés. Un pourcentage CSR type pour les appels V.34 est de 95 %. On peut s'attendre à ce que les appels V.90 se connectent correctement 92 % du temps. Les chutes prématurées sont susceptibles d'avoir lieu 10 % du temps.

Utilisez les commandes suivantes pour obtenir une vue d'ensemble du comportement du modem sur le serveur d'accès :

- **show modem**
- **show modem summary**
- **show modem connect-vitesses**
- **show modem call-stats**

Les informations suivantes sont utiles lors du dépannage d'une connexion par modem ou lors de la collecte de données pour l'analyse des tendances :

- debug modem csm
- modem call-record terse
- show modem op (MICA) / AT@E1 (Microcom) lorsqu'il est connecté
- show modem log pour la session d'intérêt après déconnexion
- ANI (numéro de l'appelant)
- Heure du jour
- Révision matérielle/microprogramme du modem client
- Informations intéressantes du client (après déconnexion) : ATI6, ATI11, AT&V, AT&V1, etc.
- Enregistrement audio (fichier .wav) de la tentative de formation à partir du modem client

Dans les sections suivantes, les commandes seront expliquées plus en détail et certaines tendances courantes seront abordées.

Afficher le résumé du modem / Afficher le résumé du modem

La commande **show modem** affiche les modems individuels. À partir de ces chiffres, l'état de santé des modems individuels peut être affiché.

```
router# show modem
  Codes:
  * - Modem has an active call
  C - Call in setup
  T - Back-to-Back test in progress
  R - Modem is being Reset
  p - Download request is pending and modem cannot be used for taking calls
  D - Download in progress
  B - Modem is marked bad and cannot be used for taking calls
  b - Modem is either busied out or shut-down
  d - DSP software download is required for achieving K56flex connections
```

```
  ! - Upgrade request is pending
                Inc calls     Out calls     Busied   Failed  No       Succ
  Mdm  Usage    Succ   Fail   Succ   Fail   Out      Dial    Answer   Pct.
* 1/0    17%      74      3      0      0       0        0       0     96%
* 1/1    15%      80      4      0      0       0        1       1     95%
* 1/2    15%      82      0      0      0       0        0       0    100%
  1/3    21%      62      1      0      0       0        0       0     98%
  1/4    21%      49      5      0      0       0        0       0     90%
* 1/5    18%      65      3      0      0       0        0       0     95%
```

Pour afficher les numéros agrégés de tous les modems du routeur, utilisez la commande **show modem summary**.

```
router#show modem summary
         Incoming calls       Outgoing calls      Busied   Failed   No    Succ
Usage  Succ   Fail  Avail   Succ   Fail  Avail    Out      Dial     Ans   Pct.
   0%  6297    185     64      0      0      0        0        0     0     97%
```

Tableau 16-3 : show modem Fields

Champs	Description
Appels entrants et sortants	Appels entrant et sortant du modem. • Utilisation : pourcentage du temps de fonctionnement total du système pendant lequel tous les modems sont utilisés. • Succ : nombre total d'appels correctement connectés. • Échec : nombre total d'appels qui n'ont pas réussi à se connecter. • Disponible : nombre total de modems disponibles pour utilisation dans le système.
Sorti	Nombre total de fois où les modems ont été retirés du service à l'aide de la commande **modem Occupé** ou de la commande **modem shutdown**.
Échec de la numérotation	Nombre total de tentatives auxquelles les modems n'ont pas raccroché ou aucune tonalité n'est apparue.
Aucune réponse	Nombre total de fois où la sonnerie d'appel a été détectée, mais où aucun modem n'a répondu aux appels.
Succ Pct.	Pourcentage de connexion réussi du nombre total de modems disponibles.

[Afficher la sortie des statistiques d'appel du modem]

```
compress  retrain lostCarr  rmtLink  trainup hostDrop wdogTimr inacTout
  Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %    #   %
 Total    9       41      271     3277        7     2114        0        0
```

Tableau 16-4 : Champs show modem call-stats

rmt Link	Ceci montre que la correction d'erreur était en vigueur et que l'appel a été raccroché par le système client connecté au modem distant.
hostDrop	Ceci indique que l'appel a été raccroché par le système hôte IOS. Voici quelques raisons courantes : délai d'inactivité, circuit dégagé de la compagnie de téléphone ou terminal PPP LCP du client. Le meilleur moyen de déterminer la raison de la suspension est d'utiliser le mot de passe d'enregistrement d'appels de modem ou la comptabilité AAA.

Les autres raisons de déconnexion devraient représenter moins de 10 % du total.

Afficher la sortie de vitesse de connexion du modem

```
router>show modem connect 33600 0
 Mdm   26400  28000  28800  29333  30667  31200  32000  33333  33600 TotCnt
Tot      614      0   1053      0      0   1682      0      0    822   6304

router>show modem connect 56000 0
 Mdm   48000  49333  50000  50666  52000  53333  54000  54666  56000 TotCnt
Tot      178    308     68     97     86     16      0      0      0   6304
```

Attendez-vous à une distribution des vitesses V.34. Il doit y avoir un pic à 26,4, si les T1 utilisent la signalisation associée au canal (CAS). Pour les connexions RNIS (PRI) T1, le pic doit être 31,2. Recherchez également quelques vitesses K56Flex, V.90. S'il n'y a pas de connexions V.90, il peut y avoir un problème de topologie de réseau.

Présentation de la commande Modem Call-Record Terse (11.3AA/12.0T)

Plutôt qu'une commande exec, il s'agit d'une commande de configuration placée au niveau système du serveur d'accès en question. Lorsqu'un utilisateur se déconnecte, un message similaire à celui-ci s'affiche :

```
*May 31 18:11:09.558: %CALLRECORD-3-MICA_TERSE_CALL_REC: DS0 slot/contr/chan=2/0/18,
slot/port=1/29, call_id=378, userid=cisco, ip=0.0.0.0, calling=5205554099,
called=4085553932, std=V.90, prot=LAP-M, comp=V.42bis both,
init-rx/tx b-rate=26400/41333, finl-rx/tx brate=28800/41333, rbs=0, d-pad=6.0 dB,
retr=1, sq=4, snr=29, rx/tx chars=93501/94046, bad=5, rx/tx ec=1612/732, bad=0,
time=337, finl-state=Steady, disc(radius)=Lost Carrier/Lost Carrier,
disc(modem)=A220 Rx (line to host) data flushing - not OK/EC condition - locally
detected/received
DISC frame -- normal LAPM termination
```

Commande Show Modem Operational-Status

La commande exec **show modem Operational-status** affiche les paramètres actuels (ou les plus récents) de la connexion du modem.

L'entrée de documentation de cette commande se trouve dans le *Guide de référence des commandes des solutions de numérotation Cisco IOS version 12.0*. **show modem Operational-status** est uniquement destiné aux modems MICA. La commande équivalente pour les modems Microcom est **modem at-mode / AT@E1**. Utilisez la commande **modem at-mode <slot>/<port>** pour vous connecter au modem, puis exécutez la commande **AT@E1**. La documentation complète de la commande **modem at-mode** se trouve dans le *Guide de configuration du logiciel Cisco AS5300*, et la documentation de la commande **AT@E1** se trouve dans le *tableau de commandes AT et le récapitulatif des enregistrements pour la référence des commandes des modules microcom*.

Procédez comme suit pour déterminer les modems sur lesquels un utilisateur entre :

1. Exécutez la commande **show user** et recherchez l'ATS auquel ils sont connectés.
2. Utilisez la commande **show line** et recherchez les numéros de port/logement du modem.

Collecte des données de performances côté client

Pour l'analyse des tendances, il est très important de recueillir des données de performances côté client. Toujours essayer d'obtenir les informations suivantes :

- version du microprogramme/modèle matériel du client (accessible avec la commande **ATI3I7** sur le modem du client)
- raisons de déconnexion signalées par le client (utilisez **ATI6** ou **AT&V1**)

Les autres informations disponibles sur l'extrémité client incluent modemlog.txt et ppplog.txt du PC. Vous devez configurer spécifiquement votre PC pour générer ces fichiers.

Analyser les données de performances

Une fois que vous avez collecté et compris les données de performances de votre système modem, vous devez examiner tous les modèles et composants restants qui pourraient nécessiter des améliorations.

Problèmes liés à des modems de serveur particuliers

Utilisez **show modem** ou **show modem call-stats** pour identifier les modems présentant des taux anormalement élevés de défaillance d'entraînement ou de mauvais taux de déconnexion (MICA). Si des paires adjacentes de modems rencontrent des problèmes, le problème est probablement un DSP suspendu/mort. Utilisez **copy flash modem** vers le HMM affecté afin de récupérer. Vérifiez que les modems exécutent la dernière version de portware. Pour vérifier que tous les modems sont correctement configurés, utilisez la commande de configuration **modem autoconfigure type mica/microcom_server** dans la configuration de ligne. Pour vous assurer que les modems sont configurés automatiquement chaque fois qu'un appel est raccroché, utilisez la commande exec **debug confmodem**. Pour réparer les modems qui sont mal configurés, vous devrez peut-être établir une session Telnet inverse.

Problèmes avec des DS0 particuliers

Les problèmes DS0 sont rares, mais possibles. Pour localiser les DS0 défectueux, utilisez la commande **show controller t1 call-counters** et recherchez les DS0 présentant des TotalCalls anormalement élevés et une TotalDuration anormalement basse. Pour cibler les DS0 suspects, vous devrez peut-être utiliser la commande de configuration **isdn service dsl** pour occuper d'autres DS0 sous l'interface série de T1. La sortie de **show controller t1 call-counters** ressemble à ceci :

```
TimeSlot   Type   TotalCalls   TotalDuration
    1       pri         873       1w6d
    2       pri         753       2w2d
    3       pri         4444      00:05:22
```

Évidemment, le point de temporisation 3 est le canal suspect dans ce cas.

Tendances communes supplémentaires

Vous trouverez ci-dessous quelques-unes des tendances les plus courantes observées par le TAC Cisco.

1. Pistes de circuits incorrectesSi vous rencontrez les problèmes suivants, vous risquez d'obtenir de mauvais chemins de circuit via le réseau téléphonique public commuté (RTPC) :les appels longue distance posent des problèmes, mais pas les appels locaux (ou vice versa)les appels à certaines heures de la journée ont des problèmesles appels d'échanges distants spécifiques ont des problèmes
2. Problèmes liés aux appels longue distanceSi votre service longue distance ne fonctionne pas correctement ou du tout (mais le service local est correct) :Assurez-vous que la ligne numérique se connecte à un commutateur numérique et non à une banque de canaux .Demander aux compagnies de téléphone d’examiner les chemins de circuits utilisés pour les longues distances.
3. Problèmes liés aux appels provenant de zones d'appel spécifiques.Si les appels provenant de régions ou d'échanges géographiques spécifiques ont tendance à poser des problèmes, vous devez obtenir la topologie du réseau auprès de la compagnie de téléphone.Si plusieurs conversions analogiques/numériques sont nécessaires, les connexions de modem V.90/K56flex ne seront pas possibles et la V.34 pourrait être quelque peu dégradée. Les conversions analogiques/numériques sont nécessaires dans les zones desservies par des commutateurs numériques non intégrés ou par des commutateurs analogiques.

Opérations RNIS

RNIS désigne un ensemble de services numériques disponibles pour les utilisateurs finaux. La technologie RNIS consiste à numériser le réseau téléphonique afin que les utilisateurs finaux puissent accéder à la voix, aux données, au texte, aux graphiques, à la musique, à la vidéo et à d’autres sources à partir d’un terminal unique, via le câblage téléphonique existant. Les partisans de la technologie RNIS imaginent un réseau mondial comme le réseau téléphonique actuel, mais avec la transmission numérique et une variété de nouveaux services.

Le RNIS est un effort de standardisation des services des abonnés, des interfaces utilisateur/réseau et des fonctionnalités réseau et interréseau. La standardisation des services

d'abonnés tente d'assurer un niveau de compatibilité internationale. La standardisation de l'interface utilisateur/réseau stimule le développement et le marketing de ces interfaces par des fabricants tiers. La standardisation des capacités réseau et interréseau permet d'atteindre l'objectif de connectivité mondiale en garantissant que les réseaux RNIS communiquent facilement entre eux.

Les applications RNIS incluent des applications d'images à haut débit (telles que les télécopies de groupe IV), des lignes téléphoniques supplémentaires dans les foyers pour desservir l'industrie du télétravail, le transfert de fichiers à haut débit et la vidéoconférence. La voix, bien sûr, est également une application populaire pour RNIS.

Le marché de l'accès domestique est divisé entre différentes technologies. Dans les domaines où de nouvelles technologies moins coûteuses, telles que la DSL et le câble, deviennent disponibles, le marché domestique s'éloigne de la technologie RNIS. Les entreprises, cependant, continuent d'utiliser RNIS sous la forme de PRI T1/E1 pour transporter de grandes quantités de données ou pour fournir un accès par ligne commutée v.90.

Composants RNIS

Les composants RNIS comprennent des terminaux, des adaptateurs de terminal (TA), des périphériques de terminaison de réseau, des équipements de terminaison de ligne et des équipements de terminaison d'échange. Les terminaux RNIS sont de deux types. Les terminaux RNIS spécialisés sont appelés équipements terminaux de type 1 (TE1). Les terminaux non RNIS, tels que les ETTD antérieurs aux normes RNIS, sont appelés équipements terminaux de type 2 (TE2). Les TE1 se connectent au réseau RNIS via une liaison numérique à quatre fils à paires torsadées. Les TE2 se connectent au réseau RNIS via une carte de terminal. L'adaptateur de terminal RNIS peut être un périphérique autonome ou une carte à l'intérieur de l'équipement TE2. Si l'équipement TE2 est mis en oeuvre en tant que périphérique autonome, il se connecte à l'adaptateur de terminal via une interface de couche physique standard. Exemples : EIA/TIA-232-C (anciennement RS-232-C), V.24 et V.35.

Au-delà des périphériques TE1 et TE2, le point de connexion suivant dans le réseau RNIS est le périphérique de terminaison de réseau de type 1 (NT1) ou NT2 (Network Termination de type 2). Il s'agit de périphériques de terminaison de réseau qui connectent le câblage d'abonné à quatre fils à la boucle locale à deux fils classique. En Amérique du Nord, le NT1 est un équipement client (CPE). Dans la plupart des autres parties du monde, la NT1 fait partie du réseau fourni par l'opérateur. La NT2 est un périphérique plus complexe, généralement présent dans les autocommutateurs privés numériques (PBX), qui exécute des fonctions de protocole de couche 2 et 3 et des services de concentration. Il existe également un périphérique NT1/2 ; il s'agit d'un seul périphérique qui combine les fonctions d'un NT1 et d'un NT2.

Un certain nombre de points de référence sont spécifiés dans RNIS. Ces points de référence définissent des interfaces logiques entre des groupes fonctionnels tels que les TA et les NT1. Les points de référence RNIS sont les suivants :

- R : point de référence entre un équipement non RNIS et un adaptateur de terminal
- S : point de référence entre les terminaux utilisateur et NT2
- T : point de référence entre les unités NT1 et NT2
- U : point de référence entre les périphériques NT1 et les équipements de terminaison de ligne du réseau de l'opérateur. Le point de référence U n'est pertinent qu'en Amérique du Nord, où la fonction NT1 n'est pas fournie par le réseau de l'opérateur

Voici un exemple de configuration RNIS. Cet exemple montre trois périphériques connectés à un

commutateur RNIS au siège social. Deux de ces périphériques sont compatibles RNIS, ils peuvent donc être connectés via un point de référence S aux périphériques NT2. Le troisième périphérique (un téléphone standard non RNIS) est relié à un adaptateur de terminal par le point de référence R. N'importe lequel de ces périphériques peut également être connecté à un périphérique NT1/2, qui remplacerait à la fois le NT1 et le NT2. Bien qu'elles ne soient pas affichées, des stations utilisateur similaires sont connectées au commutateur RNIS situé à l'extrême droite.

Exemple de configuration RNIS

```
2503B#show running-config
Building configuration...

Current configuration:
!
version 11.1
service timestamps debug datetime msec
service udp-small-servers
service tcp-small-servers
!
hostname 2503B
!
!
username 2503A password
ip subnet-zero
isdn switch-type basic-5ess
!
interface Ethernet0
 ip address 172.16.141.11 255.255.255.192
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 description phone#5553754
 ip address 172.16.20.2 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 300
 dialer map ip 172.16.20.1 name 2503A broadcast 5553759
 dialer-group 1
 ppp authentication chap
!
no ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
line aux 0
line vty 0 4
!
end

2503B#
```

Services RNIS

Le service RNIS BRI (Basic Rate Interface) offre deux canaux B et un canal D (2B+D). Le service BRI B-channel fonctionne à 64 kbits/s et est destiné à transporter des données utilisateur ; Le service de canal D BRI fonctionne à 16 kbits/s et est destiné à transporter des informations de contrôle et de signalisation, bien qu'il puisse prendre en charge la transmission de données utilisateur dans certaines circonstances. Le protocole de signalisation du canal D comprend les couches 1 à 3 du modèle de référence OSI. L'accès de base (BRI) permet également le contrôle de tramage et d'autres frais généraux, portant son débit binaire total à 192 kbits/s. La spécification de la couche physique BRI est le secteur de la normalisation des télécommunications de l'Union internationale des télécommunications (UIT-T); anciennement Comité consultatif international des télécommunications et du téléphone [CCITT] I.430.

Le service PRI (Primary Rate Interface) RNIS offre 23 canaux B et un canal D en Amérique du Nord et au Japon, pour un débit total de 1,544 Mbits/s (le canal PRI D fonctionne à 64 kbits/s). Le RNIS PRI en Europe, en Australie et dans d'autres parties du monde fournit 30 B plus un canal D de 64 kbits/s et un débit d'interface total de 2,048 Mbits/s. La spécification de couche physique PRI est UIT-T I.431.

Couche 1

Les formats de trame de couche physique RNIS (couche 1) varient selon que la trame est sortante (du terminal au réseau) ou entrante (du réseau au terminal). Les deux interfaces de couche physique sont illustrées à la Figure 16-1.

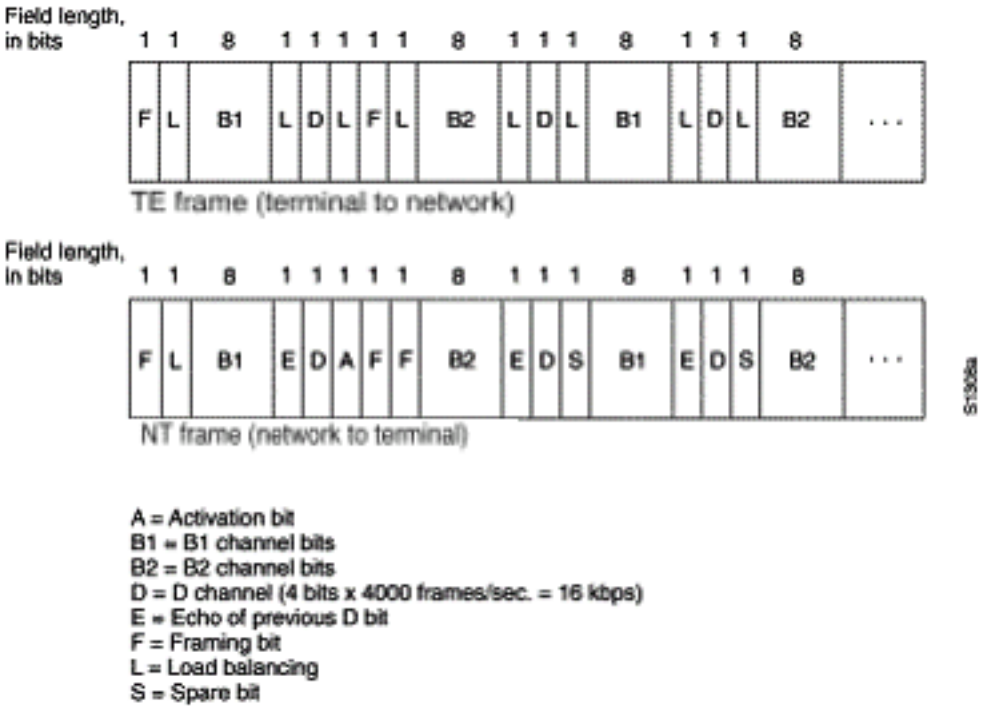

Figure 16-1 : Formats de trame de couche physique RNIS

Les trames ont une longueur de 48 bits, dont 36 bits représentent des données. Les bits d'une trame de couche physique RNIS sont utilisés comme suit :

- F : assure la synchronisation.
- L - Ajuste la valeur de bit moyenne.
- E - Utilisé pour la résolution des conflits lorsque plusieurs terminaux d'un bus passif se disputent un canal.
- A - Active les périphériques.
- S - Non affecté.
- B1, B2 et D : pour les données utilisateur.

Plusieurs périphériques utilisateur RNIS peuvent être physiquement connectés à un circuit. Dans cette configuration, les collisions peuvent se produire si deux terminaux transmettent simultanément. Par conséquent, RNIS fournit des fonctionnalités permettant de déterminer le conflit de liaison. Lorsqu'un NT reçoit un bit D de l'équipement terminal, il fait écho au bit dans la position E-bit suivante. Le TE s'attend à ce que le prochain bit E soit identique au dernier bit D transmis.

Les terminaux ne peuvent pas transmettre dans le canal D, sauf s'ils détectent d'abord un nombre spécifique de 1 (indiquant « aucun signal ») correspondant à une priorité préétablie. Si l'équipement terminal détecte un bit du canal d'écho (E) différent de ses bits D, il doit cesser immédiatement de transmettre. Cette technique simple garantit qu'un seul terminal peut transmettre son message D à la fois. Une fois la transmission du message D réussie, la priorité du terminal est réduite en étant tenue de détecter des messages plus continus avant la transmission. Les terminaux ne peuvent pas augmenter leur priorité tant que tous les autres périphériques de la même ligne n'ont pas eu la possibilité d'envoyer un message D. Les connexions téléphoniques ont une priorité plus élevée que tous les autres services et les informations de signalisation ont une priorité plus élevée que les informations non de signalisation.

Couche 2

La couche 2 du protocole de signalisation RNIS est Link Access Procedure sur le canal D, également appelé LAPD. Le protocole LAPD est similaire au protocole HDLC (High-Level Data Link Control) et au protocole LAPB (Link Access Procedure). Comme l'indique l'extension de l'abréviation LAPD, elle est utilisée sur le canal D pour s'assurer que les informations de contrôle et de signalisation circulent et sont reçues correctement. Le format de trame LAPD (voir Figure 16-2) est très similaire à celui du protocole HDLC et, comme le protocole HDLC, le protocole LAPD utilise des trames de supervision, d'informations et non numérotées. Le protocole LAPD est formellement spécifié dans les normes ITU-T Q.920 et ITU-T Q.921.

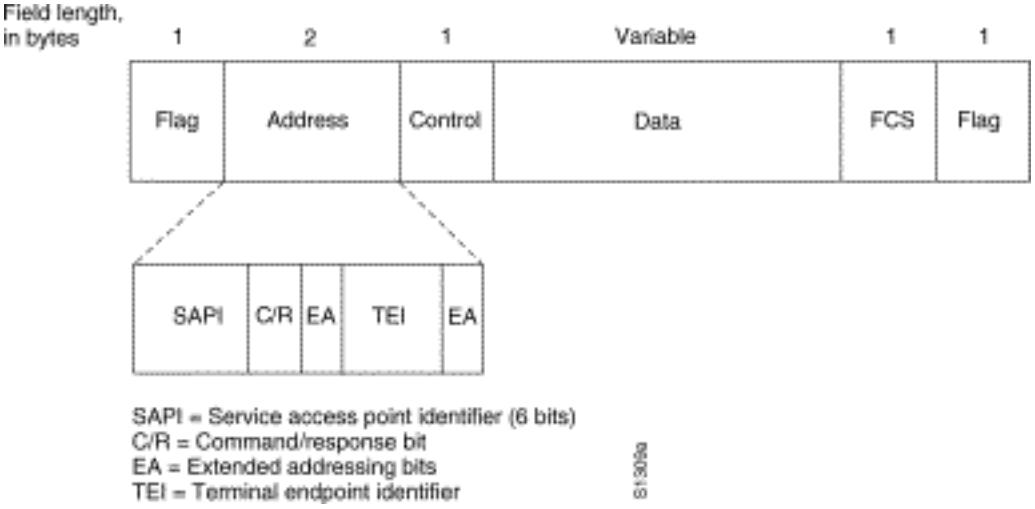

Figure 16-2 : Format de trame LAPD

Les champs Indicateur et Contrôle LAPD sont identiques à ceux de HDLC. Le champ Adresse LAPD peut avoir une longueur de 1 ou 2 octets. Si le bit d'adresse étendue du premier octet est défini, l'adresse est de 1 octet ; si elle n'est pas définie, l'adresse est de 2 octets. Le premier octet du champ d'adresse contient l'identificateur de point d'accès au service (SAPI), qui identifie le portail sur lequel les services LAPD sont fournis à la couche 3. Le bit C/R indique si la trame contient une commande ou une réponse. Le champ TEI (terminal endpoint identifier) identifie un terminal unique ou plusieurs terminaux. Un TEI de tous les uns indique une diffusion.

Couche 3

Deux spécifications de couche 3 sont utilisées pour la signalisation RNIS : ITU-T (anciennement CCITT) I.450 (également appelée ITU-T Q.930) et ITU-T I.451 (également appelée ITU-T Q.931). Ensemble, ces protocoles prennent en charge les connexions utilisateur à utilisateur, à commutation de circuits et à commutation de paquets. Différents messages d'établissement d'appel, de fin d'appel, d'informations et divers sont spécifiés, notamment SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS et DISCONNECT.

Ces messages sont fonctionnellement similaires à ceux fournis par le protocole X.25 (pour plus d'informations, reportez-vous au Chapitre 19, Dépannage des connexions X.25). La figure 16-3, de l'ITU-T I.451, illustre les étapes types d'un appel à commutation de circuits RNIS.

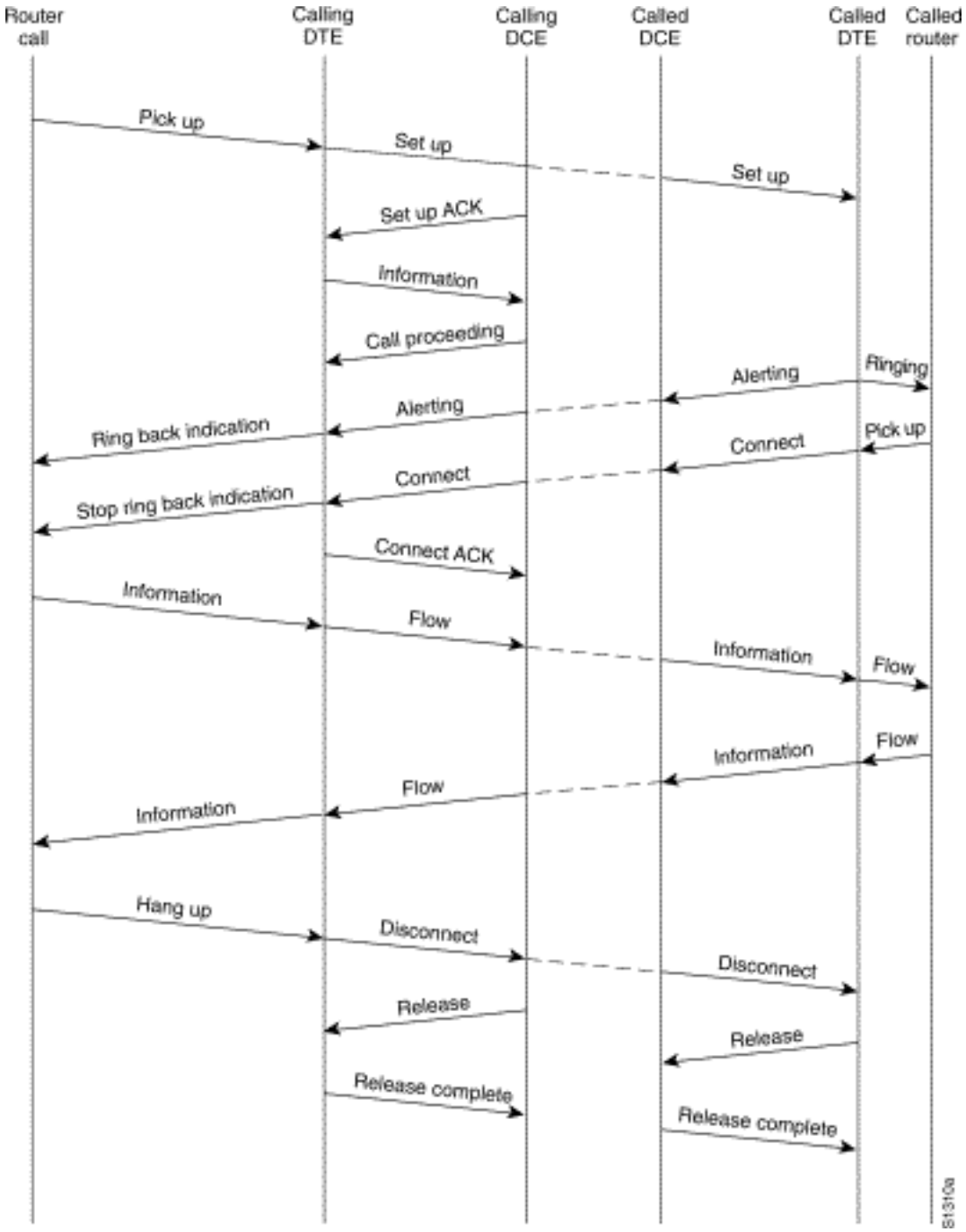

Figure 16-3 Étapes d'appel à commutation de circuits RNIS

Interprétation de la sortie Show RNIS Status

Pour connaître l'état actuel de la connexion RNIS entre le routeur et le commutateur de la compagnie de téléphone, utilisez la commande **show isdn status**. Les deux types d'interfaces pris en charge par cette commande sont BRI et PRI.

```
3620-2#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
        dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 88, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
        TEI = 97, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
```

```
Spid Status:
    TEI 88, ces = 1, state = 5(init)
        spid1 configured, no LDN, spid1 sent, spid1 valid
        Endpoint ID Info: epsf = 0, usid = 0, tid = 1
    TEI 97, ces = 2, state = 5(init)
        spid2 configured, no LDN, spid2 sent, spid2 valid
        Endpoint ID Info: epsf = 0, usid = 1, tid = 1
Layer 3 Status:
    0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
The Free Channel Mask:  0x80000003
```

Tableau 16-5 : - show isdn status for BRI

Champ	Importance
État de la couche 1 : DÉSACTIVÉ	Cela indique que l'interface BRI ne voit pas de signal sur la ligne. Il existe cinq raisons possibles à cette condition. • L'interface BRI est désactivée. Vérifiez la configuration de la commande **shutdown** sous l'interface BRI ou recherchez une indication administrativement down à partir de la commande **show interface**. Utilisez l'utilitaire de configuration et entrez **no shutdown** sous l'interface BRI. Entrez la commande **clear interface bri** à l'invite exec pour vous assurer que l'interface BRI est redémarrée. • Il existe un problème de câblage. Vous devrez remplacer le câble. Assurez-vous d'utiliser un câble droit RJ-45. Pour vérifier le câble, maintenez les extrémités du câble RJ-45 côte à côte. Si les broches sont dans le même ordre, le câble est droit. Si l'ordre des broches est inversé, le câble est enroulé. Remplacez le câble. • Le port RNIS BRI d'un routeur peut nécessiter un périphérique NT1. Dans un RNIS, NT1 est un périphérique qui fournit l'interface entre l'équipement du site du client et l'équipement de commutation du bureau central. Si le routeur ne possède pas de NT1 interne, obtenez et connectez un NT1 au port BRI. Assurez-vous que l'adaptateur BRI ou de terminal est connecté au port S/T de NT1. Reportez-vous à la documentation du fabricant pour vérifier le bon fonctionnement de la NT1 externe. • Il se peut que la ligne ne fonctionne pas. Contactez l'opérateur pour confirmer le

	fonctionnement de la connexion et vérifier les paramètres du type de commutateur. • Assurez-vous que le routeur fonctionne correctement. Si le matériel est défectueux ou défectueux, remplacez-le si nécessaire.

État de la couche 2 : État = TEI_ASSIGNED	Vérifiez le paramètre de type de commutateur et le SPIDS. Le paramètre de commutateur RNIS spécifique à l'interface remplacera le paramètre de commutateur global. L'état SPID indique si le commutateur a accepté le SPIDS (valide ou non). Contactez votre fournisseur de services pour vérifier le paramètre configuré sur le routeur. Pour modifier les paramètres SPID, utilisez la commande de configuration d'interface **isdn *spidn***. Où *n* est 1 ou 2, selon le canal en question. Utilisez la forme **no** de cette commande pour supprimer le SPID spécifié.
	`isdn spidn spid-number [ldn]`
	`no isdn spidn spid-number [ldn]`
	Description de la syntaxe:
	`spid-number`
	Numéro identifiant le service auquel vous vous êtes abonné. Cette valeur est attribuée par le fournisseur de services RNIS et correspond généralement à un numéro de téléphone à 10 chiffres avec des chiffres supplémentaires.
	`ldn`
	(Facultatif) Numéro de répertoire local (LDN), qui est un numéro à 7 chiffres attribué par le fournisseur de services. Le commutateur du message de configuration entrant fournit ces informations. Si vous n'incluez pas l'accès au répertoire local au commutateur est autorisé, mais l'autre canal B peut ne pas pouvoir recevoir d'appels entrants. Pour voir les négociations de couche 2 entre le commutateur et le routeur, utilisez la commande d'exécution privilégiée **debug isdn q921**. Les débogages q921 sont documentés dans la *référence des commandes de débogage*. Les débogages dépendent fortement des ressources du processeur, donc utilisez ces ressources avec prudence.

```
5200-1# show isdn status
Global ISDN Switchtype = primary-5ess
ISDN Serial0:23 interface
        dsl 0, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
```

```
    Activated dsl 0 CCBs = 0
    The Free Channel Mask:  0x807FFFFF
    Total Allocated ISDN CCBs = 0
5200-1#
```

Si la commande **show isdn status** ne fonctionne pas ou n'affiche pas le PRI, essayez d'utiliser la commande **show isdn service**. Assurez-vous que la commande **pri-group** apparaît dans la configuration sous le contrôleur T1/E1 dans la configuration. Si la commande n'est pas présente, configurez le contrôleur avec la commande **pri-group**.

Voici un exemple de configuration pour un routeur Cisco avec un contrôleur T1/PRI multicanal fractionné :

```
controller t1 0
framing esf
line code b8zs
pri-group timeslots 1-24
```

Tableau 16-6 : show isdn status for PRI

Champ	Importance
État de la couche 1 : DÉSACTIVÉ	Cela indique que l'interface PRI ne voit pas de tramage T1/E1 sur la ligne. Tenez compte des causes possibles suivantes pour cette condition : • L'interface PRI est arrêtée. Vérifiez la configuration de la commande **shutdown** sous l'interface serial0:23 ou recherchez une indication administrativement down à partir de la commande **show interface**. Utilisez l'utilitaire de configuration et entrez **no shutdown** sous l'interface en question. Entrez la commande **clear controller T1/E1** ***n*** à l'invite exec pour vous assurer que l'interface PRI est redémarrée. • Il existe un problème de câblage. Vous devrez remplacer le câble. Assurez-vous d'utiliser un câble droit RJ-45. Pour vérifier le câble, maintenez les extrémités du câble RJ-45 côte à côte. Si les broches sont dans le même ordre, le câble est droit. Si l'ordre des broches est inversé, le câble est enroulé. Remplacez le câble. • Il se peut que la ligne ne fonctionne pas. Contactez l'opérateur pour confirmer le fonctionnement de la connexion et vérifier les paramètres du type de commutateur. • Assurez-vous que le routeur fonctionne correctement. Si le matériel est défectueux

	ou défectueux, remplacez-le si nécessaire.
État de la couche 2 : État = TEI_ASSIGNED	Vérifiez le paramètre switchtype. Le paramètre de commutateur RNIS spécifique à l'interface remplacera le paramètre de commutateur global. Vérifiez que T1/E1 est configuré pour correspondre au commutateur du fournisseur (les problèmes T1/E1 sont abordés au chapitre 15). Pour voir les négociations de couche 2 entre le commutateur et le routeur, utilisez la commande d'exécution privilégiée **debug isdn q921**. Les débogages q921 sont documentés dans la *référence des commandes de débogage*. Les débogages dépendent fortement des ressources du processeur, donc utilisez ces ressources avec prudence.
Nombre d'appels / Blocs de contrôle d'appel en cours d'utilisation / Total des blocs de contrôle d'appel RNIS alloués	Ces numéros indiquent le nombre d'appels en cours et le nombre de ressources allouées pour prendre en charge ces appels. Si le nombre de CCB alloués est supérieur au nombre de CCB utilisés, pensez qu'il peut y avoir un problème lors de la publication des CCB. Assurez-vous que des CCB sont disponibles pour les appels entrants.

Routage à la demande : Opérations de l'interface de numérotation

Le routage à établissement de connexion à la demande (DDR) est une méthode permettant de fournir une connectivité WAN de manière économique et en fonction des besoins, soit en tant que liaison principale, soit en tant que sauvegarde pour une liaison série non commutée.

Une **interface de numérotation** est définie comme toute interface de routeur capable de passer ou de recevoir un appel. Ce terme générique doit être distingué du terme **interface de numérotation** (avec un D majuscule), qui fait référence à une interface logique configurée pour contrôler une ou plusieurs interfaces physiques d'un routeur et qui est vu dans une configuration de routeur comme interface Dialer X. À partir de maintenant, sauf indication contraire, nous utiliserons le terme dialer dans son sens générique.

La configuration de l'interface de numérotation est disponible en deux versions : basé sur une

carte de numérotation (parfois appelée DDR héritée) et des profils de numérotation. La méthode que vous utilisez dépend des circonstances dans lesquelles vous avez besoin d'une connectivité commutée. Le routage à établissement de connexion à la carte Dialer a été introduit pour la première fois dans IOS version 9.0, les profils de numérotation dans IOS version 11.2.

Déclenchement d'une numérotation

En son coeur, le routage à établissement de connexion à la demande (DDR) n'est qu'une extension du routage dans laquelle *des paquets intéressants* sont routés vers une interface de numérotation, déclenchant une tentative de numérotation. Les sections suivantes expliquent les concepts impliqués dans la définition du trafic intéressant et expliquent le routage utilisé pour les connexions DDR.

Paquets intéressants

Intéressant est le terme utilisé pour décrire les paquets ou le trafic qui déclenchera une tentative de numérotation ou, si une liaison de numérotation est déjà active, réinitialisera le compteur d'inactivité sur l'interface de numérotation. Pour qu'un paquet soit considéré comme intéressant :

- le paquet doit satisfaire aux critères d'autorisation définis par une liste d'accès
- la liste d'accès doit être référencée par la liste de numérotation ou le paquet doit être d'un protocole universellement autorisé par la liste de numérotation
- la liste de numérotation doit être associée à une interface de numérotation à l'aide d'un groupe de numérotation

Les paquets ne sont jamais automatiquement considérés comme intéressants (par défaut). Les définitions de paquets intéressantes doivent être explicitement déclarées dans une configuration de routeur ou de serveur d'accès.

Groupe de numérotation

Dans la configuration de chaque interface de numérotation sur le routeur ou le serveur d'accès, il doit y avoir une commande **dialer-group**. Si la commande **dialer-group** n'est pas présente, il n'y a pas de lien logique entre les définitions de paquets intéressantes et l'interface. Syntaxe de la commande :

```
dialer-group [group number]
```

Le numéro de groupe est le numéro du groupe d'accès au numéroteur auquel appartient l'interface spécifique. Ce groupe d'accès est défini avec la commande **dialer-list**. Les valeurs acceptables sont des entiers positifs non nuls compris entre 1 et 10.

Une interface ne peut être associée qu'à un seul groupe d'accès de numérotation ; l'affectation de groupe de numérotation multiple n'est pas autorisée. Une deuxième affectation de groupe d'accès au numéroteur remplacera la première. Un groupe d'accès de numérotation est défini à l'aide de la commande **dialer-group**. La commande **dialer-list** associe une liste d'accès à un groupe d'accès de numérotation.

Les paquets qui correspondent au groupe de numérotation spécifié déclenchent une demande de connexion.

L'adresse de destination du paquet est évaluée par rapport à la liste d'accès spécifiée dans la commande **dialer-list** associée. Si elle réussit, un appel est initié (si aucune connexion n'a déjà été établie) ou le compteur d'inactivité est réinitialisé (si un appel est actuellement connecté).

Liste des numéroteurs

La commande de configuration globale **dialer-list** permet de définir une liste de numérotation DDR pour contrôler la numérotation par protocole ou par une combinaison de protocole et de liste d'accès. Les paquets intéressants sont ceux qui correspondent à l'autorisation de niveau protocole ou qui sont autorisés par la liste dans la commande **dialer-list** : **dialer-list** *dialer-group* **protocol** *protocol-name* **{permit | refuser | list** *access-list numéro* **| access-group}**

dialer-group est le numéro d'un groupe d'accès dialer identifié dans toute commande de configuration d'interface dialer-group.

protocol-name est l'un des mots clés suivants du protocole : appletalk, bridge, clns, clns_es, clns_is, decnet, decnet_router-L1, decnet_router-L2, decnet_node, ip, ipx, vines ou xns.

permit autorise l'accès à un protocole entier.

deny refuse l'accès à un protocole entier.

list spécifie qu'une liste d'accès sera utilisée pour définir une granularité plus fine qu'un protocole entier.

access-list-number : numéros de liste d'accès spécifiés dans les listes d'accès standard ou étendues DECnet, Banyan VINES, IP, Novell IPX ou XNS, y compris les listes d'accès et les types de pontage des points d'accès de service étendu (SAP) IPX de Novell. Reportez-vous au tableau 16-7 pour connaître les types et les numéros de liste d'accès pris en charge.

access-group filter list name utilisé dans les commandes **clns filter-set** et **clns access-group**.

Tableau 16-7 : Numérotation des listes d'accès par protocole

Type de liste d'accès	Plage de numéros de liste d'accès (décimale)
AppleTalk	600-699
Banyan VINES (standard)	1-100
Banyan VINES (étendu)	101-200
DECnet	300-399
IP (standard)	1-99
IP (étendue)	100-199
Novell IPX (standard)	800-899
IPX de Novell (étendu)	900-999
Pontage transparent	200-299

XNS	500-599

Liste d'accès

Pour chaque protocole réseau à envoyer via la connexion de numérotation, une liste d'accès peut être configurée. Aux fins du contrôle des coûts, il est généralement souhaitable de configurer une liste d'accès afin d'empêcher certains trafics, tels que les mises à jour de routage, d'activer ou de conserver une connexion. Notez que lorsque nous créons des listes d'accès dans le but de définir un trafic intéressant et inintéressant, nous ne déclarons pas que les paquets non intéressants ne peuvent pas traverser la liaison de numérotation. Nous indiquons simplement qu'ils ne réinitialiseront pas le compteur d'inactivité, et qu'ils n'ouvriront pas de connexion par eux-mêmes. Tant que la connexion commutée est active, les paquets non intéressants sont toujours autorisés à circuler sur la liaison.

Par exemple, un routeur exécutant EIGRP comme protocole de routage peut avoir une liste d'accès configurée pour déclarer les paquets EIGRP inintéressants et tout autre trafic IP intéressant :

```
access-list 101 deny eigrp any any
access-list 101 permit ip any any
```

Les listes d'accès peuvent être configurées pour tous les protocoles qui peuvent traverser la liaison de numérotation. N'oubliez pas que pour tout protocole, le comportement par défaut en l'absence d'une instruction **access-list permit** est de refuser tout trafic. S'il n'y a aucune liste d'accès et aucune commande **dialer-list** autorisant le protocole, alors ce protocole ne sera pas intéressant. Dans la pratique, s'il n'y a pas de liste de numérotation pour un protocole, ces paquets ne circuleront pas du tout sur la liaison.

Exemple - Mise en pratique

Avec tous les éléments en place, vous pouvez examiner le processus complet par lequel l'état « intéressant » d'un paquet est déterminé. Dans cet exemple, IP et IPX sont les protocoles qui peuvent traverser la liaison de numérotation. L'utilisateur souhaite empêcher les diffusions et les mises à jour de routage de lancer un appel ou de maintenir la liaison active.

```
!
interface async 1
 dialer-group 7
!
access-list 121 deny eigrp any any
access-list 121 deny ip any host 255.255.255.255
access-list 121 permit ip any any
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 903 permit -1
!
dialer-list 7 protocol ip list 121
dialer-list 7 protocol ipx list 903
!
```

Un paquet doit être autorisé par les instructions **access-list 121**, avant de traverser l'**interface**

async 1, afin d'être considéré comme *intéressant*. Dans ce cas, les paquets EIGRP sont refusés, comme tous les autres paquets de diffusion, alors que tout autre trafic IP est autorisé. N'oubliez pas que cela n'empêche pas les paquets EIGRP de passer par la liaison. Cela signifie seulement que ces paquets ne réinitialiseront pas le compteur d'inactivité ou ne lanceront pas une tentative de numérotation.

De même, **access-list 903** déclare les requêtes IPX RIP, SAP et GNS inintéressantes, tandis que tout autre trafic IPX est intéressant. Sans ces instructions de refus, la connexion commutée ne serait probablement jamais arrêtée et une facture téléphonique très importante résulterait puisque les paquets de ce type circulent constamment sur un réseau IPX.

Avec **dialer-group 7** configuré sur l'interface asynchrone, nous savons que **dialer-list 7** est nécessaire pour lier les filtres de trafic intéressants (c'est-à-dire, les listes d'accès) à l'interface. Une instruction **dialer-list** est requise (et *seule* peut être configurée) pour chaque protocole, en s'assurant que le numéro de la liste dialer est identique au numéro du groupe de numérotation sur l'interface.

Encore une fois, il est important de se rappeler que les instructions *deny* dans les listes d'accès configurées pour définir le trafic intéressant *n*'empêcheront pas les paquets refusés de traverser la liaison.

À l'aide de la commande **debug dialer**, vous pouvez voir l'activité qui déclenche une tentative de numérotation :

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

Ici, nous voyons que le trafic IP dont l'adresse source est 172.16.1.111 et l'adresse de destination 172.16.2.22 a déclenché une tentative de numérotation sur l'interface Async1.

Routage

Une fois définis, les paquets intéressants doivent être routés correctement pour qu'un appel soit initié. Le processus de routage dépend de deux éléments : les entrées de la table de routage et une interface « up » sur laquelle acheminer les paquets.

Interfaces - up/up (usurpation)

Pour que les paquets soient acheminés vers et via une interface, cette interface doit être active/active comme le montre une sortie **show interfaces** :

```
Montecito# show interfaces ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is . . .
```

Qu'arrive-t-il à une interface de numérotation qui n'est pas connectée ? Si le protocole n'est pas actif et exécuté sur l'interface, cela signifie que l'interface elle-même ne sera pas active. Les routes qui dépendent de cette interface seront vidées de la table de routage et le trafic ne sera pas acheminé vers cette interface. Par conséquent, aucun appel ne sera initié par l'interface.

La solution pour contrer cette possibilité est de permettre l'état **up/up (spoofing)** pour les interfaces

de numérotation. Toute interface peut être configurée comme interface de numérotation. Par exemple, une interface série ou asynchrone peut être transformée en numéroteur en ajoutant la commande **dialer in-band** ou **dialer dtr** à la configuration de l'interface. Ces lignes sont inutiles pour les interfaces qui sont par nature une interface de numérotation (BRI et PRI). Le résultat d'une interface show ressemble à ceci :

```
Montecito# show interfaces bri 0
BRI0 is up, line protocol is up (spoofing)
  Hardware is BRI
  Internet address is . . .
```

En d'autres termes, l'interface « prétend » être **up/up** afin que les routes associées restent en vigueur et que les paquets puissent être routés vers l'interface.

Dans certaines circonstances, une interface de numérotation ne sera pas **activée (usurpation)**. La sortie **show interface** peut indiquer que l'interface est désactivée administrativement :

```
Montecito# show interfaces bri 0
BRI0 is administratively down, line protocol is down
  Hardware is BRI
  Internet address is . . .
```

Administrativement désactivée signifie simplement que l'interface a été configurée avec la commande **shutdown**. Il s'agit de l'état par défaut de toute interface de routeur lors du premier démarrage du routeur. Pour y remédier, utilisez la commande de configuration d'interface **no shutdown**.

L'interface peut également être vue en mode veille :

```
Montecito# show interfaces bri 0
BRI0 is standby mode, line protocol is down
  Hardware is BRI
  Internet address is . . .
```

Cet état indique que l'interface a été configurée comme sauvegarde pour une autre interface. Lorsqu'une connexion nécessite une redondance en cas de défaillance, une interface de numérotation peut être configurée comme sauvegarde. Pour ce faire, ajoutez les commandes suivantes à l'interface de la connexion principale :

```
backup interface [interface]
backup delay [enable-delay] [disable-delay]
```

Une fois que la commande **backup** a été configurée, l'interface utilisée comme backup sera mise en mode veille jusqu'à ce que l'interface primaire passe à un état **down/down**. À ce moment-là, l'interface de numérotation configurée en tant que sauvegarde, passe à un état **up/up (spoofing)** en attendant un événement de numérotation.

Routes statiques et routes statiques flottantes

Le meilleur moyen de router les paquets vers une interface de numérotation est le routage

statique. Ces routes sont entrées manuellement dans la configuration du routeur ou du serveur d'accès à l'aide de la commande suivante :

ip route *prefix mask* {*address* | *interface*} [*distance*]

préfixe : Préfixe de route IP pour la destination.

masque : Masque de préfixe pour la destination.

adresse : Adresse IP du tronçon suivant pouvant être utilisée pour atteindre le réseau de destination.

interface: Interface réseau à utiliser pour le trafic sortant.

distance : (Facultatif) Distance administrative. Cet argument est utilisé dans les routes statiques flottantes.

Les routes statiques sont utilisées dans les situations où la liaison de numérotation est la seule connexion au site distant. Une route statique a une valeur de distance administrative de un (1), ce qui la rend préférée aux routes dynamiques vers la même destination.

D'un autre côté, les routes statiques flottantes - c'est-à-dire les routes statiques avec une distance administrative prédéfinie - sont généralement utilisées dans les scénarios de DDR de sauvegarde. Dans ces scénarios, un protocole de routage dynamique, tel que RIP ou EIGRP, achemine les paquets sur la liaison principale.

Une route statique normale (distance administrative = 1) est préférable au protocole EIGRP (distance administrative = 90) ou au protocole RIP (distance administrative = 120). La route statique entraîne le routage des paquets sur la ligne de numérotation, même si la ligne principale est active et capable de transmettre le trafic. Si, cependant, la route statique est configurée avec une distance administrative supérieure à celle des protocoles de routage dynamique utilisés sur le routeur, la route statique flottante ne sera utilisée qu'en l'absence d'une route « meilleure » - une route avec une distance administrative inférieure.

Si le DDR de sauvegarde est appelé à l'aide de la commande d'interface de sauvegarde, la situation est quelque peu différente. Étant donné que l'interface de numérotation reste en mode veille pendant que le routeur principal est actif, une route statique ou une route statique flottante peut être configurée. L'interface de numérotation n'essaiera de se connecter qu'une fois l'interface principale désactivée/désactivée.

Pour une connexion donnée, le nombre de routes statiques (ou statiques flottantes) nécessaires est fonction de l'adressage sur les interfaces de numérotation. Dans les cas où les deux interfaces de numérotation (une sur chacun des deux routeurs) partagent un réseau ou un sous-réseau commun, généralement, une seule route statique est requise. Il pointe vers le réseau local distant en utilisant l'adresse de l'interface de numérotation du routeur distant comme adresse de tronçon suivant.

Exemples

Exemple 1 : La numérotation est la seule connexion utilisant des interfaces numérotées. Une route suffit.

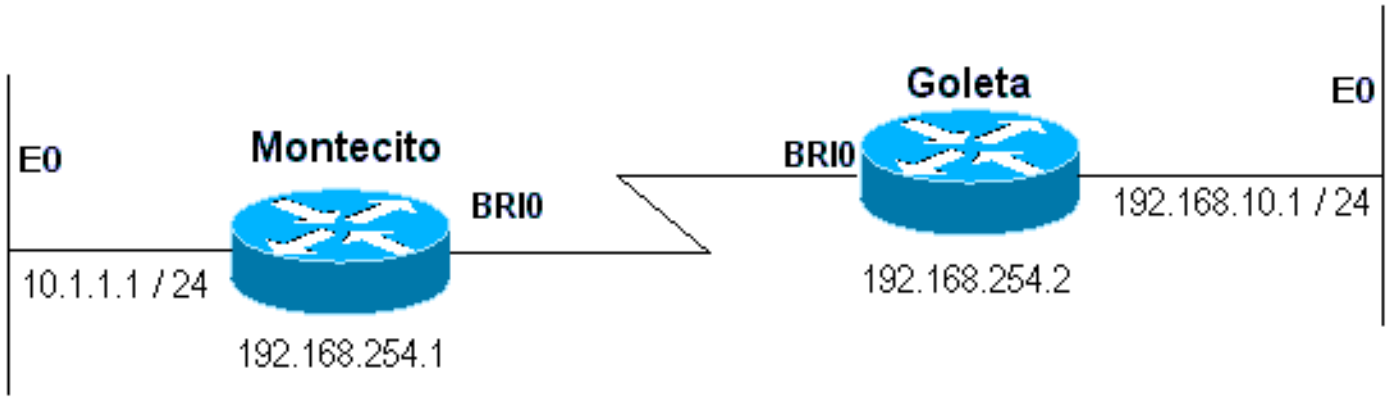

Figure 16-4 : Composer à l'aide d'interfaces numérotées

```
Montecito:
ip route 192.168.10.0 255.255.255.0 172.16.20.2
Goleta:
ip route 10.1.1.0 255.255.255.0 172.16.20.1
```

Exemple 2 : La numérotation est la seule connexion utilisant des interfaces non numérotées. Ceci peut être configuré avec une seule route, mais il est courant de configurer deux routes : une route hôte vers l'interface LAN sur le routeur distant et une route vers le LAN distant via l'interface LAN distante. Cela permet d'éviter les problèmes de mappage de couche3 à couche2, qui peuvent entraîner des échecs d'encapsulation.

Cette méthode est également utilisée si les interfaces de numérotation sur les deux périphériques sont numérotées, mais pas dans le même réseau ou sous-réseau.

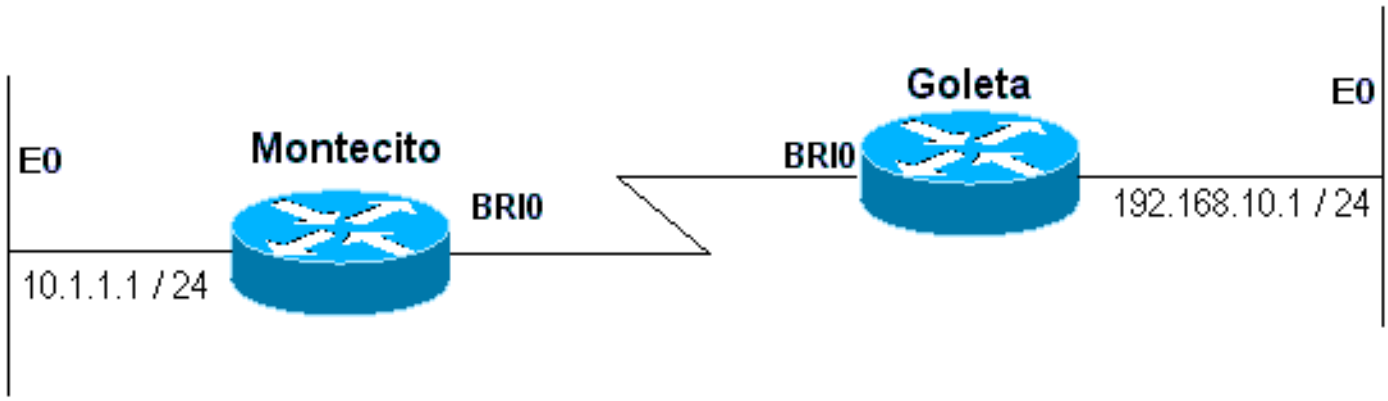

Figure 16-5 : Composer à l'aide d'interfaces non numérotées

```
Montecito:
ip route 192.168.10.0 255.255.255.0 192.168.10.1
ip route 192.168.10.1 255.255.255.255 BRI0
Goleta:
ip route 10.1.1.0 255.255.255.0 10.1.1.1
ip route 10.1.1.1 255.255.255.255 BRI0
```

Exemple 3 : La numérotation est une connexion de secours utilisant des interfaces numérotées. Une route statique flottante est requise.

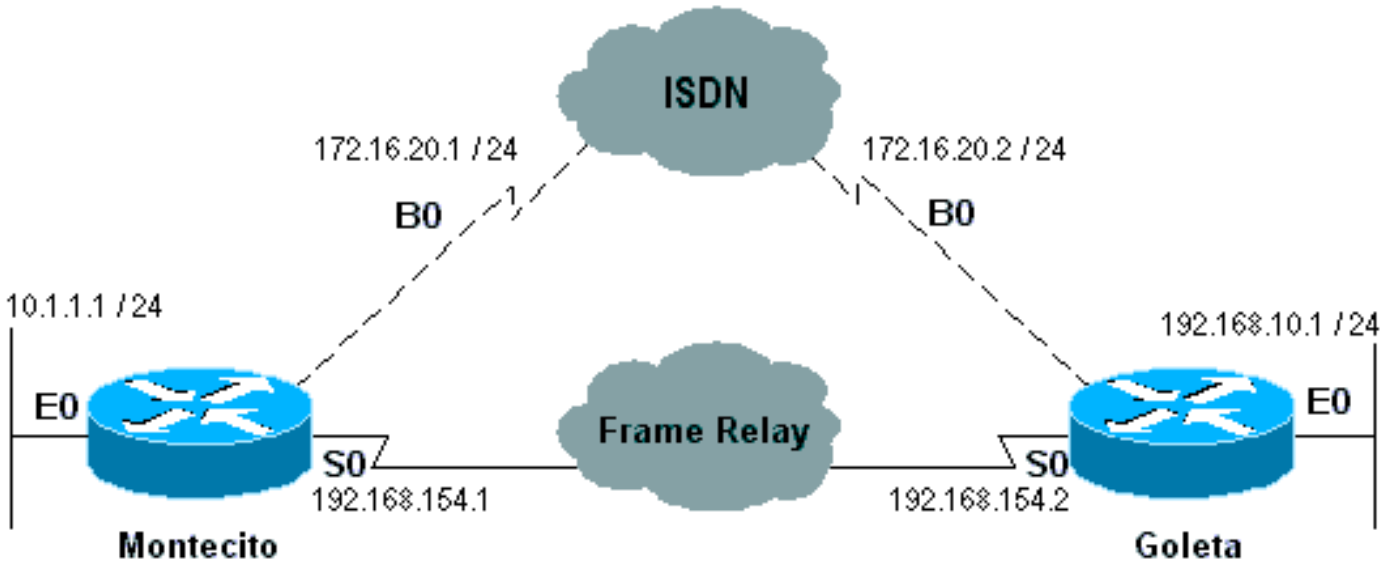

Figure 16-6 : Sauvegarde à l'aide d'interfaces numérotées

```
Montecito:
ip route 192.168.10.0 255.255.255.0 172.16.20.2 200
Goleta:
ip route 10.1.1.0 255.255.255.0 172.16.20.1 200
```

Exemple 4 : La numérotation est une connexion de secours utilisant des interfaces non numérotées. Comme dans l'exemple 2 ci-dessus, cette méthode est également utilisée si les interfaces de numérotation des deux périphériques sont numérotées, mais pas dans le même réseau ou sous-réseau.

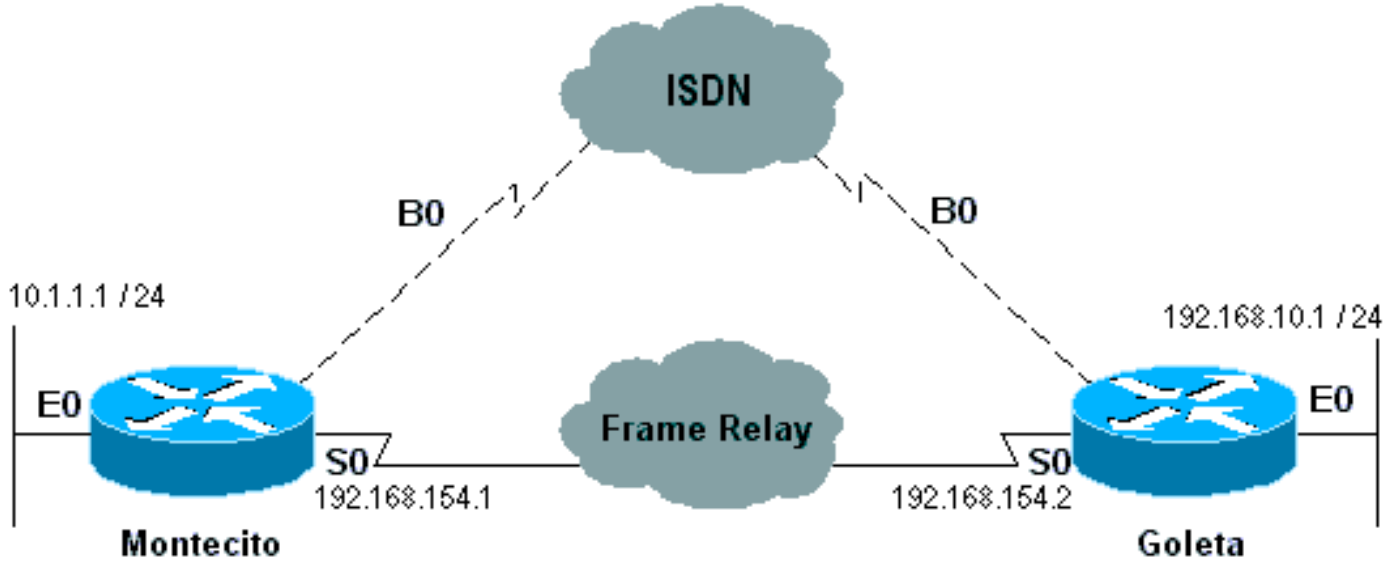

Figure 16-7 : Sauvegarde à l'aide d'interfaces non numérotées

```
Montecito:
ip route 192.168.10.0 255.255.255.0 192.168.10.1 200
ip route 192.168.10.1 255.255.255.255 BRI0 200
Goleta:
ip route 10.1.1.0 255.255.255.0 10.1.1.1 200
ip route 10.1.1.1 255.255.255.255 BRI0 200
```

Cartes de numérotation

Le routage DDR basé sur les cartes de numérotation (hérité) est puissant et complet, mais ses limites affectent l'évolutivité et l'extensibilité. Le routage à établissement de connexion à la carte du numéroteur est basé sur une liaison statique entre la spécification d'appel par destination et la configuration de l'interface physique.

Cependant, le routage à établissement de connexion à la demande (DDR) basé sur la carte de numérotation présente également de nombreux points forts. Il prend en charge Frame Relay, ISO CLNS, LAPB, le routage de clichés et tous les protocoles routés pris en charge sur les routeurs Cisco. Par défaut, le routage à établissement de connexion à la demande (DDR) Dialer Map prend en charge la commutation rapide.

Lors de la configuration d'une interface pour les appels sortants, une carte de numérotation doit être configurée pour chaque destination distante et pour chaque numéro appelé différent à la destination distante. Par exemple, si vous souhaitez une connexion PPP multiliaison lors de la composition d'une connexion RNIS BRI vers une autre interface RNIS BRI dotée d'un numéro de répertoire local différent pour chacun de ses canaux B, vous devez disposer d'une carte de numérotation pour chacun des numéros distants :

```
!
interface bri 0
 dialer map ip 172.16.20.1 name Montecito broadcast 5551234
 dialer map ip 172.16.20.1 name Montecito broadcast 5554321
!
```

L'ordre dans lequel les cartes de numérotation sont configurées peut être important. Si deux ou plusieurs commandes dialer map font référence à la même adresse distante, le routeur ou le serveur d’accès les essaiera l’une après l’autre, dans l’ordre, jusqu’à ce qu’une connexion soit établie avec succès

Remarque : IOS peut créer dynamiquement des mappages de numérotation sur un routeur recevant un appel. Le mappage de numérotation est construit en fonction du nom d'utilisateur authentifié et de l'adresse IP négociée de l'appelant. Les cartes de numérotation dynamique ne peuvent être vues que dans la sortie de la commande **show dialer map**. Vous ne pouvez pas les afficher dans la configuration en cours du routeur ou du serveur d'accès.

Syntaxe de commande

Utilisez la forme suivante de la commande de configuration d'interface **dialer map** pour :

- configurer une interface série ou une interface RNIS pour appeler un ou plusieurs sites, ou
- recevoir des appels de plusieurs sites.

Toutes les options sont affichées dans cette première forme de la commande. Pour supprimer une entrée de mappage de numérotation particulière, utilisez une forme **no** de cette commande.

```
dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
[broadcast] [modem-script modem-regexp] [system-script system-regexp]
[dial-string[:isdn-subaddress]]
```

Utilisez la forme suivante de la commande **dialer map** pour :

- configurer une interface série ou une interface RNIS pour passer un appel vers plusieurs

sites, et
- pour authentifier les appels de plusieurs sites.

```
dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
[broadcast] [dial-string[:isdn-subaddress]]
```

Utilisez la forme suivante de la commande **dialer map** pour configurer une interface série ou une interface RNIS pour prendre en charge le pontage.

```
dialer map bridge [name hostname] [spc] [broadcast] [dial-string[:isdn-subaddress]]
```

Utilisez la forme suivante de la commande **dialer map** pour configurer une interface asynchrone à laquelle passer un appel :

- un site unique qui nécessite un script système ou qui n'a pas de script de modem attribué, ou
- plusieurs sites sur une seule ligne, sur plusieurs lignes ou sur un groupe rotatif de numérotation.

```
dialer map protocol next-hop-address [name hostname] [broadcast]
[modem-script modem-regexp] [system-script system-regexp] [dial-string]
```

Description de la syntaxe

- *protocole* **-** Mots clés de protocole. Utilisez l'une des options suivantes : **appletalk, bridge, clns, decnet, ip, ipx, novell, snapshot, vines ou xns.**
- *next-hop-address* : adresse de protocole utilisée pour établir une correspondance avec les adresses auxquelles les paquets sont destinés. Cet argument n'est pas utilisé avec le mot clé **bridge** protocol.
- **name** - (Facultatif) Indique le système distant avec lequel le routeur local ou le serveur d'accès communique. Utilisé pour authentifier le système distant sur les appels entrants.
- *hostname* - (Facultatif) Nom ou ID sensible à la casse du périphérique distant (généralement le nom d'hôte). Pour les routeurs dotés d'interfaces RNIS, le champ *hostname* peut contenir le numéro fourni par l'ID de ligne appelante (dans les cas où l'identification de la ligne appelante, également appelée *CLI* , *ID de l'appelant* et *identification automatique de numéro* (ANI), est disponible).
- **spc** - (Facultatif) Spécifie une connexion semi-permanente entre l'équipement client et l'échange. Il est utilisé uniquement en Allemagne pour les circuits entre un RNIS BRI et un commutateur RNIS 1TR6 et en Australie pour les circuits entre un RNIS PRI et un commutateur TS-014.
- **vitesse 56 | 64** - (Facultatif) Mot-clé et valeur indiquant la vitesse de ligne en kilobits par seconde à utiliser. Utilisé uniquement pour RNIS. La vitesse par défaut est de 64 kbits/s.
- **broadcast** - (Facultatif) Indique que les diffusions doivent être transmises à cette adresse de protocole.
- **modem-script** - (Facultatif) Indique le script de modem à utiliser pour la connexion (pour les interfaces asynchrones).
- *modem-regexp* - (Facultatif) Expression régulière à laquelle un script de modem sera associé (pour les interfaces asynchrones).
- **system-script** - (Facultatif) Indique le script système à utiliser pour la connexion (pour les interfaces asynchrones).

- *system-regexp* - (Facultatif) Expression régulière à laquelle un script système sera associé (pour les interfaces asynchrones).
- *dial-string[:isdn-subaddress]* (Facultatif) Numéro de téléphone envoyé au périphérique de numérotation lors de la reconnaissance de paquets avec une adresse de tronçon suivant spécifiée qui correspond à la liste d'accès définie (et le numéro de sous-adresse facultatif utilisé pour les connexions multipoints RNIS). La chaîne de numérotation et la sous-adresse RNIS, si elles sont utilisées, doivent être le dernier élément de la ligne de commande.

Profils de numérotation

Remarque : dans cette section, le terme « interface de numérotation » fait référence à l'interface configurée ; pas à une interface physique sur le routeur ou le serveur d'accès.

L'implémentation des profils de numérotation de DDR, introduite dans IOS version 11.2, est basée sur une séparation entre la configuration d'interface logique et physique. Les profils de numérotation permettent également de lier dynamiquement les configurations logiques et physiques à chaque appel.

La méthodologie Profils de numérotation est avantageuse lorsque vous souhaitez effectuer les opérations suivantes :

- Partager une interface (RNIS, asynchrone ou série synchrone) pour passer ou recevoir des appels
- modifier n'importe quelle configuration par utilisateur (à l'exception de l'encapsulation dans la première phase des profils de numérotation)
- Passerelle vers de nombreuses destinations
- éviter les problèmes de découpage d'horizon

Les profils de numérotation permettent de séparer la configuration des interfaces physiques de la configuration logique requise pour un appel, et permettent également de lier les configurations logique et physique de manière dynamique par appel.

Un *profil de numérotation* comprend les éléments suivants :

- Une configuration *d'interface de numérotation* (entité logique), comprenant une ou plusieurs chaînes de numérotation (chacune étant utilisée pour atteindre un sous-réseau de destination)
- Une classe *de mappage de numérotation* qui définit toutes les caractéristiques d'un appel vers la chaîne de numérotation spécifiée
- Un *pool de numérotation* ordonné d'interfaces physiques à utiliser par l'interface de numérotation

Tous les appels allant vers ou depuis le même sous-réseau de destination utilisent le même profil de numérotation.

Une configuration d’interface de numérotation inclut tous les paramètres nécessaires pour atteindre un sous-réseau de destination spécifique (ainsi que tous les réseaux qui y sont accessibles). Plusieurs chaînes de numérotation peuvent être spécifiées pour la même interface de numérotation ; chaque chaîne de numérotation peut être associée à une classe dialer map différente. La classe de mappage de numérotation définit toutes les caractéristiques d'un appel vers la chaîne de numérotation spécifiée. Par exemple, la classe de mappage pour une destination peut spécifier une vitesse RNIS de 56 kbits/s. La classe de mappage pour une autre

destination peut spécifier une vitesse RNIS de 64 kbits/s.

Chaque interface de numérotation utilise un pool de numérotation, qui est un pool d'interfaces physiques triées en fonction de la priorité attribuée à chaque interface physique. Une interface physique peut appartenir à plusieurs pools de numérotation, les conflits étant résolus par priorité. Les interfaces RNIS BRI et PRI peuvent définir une limite sur le nombre minimal et maximal de canaux B réservés par les pools de numérotation. Un canal réservé par un pool de numérotation reste inactif jusqu'à ce que le trafic soit dirigé vers le pool.

Lorsque les profils de numérotation sont utilisés pour configurer le routage à établissement de connexion à la demande (DDR), aucune interface physique ne comporte de paramètres de configuration, à l'exception de l'encapsulation et des pools de numérotation auxquels l'interface appartient.

Note : Le paragraphe précédent comporte une exception. Les commandes qui s'appliquent avant la fin de l'authentification doivent être configurées sur l'interface physique (ou BRI ou PRI) et non sur le profil de numérotation. Les profils de numérotation ne copient pas les commandes d'authentification PPP (ou les commandes LCP) sur l'interface physique.

La figure 16-8 illustre une application type de profils de numérotation. Le routeur A dispose de l'interface de numérotation 1 pour le routage à établissement de connexion à la demande avec le sous-réseau 1.1.1.0 et de l'interface de numérotation 2 pour le routage à établissement de connexion à la demande avec le sous-réseau 2.2.2.0. L’adresse IP de l’interface de numérotation 1 est son adresse en tant que noeud du réseau 1.1.1.0. En même temps, cette adresse IP sert d'adresse IP des interfaces physiques utilisées par l'interface de numérotation 1. De même, l'adresse IP de l'interface de numérotation 2 est son adresse en tant que noeud dans le réseau 2.2.2.0.

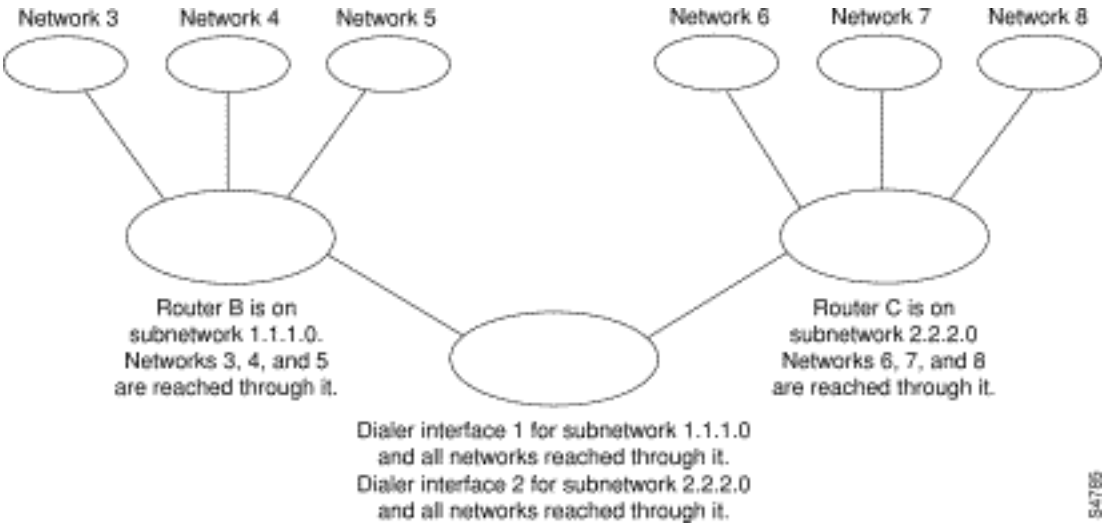

Figure 16-8 : Application de profils de numérotation standard

Une interface de numérotation utilise un seul pool de numérotation. Cependant, une interface physique peut être membre d'un ou de plusieurs pools de numérotation et un pool de numérotation peut avoir plusieurs interfaces physiques en tant que membres.

La figure 16-9 illustre les relations entre les concepts d'interface de numérotation, de pool de numérotation et d'interfaces physiques. L'interface de numérotation 0 utilise le pool de numérotation 2. L'interface physique BRI 1 appartient au pool de numérotation 2 et a une priorité spécifique dans le pool. L'interface physique BRI 2 appartient également au groupe de numérotation 2. Étant donné que les conflits sont résolus sur la base des niveaux de priorité des

interfaces physiques du pool, les priorités de l'accès de base de données BRI 1 et BRI 2 doivent être affectées à différentes priorités dans le pool. Peut-être la priorité 100 est attribuée à BRI 1 et la priorité 50 à BRI 2 dans le groupe de numérotation 2 (une priorité de 50 est supérieure à une priorité de 100). BRI 2 a une priorité plus élevée dans le pool et ses appels seront placés en premier.

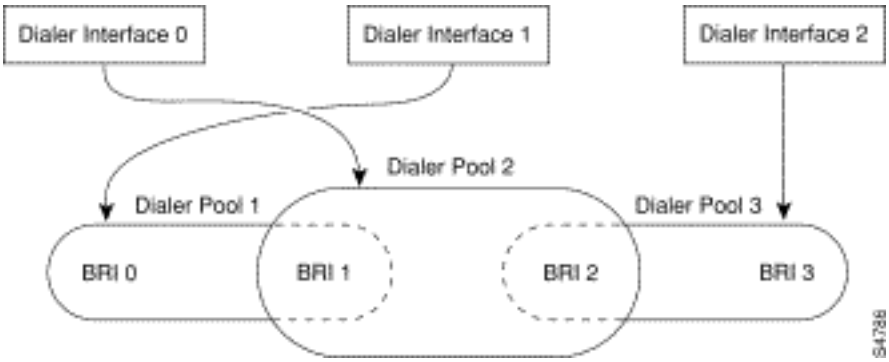

Figure 16-9 : Relations entre les interfaces de numérotation, les pools de numérotation et les interfaces physiques

Étapes de configuration du profil du numéroteur

Commande	Objectif
numéro de numéroteur d'interface	Créez une interface de numérotation.
masque d'adresse **ip**	Spécifiez l'adresse IP et le masque de l'interface de numérotation en tant que noeud du réseau de destination à appeler.
encapsulation ppp	Spécifiez l'encapsulation PPP.
dialer remote-name *username*	Spécifiez le nom d'authentification CHAP du routeur distant.
dialer string *dial-string* **class** *class-name*	Spécifiez la destination distante à appeler et la classe de mappage qui définit les caractéristiques des appels destinés à cette destination.
numéro de pool **de** *numérotation*	Spécifiez le pool de composition à utiliser pour les appels destinés à cette destination.
dialer-group *group-number*	Attribuez l'interface de numérotation à un groupe de numérotation.
dialer-list *dialer-group* **protocol** *protocol-name* **{permit | refuser | list** *access-list numéro***}**	Spécifiez une liste d'accès par numéro de liste ou par protocole et numéro de liste pour définir les paquets « intéressants » qui peuvent déclencher un appel.

Opérations PPP

Le protocole PPP (Point-to-Point Protocol) est de loin le protocole de transport de couche de liaison le plus courant, ayant complètement usurpé SLIP comme protocole de choix pour les connexions série synchrones et asynchrones commutées (et dans de nombreux cas non commutées). Le protocole PPP a été défini à l'origine en 1989 par la RFC 1134, qui a depuis été rendue obsolète par une série de RFC culminant (à l'heure de la rédaction de cet article) dans la RFC 1661. Il existe également de nombreuses RFC qui définissent des éléments du protocole, tels que RFC1990 (le protocole PPP multiliaison), RFC2125 (le protocole PPP d'allocation de bande passante), et bien d'autres. Un référentiel en ligne des RFC est disponible à l'adresse suivante :

http://www.ietf.org/rfc.html

La meilleure définition du protocole PPP se trouve peut-être dans le document RFC1661, qui stipule :

Le protocole point à point (PPP) fournit une méthode standard pour le transport de datagrammes multiprotocoles sur les liaisons de point à point. Le PPP est composé de trois éléments principaux :

1. Méthode d'encapsulation de datagrammes multiprotocoles.
2. Protocole LCP (Link Control Protocol) permettant d'établir, de configurer et de tester la connexion de liaison de données.
3. Famille de protocoles de contrôle de réseau (NCP) permettant d'établir et de configurer différents protocoles de couche réseau.

Phases de la négociation PPP

La négociation PPP se compose de trois phases : LCP (Link Control Protocol), Authentification et NCP (Network Control Protocol). Chaque opération est effectuée dans l'ordre, après l'établissement de la connexion asynchrone ou RNIS.

LCP

PPP ne suit pas de modèle client/serveur. Toutes les connexions sont peer-to-peer. Par conséquent, lorsqu'il y a un appelant et un récepteur, les deux extrémités de la connexion point à point doivent convenir des protocoles et paramètres négociés.

Lorsque la négociation commence, chacun des homologues souhaitant établir une connexion PPP doit envoyer une requête de configuration (voir dans la **négociation debug ppp** et appelée ci-après CONFREQ). Les options qui ne sont pas la liaison par défaut sont incluses dans CONFREQ. Il s'agit souvent de l'unité de réception maximale (MRU), de l'ACCM (Async Control Character Map), du protocole d'authentification (AuthProto) et du numéro magique. On peut également voir les unités MRRU (Maximum Receive Reconstructed Unit) et Endpoint Discriminator (EndpointDisc), utilisées pour le protocole PPP multiliaison.

Il existe trois réponses possibles à toute CONFREQ :

- Un message Configure-AcKnowledge (CONFACK) doit être émis si l'homologue reconnaît les options et accepte les valeurs affichées dans CONFREQ.
- Un message Configure-Reject (CONFREJ) doit être envoyé si l'une des options de CONFREQ n'est pas reconnue (par exemple, certaines options spécifiques au fournisseur) ou

si les valeurs de l'une des options ont été explicitement interdites dans la configuration de l'homologue.
- Un CONFNAK (Configure-Negative-Acknow) doit être envoyé si toutes les options de CONFREQ sont reconnues, mais les valeurs ne sont pas acceptables pour l'homologue.

Les deux homologues continuent d'échanger des CONFREQ, des CONFREJ et des CONFNAK jusqu'à ce que chacun envoie un CONFACK, jusqu'à ce que la connexion de numérotation soit interrompue ou jusqu'à ce que l'un ou les deux des homologues indique que la négociation ne peut pas être terminée.

Authentification

Une fois la négociation LCP terminée et l'accord sur AuthProto conclu, l'étape suivante est l'authentification. L'authentification, bien qu'elle ne soit pas obligatoire par RFC1661, est fortement recommandée pour toutes les connexions de numérotation. Dans certains cas, il s'agit d'une exigence de bon fonctionnement ; Les profils de numérotation en sont un exemple.

Les deux principaux types d'authentification dans PPP sont le protocole d'authentification par mot de passe (PAP) et le protocole d'authentification à échanges confirmés (CHAP), définis par la RFC1334 et mis à jour par la RFC1994.

Le protocole PAP est le plus simple des deux, mais il est moins sécurisé car le mot de passe en texte clair est envoyé via la connexion de numérotation. Le protocole CHAP est plus sécurisé car le mot de passe en texte clair n'est jamais envoyé via la connexion de numérotation.

Le protocole PAP peut être nécessaire dans l'un des environnements suivants :

- Une vaste base installée d'applications clientes qui ne prennent pas en charge CHAP
- Incompatibilités entre les implémentations de différents fournisseurs de CHAP

Lors de la discussion de l'authentification, il est utile d'utiliser les termes « demandeur » et « authentificateur » pour distinguer les rôles joués par les périphériques à chaque extrémité de la connexion, bien que l'un ou l'autre des homologues puisse agir dans l'un ou l'autre des rôles. « Demandeur » décrit le périphérique qui demande l'accès au réseau et fournit des informations d'authentification ; l'« authentificateur » vérifie la validité des informations d'authentification et autorise ou désautorise la connexion. Il est courant que les deux homologues agissent dans les deux rôles lorsqu'une connexion DDR est établie entre les routeurs.

PAP

Le protocole PAP est assez simple. Une fois la négociation LCP terminée, le demandeur envoie à plusieurs reprises sa combinaison nom d'utilisateur/mot de passe sur la liaison jusqu'à ce que l'authentificateur réponde par un accusé de réception ou jusqu'à ce que la liaison soit rompue. L'authentificateur peut déconnecter la liaison s'il détermine que la combinaison nom d'utilisateur/mot de passe n'est pas valide.

CHAP

Le protocole CHAP est un peu plus compliqué. L'authentificateur envoie une demande de confirmation au demandeur, qui répond ensuite avec une valeur. Cette valeur est calculée à l'aide d'une fonction de hachage unidirectionnel pour hacher ensemble le défi et le mot de passe CHAP. La valeur résultante est envoyée à l'authentificateur avec le nom d'hôte CHAP du demandeur (qui

peut être différent de son nom d'hôte réel) dans un message de *réponse*.

L'authentificateur lit le nom d'hôte dans le message de réponse, recherche le mot de passe attendu pour ce nom d'hôte, puis calcule la valeur qu'il attend du demandeur envoyé dans sa réponse en exécutant la même fonction de hachage que celle du demandeur. Si les valeurs résultantes correspondent, l'authentification réussit. La défaillance doit conduire à une déconnexion.

AAA

Un service AAA (Authentication, Authorization and Accounting), tel que TACACS+ ou RADIUS, peut être utilisé pour exécuter PAP ou CHAP.

NCP

Après une authentification réussie, la phase NCP commence. Comme dans le protocole LCP, les homologues échangent des CONFREQ, des CONFREJ, des CONFNAK et des CONFACK. Cependant, dans cette phase de négociation, les éléments en cours de négociation ont à voir avec les protocoles de couche supérieure - IP, IPX, Bridging, CDP, etc. Un ou plusieurs de ces protocoles peuvent être négociés. Comme il s'agit du protocole le plus couramment utilisé et que d'autres protocoles fonctionnent à peu près de la même manière, le protocole IPCP (1Internet Protocol Control Protocol2), défini dans la RFC1332, est au coeur de cette discussion. Les autres documents RFC pertinents comprennent, mais ne se limitent pas à :

- RFC1552 (protocole de contrôle IPX)
- RFC1378 (protocole de contrôle AppleTalk)
- RFC1638 (Bridging Control Protocol)
- RFC1762 (protocole de contrôle DECnet)
- RFC1763 (Vines Control Protocol)

En outre, le protocole CDPCP (Cisco Discovery Protocol Control Protocol) peut être négocié pendant le protocole NCP, bien que ce ne soit pas courant. Les ingénieurs du centre d'assistance technique Cisco vous conseillent généralement de configurer la commande no cdp enable sur n'importe quelle interface de numérotation afin d'empêcher les paquets CDP de maintenir un appel indéfiniment.

L'élément clé négocié dans IPCP est l'adresse de chaque homologue. Chacun des homologues se trouve dans l'un des deux états possibles ; soit il a une adresse IP, soit il ne l'a pas. Si l'homologue a déjà une adresse, il l'enverra dans un CONFREQ à l'autre homologue. Si l'adresse est acceptable pour l'autre homologue, un CONFACK sera retourné. Si l'adresse n'est pas acceptable, la réponse sera une CONFNAK contenant une adresse que l'homologue doit utiliser.

Si l'homologue n'a pas d'adresse, il envoie un CONFREQ avec l'adresse 0.0.0.0. Ceci indique à l'autre homologue d'attribuer une adresse, ce qui est accompli par l'envoi d'une CONFNAK avec l'adresse appropriée.

D'autres options peuvent être négociées dans IPCP. Les adresses principales et secondaires du serveur de noms de domaine et du serveur de noms NetBIOS sont généralement visibles, comme décrit dans la RFC1877 d'information. Le protocole de compression IP (RFC1332) est également courant.

Méthodes PPP alternatives

Les autres méthodologies PPP incluent le protocole PPP multiliaison, le protocole PPP multichâssis et les profils virtuels.

Multilink PPP

La fonctionnalité MLP (Multilink Point-to-Point Protocol) assure l'équilibrage de charge sur plusieurs liaisons WAN. En même temps, il assure l'interopérabilité multifournisseur, la fragmentation des paquets et le séquençage approprié, ainsi que le calcul de charge sur le trafic entrant et sortant. La mise en oeuvre de Multilink PPP par Cisco prend en charge les spécifications de fragmentation et de séquençage de paquets du document RFC1717.

Le protocole PPP multiliaison permet de fragmenter les paquets. Ces fragments peuvent être envoyés simultanément sur plusieurs liaisons point à point vers la même adresse distante. Les liaisons multiples apparaissent en réponse à un seuil de charge de numérotation que vous définissez. La charge peut être calculée sur le trafic entrant, le trafic sortant, ou sur l'un ou l'autre, selon les besoins pour le trafic entre les sites spécifiques. MLP fournit de la bande passante à la demande et réduit la latence de transmission sur les liaisons WAN.

Le protocole PPP multiliaison fonctionne sur les types d'interface suivants (simple ou multiple) configurés pour prendre en charge les groupes rotatifs à établissement de connexion à la demande et l'encapsulation PPP :

- Interfaces série asynchrones
- BRI
- PRI

Configuration

Pour configurer Multilink PPP sur des interfaces asynchrones, vous devez configurer les interfaces asynchrones pour prendre en charge l'encapsulation DDR et PPP. Vous configurez ensuite une interface de numérotation pour prendre en charge l'encapsulation PPP, la bande passante à la demande et le protocole PPP multiliaison. Cependant, à un certain point, l'ajout d'interfaces asynchrones n'améliore pas les performances. Avec la taille de MTU par défaut, Multilink PPP doit prendre en charge trois interfaces asynchrones utilisant des modems V.34. Cependant, les paquets peuvent être abandonnés occasionnellement si le MTU est petit ou si de grandes rafales de trames courtes surviennent.

Pour activer le protocole PPP multiliaison sur une seule interface RNIS BRI ou PRI, vous n'êtes pas tenu de définir un groupe de numérotation rotatif séparément, car les interfaces RNIS sont des groupes de numérotation rotatifs par défaut. Si vous n'utilisez pas de procédures d'authentification PPP, votre service téléphonique doit transmettre les informations d'identification de l'appelant.

Un numéro de seuil de charge est requis. Pour obtenir un exemple de configuration du protocole PPP multiliaison sur une interface RNIS BRI unique, reportez-vous à *Exemple de protocole PPP multiliaison sur une interface RNIS* ci-dessous.

Lorsque le protocole PPP multiliaison est configuré et que vous souhaitez connecter indéfiniment un bundle multiliaison, utilisez la commande **dialer idle-timeout** pour définir un compteur d'inactivité très élevé. La commande **dialer-load threshold 1** ne permet pas de maintenir un ensemble multiliaison de *n liaisons connectées indéfiniment, et la* commande **dialer-load threshold**

2 ne permet pas de maintenir un ensemble multiliaison de deux liaisons connectées indéfiniment.

Pour activer le protocole PPP multiliaison sur plusieurs interfaces RNIS BRI ou PRI, vous devez configurer une interface rotative Dialer et la configurer pour le protocole PPP multiliaison. Vous configurez ensuite les BRI séparément et les ajoutez chacun au même groupe rotatif. Reportez-vous à l'*exemple de protocole PPP multiliaison sur plusieurs interfaces RNIS* ci-dessous.

Exemple de protocole PPP multiliaison sur une interface RNIS

L'exemple suivant active Multilink PPP sur l'interface BRI 0. Lorsqu'un BRI est configuré, aucune configuration de groupe rotatif de numérotation n'est requise (l'interface RNIS est un groupe rotatif par défaut).

```
interface bri 0
ip address 171.1.1.7 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 30
 dialer load-threshold 40 either
 dialer map ip 172.16.20.2 name Goleta 5551212
 dialer-group 1
 ppp authentication pap
 ppp multilink
```

Exemple de protocole PPP multiliaison sur plusieurs interfaces RNIS

L'exemple suivant configure plusieurs BRI RNIS pour appartenir au même groupe de numérotation rotatif pour Multilink PPP. Utilisez la commande **dialer rotatif-group** pour affecter chacun des accès de base RNIS à ce groupe rotatif de numérotation qui doit correspondre au numéro de l'interface de numérotation (numéro 0 dans ce cas).

```
interface BRI0
 no ip address
 encapsulation ppp
 dialer rotary-group 0
!
interface BRI1
 no ip address
 encapsulation ppp
 dialer rotary-group 0
!
interface Dialer0
 ip address 172.16.20.1 255.255.255.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 172.16.20.2 name Goleta broadcast 5551212
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

PPP multiliaison multichâssis

Le protocole PPP multiliaison permet de fractionner et de recombiner des paquets vers un seul

système d'extrémité sur un canal logique (également appelé *bundle*) formé de plusieurs liaisons. Le protocole PPP multiliaison fournit de la bande passante à la demande et réduit la latence de transmission sur les liaisons WAN.

Le protocole MMP (Multichassis Multilink PPP), en revanche, offre la possibilité supplémentaire pour les liaisons de se terminer sur plusieurs routeurs avec des adresses distantes différentes. MMP peut également gérer le trafic analogique et numérique.

Cette fonctionnalité est destinée aux situations dans lesquelles il existe de grands pools d'utilisateurs commutés, dans lesquels un seul serveur d'accès ne peut pas fournir suffisamment de ports commutés. MMP permet aux entreprises de fournir un numéro d'accès unique à ses utilisateurs et d'appliquer la même solution aux appels analogiques et numériques. Cette fonctionnalité permet aux fournisseurs de services Internet, par exemple, d'attribuer un numéro rotatif RNIS unique à plusieurs PRI RNIS sur plusieurs routeurs.

Pour obtenir une description complète des commandes MMP mentionnées dans le présent document, reportez-vous à la *référence des commandes des solutions de numérotation Cisco*. Pour rechercher la documentation des autres commandes qui apparaissent dans ce chapitre, utilisez l'index maître de référence de commande ou effectuez une recherche en ligne.

Le protocole MMP est pris en charge sur les plates-formes des gammes Cisco 7500, 4500 et 2500 et sur les interfaces série synchrones, série asynchrone, RNIS BRI, RNIS PRI et numéroteur.

Le protocole MMP ne nécessite pas de reconfiguration des commutateurs de compagnie de téléphone.

Configuration

Les routeurs ou les serveurs d'accès sont configurés pour appartenir à des groupes d'homologues, appelés *groupes de pile*. Tous les membres du groupe de pile sont des homologues ; les groupes de piles n'ont pas besoin d'un routeur principal permanent. Tout membre d'un groupe de pile peut répondre à des appels provenant d'un numéro d'accès unique, qui est généralement un groupe de recherche RNIS PRI. Les appels peuvent provenir de périphériques utilisateur distants, tels que des routeurs, des modems, des cartes de terminal RNIS ou des cartes PC.

Une fois qu'une connexion est établie avec un membre d'un *groupe de pile*, ce membre est propriétaire de l'appel. Si un deuxième appel provient du même client et qu'un autre routeur répond à l'appel, le routeur établit un tunnel et transfère tous les paquets appartenant à l'appel au routeur qui est propriétaire de l'appel. Le processus d'établissement d'un tunnel et de transfert d'appels via celui-ci vers le routeur propriétaire de l'appel est parfois appelé *projection de la liaison PPP vers le maître d'appels*.

Si un routeur plus puissant est disponible, il peut être configuré en tant que membre du groupe de pile et les autres membres du groupe de pile peuvent établir des tunnels et lui transférer tous les appels. Dans ce cas, les autres membres du groupe de pile répondent aux appels et transfèrent le trafic vers le routeur *de déchargement* le plus puissant.

Remarque : Les lignes WAN à latence élevée entre les membres du groupe de pile peuvent rendre le fonctionnement du groupe de piles inefficace.

Les opérations de traitement des appels MMP, d'appel d'offres et de transfert de couche 2 dans le

groupe de pile se déroulent comme suit. Elle est également illustrée à la figure 16-10.

1. Lorsque le premier appel arrive au groupe de piles, le routeur A répond.
2. Dans l'appel d'offres, le routeur A gagne car il a déjà l'appel. Le routeur A devient le *maître d'appels* pour cette session avec le périphérique distant. Le routeur A peut également être appelé *hôte de l'interface de l'ensemble maître*.
3. Lorsque le périphérique distant qui a initié l'appel a besoin de plus de bande passante, il effectue un deuxième appel PPP multiliaison au groupe.
4. Lorsque le deuxième appel arrive, le routeur D le répond et informe le groupe de pile. Le routeur A remporte l'appel d'offres car il gère déjà la session avec ce périphérique distant.
5. Le routeur D établit un tunnel vers le routeur A et transfère les données PPP brutes vers le routeur A.
6. Le routeur A réassemble et séquence les paquets.
7. Si d'autres appels arrivent sur le routeur D et qu'ils appartiennent également au routeur A, le tunnel entre A et D s'agrandit pour gérer le trafic ajouté. Le routeur D n'établit pas de tunnel supplémentaire vers A.
8. Si d'autres appels arrivent et reçoivent une réponse d'un autre routeur, ce routeur établit également un tunnel vers A et transfère les données PPP brutes.
9. Les données réassemblées sont transmises sur le réseau d'entreprise comme si elles étaient toutes issues d'une liaison physique.

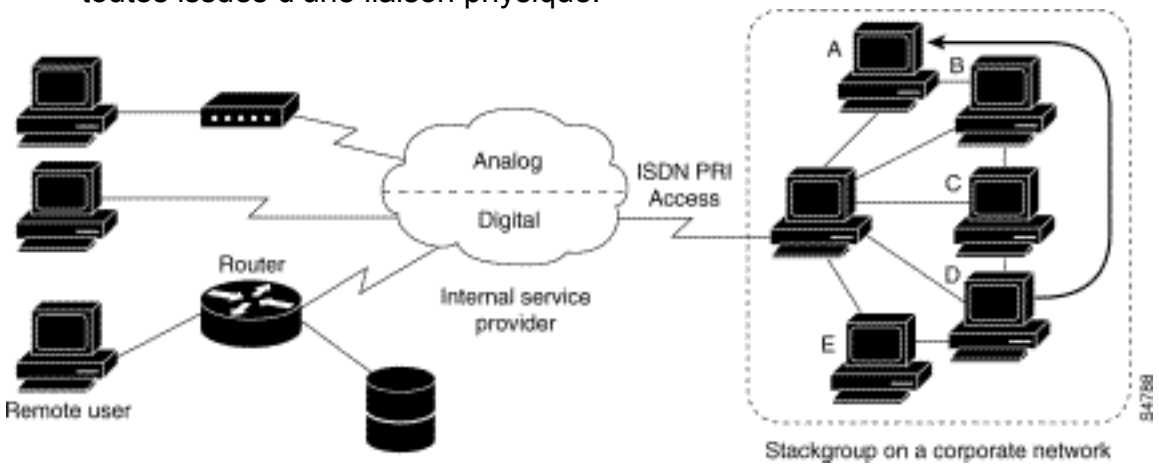

Figure 16-10 : Scénario PPP multiliaison multichâssis type

Contrairement à la figure précédente, la figure 16-11 présente un routeur de déchargement. Les serveurs d'accès qui appartiennent à un groupe de pile répondent aux appels, établissent des tunnels et transfèrent les appels vers un routeur Cisco 4700 qui remporte l'appel d'offres et est le maître d'appels pour tous les appels. Le Cisco 4700 réassemble et reséquence tous les paquets entrant par le biais du groupe de piles.

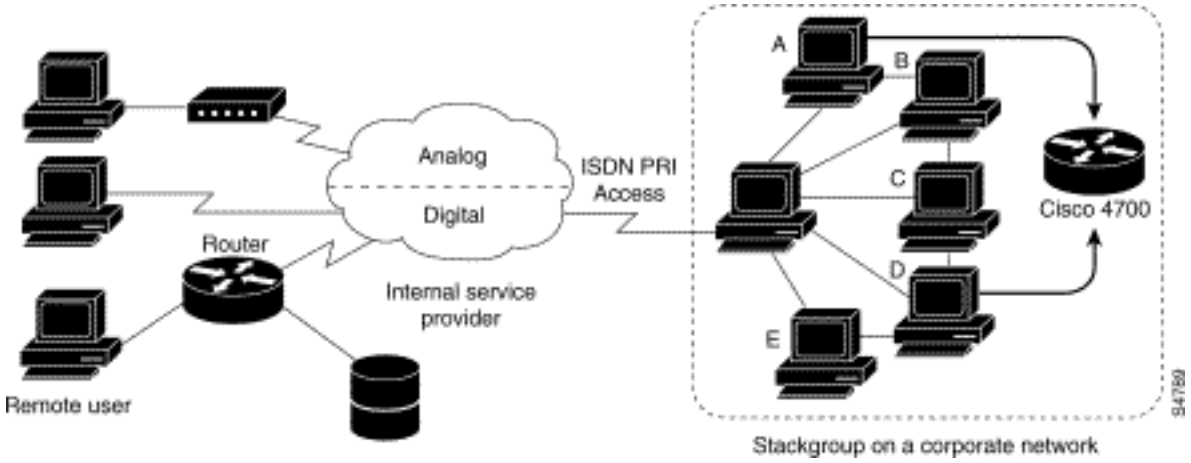

Figure 16-11 : Multichassis Multilink PPP avec un routeur de déchargement en tant que membre du groupe de pile

Remarque : Vous pouvez créer des groupes de piles à l'aide de différentes plates-formes de serveurs d'accès, de commutation et de routeurs. Cependant, les serveurs d'accès universel tels que le Cisco AS5200 ne doivent pas être combinés à RNIS. Cela ne doit être fait qu'avec des serveurs d'accès tels que la plate-forme 4x00. Étant donné que les appels provenant du bureau central sont alloués de manière arbitraire, cette combinaison pourrait entraîner la transmission d'un appel analogique à un serveur d'accès numérique uniquement, qui ne serait pas en mesure de traiter l'appel.

La prise en charge de MMP sur un groupe de routeurs nécessite que chaque routeur soit configuré pour prendre en charge les éléments suivants :

- Multilink PPP
- Protocole SGBP (Stack Group Bidding Protocol)
- Modèle virtuel utilisé pour le clonage de la configuration d'interface pour prendre en charge MMP

Profils virtuels

Les profils virtuels sont une application PPP (Point-to-Point Protocol) unique qui peut créer et configurer une interface d'accès virtuel de manière dynamique lorsqu'un appel entrant est reçu et désactiver l'interface de manière dynamique lorsque l'appel se termine. Les profils virtuels fonctionnent avec le protocole PPP simple et avec le protocole MLP (Multilink PPP).

Les informations de configuration d'une interface d'accès virtuel Profiles peuvent provenir d'une interface de modèle virtuel, ou d'une configuration spécifique à l'utilisateur stockée sur un serveur AAA (Authentication, Authorization, and Accounting), ou les deux.

La configuration AAA spécifique à l'utilisateur utilisée par les profils virtuels est une configuration *d'interface* et est téléchargée pendant les négociations LCP. Une autre fonctionnalité, appelée Configuration par utilisateur, utilise également les informations de configuration obtenues à partir d'un serveur AAA. Cependant, la configuration par utilisateur utilise la configuration *réseau* (telles que les listes d'accès et les filtres de route) téléchargée lors des négociations NCP.

Deux règles régissent la configuration d'interface d'accès virtuel par les interfaces de modèle virtuel de profils virtuels et les configurations AAA :

- Chaque application d'accès virtuel peut avoir au maximum un modèle à partir duquel cloner. Cependant, il peut avoir plusieurs configurations AAA à partir desquelles cloner (informations de Virtual Profiles AAA et configuration AAA par utilisateur, qui peuvent à leur tour inclure la configuration pour plusieurs protocoles).
- Lorsque les profils virtuels sont configurés par modèle virtuel, leur modèle a une priorité plus élevée que tout autre modèle virtuel.

Reportez-vous à la section Interopérabilité avec d'autres fonctions de numérotation Cisco ci-dessous pour obtenir une description des séquences de configuration possibles qui dépendent de la présence ou de l'absence de MLP ou d'une autre fonction d'accès virtuel qui clone une interface de modèle virtuel.

Cette fonctionnalité s'exécute sur toutes les plates-formes Cisco IOS qui prennent en charge MLP.

Pour obtenir une description complète des commandes mentionnées dans cette section, reportez-vous au chapitre « Commandes de profils virtuels » de la *Référence des commandes des solutions de numérotation* dans le jeu de documentation Cisco IOS. Pour rechercher la documentation des autres commandes qui apparaissent dans ce chapitre, vous pouvez utiliser l'index maître de référence de commande ou effectuer une recherche en ligne.

Informations générales

Cette section présente des informations générales sur les profils virtuels pour vous aider à comprendre cette application avant de commencer à la configurer.

Restrictions

Nous vous recommandons d'utiliser des adresses non numérotées dans les interfaces de modèle virtuel pour vous assurer que les adresses réseau en double ne sont pas créées sur les interfaces d'accès virtuel.

Conditions préalables

L'utilisation d'informations de configuration d'interface AAA spécifiques à l'utilisateur avec des profils virtuels nécessite que le routeur soit configuré pour AAA et que le serveur AAA dispose de paires AV de configuration d'interface spécifiques à l'utilisateur. Les paires AV pertinentes (sur un serveur RADIUS) commencent comme suit :

```
cisco-avpair = "lcp:interface-config=...",
```

Les informations qui suivent le signe égal (=) peuvent être n'importe quelle commande de configuration d'interface Cisco IOS. Par exemple, la ligne peut être la suivante :

```
cisco-avpair = "lcp:interface-config=ip address 200.200.200.200
255.255.255.0",
```

L'utilisation d'une interface de modèle virtuel avec des profils virtuels nécessite la définition d'un modèle virtuel spécifique pour les profils virtuels.

Interopérabilité avec d'autres fonctions de numérotation Cisco

Les profils virtuels interagissent avec Cisco DDR, Multilink PPP (MLP) et des numéroteurs tels que RNIS.

Configuration DDR des interfaces physiques

Les profils virtuels interagissent pleinement avec les interfaces physiques dans les états de configuration DDR suivants lorsqu'aucune autre application d'interface d'accès virtuel n'est configurée :

- Les profils de numérotation sont configurés pour l'interface. Le profil de numérotation est utilisé à la place de la configuration des profils virtuels.
- DDR n'est pas configuré sur l'interface. Les profils virtuels remplacent la configuration actuelle.
- Le DDR hérité est configuré sur l'interface. Les profils virtuels remplacent la configuration actuelle.

Remarque : si une interface de numérotation est utilisée (y compris tout numéroteur RNIS), sa configuration est utilisée sur l'interface physique au lieu de la configuration des profils virtuels.

Effet PPP multiliaison sur la configuration de l'interface d'accès virtuel

Comme le montre le tableau 16-8, la configuration exacte d'une interface d'accès virtuel dépend des trois facteurs suivants :

- Indique si les profils virtuels sont configurés par Virtual Template, par AAA, par les deux, ou par aucun des deux. Ces états sont indiqués respectivement sous les rubriques « VP VT only », « VP AAA only », « VP VT and VP AAA » et « No VP in all ».
- La présence ou l'absence d'une interface de numérotation.
- La présence ou l'absence de MLP. L'étiquette de colonne « MLP » est un composant autonome pour toute fonctionnalité d'accès virtuel qui prend en charge MLP et les clones à partir d'une interface de modèle virtuel.

Dans le tableau 16-8, « Multilink VT » signifie qu'une interface de modèle virtuel est clonée *si* une est définie pour MLP ou une fonction d'accès virtuel qui utilise MLP.

Tableau 16-8 : Séquence de clonage des profils virtuels

Configuration des profils virtuels	MLP No Dialer	Numéroteur MLP	Pas de numéroteur MLP	Pas de numéroteur MLP
VP VT uniquement	VP VT	VP VT	VP VT	VP VT
VP AAA uniquement	(Multilink VT) VP AAA	(Multilink VT) VP AAA	Vice-président AAA	Vice-président AAA
VP VT et VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA

Pas du tout de vice-président	(VT multiliaison)	Numéroteur	Aucune interface d'accès virtuel n'est créée.	Aucune interface d'accès virtuel n'est créée.

L'ordre des éléments dans n'importe quelle cellule du tableau est important. Lorsque VP VT est affiché au-dessus de VP AAA, cela signifie que le modèle virtuel des profils virtuels est d'abord cloné sur l'interface, puis que la configuration de l'interface AAA de l'utilisateur lui est appliquée. La configuration d'interface AAA spécifique à l'utilisateur ajoute à la configuration et remplace toute commande de configuration d'interface physique ou de modèle virtuel en conflit.

Interopérabilité avec d'autres fonctionnalités utilisant des modèles virtuels

Les profils virtuels interagissent également avec les applications d'accès virtuel qui clonent une interface de modèle virtuel. Chaque application d'accès virtuel peut avoir au maximum un modèle à partir duquel cloner, mais peut cloner à partir de plusieurs configurations AAA.

L'interaction entre les profils virtuels et les autres applications de modèles virtuels est la suivante :

- Si l'option Profils virtuels est activée et qu'un modèle virtuel est défini pour celui-ci, le modèle virtuel Profils virtuels est utilisé.
- Si les profils virtuels sont configurés par AAA seul (aucun modèle virtuel n'est défini pour les profils virtuels), le modèle virtuel d'une autre application d'accès virtuel (VPDN, par exemple) peut être cloné sur l'interface d'accès virtuel.
- Un modèle virtuel, le cas échéant, est cloné à une interface d'accès virtuel avant la configuration AAA ou AAA par utilisateur des profils virtuels. La configuration AAA par utilisateur, si elle est utilisée, est appliquée en dernier.

Terminologie

Ce chapitre utilise les termes nouveaux ou peu courants suivants :

Paire AV : Un paramètre de configuration sur un serveur AAA ; partie de la configuration utilisateur que le serveur AAA envoie au routeur, en réponse à des demandes d'autorisation spécifiques à l'utilisateur. Le routeur interprète chaque paire AV comme une commande de configuration de routeur Cisco IOS et applique les paires AV dans l'ordre. Dans ce chapitre, le terme paire d'antivirus fait référence à un paramètre de configuration d'interface sur un serveur RADIUS.

Une paire AV de configuration d'interface pour les profils virtuels peut prendre la forme suivante :

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",
```

clonage : Création et configuration d'une interface d'accès virtuel en appliquant des commandes de configuration à partir d'un modèle virtuel spécifique. Le modèle virtuel est la source des informations utilisateur génériques et des informations dépendantes du routeur. Le résultat du clonage est une interface d'accès virtuel configurée avec toutes les commandes du modèle.

interface d'accès virtuel : Instance d'une interface virtuelle unique créée dynamiquement et qui existe temporairement. Les interfaces d'accès virtuel peuvent être créées et configurées différemment par différentes applications, telles que les profils virtuels et les réseaux commutés

privés virtuels.

interface de modèle virtuel : Configuration d'interface générique pour certains utilisateurs ou à une fin déterminée, plus informations dépendantes du routeur. Il s'agit d'une liste de commandes d'interface Cisco IOS à appliquer à l'interface virtuelle selon les besoins.

profil virtuel : Instance d'une interface d'accès virtuelle unique créée dynamiquement lorsque certains utilisateurs appellent et désactivée dynamiquement lorsque l'appel se déconnecte. Un profil virtuel d'utilisateur spécifique peut être configuré par une interface de modèle virtuel, une configuration d'interface spécifique à l'utilisateur stockée sur un serveur AAA, ou à la fois une interface de modèle virtuel et une configuration d'interface spécifique à l'utilisateur à partir d'AAA.

La configuration d'une interface d'accès virtuel commence par une interface de modèle virtuel (le cas échéant), suivie par l'application d'une configuration spécifique à l'utilisateur pour la session de numérotation de l'utilisateur concerné (le cas échéant).

Exemple annoté de négociation PPP

Dans cet exemple, une requête ping établit une liaison RNIS entre les routeurs *Montecito* et *Goleta*. Notez que, bien qu'il n'y ait pas d'horodatage dans cet exemple, il est généralement recommandé d'utiliser la commande de configuration globale **service timestamps debug datetime msec**.

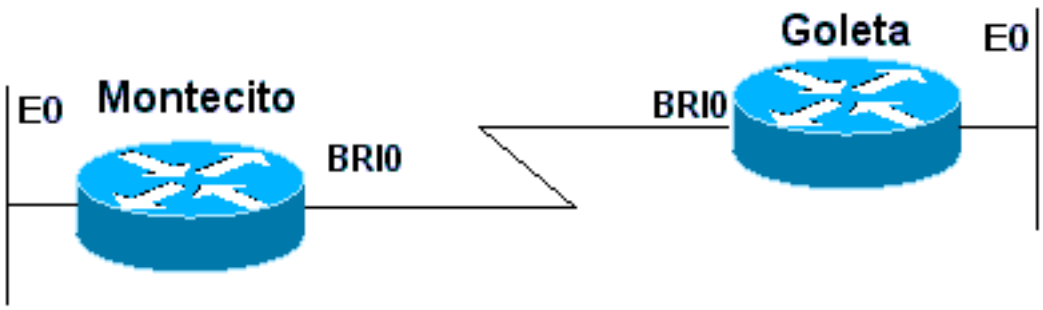

Figure 16-12 : Routeur-RNIS-Routeur

Ces débogages sont extraits de *Montecito* ; cependant, le débogage sur *Goleta* serait à peu près le même.

Remarque : Vos débogages peuvent apparaître dans un format différent. Ce résultat est le format de sortie de débogage PPP plus ancien, avant les modifications introduites dans IOS version 11.2(8). Reportez-vous au chapitre 17 pour un exemple de débogage PPP dans les versions plus récentes d'IOS.

```
Montecito#show debugging

  PPP:

    PPP authentication debugging is on

    PPP protocol negotiation debugging is on

A
 Montecito#ping 172.16.20.2
```

```
  Type escape sequence to abort.

  Sending 5, 100-byte ICMP Echoes to 172.16.20.2, timeout is 2 seconds:


B
 %LINK-3-UPDOWN: Interface BRI0: B-Channel 1, changed state to up

C
 ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5

C
 ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 29EBD1A7

D
 PPP BRI0: B-Channel 1: received config for type = 0x3 (AUTHTYPE)
value = 0xC223 digest = 0x5 acked

D
 PPP BRI0: B-Channel 1: received config for type = 0x5 (MAGICNUMBER)
value = 0x28FC9083 acked

E
 PPP BRI0: B-Channel 1: state = ACKsent fsm_rconfack(0xC021): rcvd id 0x65

F
 ppp: config ACK received, type = 3 (CI_AUTHTYPE), value = C223

F
 ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 29EBD1A7

G
 PPP BRI0: B-Channel 1: Send CHAP challenge id=1 to remote

H
 PPP BRI0: B-Channel 1: CHAP challenge from Goleta

J
 PPP BRI0: B-Channel 1: CHAP response id=1 received from Goleta

K
 PPP BRI0: B-Channel 1: Send CHAP success id=1 to remote

L
 PPP BRI0: B-Channel 1: remote passed CHAP authentication.

M
 PPP BRI0: B-Channel 1: Passed CHAP authentication with remote.

N
 ipcp: sending CONFREQ, type = 3 (CI_ADDRESS), Address = 172.16.20.1

P
 ppp BRI0: B-Channel 1: Negotiate IP address: her address 172.16.20.2 (ACK)

Q
 ppp: ipcp_reqci: returning CONFACK.

R
 PPP BRI0: B-Channel 1: state = ACKsent fsm_rconfack(0x8021): rcvd id 0x25

S
 ipcp: config ACK received, type = 3 (CI_ADDRESS), Address = 172.16.20.1
```

```
T
 BRI0: install route to 172.16.20.2

U
 %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0: B-Channel 1,
changed state to up
```

A - Le trafic est généré afin de lancer une tentative de numérotation.

B - La connexion est établie (les débogages RNIS ne sont pas utilisés dans cet exemple).

Commencer LCP :

C - *Montecito* envoie des requêtes de configuration LCP pour AUTHTYPE et MAGICNUMBER.

D - *Goleta* envoie ses CONFREQ. Si la valeur de MAGICNUMBER est identique à la valeur envoyée par *Montecito*, il y a une forte probabilité que la ligne soit bouclée.

E - Cela indique que *Montecito* a envoyé des accusés de réception aux CONFREQ de *Goleta*.

F - *Montecito* reçoit des CONFACK de *Goleta*.

Commencer la phase d'authentification :

G, H - *Montecito* et *Goleta* se contestent pour l'authentification.

J - *Goleta* répond au défi.

K, L - *Goleta* réussit l'authentification.

M - Message de *Goleta* à *Montecito* : authentification réussie.

La négociation NCP commence :

N, P : chaque routeur envoie son adresse IP configurée dans un CONFREQ.

Q, R - *Montecito* envoie un CONFACK au CONFREQ *de Goleta*.

S - ? et vice versa.

T, U - Une route est installée de *Montecito* à *Goleta* et le protocole sur l'interface passe à « up », indiquant que les négociations NCP ont réussi.

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

- Guide des solutions de numérotation Cisco IOS
- Vue d'ensemble des interfaces, des contrôleurs et des lignes utilisés pour l'accès à la numérotation
- Routage sur les lignes du modem
- Configuration du port série et de la liaison T1/E1
- Conception d'interréseaux DDR
- Choix et préparation de la configuration du routage à établissement de connexion à la demande (DDR)
- Configuration de DDRtitle
- Présentation de la technologie PPP
- Conception d'interréseaux RNIS
- Types, codes et valeurs de commutateurs RNIS
- Mise en service de la ligne RNIS
- Support et documentation techniques - Cisco Systems