Technologie d'accès commuté : Présentation et explications

Contenu

Introduction

Ce chapitre introduit et explique certaines des Technologies utilisées dans les réseaux commutés. Vous trouverez des conseils de configuration et des traductions de certaines des **commandes show**, qui sont utiles pour vérifier l'exécution correcte du réseau. Les procédures de dépannage sont hors de portée de ce document et peuvent être trouvées dans le document autorisé *dépannage de la numérotation*.

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.

Composants utilisés

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. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Exécutions de modem

Cette section explique le problème lié spécifiquement à l'installation, à la vérification, et à l'utilisation des Modems avec des Routeurs de Cisco.

Utilisant le modem Autoconfigure la commande

Si vous utilisez la version 11.1 de Cisco Internetwork Operating System (Cisco IOS) ou plus tard, vous pouvez configurer votre routeur de Cisco communiquer avec et configurer votre modem automatiquement.

Employez la procédure suivante pour configurer un routeur de Cisco pour tenter automatiquement de découvrir ce qu'un peu le modem est connecté à la ligne, et configurer alors le modem :

1. Pour découvrir le type de modem relié à votre routeur, utilisez la ligne commande de **modem autoconfigure discovery de** configuration.
2. Quand le modem est avec succès découvert, configurez le modem automatiquement utilisant la ligne commande de modem-*nom de* **modem autoconfigure type de** configuration.

Si vous voulez afficher la liste de Modems pour lesquels le routeur prend des entrées, utilisez le modem-*nom de* **show modemcap**. Si vous voulez changer une valeur de modem qui a été retournée de la commande de **show modemcap**, utilisez la ligne commande de *valeur d'attribut de modem-nom de* **modemcap edit de** configuration.

Pour des informations complètes sur l'utilisation de ces commandes, référez-vous aux *solutions guide de configuration de cadran de documentation Cisco IOS et à la référence de commandes de solutions de cadran*.

Remarque: N'écrivez pas le **&W** dans le modemcap entry qui est utilisé pour l'autoconfigure. Ceci cause le NVRAM d'être réécrit chaque fois qu'un modem autoconfigure est exécuté et détruira le modem.

Établissement d'une session Reverse Telnet sur un modem

Pour les buts diagnostiques, ou pour configurer au commencement le modem si vous exécutez la Cisco IOS version 11.0 ou antérieures, vous devez établir une session de telnet inverse pour configurer un modem pour communiquer avec un périphérique de Cisco. Tant que vous verrouillez la vitesse du modem de côté de l'équipement pour terminal de données (DTE), le modem communiquera toujours avec le serveur d'accès ou le routeur à la vitesse désirée. Référez-vous au tableau 16-5 pour les informations sur verrouiller la vitesse du modem. Soyez certain que la vitesse du périphérique de Cisco est configurée avant d'émettre des commandes au modem par l'intermédiaire d'une session de telnet inverse. De nouveau, référez-vous au tableau 16-5 pour les informations sur configurer la vitesse du serveur d'accès ou du routeur.

Pour configurer le modem pour une session de telnet inverse, utilisez la ligne **telnet de transport input de** commande de configuration. Pour installer un groupe tournant (dans ce cas, sur le port 1), écrivent la ligne la commande de configuration **1. rotary** plaçant ces commandes sous la ligne IOS de causes de configuration d'allouer des auditeurs IP pour les connexions entrantes aux plages de port commençant par les numérations de base suivantes :

2000	Protocole Telnet
3000	Protocole Telnet avec rotary
4000	Protocole Raw TCP
5000	Protocole Raw TCP avec rotary
6000	Protocole Telnet, mode binaire
7000	Protocole Telnet, mode binaire avec rotary
9000	Protocole xremote
10000	Protocole xremote avec rotary

Pour initier une session de telnet inverse à votre modem, exécutez les étapes suivantes :

1. De votre terminal, utilisez l'**IP address 20yy de telnet de** commande où l'*IP address* est l'adresse IP de n'importe quel active, interface connectée sur le périphérique de Cisco, et le yy est le numéro de ligne auquel le modem est connecté.Par exemple, la commande suivante vous connecterait au port auxiliaire sur un Routeur Cisco 2501 à l'adresse IP 192.169.53.52 : **telnet 192.169.53.52 2001**. Généralement, une commande telnet de cette sorte peut être émise n'importe où en fonction du réseau, si elle peut **cingler l'**adresse IP en question.**Remarque:** Sur la plupart des Routeurs de Cisco, le port 01 est le port auxiliaire. Sur un serveur d'accès Cisco, le port auxiliaire est le dernier téléscripteur +1. Comme exemple, le port auxiliaire sur des 2511 est le port 17 (16 ports TTY + 1). Utilisez toujours la commande EXEC de **show line** de trouver le numéro d'accès auxiliaire - en particulier sur les gammes 2600 et 3600, qui utilisent les numéros d'accès non-contigus pour faciliter des tailles async variables de module.
2. Si la connexion est refusée, elle pourrait indiquer qu'il n'y a ou aucun auditeur à l'adresse spécifiée et port, ou que quelqu'un est déjà connecté à ce port. Vérifiez l'adresse et le numéro de port de connexion. En outre, assurez-vous le **modem inout** ou le **modem dtr-active de** commande, aussi bien que le **transport input tous**, apparaissent sous la ligne configuration pour les lignes étant atteintes.Si utilisant la fonction rotary, assurez-vous que la commande *n rotary* apparaît également dans la ligne configuration où n est le nombre du groupe tournant. Pour vérifier si quelqu'un est déjà connecté, le telnet au routeur et utiliser le **show line de** commande *N.* recherchent un astérisque pour indiquer que la ligne est en service. Assurez-vous que CTS est élevé et DSR n'est pas. Employez le **clear line de**

commande *n* pour déconnecter la session en cours sur le numéro de port N. Si la connexion est encore refusée, le modem pourrait affirmer la Détection Onde Porteuse (CD) tout le temps. Démontez le modem de la ligne, établissez une session de telnet inverse, et puis connectez le modem.

3. Après avoir avec succès établi le rapport de telnet, entrez À et soyez sûr les réponses de modem avec l'OK.
4. Si le modem n'est pas sensible, référez-vous au tableau suivant.

Les causes possibles d'ensembles ci-dessous du tableau 16-1 des symptômes du problème de Connectivité de modem-à-routeur et décrit des 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 EXEC de **show line** sur le serveur d'accès ou le routeur. La sortie pour le port auxiliaire devrait afficher **InOut** ou **RIisCD** dans la colonne Modem. Ceci indique que le contrôle de modem est activé sur la ligne du serveur d'accès ou du routeur. Pour une explication de sortie de **show line**, référez-vous au « utilisant des commandes de debug » en chapitre 15. 2. Configurez la ligne pour le contrôle de modem utilisant la ligne commande de **modem inout de** configuration. Le contrôle de modem est maintenant activé sur le serveur d'accès. Exemple : L'exemple suivant montre comment configurer une ligne pour les deux appels entrant et sortants : `line 5` `modem inout` **Remarque:** Soyez sûr d'utiliser la commande de **modem inout**, et pas la commande de **modem dialin** tandis que la Connectivité du modem est en question. La dernière commande permet à la ligne pour recevoir des appels entrant seulement. Des appels sortants seront refusés et il sera impossible d'établir une session de telnet avec le modem afin de le configurer. Si vous voulez utiliser la commande de **modem dialin**, faites ainsi seulement après que vous êtes certain que le modem fonctionne correctement.
Le modem a pu miscon figured	Écrivez **AT&FE1Q0** pour le renvoyer aux par défaut d'usine et veiller le modem est placée pour faire écho des caractères et renvoie la sortie. Le modem peut avoir une session interrompue. Employez le « ^U » pour effacer la

ou avoir une session interrompue.	ligne et le « ^Q » pour ouvrir le contrôle de flux (XON). Vérifiez les configurations de parité.
Câblage incorrect	1. Vérifiez le câblage entre le modem et le serveur d'accès ou le routeur. Confirmez que le modem est connecté au port auxiliaire sur le serveur d'accès ou le routeur à un câble roulé de RJ-45 et à un adaptateur MMOD DB-25. Cette configuration de câblage est recommandée et prise en charge par Cisco pour des ports de RJ-45. (Ces connecteurs sont typiquement étiquetés « Modem.") 2. Utilisez la commande EXEC de **show line** de vérifier que le câblage est correct. Voyez l'explication de la sortie de commande de **show line** dans la section intitulée « utilisant des commandes de debug » en chapitre 15.
Problème matériel	1. Vérifiez que vous utilisez le câblage correct et que toutes les connexions sont bonnes. 2. Vérifiez tout le matériel pour des dommages, y compris le câblage (fils rompus), les adaptateurs (broches lâches), les ports de serveur d'accès, et le modem. 3. Voir le chapitre 3, « dépannage du matériel et des problèmes de démarrage, » pour plus d'informations sur le dépannage matériel.

Utilisant des groupes tournants

Pour quelques applications, les Modems sur un routeur donné doivent être partagés par un groupe d'utilisateurs. L'utilitaire d'accès sortant de Cisco est un exemple de ce type d'application. Fondamentalement, les utilisateurs se connectent à un port qui les connecte à un modem disponible. Pour ajouter une ligne asynchrone à un groupe tournant, écrivez simplement *n* **rotary** où *n* est le nombre du groupe tournant dans la configuration pour la ligne asynchrone. Référez-vous à l'exemple ci-dessous.

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

La ligne configuration ci-dessus permettrait à des utilisateurs pour se connecter au groupe tournant en entrant dans le **telnet 192.169.53.52 3001** pour le telnet normal. Les solutions de

rechange incluent les ports 5001 pour le TCP cru, 7001 pour le telnet binaire (que l'utilitaire d'accès sortant de Cisco utilise), et 10001 pour des connexions de Xremote.

Remarque: Pour vérifier la configuration de l'utilitaire d'accès sortant de Cisco, double-cliquer sur l'icône d'utilitaire d'accès sortant au en bas à droite de l'écran et appuyez sur le bouton de More>. Ensuite, appuyez sur le bouton de Ports> de configurer. Assurez-vous que le port est dans la plage 7000, si utilisant les groupes tournants, et la plage 6000, si l'utilitaire d'accès sortant vise un modem individuel. Vous devriez également activer le modem ouvrant une session le PC. Ceci est fait en sélectionnant l'ordre suivant : **Modems-> de Start->Control Panel->** (choisissez votre modem de Cisco Dialout) - >Properties->Connection->Advanced… - >Record un **fichier journal**.

Interprétation de la sortie de show line

La sortie de la commande EXEC de *numéro de ligne de* **show line** est pour le dépannage utile un serveur ou une connexion du routeur de modem-à-Access. Est ci-dessous la sortie de la commande de **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#
```

Quand les problèmes de Connectivité se posent, l'importante sortie apparaît dans l'état de modem et les champs d'état matériel du modem.

Remarque: Le champ d'état matériel du modem n'apparaît pas dans le **show line** sorti pour chaque plate-forme. Dans certains cas, les indications pour des états des signaux seront affichées dans le domaine d'état de modem à la place.

L'état de modem d'expositions du tableau 16-2 et les chaînes typiques d'état matériel du modem de la sortie du **show line** commandent. Il explique également la signification de chaque état.

Tableau 16-2 : Modem et états matériels du modem dans la sortie de show line

État de modem	État matériel du modem	Signification
Inactif	RTS du no	Ce sont les états appropriés de modem pour des connexions entre un serveur d'accès ou un routeur et un modem (quand il n'y a aucun appel entrant). La sortie de n'importe quelle

	DSR DTR CTS	autre sorte indique généralement un problème.
Prêt	-	Si l'état de modem est prêt, au lieu de l'inactif, considérez ce qui suit : 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 avec la ligne commande de **modem inout de** configuration. 2. Une session existe sur la ligne. Utilisez la commande EXEC d'**utilisateurs d'exposition** et utilisez la commande de privileged exec de **clear line** d'arrêter la session si désiré. 3. DSR est élevé. Il y a deux possibles raison pour ceci : Problèmes de câblage. Si votre connecteur utilise DB-25 la borne 6 et n'a aucune borne 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 devrait être modifié pour avoir la haute DCD seulement un CD(1). Ceci est habituellement fait avec la commande du modem **&C1**, mais vérifie votre documentation de modem pour la syntaxe exacte pour votre modem. Si votre logiciel ne prend en charge pas le contrôle de modem, vous devez configurer la ligne du serveur d'accès à laquelle le modem est connecté à l'**aucune** ligne commande d'**exécutif de** configuration. Effacez la ligne avec la commande de privileged exec de **clear line**, initiez une session de telnet inverse avec le modem, et modifiez le modem de sorte que DCD soit élevé seulement sur le CD. Finissez la session de telnet en écrivant le **débranchement** et modifiez la ligne du serveur d'accès avec la ligne commande d'exécutif de configuration.
Prêt	noDSR	La chaîne de noCTS apparaît dans le champ d'état matériel du modem pour une des quatre raisons suivantes :

	de no CTS DTR RTS(2)	1. Le modem est arrêté. 2. Le modem n'est pas correctement connecté au serveur d'accès. Vérifiez les jonctions de câble du modem au serveur d'accès. 3. Câblage incorrect (MDCE roulé, ou MDTE droit, mais sans broches déplacées). La configuration de câblage recommandée est donnée plus tôt dans cette table. 4. Le modem n'est pas configuré pour le contrôle de flux matériel. N'utilisez l'**aucune** ligne commande de **flowcontrol hardware de** configuration de désactiver le contrôle de flux matériel sur le serveur d'accès. Activez alors le contrôle de flux matériel sur le modem par l'intermédiaire d'une session de telnet inverse. (Consultez votre documentation de modem et voyez la section « établir une session Reverse Telnet à un modem » plus tôt en ce chapitre.) Réactivez le contrôle de flux matériel sur le serveur d'accès avec la ligne commande de **flowcontrol hardware de** configuration.
Prêt	CTS DSR DTR RTS(2)	La chaîne DSR (au lieu de la chaîne de noDSR) apparaît dans le champ d'état matériel du modem pour une des raisons suivantes : 1. Câblage incorrect (MDCE roulé, ou MDTE droit, mais sans broches déplacées). La configuration de câblage recommandée est donnée plus tôt dans cette table. 2. Le modem est configuré pour DCD toujours élevé. Modifiez le modem de sorte que DCD soit seulement élevé sur le CD. Ceci est habituellement fait avec la commande du modem **&C1**, mais vérifie votre documentation de modem pour la syntaxe exacte pour votre modem. Configurez la ligne du serveur d'accès à laquelle le modem est connecté à l'**aucune** ligne commande d'**exécutif de** configuration. Effacez la ligne avec la commande de privileged exec de **clear line**, initiez une session de telnet inverse avec le modem, et modifiez le modem de sorte que DCD soit élevé seulement sur le CD. Finissez la session de telnet en

		écrivant le **débranchement**. Modifiez la ligne du serveur d'accès avec la ligne commande d'exécutif de configuration.
Prêt	CTS* DSR* DTR RTS(2)	Si cette chaîne apparaît dans le champ d'état matériel du modem, le contrôle de modem n'est pas probablement activé sur le serveur d'accès. Utilisez la ligne commande de **modem inout de** configuration d'activer le contrôle de modem sur la ligne. Les informations complémentaires sur configurer le contrôle de modem sur un serveur d'accès ou une ligne du routeur sont fournies plus tôt dans cette table.

(1) CD = Détection Onde Porteuse

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

Collecte des informations sur les performances du modem

Cette section explique des méthodes pour recueillir des données de performance sur les Modems numériques de MICA trouvés dans la famille de Cisco AS5x00 des serveurs d'accès. Les données de performance peuvent être utilisées pour l'analyse de tendance et sont utiles dans les problèmes de performances de dépannage qui pourraient être produits. Quand regarder les nombres a présenté ci-dessous, considérez que la perfection n'est pas possible dans le monde réel. Le taux de réussite possible d'appel par modem (CSR) est une fonction de la qualité des circuits, de l'userbase de modem client, et de l'ensemble de modulations étant utilisées. Un pourcentage typique CSR pour les appels V.34 est 95%. Les appels V.90 peuvent être prévus pour connecter avec succès 92% du temps. Les baisses prématurées sont susceptibles de se produire 10% du temps.

Utilisez les commandes suivantes de gagner une vue globale du comportement du modem sur le serveur d'accès :

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

Les informations suivantes sont pour le dépannage utile des données de connexion ou de collecte de modem individuel pour l'analyse de tendance :

- debug modem csm
- modem call-record laconique
- show modem op) (de MICA/AT@E1 (Microcom) tandis que connecté
- show modem log pour la session d'intérêt après débranchement
- ANI (le nombre de l'appelant)
- Heure
- Matériel/révision de microprogramme de modem client
- Les informations intéressantes du client (après disconnect)-ATI6, ATI11, AT&V, AT&V1, et ainsi de suite

- Un enregistrement sonore (fichier .wav) de la tentative de trainup du modem client

Dans les sections suivantes, les commandes seront expliquées plus loin et quelques tendances communes seront discutées.

Show modem/show modem summary

La commande de **show modem** donne un avis des modems individuels. De ces nombres les santés des modems individuels peuvent être visualisées.

```
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 voir les nombres totas pour tous les Modems sur le routeur, utilisez la commande de **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 : gisements de show modem

Champs	Descriptions
Appels entrant et sortants	Appels composant dans et hors du modem. • Utilisation - Pourcentage de toute la disponibilité système que tous les Modems sont en service. • Succ - Totaux des appels avec succès connectés. • Échouer - Totaux des appels qui ne se sont pas avec succès connectés. • Disponibilité - Modems totaux disponibles pour l'usage dans le système.
Busied	Le nombre total de périodes les Modems ont été pris hors service avec la commande **occupée de modem** ou la commande de **modem shutdown**.
Cadran défectueux	Nombre total de tentatives que les Modems ne se sont pas arrêtées ou il n'y avait aucune tonalité.
Aucun Rép.	Le nombre total d'appel en sonnerie de périodes a été détecté, mais les appels n'ont pas été répondus par un modem.
PCT de Succ.	Pourcentage réussi de connexion des Modems disponibles totaux.

Sortie de show modem call-stats

```
compress  retrain lostCarr  rmtLink  trainup hostDrop wdogTimr inacTout
```

```
  Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %    #   %
 Total    9       41      271     3277        7     2114        0        0
```

Tableau 16-4 : champs de show modem call-stats

rmt Link	Cette exposition que la correction d'erreurs était en vigueur, et l'appel ont été arrêtés par le système client relié au modem distant.
hostDrop	Ceci affiche que l'appel a été arrêté par le système hôte IOS. Quelques raisons communes incluent : délai d'attente de veille, un circuit clair de l'opérateur téléphonique, ou un termreq du PPP LCP du client. La meilleure manière de déterminer la raison pour le coup est en hausse à l'aide du modem call-record laconique ou de l'aaa accounting.

Les autres raisons de débranchement devraient ajouter à moins de 10% du total.

Sortie de show modem connect-speeds

```
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
```

Comptez voir une distribution des vitesses V.34. Il devrait y a une crête à 26.4, si T1 le canal de signalisation associé d'utilisation (CAS). Pour le RNIS (PRI) T1, la crête devrait être à 31.2. En outre, recherchez quelques K56Flex, V.90 expédie. S'il n'y a aucune connexion V.90 il peut y a un problème de topologie du réseau.

Compréhension de la commande laconique de modem call-record (11.3AA/12.0T)

Plutôt qu'une commande EXEC, c'est une commande de configuration placée au niveau du système du serveur d'accès en question. Quand débranchements d'un utilisateur, un message semblable aux affichages suivants :

```
*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 de show modem operational-status

Le show modem operational-status de commande EXEC affiche les paramètres en cours (ou la plupart de récent) concernant la connexion du par modem.

L'entrée de documentation pour cette commande est trouvée dans la *référence de commandes de*

solutions de cadran de Cisco IOS version 12.0. **le show modem operational-status** est seulement pour des modems MICA. La commande équivalente pour des modems Microcom est **modem at-mode/AT@E1**. Utilisez la commande du **modem at-mode <slot>/<port>** de se connecter au modem, puis émettez la commande d'**AT@E1**. La documentation complète pour la commande de **modem at-mode** peut être trouvée dans le *guide de configuration du logiciel de Cisco AS5300*, et la documentation pour la commande d'**AT@E1** est en *commande AT réglée et récapitulation du registre pour la référence de commandes de modules de modem Microcom*.

Employez les étapes suivantes pour déterminer sur quels Modems un utilisateur est livré dedans :

1. Émettez l'**utilisateur d'exposition de** commande et recherchez le téléscripteur auquel ils sont connectés.
2. Utilisez le **show line de** commande et recherchez l'emplacement de modem/numéros de port.

Collecte des données de performances côté client

Pour l'analyse de tendance, il est très important de recueillir des données de performances côté client. Toujours essai pour obtenir les informations suivantes :

- modèle/version de firmware de matériel client (possible avec la commande **ATI3I7** sur le modem du client)
- le débranchement client-signalé raisonne (utilisation **ATI6** ou **AT&V1**)

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

Analysez les données de performance

Une fois que vous avez collecté et avez compris les données de performance pour votre système de modem, vous devez regarder tous modèles et composants restants qui peuvent avoir besoin d'amélioration.

Problèmes avec les modems du serveur particuliers

Employez le **show modem** ou le **show modem call-stats** pour identifier tous les Modems avec anormalement des hauts débits d'échec d'apprentissage ou de mauvais débits de débranchement (MICA). Si les paires adjacentes de Modems ont des problèmes, le problème est probable arrêté/complètement DSP. Utilisez le **modem de copy flash à l'**affecté HMM afin de récupérer. Assurez-vous que les Modems exécutent la dernière version du portware. Pour vérifier que tous les Modems sont correctement configurés, utilisez le **mica/microcom_server de modem autoconfigure type de** commande de configuration dans la ligne configuration. Pour s'assurer les Modems autoconfigured toutes les fois qu'un appel est arrêté, utilisent le **debug confmodem de** commande EXEC. Afin de réparer les Modems qui misconfigured mal, vous pouvez devoir établir une session de telnet inverse.

Problèmes avec DS0s particulier

Les problèmes DS0 sont rares, mais possibles. Pour localiser DS0s de défaut de fonctionnement, utilisez les appel-**compteurs de t1 de show controller de** commande et recherchez n'importe quel DS0s avec TotalCalls anormalement élevé et TotalDuration anormalement bas. Pour viser a suspecté DS0s, vous peut avoir besoin occupé de l'autre DS0s avec le **service DSL de la**

commande de configuration le **RNIS, le busyout ds0** sous l'interface série pour le t1. La sortie des appel-**compteurs de t1 de show controller** ressemble à ceci :

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

Évidemment, le créneau horaire 3 est le canal suspect dans ce cas.

Tendances communes supplémentaires

Sont ci-dessous quelques unes des tendances plus communes vues par Cisco TAC.

1. Mauvais chemins d'accès du circuitVous pourriez obtenir de mauvais chemins d'accès du circuit par le réseau téléphonique public commuté (PSTN) si vous avez les problèmes suivants :les appels longue distance ont des problèmes, mais les gens du pays ne font pas (ou vice versa)les appels par moments du jour ont des problèmesles appels des échanges distants spécifiques ont des problèmes
2. Problèmes avec des appels longue distanceSi votre service interurbain ne fonctionne pas correctement ou du tout (mais le service local est bien) :Soyez sûr que la ligne numérique se connecte dans un commutateur numérique, pas un banc canal.Instruisez les opérateurs téléphoniques examiner les chemins d'accès du circuit utilisés pour la longue distance.
3. Problèmes avec des appels de la particularité appelle des zones.Si les appels des régions géographiques/échanges spécifiques tendent à avoir des problèmes, vous devriez obtenir la topologie du réseau de l'opérateur téléphonique.Si de plusieurs conversions analogique-numériques sont exigées, le modem V.90/K56flex se connecte ne sera pas possible et V.34 peut être en quelque sorte dégradé. Des conversions analogique-numériques sont exigées dans les zones qui sont servies par les commutateurs numériques non-intégrés ou par les Commutateurs analogiques.

Fonctionnements de RNIS

Le RNIS se rapporte à un ensemble de services numériques qui sont à la disposition des utilisateurs finaux. Le RNIS comporte la numérisation du réseau téléphonique de sorte que la Voix, les données, le texte, les graphiques, la musique, le vidéo, et tout autre matériau de base puissent être fournis aux utilisateurs finaux d'un simple, terminal d'utilisateur au-dessus de câblage téléphonique existant. Les partisans du RNIS imaginent un réseau mondial tout comme le réseau téléphonique actuel, mais avec la transmission numérique et un grand choix de nouveaux services.

Le RNIS est un effort de normaliser les services pour les abonnés, l'utilisateur/interfaces réseau, et le réseau et les interconnexions de réseaux. Normalisation des tentatives de services pour les abonnés d'assurer un niveau de compatibilité internationale. La normalisation de l'utilisateur/d'interface réseau stimule le développement et le marketing de ces interfaces par de tiers fabricants. En normalisant des aides de réseau et d'interconnexions de réseaux atteignez le but de la Connectivité mondiale en s'assurant que les réseaux RNIS communiquent facilement entre eux.

Les applications RNIS incluent des applications ultra-rapides d'image (telles que la télécopie de groupe IV), des lignes téléphoniques supplémentaires dans les maisons pour servir le secteur de

télétravail, le transfert de fichiers ultra-rapide, et la vidéoconférence. Voix, naturellement, ISL également une demande populaire de RNIS.

Le marché d'accès de maison est divisé parmi différentes Technologies. Dans les zones où de plus nouvelles Technologies moins chères telles que le DSL et le câble deviennent disponibles le marché domestique s'éloigne du RNIS. Les entreprises, cependant, continuent à employer le RNIS sous forme de PRI T1/E1s pour porter un grand nombre de données ou pour fournir l'accès du dialin v.90.

Composants RNIS

Les composants RNIS incluent des terminaux, des adaptateurs de terminal (TAS), des périphériques de terminaison de réseau, l'équipement de terminaison de ligne, et l'équipement d'échange et d'arrêt. Terminaux RNIS été livré dans deux types. Des terminaux spécialisés RNIS désigné sous le nom du type 1 de matériel de terminal (TE1). Les terminaux le Non-RNIS, tels que le DTE qui antidatent les normes RNIS, désigné sous le nom du type-2 de matériel de terminal (TE2). TE1s se connectent au réseau RNIS par un lien numérique à quatre fils et torsadé. TE2s se connectent au réseau RNIS par un adaptateur de terminal. Le RNIS MERCI peut être un périphérique autonome ou un panneau à l'intérieur du TE2. Si le TE2 est mis en application comme périphérique autonome, il se connecte aux VENTRES par l'intermédiaire d'une interface standard de couche physique. Les exemples incluent EIA/TIA-232-C (autrefois RS-232-C), V.24, et V.35.

Au delà des périphériques TE1 et TE2, le prochain point de connexion dans le réseau RNIS est le type 1 de terminaison de réseau (NT1) ou périphérique du type-2 de terminaison de réseau (NT2). Ce sont des périphériques de terminaison de réseau qui connectent l'abonné à quatre fils câblant à la boucle locale à deux fils conventionnelle. En Amérique du Nord, le NT1 est un périphérique de la CPE (CPE). À la plupart des autres parties du monde, le NT1 fait partie du réseau fourni par le transporteur. Le NT2 est un périphérique plus compliqué, typiquement trouvé dans des autocommutateurs privés numériques (PBX), qui assure services de concentration en couche 2 et 3 fonctions de protocole et. Un périphérique NT1/2 existe également ; il est un à un dispositif que combine les fonctions d'un NT1 et d'un NT2.

Un certain nombre de points de référence sont spécifiés dans le RNIS. Ces points de référence définissent des interfaces logiques entre les groupements fonctionnels tels que le TAS et le NT1s. Les points de référence RNIS incluent ce qui suit :

- Point de référence de R-The entre le matériel le non-RNIS et VENTRES
- Point de référence de S-The entre les terminaux d'utilisateur et le NT2
- Point de référence de T-The entre les périphériques NT1 et NT2
- Point de référence d'U-The entre les périphériques NT1 et l'équipement de terminaison de ligne dans le réseau d'opérateur. Le point de référence U est approprié seulement en Amérique du Nord, où la fonction NT1 n'est pas fournie par le réseau d'opérateur

Ce qui suit est un exemple de configuration RNIS. Cet échantillon affiche trois périphériques reliés à un commutateur RNIS au bureau central. Deux de ces périphériques sont RNIS-compatibles, ainsi ils peuvent être reliés par un point de référence S aux périphériques NT2. Le troisième périphérique (une norme, téléphone le non-RNIS) relie par le point de référence R à l'des VENTRES. L'un de ces périphériques pourraient également se relier à un périphérique NT1/2, qui remplacerait le NT1 et le NT2. Et, bien qu'elles ne soient pas affichées, des stations utilisateur semblables sont reliées au commutateur de l'extrême droite le RNIS.

Un 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 d'accès de base (BRI) RNIS offre deux canaux B et un canal D (2B+D). Le service de canal B BRI fonctionne aux 64 Kbits/s et est censé porter des données d'utilisateur ; Le service de canal D BRI fonctionne aux 16 Kbit/s et est censé diffuser le contrôle et les informations de signalisation, bien qu'il puisse prendre en charge la transmission de données d'utilisateur sous certaines circonstances. Le protocole de signalisation de canal D comporte les couches 1 à 3 du modèle de référence OSI. BRI prévoit également le contrôle de tramage et tout autre supplémentaire, apportant son débit total à 192 Kbps. La spécification de la couche physique BRI est l'Union internationale des télécommunications - Secteur de la normalisation des télécommunications (ITU-T ; autrefois le Comité consultatif international télégraphique et téléphonique [CCITT]) I.430.

Le service de l'interface PRI RNIS (PRI) offre 23 canaux B et un canal D en Amérique du Nord et au Japon, rapportant un débit total de 1.544 Mbits/s (le canal D PRI fonctionne aux 64 Kbits/s). Le PRI RNIS à l'Europe, à l'Australie, et à d'autres parties du monde fournit 30 B plus un canal D 64-kbps et un débit total d'interface de 2.048 Mbits/s. La spécification de la couche physique PRI est ITU-T I.431.

Couche 1

La couche physique RNIS (formats de trame de couche 1) diffèrent selon si la trame est sortante (du terminal au réseau) ou d'arrivée (du réseau au terminal). Les deux interfaces de couche physique sont affichées dans la figure 16-1.

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

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

- F - Fournit la synchronisation.
- L - Ajuste la valeur de bit moyenne.
- E - Utilisé pour la résolution de conflit quand plusieurs terminaux sur un bus passif contestent pour un canal.
- A - Lance des périphériques.
- S - Non affecté.
- B1, B2, et D - Pour des données d'utilisateur.

De plusieurs périphériques d'utilisateur RNIS peuvent être physiquement reliés à un circuit. Dans cette configuration, les collisions peuvent résulter si deux terminaux transmettent simultanément. Par conséquent, le RNIS fournit des caractéristiques pour déterminer le conflit de lien. Quand un NT reçoit un bit D du TE, il fait écho de retour le bit en prochaine position d'E-bit. Le TE s'attend à ce que le prochain bit E soit identique que son dernier bit transmis D.

Les terminaux ne peuvent pas transmettre dans le canal D à moins qu'ils détectent d'abord un nombre spécifique de ceux (n'indiquant « aucun signal ») qui correspondent à une priorité préétablie. Si le TE détecte un bit dans le canal de l'écho (e) qui est différent de ses bits D, il doit cesser de transmettre immédiatement. Cette technique simple s'assure que seulement un terminal peut transmettre son message D en même temps. Après la transmission de message réussie D, le terminal a sa priorité réduite en étant exigé pour détecter les plus continus avant la transmission. Les terminaux ne peuvent pas soulever leur priorité jusqu'à ce que tous autres périphériques sur la même ligne aient eu une occasion d'envoyer un message D. Les connexions téléphoniques ont la haute priorité que tous autres services, et les informations de signalisation ont une haute priorité que les informations nonsignaling.

Couche 2

La couche 2 du protocole de signalisation RNIS est procédure de Link Access sur le canal D, également connu sous le nom de LAPD. LAPD est semblable au High-Level Data Link Control (HDLC) et à la procédure de Link Access, équilibrés (LAPB). Pendant que l'extension de l'abréviation LAPD indique, elle est utilisée à travers le canal D pour s'assurer que des flots d'information de contrôle et d'informations de signalisation et est reçue correctement. Le format de trame LAPD (voir la figure 16-2) est très semblable à celui du HDLC et, comme le HDLC, du LAPD utilise de surveillance, les informations, et des trames non numérotées. Le protocole LAPD est formellement spécifié dans ITU-T Q.920 et ITU-T Q.921.

Figure 16-2 : Format de trame LAPD

L'indicateur et les champs de contrôle LAPD sont identiques à ceux du HDLC. La zone adresse LAPD peut être de 1 ou 2 octets de long. Si le bit étendu d'adresse du premier octet est placé, l'adresse est de 1 octet ; s'il n'est pas placé, l'adresse est de 2 octets. Le premier octet de zone adresse contient l'indentifiant de point d'accès de service (SAPI), qui identifie le portail auquel des services LAPD sont fournis pour poser 3. Le bit C/R indique si la trame contient une commande ou une réponse. Le gisement de l'indentifiant de point de terminaison de terminal (TEI) identifie des terminaux terminaux ou plusieurs simples. Un TEI de tout l'indique une émission.

Couche 3

Deux caractéristiques de la couche 3 sont utilisées pour la signalisation RNIS : ITU-T (autrefois CCITT) I.450 (également connu sous le nom d'ITU-T Q.930) et ITU-T I.451 (également connu sous le nom d'ITU-T Q.931). Ensemble, ces protocoles les prennent en charge les connexions individuelles, avec commutation à circuit, et de commutation de paquets. Un grand choix d'établissement d'appel, de terminaison d'appel, d'informations, et de messages divers sont spécifiés, y compris l'INSTALLATION, SE CONNECTENT, LIBÈRENT, les INFORMATIONS UTILISATEUR, ANNULATION, ÉTAT, et DÉBRANCHEMENT.

Ces messages sont fonctionellement semblables à ceux fournis par le protocole de X.25 (voir le chapitre 19, « dépannage des connexions de X.25, » du pour en savoir plus). La figure 16-3, d'ITU-T I.451, affiche les étapes typiques d'un appel à commutation de circuits RNIS.

Étapes d'appel à commutation de circuits de la figure 16-3 le RNIS

Interprétation de la sortie d'état de show isdn

Pour découvrir ce qui est l'état en cours de la connexion RNIS entre le routeur et le commutateur

d'opérateur téléphonique, utilisez l'**état de show isdn de** commande. Les deux genres d'interfaces qui sont prises en charge par cette commande sont les BRI et le 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
```

État de show isdn du tableau 16-5:- pour BRI

Champ	Importance
État de la couche 1 : DÉSACTIVÉ	Ceci indique que l'interface BRI ne voit pas un signal sur la ligne. Il y a cinq possibles raison pour cette condition. • L'interface BRI est arrêt. Vérifiez la configuration pour l'**arrêt de** commande sous l'interface BRI, ou recherchez administrativement vers le bas une indication de la **commande d'interface d'exposition**. Utilisez l'utilitaire de configuration et n'écrivez **aucun arrêt** sous l'interface BRI. Entrez dans le **bri de clear interface de** commande à la demande d'exécutif pour s'assurer que l'interface BRI est redémarrée. • Un problème existe avec le câblage. Vous devrez remplacer le câble. Assurez-vous que vous utilisez un câble direct de RJ-45. Pour vérifier le câble, tenez les extrémités du câble de RJ-45 côte à côte. Si les broches sont dans la même commande, le câble est direct. Si la commande des broches est renversée, le câble est roulé. Remplacez le câble. • Le port RNIS BRI d'un routeur pourrait exiger un périphérique NT1. Dans le RNIS, NT1 est un périphérique qui fournit l'interface entre la CPE et le matériel de commutation de bureau central. Si le routeur n'a pas un NT1 interne, obtient et connecte un NT1 au port BRI. Assurez-vous que le BRI ou l'adaptateur de terminal est relié au port S/T du NT1. Référez-vous à la documentation du fabricant pour vérifier l'exécution correcte du NT1 externe. • La ligne ne pourrait pas fonctionner. Entrez en contact avec le transporteur pour

	confirmer l'exécution de la connexion et pour vérifier les configurations de type de commutateur. • Assurez-vous que le routeur fonctionne correctement. S'il y a défectueux ou de matériel défaillant, remplacez selon les besoins.
État de la couche 2 : État = TEI_ASSIGNED	Vérifiez la configuration switchtype et le SPIDS. Le paramétrage du commutateur RNIS spécifique à l'interface ignorera le paramétrage global du commutateur. L'état SPID indiquera si le commutateur a reçu le SPIDS (valide ou non valide). Entrez en contact avec votre fournisseur de services pour vérifier la configuration configurée sur le routeur. Pour changer les configurations SPID, utilisez la commande de configuration d'interface de **spidn RNIS**. Là où *n* est 1 ou 2, selon le canal en question. Utilisez le **forme no de** cette commande de retirer le SPID spécifié. `isdn spidn spid-number [ldn]` `no isdn spidn spid-number [ldn]`**Description de syntaxe :** `spid-number`Le nombre identifiant le service auquel vous vous êtes abonné. Cette valeur est assignée par le fournisseur de services RNIS et est habituellement un numéro du téléphone 10-digit avec les chiffres supplémentaires. `ldn`Le numéro dans le répertoire local (facultatif) (LDN), qui est un nombre à 7 chiffres a assigné par le fournisseur de services. Le commutateur dans le message de configuration entrant fournit ces informations. Si vous n'incluez pas l'accès de répertoire local au commutateur est permis, mais l'autre canal B peut ne pas pouvoir recevoir des appels entrant. Pour voir les négociations de la couche 2 entre le commutateur et le routeur, utilisez le **debug isdn q921 de** commande de privileged exec. Le q921 met au point est documenté dans la *référence de débogage des commandes*. Les debugs se fondent fortement sur des ressources CPU, ainsi précaution d'usage en les utilisant.

```
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 d'**état de show isdn** ne fonctionne pas ou n'affiche pas le PRI, essayez utilisant la commande de **service de show isdn**. Assurez-vous que l'ordre de **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 l'ordre de **pri-group**.

Ce qui suit est un exemple d'une configuration pour un routeur de Cisco avec un contrôleur canalisé T1/PRI :

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

Tableau 16-6 : état de show isdn pour le PRI

Champ	Importance
État de la couche 1 : DÉSACTIVÉ	Ceci indique que l'interface PRI ne voit pas le tramage T1/E1 sur la ligne. Considérez les causes possibles suivantes pour cette condition : • L'interface PRI est arrêt. Vérifiez la configuration pour l'**arrêt de** commande sous l'interface serial0:23 ou recherchez administrativement vers le bas une indication de la **commande d'interface d'exposition**. Utilisez l'utilitaire de configuration et n'écrivez **aucun arrêt** sous l'interface en question. Entrez dans le **clear controller T1/E1** *n de* commande à la demande d'exécutif pour s'assurer que l'interface PRI est redémarrée. • Un problème existe avec le câblage. Vous devrez remplacer le câble. Assurez-vous que vous utilisez un câble direct de RJ-45. Pour vérifier le câble, tenez les extrémités du câble de RJ-45 côte à côte. Si les broches sont dans la même commande, le câble est direct. Si la commande des broches est renversée, le câble est roulé. Remplacez le câble. • La ligne ne pourrait pas fonctionner. Entrez en contact avec le transporteur pour confirmer l'exécution de la connexion, et pour vérifier les configurations de type de commutateur. • Assurez-vous que le routeur fonctionne correctement. S'il y a défectueux ou de matériel défaillant, remplacez selon les besoins.
État de la couche 2 : État = TEI_ASSIGNED	Vérifiez la configuration switchtype. Le paramétrage du commutateur RNIS spécifique à l'interface ignorera le paramétrage global du commutateur. Vérifiez le T1/E1 est configuré pour apparier le commutateur du fournisseur (les problèmes T1/E1 sont discutés en chapitre 15). Pour voir

	les négociations de la couche 2 entre le commutateur et le routeur, utilisez le **debug isdn q921 de** commande de privileged exec. Le q921 met au point est documenté dans la *référence de débogage des commandes*. Les debugs se fondent fortement sur des ressources CPU, ainsi précaution d'usage en les utilisant.
Le nombre d'appels/ Contrôle d'appel bloque en service/total RNIS de blocs alloués de Contrôle d'appel	Ces nombres indiquent combien d'appels sont en cours, et le nombre de ressources qui sont allouées pour prendre en charge ces appels. Si le nombre de CCBs alloué est supérieur au nombre de CCBs étant utilisé, considérez qu'il pourrait y a un problème en libérant CCBs. Assurez-vous qu'il y a de CCBs disponible pour des appels entrant.

Routage sur demande de cadran : Exécutions d'interface de numérotation

Le routage sur demande de cadran (DDR) est une méthode de fournir la connectivité WAN sur un économique, un suivant les nécessités, comme liaison principale ou comme sauvegarde pour un lien de liaison série sans numérotation.

Une interface de numérotation est définie en tant que n'importe quelle interface de routeur capable de placer ou de recevoir un appel. Ce terme générique devrait être distingué de l'**interface de numérotation de** terme (avec un D) capital, qui se rapporte à une interface logique configurée pour contrôler un ou plusieurs interfaces physiques d'un routeur et qui est vu en configuration de routeur comme interface dialer X. De ce point en avant, sauf indication contraire, nous utiliserons le numéroteur de terme dans son sens générique.

La configuration de l'interface du numéroteur est livré dans deux saveurs : numéroteur à base de cartes (parfois désigné sous le nom de legs DDR), et Profils de composeur. Quelle méthode vous utilisez dépend des circonstances sous lesquelles vous avez besoin de la Connectivité de cadran. Le numéroteur DDR à base de cartes a été introduit la première fois dans la version IOS 9.0, des Profils de composeur dans la version IOS 11.2.

Déclenchement d'un cadran

Àson coeur, le DDR est juste une extension du routage où des *paquets intéressants* sont conduits à une interface de numérotation, déclenchant une tentative de cadran. Les sections suivantes expliquent les concepts impliqués en définissant le trafic intéressant et expliquent le routage utilisé pour des connexions DDR.

Paquets intéressants

Intéressant est le terme utilisé pour décrire les paquets ou trafiquer qui ou déclencheront une tentative de cadran ou, si une liaison commutée est déjà en activité, remettra à l'état initial le temporisateur de veille sur l'interface de numérotation. Pour qu'un paquet soit considéré intéressant :

- le paquet doit répondre aux critères de « autorisation » définis par une liste d'accès
- la liste d'accès doit être mise en référence par le dialer-list ou le paquet doit être d'un protocole qui est universellement permis par le dialer-list
- la liste d'appels doit être associée avec une interface de numérotation au moyen d'un dialer-group

Des paquets jamais sont automatiquement considérés intéressants (par défaut). Des définitions des paquets intéressants doivent être explicitement déclarées en routeur ou configuration de serveur d'accès.

Groupe de routeurs d'appels

Dans la configuration de chaque interface de numérotation sur le routeur ou le serveur d'accès, il doit y a un ordre de **dialer-group**. Si l'ordre de **dialer-group** n'est pas présent, il n'y a aucun lien logique entre les définitions des paquets intéressants et l'interface. La syntaxe de commande :

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

Le nombre de groupe est le nombre du groupe d'accès par routeur d'appels auquel l'interface spécifique appartient. Ce groupe d'accès est défini avec la commande de **dialer-list**. Les valeurs acceptables sont différentes de zéro, des entiers positifs entre 1 et 10.

Une interface peut être associée avec un seul groupe d'accès par routeur d'appels seulement ; on ne permet pas la plusieurs affectation de dialer-group. Une deuxième affectation de groupe d'accès par routeur d'appels ignorera la première. Un groupe d'accès par routeur d'appels est défini avec l'ordre de **dialer-group**. La commande de **dialer-list** associe une liste d'accès avec un groupe d'accès par routeur d'appels.

Paquets qui apparient le déclencheur de groupe de numéroteur indiqué une demande de connexion.

L'adresse de destination du paquet est évaluée contre la liste d'accès spécifiée dans la commande associée de **dialer-list**. S'il passe, ou un appel est initié (si aucune connexion n'a été déjà établie) ou le temporisateur de veille est remis à l'état initial (si un appel est actuellement connecté).

Liste d'appels

La commande de configuration globale de **dialer-list** est utilisée de définir une liste de numéroteur DDR pour contrôler la composition par protocole, ou par une combinaison de protocole et de liste d'accès. Les paquets intéressants sont ceux qui apparient l'autorisation niveau de la Protocol ou qui sont permis par la liste dans la commande de **dialer-list** : *nom du protocole de* **protocole de** *dialer-group de* **dialer-list {autorisation | refusez |** *access-list-number de* **liste | access-group}**

le dialer-group est le nombre d'un groupe d'accès par routeur d'appels identifié dans n'importe quelle commande de configuration d'interface de dialer-group.

le nom du protocole est l'un des mots clé suivants de protocole : AppleTalk, passerelle, CLNS,

clns_es, clns_is, DECNet, decnet_router-L1, decnet_router-L2, decnet_node, IP, IPX, vignes, ou XNS.

accès d'autorisations d'**autorisation à un** protocole entier.

refusez refuse l'accès à un protocole entier.

la liste spécifie qu'une liste d'accès sera utilisée pour définir une finesse plus correcte qu'un protocole entier.

access-list-number - Les nombres de listes d'accès spécifiés les Listes d'accès dans n'importe quel DECNet, Banyan VINES, IP, de Novell IPX, ou XNS standard ou étendues, y compris l'IPX de Novell ont étendu des Listes d'accès de point d'accès services (SAP) et des types de transition. Voir le tableau 16-7 pour les types et les nombres pris en charge de liste d'accès.

nom de liste de filtre d'*access-group* utilisé dans les commandes de **clns filter-set** et de **clns access-group**.

Tableau 16-7 : Numérotation de liste d'accès de Protocol

Type de liste d'accès	Chaîne de nombre de listes d'accès (décimale)
AppleTalk	600-699
Banyan VINES (standard)	1-100
Banyan VINES (étendu)	101-200
DECNet	300-399
IP (standard)	1-99
IP (étendu)	100-199
IPX de Novell (standard)	800-899
IPX de Novell (étendu)	900-999
Pontage transparent	200-299
XNS	500-599

Liste d'accès

Pour chaque protocole de réseau qui doit être envoyé à travers la connexion de cadran, une liste d'accès peut être configurée. Aux fins du contrôle des coûts, il est habituellement desirable de configurer une liste d'accès afin d'empêcher certain trafic, tel que des mises à jour de routage, d'évoquer ou de maintenir une connexion. Notez que quand nous créons des Listes d'accès afin de définir le trafic intéressant et inintéressant, nous ne déclarent pas que les paquets inintéressants ne peuvent pas croiser la liaison commutée. Nous indiquons juste qu'ils ne remettront pas à l'état initial le temporisateur de veille, ni ils évoqueront une connexion sur leurs propres moyens. Tant que la connexion de cadran est en hausse, on permettra encore aux des paquets inintéressants pour circuler à travers le lien.

Par exemple, un routeur exécutant l'EIGRP en tant que son protocole de routage peut faire configurer une liste d'accès pour déclarer des paquets EIGRP inintéressants et tout autre trafic IP intéressant :

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

Des Listes d'accès peuvent être configurées pour tous les protocoles qui pourraient croiser la liaison commutée. Souvenez-vous cela pour n'importe quel protocole, le comportement par défaut faute de déclaration d'**autorisation de liste d'accès** est de refuser tout le trafic. S'il n'y a aucune liste d'accès et aucune commande de **dialer-list** permettant le protocole, alors ce protocole sera inintéressant. Dans la pratique réelle, s'il n'y a aucune liste d'appels pour un protocole, ces paquets ne circuleront pas à travers le lien du tout.

Exemple - Le remontant tout

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, l'IP et l'IPX sont les protocoles qui peuvent croiser la liaison commutée. L'utilisateur veut empêcher des émissions et des mises à jour de routage d'initier un appel ou de garder le lien.

```
!
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
!
```

On doit permettre un paquet par les déclarations de la **liste d'accès 121**, avant de croiser l'**interface 1 async**, afin de pour être considéré *intéressant*. Dans ce cas, des paquets EIGRP sont refusés, de même que tous les autres paquets d'émission, alors que tout autre trafic IP est permis. Souvenez-vous que ceci n'empêche pas des paquets EIGRP de transiter le lien. Il signifie seulement que ces paquets ne remettront pas à l'état initial le compteur de durée d'inactivité ou initieront une tentative de cadran.

De même, la **liste d'accès 903** déclare le RIP IPX, les sèves et les demandes GNS d'être inintéressant, alors que tout autre trafic IPX est intéressant. Sans ces instructions de refus, la connexion de cadran ne descendrait vraisemblablement jamais et une facture téléphonique très grande résulterait puisque les paquets de ces types circulent constamment à travers un réseau IPX.

Le dialer-group 7 étant configuré sur l'interface asynchrone, nous savons que le **dialer-list 7** est nécessaire pour attacher les filtres de trafic intéressant (c'est-à-dire, Listes d'accès) à l'interface. Une déclaration de **dialer-list** est exigée (et *seulement* une peut être configurée) pour chaque protocole, veillant que le nombre de liste d'appels est identique que le nombre de groupe de routeurs d'appels sur l'interface.

De nouveau, il est important de se souvenir que les *instructions de refus* dans les Listes d'accès

configurées pour définir le trafic intéressant n'empêcheront pas les paquets refusés de croiser le lien.

Utilisant la commande **mettez au point le numéroteur**, vous peut voir l'activité qui déclenche une tentative de cadran :

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

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

Acheminement

Une fois que définis, des paquets intéressants doivent être conduits correctement pour qu'un appel soit initié. Le processus de routage dépend de deux choses : conduisant des entrées de table et « vers le haut » de l'interface au-dessus de laquelle pour conduire des paquets.

Interfaces - up/up (mystification)

Pour que les paquets soient conduits et par à une interface, cette interface doit être up/up comme vu dans des **interfaces d'une exposition** sorties :

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

Qu'arrive à une interface de numérotation qui n'est pas connectée ? Si le protocole n'est pas en service sur l'interface, l'implication est que l'interface elle-même ne sera pas en hausse. Conduit qui se fondent sur cette interface seront vidés de la table de routage, et le trafic ne sera pas conduit à cette interface. Le résultat est qu'aucun appel ne serait initié par l'interface.

La solution pour parer cette possibilité est de permettre l'état **up/up (mystification)** pour des interfaces de numérotation. N'importe quelle interface peut être configurée comme interface de numérotation. Par exemple, une interface série ou une interface asynchrone a pu être transformée en numéroteur en ajoutant l'**intrabande** ou le **dialer dtr de** commande dialer à la configuration de l'interface. Ces lignes sont inutiles pour les interfaces qui sont par nature une interface de numérotation (BRIs et PRIs). La sortie pour une interface d'exposition ressemblera 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 « feint » pour être **up/up** de sorte que les artères associées restent en vigueur et de sorte que des paquets puissent être conduits à l'interface.

Il y a des circonstances sous lesquelles une interface de numérotation ne sera pas **up/up (mystification)**. **La sortie d'interface d'exposition** peut afficher l'interface en tant qu'étant administrativement vers le bas :

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

Administrativement en bas de simplement signifie que l'interface a été configurée avec l'**arrêt de** commande. C'est l'état par défaut de n'importe quelle interface de routeur quand le routeur est amorcé pendant la toute première fois. Pour remédier à de ceci, utilisez la commande de configuration d'interface **aucun arrêt**.

L'interface peut également être vue pour être dans le mode standby :

```
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 car la sauvegarde pour une autre interface. Quand une connexion exige la Redondance en cas de panne, une interface de numérotation peut être installée comme sauvegarde. Ceci est accompli en ajoutant 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 interface** a été configurée, l'interface utilisée comme sauvegarde sera mise dans le mode standby jusqu'au moment où l'interface principale descend à un état de **vers le bas/**. À ce moment-là, l'interface de numérotation configurée comme sauvegarde, ira à un état d'**up/up (mystification)** en attendant un événement de cadran.

Artères et Routes statiques flottantes de charge statique

La manière la plus sûre de conduire des paquets à une interface de numérotation est avec le routage statique. Ces artères sont manuellement entrées dans la configuration du routeur ou du serveur d'accès avec la commande :

*masque de préfixe d'***artère d'IP {***adresse* **|** *interface***} [***distance***]**

préfixe : Préfixe d'artère IP pour la destination.

masque : Masque de préfixe pour la destination.

adresse : Adresse IP du prochain saut qui peut être utilisé pour atteindre le réseau de destination.

interface : Interface réseau à l'utiliser pour le trafic sortant.

distance : (Facultatif) une distance administrative. Cet argument est utilisé dans des Routes statiques flottantes.

Des artères statiques sont utilisées dans les situations où la liaison commutée est la seule connexion au site distant. Une artère statique a une valeur de distance administrative d'un (1), qui la fait préférée au-dessus des artères dynamiques à la même destination.

D'autre part, des Routes statiques flottantes - c.-à-d., les artères statiques avec une distance administrative prédéfinie - sont typiquement utilisées dans les scénarios de sauvegarde DDR. Dans ces scénarios un protocole de routage dynamique, tel que le RIP ou l'EIGRP, conduit des paquets à travers la liaison principale.

Une artère statique normale (la distance administrative = 1) est préférable à l'EIGRP (distance administrative = 90) ou au RIP (distance administrative = 120). L'artère statique cause des paquets d'être conduits à travers la ligne commutée, même si le primaire est haut et capable de passer le trafic. Si, cependant, l'artère statique est configurée avec un supérieur à de distance administrative qui des protocoles de routage dynamique l'uns des en service relatif au routeur, la Route statique flottante sera seulement utilisé faute de « meilleure » artère - une avec une distance administrative inférieure.

Si la sauvegarde DDR est appelée au moyen de la **commande backup interface**, la situation est quelque peu différente. Puisque l'interface de numérotation demeure dans le mode standby tandis que le primaire est, une artère statique ou une Route statique flottante peut être configurée.

L'interface de numérotation ne tentera pas de se connecter jusqu'après que l'interface principale descend **en bas de/**.

Pour une connexion indiquée, le nombre charge statique) statique (ou flottante d'artères nécessaires est une 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 commun ou un sous-réseau, en général seulement une artère statique est exigée. Il indique le RÉSEAU LOCAL distant utilisant l'adresse de l'interface de numérotation de routeur distant comme adresse du prochain saut.

Exemples

Exemple 1 : Le cadran est la seule connexion utilisant les interfaces numérotées. Une artère est suffisante.

Figure 16-4 : Cadran utilisant les 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 : Le cadran est la seule connexion utilisant des interfaces non numérotées. Ceci peut être configuré avec juste une artère, mais il est commun pour configurer deux artères : une route hôte à l'interface de RÉSEAU LOCAL sur le routeur distant et une artère au RÉSEAU LOCAL distant par l'intermédiaire du RÉSEAU LOCAL distant relient. Ceci est fait pour empêcher les problèmes du mappage Layer3-to-Layer2, qui peuvent avoir comme conséquence les 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 : Cadran utilisant des 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 : Le cadran est une connexion de sauvegarde utilisant les interfaces numérotées. Une Route statique flottante est exigée.

Figure 16-6 : Sauvegarde utilisant les 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 : Le cadran est une connexion de sauvegarde utilisant des interfaces non numérotées. Comme dans l'exemple 2 ci-dessus, 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 16-7 : Sauvegarde utilisant des interfaces d'Unumbered

```
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 composeur

Le numéroteur (legs) DDR à base de cartes est puissant et complet, mais ses limites affectent l'évolution et l'extensibilité. Le numéroteur DDR à base de cartes est basé sur une attache statique entre la spécification d'appel de par-destination et la configuration d'interface physique.

Cependant, le numéroteur DDR à base de cartes a également beaucoup de forces. Il prend en charge le Relais de trames, le CLNS OIN, le LAPB, la Fonction Snapshot Routing, et tous les protocoles conduits qui sont pris en charge sur des Routeurs de Cisco. Par défaut, le numéroteur DDR à base de cartes prend en charge la commutation rapide.

En configurant une interface pour appeler sortant, une carte de numéroteur doit être configurée pour chaque destination distante, et pour chaque numéro appelé différent à la destination distante. Par exemple, si vous voulez une connexion de PPP à liaisons multiples en introduisant d'un RNIS BRI dans une autre interface RNIS BRI qui a un numéro dans le répertoire local différent pour chacun de ses canaux B, vous avez besoin d'une carte de numéroteur 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
!
```

La commande dans laquelle des Cartes de composeur sont configurées peut être importante. Si deux commandes ou plus de carte de numéroteur se rapportent à la même adresse distante, le routeur ou le serveur d'accès les essayera l'un après l'autre, dans la commande, jusqu'à ce qu'elle établisse avec succès une connexion

Remarque: L'IOS peut dynamiquement construire des Cartes de composeur sur un routeur recevant un appel. La carte de numéroteur est construite a basé sur le nom d'utilisateur authentifié et l'adresse IP négociée de l'appelant. Des profils d'appel dynamique peuvent seulement être vus dans la sortie du **show dialer map de** commande. Vous ne pouvez pas les visualiser en configuration en cours du routeur ou du serveur d'accès.

Syntaxe de commande

Utilisez la forme suivante de la commande de configuration d'interface de **carte de numéroteur** à :

- configurez une interface série ou l'interface RNIS pour appeler un ou des plusieurs sites, ou
- recevez les appels des plusieurs sites.

Toutes les options sont affichées sous cette première forme de la commande. Pour supprimer une entrée du profil d'appel particulière, utilisez un **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 de **carte de numéroteur** à :

- configurez une interface série ou l'interface RNIS pour placer un appel aux plusieurs sites, et
- pour authentifier des appels des 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 de **carte de numéroteur** de configurer une interface série ou l'interface RNIS pour prendre en charge la transition.

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

Utilisez la forme suivante de la commande de **carte de numéroteur** de configurer une interface asynchrone pour placer un appel à :

- un site unique qui exige un script système ou qui n'a aucun script assigné de modem, ou
- plusieurs sites sur une ligne simple, sur des plusieurs lignes, ou sur un groupe rotatif de routeurs d'appels.`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 clé de Protocol. Utilisation une de ce qui suit : **AppleTalk**, **passerelle**, **CLNS**, **DECNet**, **IP**, **IPX**, **Novell**, **instantané**, **vignes**, ou **XNS**.
- *adresse du prochain saut* - L'adresse de protocole utilisée pour apparier contre les adresses auxquelles les paquets sont destinés. Cet argument n'est pas utilisé avec le mot clé de protocole de **passerelle**.
- **nom** - (facultatif) indique le système distant avec lequel le routeur local ou le serveur d'accès communique. Utilisé pour authentifier le système distant sur des appels entrant.
- *adresse Internet* - nom sensible à la casse ou ID (facultatif) du périphérique distant (habituellement le nom d'hôte). Pour des Routeurs avec des interfaces RNIS, le champ d'*adresse Internet* peut contenir le nombre que l'ID ligne appelant fournit (dans les cas où identification de ligne d'appel, également désignée sous le nom du *CLI*, *Identification de l'appelant*, et *identification du numéro automatique* (ANI), est disponible).
- **spc** - (facultatif) spécifie une connexion semi-permanente entre le matériel de client et l'échange. Il est utilisé seulement en Allemagne pour des circuits entre un RNIS BRI et un commutateur 1TR6 LE RNIS et en Australie pour des circuits entre un PRI RNIS et un commutateur TS-014.
- **vitesse 56 | 64** - mot clé (facultatif) et valeur indiquant la vitesse linéaire dans les kilobits par seconde pour utiliser. Utilisé pour le RNIS seulement. La vitesse par défaut est des 64 Kbits/s.
- **émission** - (facultatif) indique que des émissions devraient être expédiées à cette adresse de protocole.
- **modem-script** - (facultatif) indique le script de modem à utiliser pour la connexion (pour les interfaces asynchrones).
- *le modem-regexp* - l'expression régulière (facultative) à laquelle un script de modem sera apparié (pour les interfaces asynchrones).
- **script système** - (facultatif) indique le script système à utiliser pour la connexion (pour les interfaces asynchrones).
- *système-regexp* - expression régulière (facultative) à laquelle un script système sera apparié (pour les interfaces asynchrones).
- *cadran-chaîne [:* numéro de téléphone (facultatif) de RNIS-*subaddress]* envoyé au périphérique de composition à la reconnaissance des paquets avec une adresse du prochain saut spécifiée qui apparie la liste d'accès définie (et le nombre facultatif de subaddress utilisé

pour les connexions multipoints RNIS). La chaîne de cadran et le subaddress RNIS, si utilisés, doivent être le dernier élément dans la ligne de commande.

Profils de composeur

Remarque: Dans cette section le terme « interface de numérotation » se rapporte à l'interface configurée ; pas à une interface physique sur le routeur ou le serveur d'accès.

L'implémentation de Profils de composeur du DDR, introduite dans la version IOS 11.2, est basée sur une séparation entre logique et la configuration d'interface physique. Les Profils de composeur permettent également les configurations logiques et physiques à lier ensemble dynamiquement sur une base de par-appel.

La méthodologie de Profils de composeur est avantageuse quand vous voulez faire ce qui suit :

- partagez une interface (le RNIS, asynchrone, ou l'interface série synchrone) pour placer ou recevoir des appels
- changez n'importe quelle configuration sur une base par utilisateur (excepté l'encapsulation pendant la première phase des Profils de composeur)
- passerelle à beaucoup de destinations
- évitez les problèmes fendus d'horizon

Les Profils de composeur permettent la configuration des interfaces physiques à séparer de la configuration logique exigée pour un appel, et ils permettent également les configurations logiques et physiques à lier ensemble dynamiquement sur une base de par-appel.

Un profil du numéroteur comprend les éléments suivants :

- Une configuration d'*interface de numérotation* (une entité logique), y compris un ou plusieurs chaînes de cadran (qui est utilisée pour atteindre un sous-réseau de destination)
- *Une classe de profil d'appel* qui définit toutes les caractéristiques pour n'importe quel appel à la chaîne de numérotation indiquée
- *Un groupe de numérotation* commandé d'interfaces physiques à utiliser par l'interface de numérotation

Tout appelle aller à ou de la même utilisation de sous-réseau de destination le même profil du numéroteur.

Une configuration de l'interface du numéroteur inclut toutes les configurations requises pour atteindre un sous-réseau spécifique de destination (et tous réseaux accédés par lui). De plusieurs chaînes de cadran peuvent être spécifiées pour la même interface de numérotation ; chaque chaîne de cadran peut être associée avec une classe de profil d'appel différente. La classe de profil d'appel définit toutes les caractéristiques pour n'importe quel appel à la chaîne de numérotation indiquée. Par exemple, le map-class pour une destination pourrait spécifier une vitesse 56-kbps le RNIS. Le map-class pour une destination différente pourrait spécifier une vitesse 64-kbps le RNIS.

Chaque interface de numérotation utilise un groupe de numérotation, qui est un pool d'interfaces physiques commandé sur la base de la priorité assignée à chaque interface physique. Une interface physique peut appartenir aux pools de numéroteur multiple, avec le conflit résolu par priorité. Les interfaces RNIS BRI et PRI peuvent fixer une limite sur le minimum et le nombre maximal de canaux B réservés par tous les groupes de numérotation. Un canal réservé par un groupe de numérotation demeure inactif jusqu'à ce que le trafic soit dirigé vers le groupe.

Quand des Profils de composeur sont utilisés pour configurer le DDR, une interface physique n'a aucun paramètre de configuration excepté l'encapsulation et les groupes de numérotation auxquels l'interface appartient.

Remarque: Le paragraphe précédent a une exception. Des commandes qui s'appliquent avant que l'authentification soit complète doivent être configurées sur l'interface physique (ou BRI ou PRI) et pas sur le profil du numéroteur. Les Profils de composeur ne copient pas des authentications command de PPP (ou des commandes LCP) sur l'interface physique.

La figure 16-8 affiche une application type des Profils de composeur. Le routeur A a le routage de Connexion à la demande de 1par d'interface de numérotation avec le sous-réseau 1.1.1.0, et l'interface de numérotation 2 pour le routage de Connexion à la demande avec le sous-réseau 2.2.2.0. L'adresse IP pour l'interface de numérotation 1 est son adresse comme noeud dans le 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 pour l'interface de numérotation 2 est son adresse comme noeud dans le réseau 2.2.2.0.

Figure 16-8 : Application typique de Profils de composeur

Une interface de numérotation utilise seulement un groupe de numérotation. Une interface physique, cependant, peut être un membre d'un ou beaucoup de groupes de numérotation, et un groupe de numérotation peut avoir plusieurs interfaces physiques comme membres.

La figure 16-9 montre les relations parmi les concepts de l'interface de numérotation, du groupe de numérotation, et des interfaces physiques. L'interface physique BRI 1 du groupe de numérotation 2. d'utilisations de l'interface de numérotation 0 appartient au groupe de numérotation 2 et a une priorité spécifique dans le groupe. L'interface physique BRI 2 appartient également au groupe de numérotation 2. Puisque le conflit est résolu sur la base des niveaux de priorité des interfaces physiques dans le groupe, BRI 1 et BRI 2 doivent être assignés différentes priorités dans le groupe. Peut-être BRI 1 est assigné la priorité 100 et BRI 2 est assigné la priorité 50 dans le groupe de numérotation 2 (une priorité de 50 est supérieur à par priorité de 100). BRI 2 a une haute priorité dans le groupe, et ses appels seront placés d'abord.

Figure 16-9 : Relations parmi des interfaces de numérotation, des groupes de numérotation, et des interfaces physiques

Étapes de configuration de profil du numéroteur

Commande	But
nombre d'interface dialer	Créez une interface de numérotation.
*masque d'adresse d'***IP address**	Spécifiez l'adresse IP et le masque de l'interface de numérotation comme noeud dans le réseau de destination à s'appeler.
encapsulation ppp	Spécifiez l'encapsulation PPP.
nom d'utilisateur de **dialer remote-name**	Spécifiez le nom d'authentification CHAP de routeur distant.
dialer string dial-string	Spécifiez la destination distante

class class-name	pour appeler et la classe de carte qui définit des caractéristiques pour des appels à cette destination.
poolnumber de numéroteur	Spécifiez le dialing pool pour l'utiliser pour des appels à cette destination.
groupe-nombre de **dialer-group**	Assignez l'interface de numérotation à un groupe de routeurs d'appels.
nom du protocole de **protocole de** *dialer-group de* **dialer-list {autorisation | refusez |** *access-list-number de* **liste}**	Spécifiez une liste d'accès par le numéro de liste ou par protocole et numéro de liste pour définir les paquets « intéressants » qui peuvent déclencher un appel.

Opérations PPP

Le Protocole point à point (PPP) est de loin le protocole de transport de couche de liaison le plus commun, ayant complètement usurpé le SLIP comme protocole de choix pour le cadran (et dans de nombreux cas, non-cadran) synchrone et les connexions de série asynchrone. Le PPP a été initialement défini en 1989 par RFC 1134, qui a été depuis rendu Désuet(e) par une gamme de RFC aboutissant (en date de cette écriture) à RFC1661. Il y a également des RFC nombreux qui définissent des éléments du protocole, tels que RFC1990 (le ppp multilink Protocol), RFC2125 (l'allocation Protocol de bande passante de PPP), et beaucoup d'autres. Un référentiel en ligne des RFC peut être trouvé à :

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

Peut-être la meilleure définition du PPP peut être trouvée dans RFC1661, qui énonce :

Le Protocole point à point (PPP) fournit une méthode standard pour transporter les datagrammes multiprotocole au-dessus des liens point par point. Le PPP est composé de trois composants principaux :

1. Une méthode pour encapsuler les datagrammes multiprotocole.
2. Un Link Control Protocol (LCP) pour établir, configurer, et tester la connexion logique.
3. Une famille des protocoles de contrôle de réseau (NCPs) pour établir et configurer différents protocoles de couche réseau.

Phases de négociation PPP

La négociation PPP se compose de trois phases : Link Control Protocol (LCP), authentification, et protocole de contrôle de réseau (NCP). Chacun poursuit dans la commande, suivant l'établissement de l'async ou de la connexion RNIS.

LCP

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

Quand la négociation commence, chacun des pairs voulant établir une connexion PPP doit envoyer une demande de configurer (vue dans le **debug ppp negotiation** et désignée ci-après sous le nom de CONFREQ). Incluses dans le CONFREQ sont toutes les options qui ne sont pas le par défaut de lien. Ceux-ci incluent souvent le maximum reçoivent l'unité (MRU), la table de caractères async de contrôle (ACCM), l'authentification Protocol (AuthProto), et le nombre magique. Également vus sont le maximum reçoivent l'unité reconstruite (MRRU) et le discriminateur de point d'extrémité (EndpointDisc), utilisé pour le PPP à liaisons multiples.

Il y a trois réponses possibles à n'importe quel CONFREQ :

- Une Configurer-reconnaissance (CONFACK) doit être émise si le pair identifie les options et est d'accord sur les valeurs vues dans le CONFREQ.
- Une Configurer-anomalie (CONFREJ) doit être envoyée si des options l'unes des dans le CONFREQ ne sont pas identifiées (par exemple, quelques options de constructeur-particularité) ou si les valeurs pour des options l'unes des ont été explicitement rejetées dans la configuration du pair.
- Une Configurer-Négatif-reconnaissance (CONFNAK) doit être envoyée si toutes les options dans le CONFREQ sont identifiées, mais le ne sont pas acceptables de valeurs au pair.

Les deux pairs continuent à permuter CONFREQs, CONFREJs et CONFNAKs jusqu'à ce que chacun envoie un CONFACK, jusqu'à ce que la connexion de cadran soit cassée, ou jusqu'à un ou à chacun des deux pairs indique que la négociation ne peut pas être terminée.

Authentification

Après la réussite de la négociation LCP et de conclure un accord sur AuthProto, l'étape suivante est authentification. L'authentification, tandis que non obligatoire par RFC1661, est fortement recommandée sur toutes les connexions de cadran. Parfois, c'est une condition requise pour le bon fonctionnement ; Profils de composeur étant un exemple.

Les deux principaux types d'authentification dans le PPP sont le Password Authentication Protocol (PAP) et le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol), définis par RFC1334 et mis à jour par RFC1994.

Le PAP est le plus simple des deux, mais est moins sécurisé parce que le mot de passe de texte brut est envoyé à travers la connexion de cadran. Le CHAP est plus sécurisé parce que le mot de passe de texte brut n'est pas jamais envoyé à travers la connexion de cadran.

Le PAP peut être nécessaire dans un des environnements suivants :

- Grandes bases installées d'applications clientes qui ne prennent en charge pas le CHAP
- Incompatibilités entre les réalisations de différent constructeur du CHAP

En discutant l'authentification, il est utile d'employer les termes « demandeur » et « authentificateur » pour distinguer les rôles joués par les périphériques à l'un ou l'autre d'extrémité de la connexion, bien que l'un ou l'autre de pair puisse agir dans l'un ou l'autre de rôle. Le « demandeur » décrit le périphérique qui demande l'accès au réseau et fournit les informations d'authentification ; le « authentificateur » vérifie la validité des informations d'authentification et permet ou rejette la connexion. Il est commun pour que les deux pairs agissent dans les deux

rôles quand une connexion DDR est établie entre les Routeurs.

PAP

Le PAP est assez simple. Après la réussite de la négociation LCP, le demandeur envoie à plusieurs reprises sa combinaison de nom d'utilisateur/mot de passe à travers le lien jusqu'à ce que l'authentificateur réponde avec un accusé de réception ou jusqu'à ce que le lien est cassé. L'authentificateur peut déconnecter le lien s'il détermine que la combinaison de nom d'utilisateur/mot de passe est non valide.

CHAP

Le CHAP est en quelque sorte plus compliqué. L'authentificateur envoie un défi au demandeur, qui répond alors avec une valeur. Cette valeur est calculée à l'aide d'une fonction « d'informations parasites à sens unique » pour hacher le défi et le mot de passe CHAP ensemble. La valeur en résultant est envoyée à l'authentificateur avec l'adresse Internet du CHAP du demandeur (qui peut être différente de son adresse Internet réelle) dans un message de *réponse*.

L'authentificateur lit l'adresse Internet dans le message de réponse, des consultations le mot de passe prévu pour cette adresse Internet, et puis calcule la valeur qu'elle attend le demandeur introduit sa réponse en exécutant la même fonction d'informations parasites le demandeur exécuté. Si résulter évalue la correspondance, l'authentification est réussie. La panne devrait mener à un débranchement.

AAA

Un service d'authentification, d'autorisation et de comptabilité (AAA), tel que TACACS+ ou RAYON, peut être utilisé en accomplissant le PAP ou le CHAP.

NCP

Après l'authentification réussie, la phase de NCP commence. Comme dans LCP, les pairs permutent CONFREQs, CONFREJs, CONFNAKs et CONFACKs. Cependant, dans cette phase de négociation, les éléments étant négociés doivent faire avec des protocoles de couche plus élevée - IP, IPX, jetant un pont sur, CDP, et ainsi de suite. Un ou plusieurs de ces protocoles peuvent être négociés. Car il est le plus utilisé généralement, et parce que d'autres protocoles actionnent dans le plus ou moins la même mode, le Control Protocol d'Internet Protocol (IPCP), défini dans RFC1332, est le centre de cette discussion. D'autres RFC pertinents incluent, mais ne sont pas limités à :

- RFC1552 (protocole de contrôle IPX)
- RFC1378 (protocole de contrôle Appletalk)
- RFC1638 (jetant un pont sur le Control Protocol)
- RFC1762 (Control Protocol de DECNet)
- RFC1763 (Control Protocol de vignes)

En outre, le Control Protocol de Cisco Discovery Protocol (CDPCP) peut être négocié pendant le NCP, bien que ce ne soit pas commun. Les ingénieurs TAC Cisco informeront habituellement que la commande aucun cdp enable soit configurée sur l'intégralité d'interfaces de numérotation d'empêcher des paquets de CDP gardant un appeler indéfiniment.

L'élément principal négocié dans IPCP est l'adresse de chaque pair. Chacun des pairs est dans un de deux états possibles ; ou il a une adresse IP ou il ne fait pas. Si le pair a déjà une adresse, elle enverra cette adresse dans un CONFREQ à l'autre pair. Si l'adresse semble acceptable à l'autre pair, un CONFACK sera retourné. Si l'adresse n'est pas acceptable, la réponse sera un CONFNAK contenant une adresse pour que le pair l'utilise.

Si le pair n'a aucune adresse, elle enverra un CONFREQ avec l'adresse 0.0.0.0. Ceci indique l'autre pair assigner une adresse, qui est accomplie par l'envoi d'un CONFNAK avec l'adresse appropriée.

D'autres options peuvent être négociées dans IPCP. Généralement - vues sont les adresses primaires et secondaires pour le Domain Name Server et le serveur de noms de NetBIOS, comme décrit dans RFC1877 informationnel. Le protocole de compression IP (RFC1332) est également commun.

Méthodologies PPP alternatives

Les méthodologies PPP alternatives incluent le PPP à liaisons multiples, le PPP de multichassis, et les Profils virtuels.

Multilink PPP

La caractéristique du protocole point-à-point de Multilien (MLP) fournit la fonctionnalité d'Équilibrage de charge au-dessus des plusieurs liaisons WAN. En même temps il fournit l'Interopérabilité pluri-constructeurs, la fragmentation de paquets et le séquençage approprié, et le calcul de charge sur des les deux le trafic en entrée et en sortie. L'implémentation de Cisco du PPP à liaisons multiples prend en charge les caractéristiques de fragmentation et de séquençage de paquet dans RFC1717.

Le PPP à liaisons multiples permet des paquets à fragmenter. Ces fragments peuvent être envoyés en même temps au-dessus de plusieurs liens point par point à la même adresse distante. Les plusieurs liens sont soulevés en réponse à un seuil de charge de routeur d'appels que vous définissez. Le chargement peut être calculé sur le trafic d'arrivée, le trafic sortant, ou sur l'un ou l'autre, comme nécessaire pour le trafic entre les sites spécifiques. MLP fournit le à la demande de bande passante et réduit la latence de transmission à travers des liens WAN.

Le PPP à liaisons multiples fonctionne au-dessus des types d'interface suivants (choisissez ou multiple) qui sont configurés pour prendre en charge des groupes tournants et l'encapsulation PPP de Connexion à la demande :

- interfaces de série asynchrone
- BRIs
- PRIs

Configuration

Pour configurer le PPP à liaisons multiples sur les interfaces asynchrones, vous configurez les interfaces asynchrones pour prendre en charge le DDR et l'encapsulation PPP. Vous configurez alors une interface de numérotation pour prendre en charge l'encapsulation PPP, le à la demande de bande passante, et le PPP à liaisons multiples. À un certain point, cependant, ajouter des interfaces plus asynchrones n'améliore pas la représentation. Avec la taille de MTU par défaut, le

PPP à liaisons multiples devrait prendre en charge trois interfaces asynchrones utilisant les Modems V.34. Cependant, des paquets pourraient être lâchés de temps en temps si le MTU est petit ou si les grandes rafales des trames courtes se produisent.

Pour activer le PPP à liaisons multiples sur une interface simple RNIS BRI ou PRI, vous n'êtes pas requis de définir un groupe rotatif de routeurs d'appels séparément parce que les interfaces RNIS sont des groupes rotatifs de routeurs d'appels par défaut. Si vous n'utilisez pas des procédures d'authentification de PPP, votre service de téléphonie doit passer les informations d'identification de l'appelant.

Un nombre de seuil de charge est exigé. Pour un exemple de configurer le PPP à liaisons multiples sur une interface simple RNIS BRI, voyez l'*exemple de liaison multiple PPP sur une interface RNIS* ci-dessous.

Quand le PPP à liaisons multiples est configuré et vous voulez qu'un ensemble multiliaison soit connecté indéfiniment, utilisez la commande de **dialer idle-timeout** de placer un temporisateur de veille très élevé. La commande du **seuil de charge de routeur d'appels 1** ne garde pas un ensemble multiliaison de liens *n* connectés indéfiniment, et la commande du **seuil de charge de routeur d'appels 2** ne garde pas un ensemble multiliaison de deux liens connectés indéfiniment.

Pour activer le PPP à liaisons multiples sur le multiple le RNIS BRI ou les interfaces PRI, vous installez une interface rotary de numéroteur et la configurez pour le PPP à liaisons multiples. Vous configurez alors le BRIs séparément et les ajoutez chacun au même groupe tournant. Voyez l'*exemple de liaison multiple PPP sur de plusieurs interfaces RNIS* ci-dessous.

Exemple de liaison multiple PPP sur une interface RNIS

L'exemple suivant active le PPP à liaisons multiples sur l'interface 0 BRI. Quand un BRI est configuré, aucune configuration de groupe rotatif de routeurs d'appels n'est exigée (l'interface RNIS est un groupe tournant 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 liaison multiple PPP sur de plusieurs interfaces RNIS

L'exemple suivant configure le multiple le RNIS BRIs pour appartenir au même groupe rotatif de routeurs d'appels pour le PPP à liaisons multiples. Utilisez l'ordre de **groupe rotatif de routeurs d'appels** d'assigner chacun du RNIS BRIs à ce groupe rotatif de routeurs d'appels qui doit apparier le nombre 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 de Multichassis Multilink

Le PPP à liaisons multiples fournit la capacité de séparer et de recombiner des paquets à un système d'extrémité simple à travers un conduit logique (également appelé un *paquet*) constitué par de plusieurs liens. Le PPP à liaisons multiples fournit le à la demande de bande passante et réduit la latence de transmission à travers des liens WAN.

Le PPP de Multichassis Multilink (MMP), d'autre part, fournit la capacité supplémentaire pour que les liens se terminent aux plusieurs routeurs avec différentes adresses distantes. MMP peut également traiter l'analogue et le trafic numérique.

Cette fonctionnalité est destinée pour les situations dans lesquelles il y a de grands groupes d'utilisateurs en accès entrant, dans lesquels un unique serveur d'accès ne peut pas fournir assez de ports d'accès distant. MMP permet à des sociétés pour fournir un seul numéro d'appel à ses utilisateurs et pour appliquer la même solution aux appels analogiques et numériques. Cette caractéristique permet à des fournisseurs de services d'Internet, par exemple, pour allouer un seul nombre rotatif RNIS à plusieurs PRIs RNIS à travers plusieurs Routeurs.

Pour une description complète des commandes MMP référencées dans le présent, référez-vous à la *référence de commandes de solutions de cadran de Cisco*. Pour localiser la documentation d'autres commandes qui apparaissent en ce chapitre, utilisent l'index principal de référence de commandes ou le recherchent en ligne.

MMP est pris en charge sur le Cisco 7500, 4500, et des Plateformes de gamme 2500 et sur l'interface série, la série asynchrone, le RNIS BRI, le PRI RNIS, et les interfaces de numérotation synchrones.

MMP n'exige pas la reconfiguration des Commutateurs d'opérateur téléphonique.

Configuration

Des Routeurs ou les serveurs d'accès sont configurés pour appartenir aux groupes de pairs, des *groupes de pile des appels*. Tous les membres du groupe de pile sont des pairs ; les groupes de pile n'ont pas besoin d'un routeur permanent de pôle. N'importe quel membre du groupe de pile peut répondre à des appels provenant un seul nombre d'accès, qui est habituellement un groupe de recherche de PRI RNIS. Les appels peuvent entrer des périphériques d'utilisateur distant, tels que des Routeurs, des Modems, des adaptateurs terminaux RNIS, ou des cartes PC.

Une fois qu'une connexion est établie avec un membre d'un *groupe de pile*, ce membre possède l'appel. Si un deuxième appel entre du même client et un routeur différent répond à l'appel, le routeur établit un tunnel et en avant tous paquets appartenant à l'appel au routeur qui possède l'appel. Le processus d'établir un tunnel et de la transmission appelle par lui au routeur qui

possède l'appel s'appelle parfois *projection du lien de PPP au maître d'appel*.

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 en avant tous les appels à lui. En pareil cas, les autres membres du groupe de pile sont juste des réponses aux appels et le trafic d'expédition au plus puissant *débarquent le* routeur.

Remarque: les lignes WAN de Haute-latence entre les membres du groupe de pile peuvent rendre l'exécution de groupe de pile inefficace.

La gestion des appels MMP, offrant, et posent 2 opérations à terme dans le groupe de pile opèrent comme suit. On lui affiche également dans la figure 16-10.

1. Quand le premier appel entre au groupe de pile, des réponses du routeur A.
2. Dans l'offre, le routeur A gagne parce qu'elle a déjà l'appel. Le routeur A devient l'appel-*maître* pour cette session avec le périphérique distant. Le routeur A pourrait également s'appeler l'*hôte à l'interface du lot principal*.
3. Quand le périphérique distant qui a initié l'appel a besoin de plus de bande passante, il fait un deuxième appel de PPP à liaisons multiples au groupe.
4. Quand le deuxième appel entre, le routeur D lui répond et informe le groupe de pile. Le routeur A gagne l'offre parce qu'elle déjà manipule la session avec ce périphérique distant.
5. Le routeur D établit un tunnel au routeur A et en avant les données brutes de PPP au routeur A.
6. Le routeur A rassemble et des re-ordres les paquets.
7. Si plus appelle entré au routeur D et elles appartiennent aussi au routeur A, le tunnel entre A et D agrandit pour traiter le trafic ajouté. Le routeur D n'établit pas un tunnel supplémentaire au R.
8. Si plus appelle entré et est répondu par n'importe quel autre routeur, ce routeur établit également un tunnel à A et en avant aux données brutes de PPP.
9. Les données rassemblées sont passées sur le réseau d'entreprise comme si elles toutes avaient été livré par un lien physique.

Figure 16-10 : Scénario typique de PPP de Multichassis Multilink

Contrairement à la figure précédente, la figure 16-11 comporte un routeur de débarquement. Les serveurs d'accès qui appartiennent aux appels d'une réponse de groupe de pile, établissent des tunnels, et en avant appellent à Cisco 4700 un routeur qui gagne l'offre et sont l'appel-maître pour tous les appels. Cisco 4700 rassemble et des re-ordres tous les paquets étant livré dedans par le groupe de pile.

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

Remarque: Vous pouvez établir des groupes de pile utilisant le serveur d'accès différent, la commutation, et les Plateformes de routeur. Cependant, des serveurs d'accès universels tels que Cisco AS5200 ne devraient pas être combinés avec le RNIS. Ceci devrait seulement être fait avec des serveurs d'accès tels que la plate-forme 4x00. Puisque des appels du bureau central sont alloués d'une manière arbitraire, cette combinaison pourrait avoir comme conséquence un appel analogique étant livré à un serveur d'accès réservé numérique, qui ne pourrait pas traiter l'appel.

Le support MMP sur un groupe de Routeurs exige que chaque routeur soit configuré pour prendre en charge ce qui suit :

- Multilink PPP
- Groupe de pile offrant Protocol (SGBP)
- Modèle virtuel utilisé pour copier la configuration d'interface pour prendre en charge MMP

Profils virtuels

Les Profils virtuels sont une seule application de Protocole point à point (PPP) qui peut créer et configure une interface d'accès virtuelle dynamiquement quand un appel d'accès distant est reçu, et démolir l'interface dynamiquement quand l'appel finit. Les Profils virtuels fonctionnent avec le PPP simple et avec le PPP à liaisons multiples (MLP).

Les informations de configuration pour une interface d'accès virtuelle de Profils virtuels peuvent provenir une interface de modèle virtuel, ou de la configuration spécifique à l'utilisateur enregistrée sur un serveur d'Authentification, autorisation et comptabilité (AAA), ou chacun des deux.

La configuration d'AAA propre à l'utilisateur utilisée par des Profils virtuels est *configuration d'interface* et est téléchargée pendant les négociations LCP. Une autre caractéristique, appelée la Configuration propre à l'utilisateur, utilise également les informations de configuration obtenues d'un serveur d'AAA. Cependant, la Configuration propre à l'utilisateur utilise la *configuration réseau* (telle que des Listes d'accès et des filtres d'artère) téléchargée pendant les négociations de NCP.

Deux règles régissent la configuration de l'interface d'accès virtuel par des interfaces de modèle virtuel de Profils virtuels et des configurations d'AAA :

- Chaque application d'accès virtuelle peut dont avoir, tout au plus, un modèle à copier. Cependant, il peut avoir des configurations AAA multiples dont pour copier (les informations d'AAA de Profils virtuels et la Configuration propre à l'utilisateur d'AAA, qui consécutivement pourrait inclure la configuration pour de plusieurs protocoles).
- Quand des Profils virtuels sont configurés par le modèle virtuel, son modèle a la haute priorité que n'importe quel autre modèle virtuel.

Voyez « Interopérabilité avec la section d'autres fonctionnalités de numérotation de Cisco » ci-dessous pour une description des ordres possibles de configuration qui dépendent de la présence ou de l'absence par un MLP ou une caractéristique virtuelle différente d'accès qui copie une interface de modèle virtuel.

Cette caractéristique fonctionne sur toutes les plates-formes Cisco IOS qui prennent en charge MLP.

Pour une description complète des commandes mentionnées dans cette section, référez-vous aux « Profils virtuels commande » le chapitre dans la *référence de commandes de solutions de cadran* dans le positionnement de documentation Cisco IOS. Pour localiser la documentation d'autres commandes qui apparaissent en ce chapitre, vous pouvez utiliser l'index principal de référence de commandes ou le rechercher en ligne.

Informations générales

Cette section présente l'information générale au sujet des Profils virtuels pour vous aider à comprendre cette application avant que vous commenciez à la configurer.

Restrictions

Nous recommandons que des adresses non-numérotées soient utilisées dans les interfaces de modèle virtuel pour s'assurer que des adresses de réseau en double ne sont pas créées sur les interfaces d'accès virtuelles.

Conditions préalables

L'utilisation des informations de configuration d'interface AAA propre à l'utilisateur avec des Profils virtuels exige du routeur d'être configuré pour l'AAA et exige du serveur d'AAA d'avoir des paires AV de configuration de l'interface propre à utilisateur. Les paires AV appropriées (sur un serveur de RAYON) commencent comme suit :

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

Les informations qui suivent le signe d'égalité (=) pourraient être n'importe quelle commande de configuration d'interface de Cisco IOS. Par exemple, la ligne pourrait 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 exige d'un modèle virtuel d'être défini spécifiquement pour des Profils virtuels.

Interopérabilité avec d'autres fonctionnalités de numérotation de Cisco

Les Profils virtuels interopèrent avec Cisco DDR, PPP à liaisons multiples (MLP), et numéroteurs tels que le RNIS.

Configuration DDR des interfaces physiques

Les Profils virtuels interopèrent entièrement avec des interfaces physiques dans les états suivants de configuration DDR quand la pas autre application virtuelle d'interface d'accès est configurée :

- Des Profils de composeur sont configurés pour l'interface. Le profil du numéroteur est utilisé au lieu de la configuration de Profils virtuels.
- Le DDR n'est pas configuré sur l'interface. Les Profils virtuels ignorent la configuration en cours.
- Le legs DDR est configuré sur l'interface. Les Profils virtuels ignorent la configuration en cours.

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

Effet de PPP à liaisons multiples sur la configuration de l'interface d'accès virtuel

Suivant les indications du tableau 16-8, la configuration exacte d'une interface d'accès virtuelle dépend des trois facteurs suivants :

- Si des Profils virtuels sont configurés par le modèle virtuel, par AAA, par chacun des deux, ou par ni l'un ni l'autre. Ces états sont affichés en tant que « VT VP seulement, » « AAA VP seulement, » « VT VP et AAA VP, » et « aucun VP du tout, » respectivement, dans la table.

- La présence ou l'absence d'une interface de numérotation.
- La présence ou l'absence de protocole MLP. L'étiquette « MLP » de colonne est un remplacement n'importe quelle caractéristique virtuelle d'accès qui prend en charge MLP et le copie d'une interface de modèle virtuel.

Dans le tableau 16-8, le « VT de Multilien » signifie qu'une interface de modèle virtuel est copiée *si* on est défini pour MLP ou une caractéristique virtuelle d'accès qui utilise MLP.

Tableau 16-8 : Ordre de clonage de configuration de Profils virtuels

Configuration de Profils virtuels	MLP aucun numéroteur	Numéroteur MLP	Aucun MLP aucun numéroteur	Aucun numéroteur MLP
VT VP seulement	VT VP	VT VP	VT VP	VT VP
AAA VP seulement	(VT de Multilien) AAA VP	(VT de Multilien) AAA VP	AAA VP	AAA VP
VT VP et AAA VP	AAA VT VP VP	AAA VT VP VP	AAA VT VP VP	AAA VT VP VP
Aucun VP du tout	(VT de Multilien)	Numéroteur	Aucune interface d'accès virtuelle n'est créée.	Aucune interface d'accès virtuelle n'est créée.

La commande des éléments en n'importe quelle cellule de la table est importante. Là où le VT VP est affiché ci-dessus l'AAA VP, il signifie que d'abord le modèle virtuel de Profils virtuels est copié sur l'interface, et alors la configuration d'interface AAA pour l'utilisateur est appliquée à elle. La configuration d'interface AAA propre à l'utilisateur ajoute à la configuration et ignore toutes les commandes contradictoires d'interface physique ou de configuration de modèle virtuel.

Interopérabilité avec d'autres configurations qui utilisent les modèles virtuels

Les Profils virtuels interopèrent également avec les applications d'accès virtuelles qui copient une interface de modèle virtuel. Chaque application d'accès virtuelle peut dont avoir, tout au plus, un modèle à copier, mais peut copier des configurations AAA multiples.

L'interaction entre les Profils virtuels et d'autres applications virtuelles de modèle est comme suit :

- Si des Profils virtuels sont activés et un modèle virtuel est défini pour lui, le modèle virtuel de Profils virtuels est utilisé.
- Si des Profils virtuels sont configurés par seul AAA (aucun modèle virtuel n'est défini pour des Profils virtuels), le modèle virtuel pour une autre application d'accès virtuelle (VPDN, par exemple) peut être copié sur l'interface d'accès virtuelle.
- Un modèle virtuel, le cas échéant, est copié à une interface d'accès virtuelle avant la configuration d'AAA de Profils virtuels ou la Configuration propre à l'utilisateur d'AAA. La

Configuration propre à l'utilisateur d'AAA, si utilisée, est bout appliqué.

Terminologie

Les nouveaux ou rares termes suivants sont utilisés en ce chapitre :

Paire AV : Un paramètre de configuration sur un serveur d'AAA ; une partie de la configuration utilisateur que le serveur d'AAA envoie au routeur, en réponse aux demandes d'autorisation d'utilisateur-particularité. Le routeur interprète chaque paire AV comme commande de configuration de routeur Cisco IOS et applique les paires AV dans la commande. En ce chapitre, la paire AV de terme se rapporte à un paramètre de configuration d'interface sur un serveur de RAYON.

Une paire AV de configuration d'interface pour des Profils virtuels peut prendre une forme de ce type :

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

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

interface d'accès virtuelle : Exemple d'une seule interface virtuelle qui est créée dynamiquement et existe temporairement. Des interfaces d'accès virtuelles peuvent être créées et configurées différemment par des applications différentes, telles que des Profils virtuels et des réseaux de connexion privée virtuelle.

interface de modèle virtuel : Configuration d'interface générique pour certains utilisateurs ou pour un certain but, plus les informations dépendantes du routeur. Ceci prend la forme d'une liste de commandes d'interface de Cisco IOS d'être appliqué à l'interface virtuelle comme nécessaire.

profil virtuel : L'exemple d'une seule interface d'accès virtuelle qui est créée dynamiquement quand certains utilisateurs appellent dedans, et est démoli dynamiquement quand l'appel déconnecte. Le profil virtuel d'un utilisateur spécifique peut être configuré par une interface de modèle virtuel, configuration de l'interface propre à utilisateur enregistrée sur un serveur d'AAA, ou une interface de modèle virtuel et configuration de l'interface propre à utilisateur d'AAA.

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

Exemple annoté de négociation PPP

Dans cet exemple, un ping évoque une liaison RNIS entre les Routeurs *Montecito* et *Goleta*. Notez que, alors qu'il n'y a aucun horodatage dans cet exemple, on le recommande habituellement que vous utilisiez les **horodateurs de service de** commande de configuration globale **mettiez au point la milliseconde date-heure**.

Figure 16-12 : Routeur-RNIS-routeur

Ceux-ci met au point sont pris de *Montecito* ; cependant, l'élimination des imperfections sur *Goleta* regarderait la plus ou moins même chose.

Remarque: Votre met au point peut apparaître dans un format différent. Cette sortie est le format plus ancien de sortie de débogage de PPP, avant les modifications introduites dans la version IOS 11.2(8). Voir le chapitre 17 pour un exemple de l'élimination des imperfections de PPP dans de plus nouvelles versions 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 d'initier une tentative de cadran.

B - La connexion est établie (le RNIS met au point non utilisé dans cet exemple).

Commencez LCP :

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

D - *Goleta* envoie son CONFREQs. Si la valeur pour MAGICNUMBER est identique que la valeur envoyée par *Montecito*, il y a une probabilité forte que la ligne est faite une boucle.

E - Ceci indique que *Montecito* a envoyé des accusés de réception à CONFREQs de *Goleta*.

F - *Montecito* reçoit CONFACKs de *Goleta*.

Commencez phase d'authentification :

G, H - Défi de *Montecito* et de *Goleta* pour l'authentification.

J - *Goleta* relève le défi.

K, L - *Goleta* passe avec succès l'authentification.

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

La négociation de 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 artère est installée de *Montecito* sur *Goleta* et le protocole relatif à l'interface change à « vers le haut de », indiquant que les négociations de NCP se sont terminées avec succès.

Avant d'appeler l'équipe de Cisco Systems TAC

Avant d'appeler le centre d'assistance technique de Cisco Systems (TAC), veillez-vous pour avoir lu par ce chapitre et pour s'être terminé les actions suggérées pour votre problème de système.

Supplémentaire, faites le suivant et documentez les résultats de sorte que nous puissions mieux vous aider :

Pour tous les problèmes, collectez la sortie du **show running-config** et du **show version**. Assurez-vous que les **horodateurs de service de** commande **mettent au point la milliseconde date-heure** est dans la configuration.

Pour des problèmes DDR, collectez ce qui suit :

- **show dialer map**
- **mettez au point le numéroteur**
- **debug ppp negotiation**
- **debug ppp authentication**

Si le RNIS est impliqué, collectez :

- **état de show isdn**
- **debug isdn q931**
- **debug isdn event**

Si les Modems sont impliqués, collectez :

- shows line
- show line [x]
- **show modem** (si les modems intégrés sont impliqués)
- **show modem version** (si les modems intégrés sont impliqués)
- **debug modem**
- **debug modem csm** (si les modems intégrés sont impliqués)
- **mettez au point la conversation** (si un scénario DDR)

Si T1 ou PRIs sont impliqué, collectez :

- **t1 de show controller**

Informations connexes

- Guide de solutions de numérotation de Cisco IOS
- Aperçu des interfaces, des contrôleurs, et des lignes utilisées pour l'accès commuté
- Routage à travers des lignes du modem
- Configuration de port série et de joncteur réseau T1/E1
- Concevoir des interréseaux DDR

- Décision et préparation pour configurer du DDR
- Configurer DDRtitle
- Vue d'ensemble de la technologie de PPP
- Concevoir des interréseaux RNIS
- Types, codes et valeurs de commutateurs RNIS
- Ravitaillement la ligne RNIS
- Support et documentation techniques - Cisco Systems