Présentation et dépannage des problèmes Novell IP et IPX courants

Contenu

Introduction

Ce document fournit un certain divers relatif à l'information au protocole IPX. Notre idée n'est pas de documenter entièrement le Novell, mais crée plutôt une liste minimale de questions fréquentes classifiées par des thèmes.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Conventions

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

Informations générales

Compréhension des numéros de réseau IPX

Comme avec d'autres adresses réseau, les adresses de réseau Novell IPX doivent être seules. Ces adresses sont représentées dans le format hexadécimal et se composent de deux parts : un network number et un numéro du noeud. Le numéro de réseau IPX, qui est assigné par l'administrateur réseau, est 32 bits longs. Le numéro du noeud, qui est habituellement l'adresse de Contrôle d'accès au support (MAC) pour un des networks interface cards du système (NIC), est 48 bits longs.

- Réseau32 nombres de bits représentés dans l'hexaAdministrativement assignéPlage : 0x00000001 - 0xFFFFFFFE0xFFFFFFFF = émission0xFFFFFFFE = default route
- Noeud :48 nombres de bits représentés dans l'hexaAdresse MAC de carte NIC (peut être administrativement assigné)

L'utilisation de l'IPX d'une adresse MAC pour le numéro du noeud permet au système d'envoyer des Noeuds pour prévoir quelle adresse MAC à l'utiliser sur une liaison de données. (En revanche, parce que la partie hôte d'une adresse de réseau IP n'a aucune corrélation à l'adresse MAC, les Noeuds IP doivent employer le Protocole ARP (Address Resolution Protocol) pour déterminer l'adresse MAC de destination.)

Le système d'adressage a initialement permis 0xFFFFFFFE à utiliser comme adresse. Après l'introduction du NLSP, le réseau -2 est utilisé pour représenter le default route. Les Routeurs de Cisco traiteront 0xFFFFFFFE comme default route, bien qu'il soit réglable.

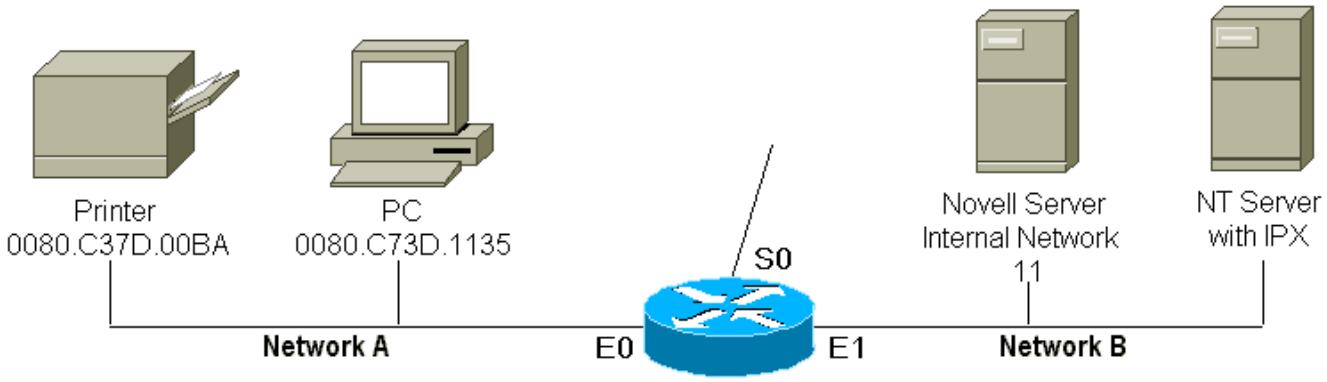
Exemples des adresses Network.Node

C15C0.0000.0000.0001

BAD.0000.123d.3423

Compréhension interne et numéros de réseau externe sur des serveurs Novell

Depuis l'introduction de NetWare 3.x, l'architecture du serveur a été modulairement construite et chaque processus (passerelle, routage, fichier, copie) communique avec l'engine de SYSTÈME D'EXPLOITATION de noyau de multitâche. Les principales engines de SYSTÈME D'EXPLOITATION sont assignées une adresse de réseau IPX connue sous le nom de numéro de réseau interne, et cet ID de noeud est toujours 0000.0000.0001. Par conséquent, chaque serveur du Novell 3.x/4.x a un numéro de réseau interne avec un numéro de réseau externe attaché à l'adaptateur réseau. L'adaptateur réseau peut être lié à de plusieurs adresses réseau chacune avec un seul type de trame. En outre, les serveurs Novell peuvent contenir de plusieurs adaptateurs réseau et artère entre les segments de réseau indépendant. Un IPX de serveur exécutant de Microsoft NT n'apparaîtra pas avec l'ID de noeud de 0000.0000.0001 et n'utilise pas le concept d'interne et le numéro de réseau externe par défaut.




```
IPX Routing  0000.0C34.E923

interface ethernet 0
   ipx network A

interface ethernet 1
   ipx network B
```

Device	Network	Node
Printer	A	0080.C73D.00BA
PC	A	0080.C73D.1135
RTR-E0	A	0000.0C34.C923
RTR-E1	B	0000.0C29.DCFA
Novell Server (Int)	11	0000.0000.0001
Novell Server (Ext)	B	0000.1B3D.5678

Encapsulation Novell

Il y a beaucoup de différentes encapsulations Novell. Pour des Ethernets seulement, il y a autant d'en tant que quatre. Le type d'encapsulation est très important en tant que deux périphériques suivre différentes méthodes d'encapsulation sur le même support ne pourra pas communiquer. Les clients Novell peuvent généralement s'adapter à l'encapsulation disponible sur leurs liens, mais des serveurs IPX doivent faire coder en dur un type d'encapsulation cohérent.

Les noms d'encapsulation sont différents en Novell ou terminologie Cisco. Le tableau suivant fournit un résumé des encapsulations IPX disponibles pour différents types de medias.

Encapsulation IPX nommant des conventions

	Cisco IOS nommant la convention	Commutateur Cisco Catalyst nommant la convention *	Convention de dénomination du logiciel de Novell	LSAP	Description
Ethernets	Novell-Ether	8023RAW	Ethernet_802.3 (cru)	FFFF	Ethernets sans le LLC ou le SNAP
	ARPA	Ethernet II (EII)	Ethernet_II	8137	Type 8137 s d'Ethernet II
	SAP	8023	Ethernet_802.2	E0E0	Ethernets avec l'enveloppe 802.2

	SNAP	SNAP	Ethernet_SNAP	AAAA	Enveloppe + SNAPs 802.2 d'Ethernets
FDDI	SNAP	SNAP	FDDI_SNAP	AAAA	FDDI utilisant 802.2 + SNAP
	SAP	SAP	FDDI_802.2	E0E0	FDDI utilisant l'enveloppe 802.2
Token Ring	SAP	S/O	Token Ring	E0E0	Anneau à jeton avec 802.2
	SNAP	S/O	Ring_SNAP symbolique	AAAA	Anneau à jeton avec 802.2 + SNAP

- Le type ETHERNET_802.3 de vue est l'encapsulation de propriété industrielle du Novell. Ils mettent des paquets SPX/IPX directement à moins de 802.3 trames et n'utilisent pas LLC 802.2 ou SE CASSENT. C'est l'encapsulation Novell NOVELL-ETHER en terminologie de Cisco.
- Le type ETHERNET_II de vue est encadrement « standard » d'Ethernet II. Les paquets SPX/IPX sont bourrés dans des trames d'Ethernet II, utilisant le code 8137 de type. Ces trames diffèrent des trames de NOVELL seulement dans le domaine de code de type de deux-octet/longueur de trame ; autrement, ils sont identiques. C'est encapsulation Novell ARPA en terminologie de Cisco.
- Le type ETHERNET_802.2 de vue est l'encapsulation préférée du Novell pour NetWare 3.12, des serveurs de NetWare 4.X : c'est Ethernet avec l'enveloppe 802.2. C'est encapsulation Novell SAP pour 9.21 en terminologie de Cisco.
- Le type ETHERNET_SNAP de vue est Ethernet avec l'enveloppe 802.2 + le SNAP. Ceci n'est pas généralement utilisé. C'est SNAP d'encapsulation Novell en terminologie de Cisco.

*** Les configurations IPX sur des Commutateurs de gamme de Catalyst s'appliquent seulement pour des Ethernets au FDDI jetant un pont sur des configurations.**

Protocoles de routage ipx

Utilisant les protocoles répertoriés ci-dessous, les artères et entretient un routeur IPX sait du du pouvoir être défini et géré dynamiquement :

- **SAP (publicité Protocol de service)** : Un protocole IPX qui permet à des ressources de réseau telles que des serveurs et des Routeurs pour devenir notoire aux clients réseau. SAP est exigé pour déterminer où les différents services réseau résident sur l'interréseau.
- **RIP (Protocole d'Information de Routage)** : Un Protocole IGP (Interior Gateway Protocol) qui utilise le compte de saut et fait tic tac comme mesures de routage. Le compte de saut mesure la distance entre une source et une destination. Le temps de réponse aller-retour entre la

source et la destination est mesuré dans les coutils, ou 1/18 des seconde intervalles. DÉCHIREZ apprend, sélectionne, et met à jour la table de routage. Le RIP est un protocole de vecteur de distance utilisé pour permuter les informations de routage dans un système indépendant.Le travail de RIP et de SAP ensemble en équipe pour aider des clients, des serveurs, et des Routeurs trouvent des services réseau, et des artères à chaque service. Ils sont également utilisés pour des communications client-serveur aussi bien que des transmissions de routeur à routeur.

- **IPX EIGRP** : L'IGRP est Interior Gateway Routing Protocol de Cisco utilisé dans des Internet TCP/IP et d'OSI. L'IGRP utilise la technologie de routage de vecteur de distance de sorte que chaque routeur n'ait pas besoin de connaître toutes les relations de routeur/lien pour le tout le réseau. Chaque routeur annonce des destinations avec une distance correspondante. Chaque routeur qui entend l'information règle la distance et la propage aux routeurs voisins.Les informations de distance dans IGRP sont représentées comme un composite de bande passante disponible, du retard, de l'utilisation de la charge et de la fiabilité de la liaison. Ceci permet à des réglages des caractéristiques de la liaison pour réaliser des chemins optimaux que l'EIGRP est une version améliorée d'IGRP. La technologie du vecteur de distance trouvée dans IGRP est également utilisée dans EIGRP et l'information de distance sous-jacente demeure sans changement. Les propriétés de convergence et l'efficacité opérationnelle de ce protocole se sont sensiblement améliorées. Ceci permet une architecture améliorée tout en conservant l'investissement existant dans IGRP. Pour des détails sur l'EIGRP, voyez s'il vous plaît le document suivant :Introduction à l'Enhanced IGRP (EIGRP)Les modules dépendants du protocole sont responsables des conditions requises de particularité de protocole de couche réseau. Par exemple, le module d'IPX EIGRP est responsable d'envoyer et de recevoir les paquets EIGRP qui sont encapsulés dans l'IPX. L'IPX EIGRP est responsable d'analyser le Diffusing Update Algorithm de paquets EIGRP et d'information (DOUBLE) des nouvelles informations reçues. L'IPX EIGRP demande DOUBLE à faire à des décisions de routage les résultats dont sont enregistrés dans la table de routage ipx. L'IPX EIGRP fournit les caractéristiques suivantes.Redistribution automatique - Des routes RIP IPX sont automatiquement redistribuées dans des artères EIGRP et d'IPX EIGRP ne sont automatiquement redistribuées dans le RIP sans aucune commande entré par l'utilisateur. La redistribution peut être arrêtée avec l'utilisation de l'**aucun redistribuent la** sous-commande du routeur de **protocole**. IPX-RIP et IPX EIGRP peuvent être arrêtés complètement sur le routeur.Largeur de réseau accrue - Avec le RIP IPX, la plus grande possible largeur de votre réseau est 15 sauts. Quand l'IPX EIGRP est activé la plus grande possible largeur est 224 sauts. Puisque la mesure EIGRP est suffisamment assez grande pour prendre en charge des milliers de sauts, la seule barrière à développer le réseau est le compteur de saut de couche transport. Cisco fonctionne autour de ce problème à côté d'incrémenter seulement le champ de contrôle de transport quand un paquet IPX a traversé 15 Routeurs et le prochain saut à la destination a été appris par l'intermédiaire de l'EIGRP. Quand une route RIP est utilisée comme prochain saut à la destination, le champ de contrôle de transport est incrémenté comme d'habitude.Mise à jour incrémentielle des points d'accès au service - Des mises à jour SAP complètes sont envoyées périodiquement jusqu'à ce qu'un voisin EIGRP soit trouvé et ensuite seulement quand il y a des modifications à la table SAP. Ceci fonctionne à côté de tirer profit du mécanisme de transport fiable de l'EIGRP ainsi un pair d'IPX EIGRP doit être présent pour que les sèves incrémentales soient envoyées. Si aucun pair n'existe sur une interface spécifique, alors des messages SAP périodiques seront envoyés sur cette interface jusqu'à ce qu'un pair soit trouvé. Cette fonctionnalité est automatique sur des interfaces série et peut être configurée sur des medias de RÉSEAU

LOCAL si désirée.

- **NLSP (services de lien de NetWare Protocol) :** Ce protocole de routage peut être utilisé en même temps que, ou au lieu de SAP et du RIP. Lui adresse les limites de RIP et SAP quand ils sont mis en application dans de grands, complexes interréseaux. Typiquement, le NLSP utilise moins de bande passante, est plus rapide à mettre à jour sa table de routage, et est plus extensible à de grands interréseaux que le RIP et le SAP. Le NLSP n'est pas un routage ipx utilisé généralement Protocol.

Études de cas de réseau Novell IPX

Étude de cas #1 : Cisco à l'Interopérabilité 3Com sur des interfaces WAN

Par défaut, des Routeurs de Cisco sont configurés pour les mises à jour périodique par SAP qui se produisent toutes les 60 secondes sur toutes les interfaces. Cependant, sur des Routeurs de l'entreprise 3Com, l'interface WAN est configurée pour les mises à jour SAP non périodiques par défaut. Les mises à jour non périodiques sont des mises à jour SAP qui se produisent seulement quand un lien est soulevé, quand le lien en baisse administrativement, ou quand des changements des informations de service au lieu d'un intervalle périodique. Ce paramètre est pris en charge pour des mises à jour SAP seulement. Quand connectant un routeur de Cisco à un routeur 3Com exécutant l'IPX au-dessus d'une interface WAN avec une configuration IPX de par défaut, les entrées de serveur IPX dans le routeur de Cisco apparaîtront seulement pendant 240 secondes après que modification de lien ou de topologie due à la configuration par défaut du routeur 3Com étant placé pour les mises à jour SAP non périodiques. Pour corriger cette question, une modification de configuration est exigée sur le routeur Cisco ou 3Com.

Pour changer le routeur 3Com aux mises à jour périodique par SAP sur une interface WAN, émettez les étapes suivantes :

1. Vérifiez la configuration IPX sur l'interface WAN sur le routeur 3Com en émettant la commande : **affichez [! <port]|! *] - contrôle de sève**Exemple : **SH - CONT DE SAP**
2. Si le routeur 3Com est configuré pour « non périodique » sur l'interface WAN, la configuration devra être changée à « périodique » utilisant la commande : **setdefault ! <port> - sève control=periodic**Pour changer le routeur de Cisco aux mises à jour non périodiques d'IPX SAP sur une interface, émettez la commande d'interface suivante :sève d'ipx update interval modification modification

Étude de cas #2 : File d'attente de diffusion en relais de trame et perte de connectivité IPX à travers des réseaux de Relais de trames

Un routeur de Cisco qui est configuré pour l'IPX et placé comme hub d'un nuage de Relais de trames peut devoir avoir des modifications de configuration associées avec la file d'attente de diffusion en relais de trame. C'est un résultat de la file d'attente de diffusion en relais de trame se transférant sur une taille d'une interface unique seulement tandis qu'en fait l'interface peut servir des plusieurs sites. La taille de la file d'attente par défaut de diffusion en relais de trame est 64 et doit être configurée en tant que 64 fois le nombre de sous-interfaces. La taille de file d'attente étant trop petite configuré peut avoir comme conséquence la perte de mises à jour IPX RIP/SAP à travers le WAN. La perte de mises à jour IPX RIP/SAP entraînera la perte de connectivité entre le hub et les sites distants.

Exemple : Trop petit configuré par file d'attente de diffusion en relais de trame :

```
lt-3810b#show int s0 Serial0 is up, line protocol is up ... Encapsulation FRAME-RELAY, crc 16,
loopback not set .. Broadcast queue 61/64, broadcasts sent/dropped 17423/14021,
interfacebroadcasts 42032 Last input 3d19h, output 3d19h, output hang never Last clearing of
"show interface" counters 00:00:07 Input queue: 74/75/0 (size/max/drops); Total output drops:
14453 Queueing strategy: weighted fair Output queue: 25/1000/64/1578 (size/max
total/threshold/drops)
```

[Instructions de configuration pour configurer la file d'attente de diffusion en relais de trame]

File d'attente de diffusion en relais de trame

- Pour créer une file d'attente spéciale pour qu'une interface spécifiée tienne le trafic d'émission qui a été répliqué pour la transmission sur les plusieurs identificateurs de connexion de liaison de données (DLCI), utilisez la commande de configuration d'interface de file d'attente de diffusion en relais de trame :
- **débit de paquets d'octet-débit de taille de frame-relay broadcast-queue**

Description de la syntaxe

- **taille** - Nombre de paquets à tenir dans la file d'attente de diffusion. La recommandation pour le réseau IPX RIP/SAP est d'avoir 64 paquets chronomètre le nombre de sites distants. Par exemple, s'il y a 7 sites distants, configurez la profondeur de la file d'attente en tant que 448.
- **octet-débit** - Nombre maximal d'octets à envoyer par seconde. La recommandation est utilisation la configuration par défaut de 256000 octets par seconde
- **débit de paquets** - Nombre maximal de paquets à envoyer par seconde. La recommandation est utilisation le par défaut de 36 paquets par seconde.

Étude de cas #3 : Incohérence d'IPX SAP en utilisant l'IPX EIGRP comme routage ipx Protocol

De temps en temps, il peut y a une perte de connectivité soudaine à un serveur Novell spécifique ou au service IPX. Les serveurs Novell ou les services IPX peuvent disparaître aléatoirement des tables SAP d'IPX. Ceci peut également faire varier des tailles de table SAP par quelques sèves à travers le réseau.

Si vous rencontrez ces problèmes, visualisez ces erreurs de programmation et les améliorez à une version de logiciel qui n'éprouve pas ces questions.

Examinez ces notes de mise à jour :

[CSCdp13795 - Incohérence d'IPX SAP avec l'IPX EIGRP]

Si vous utilisez le Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) IPX, vous pourriez éprouver une incohérence en service annonçant des mises à jour de Protocol (SAP) sur un routeur distant, si l'interface série est réduite pendant un bref temps et de nouveau alors évoquée. Pour vérifier la question, entrer dans l'EXÉCUTIF de **clear ip eigrp neighbors de** commande, ou ne sélectionner l'**aucune** commande de **sève de lien-demande IPX** pour les interfaces série et la vérifier que le problème ne se reproduit pas.

[CSCdk13645 - La table SAP d'IPX peut devenir contradictoire après que de plusieurs serveurs]

soient retirés du Tableau

En utilisant les mise à jour incrémentielle des points d'accès au service d'IPX EIGRP (RSUP), les tables des serveurs entre deux voisins ou plus EIGRP peut devenir contradictoire. Spécifiquement, le problème peut se poser quand seulement trois douzaine serveurs partent en même temps, alors que les artères à ces services restent dans la table de routage s'il y a de plusieurs voisins ou chemins EIGRP à un voisin. Vers le bas la mise à jour rapide pour certains des serveurs récemment avalés n'est pas envoyée à toutes les interfaces, ainsi quelques périphériques ont les serveurs retirés et d'autres ne font pas. Le contournement est d'effacer les voisins IPX EIGRP sur l'unité qui affiche ces serveurs restant dans la table.

Une mise à jour rapide est une annonce immédiate de tous les changements du réseau, et l'apparition de nouveaux services ou la disparition des services existants. Pendant que la sortie de débogage suivante de laboratoire témoin affiche, la mise à jour rapide est envoyée à toutes les interfaces qui exécutent l'IPX :

```
5d10h: IPXSAP: positing update to 1.ffff.ffff.ffff via Serial1 (
broadcast) (flash)
5d10h: IPXSAP: positing update to 2.ffff.ffff.ffff via Serial0 (
broadcast) (flash)
5d10h: IPXSAP: positing update to 100.ffff.ffff.ffff via Etherne
t0 (broadcast) (flash)
```

CSCdm23488 - Sèves manquantes après lien/vers le bas

En configurations réseau avec l'interface IPX interconnectant un routeur local et un routeur distant configurés avec l'IPX EIGRP SAP-incrémental (le mode par défaut sur le non-RÉSEAU LOCAL relie quand l'IPX EIGRP est utilisé), les routeurs distants peuvent perdre quelques sèves si l'interface du routeur local (l'interface d'où des services IPX sont entendus mais pas connectés au routeur distant) subissent une transition rapide down/up. Le travail est autour de rétablir la contiguïté d'IPX EIGRP en émettant les **voisins clairs d'IPX EIGRP** commandent aux routeurs distants.

La cause principale de CSCdm23488 est une question de synchronisation avec les processus de logiciel qui s'appellent par le lien suivant IPX vers le bas et joignent vers le haut des ordres. Quand un grand nombre de services IPX sont impliqués, l'interface est soulevée tandis que des sèves de poison sont envoyées. En conséquence, les sèves de poison ignorent les nouvelles annonces et empêchent efficacement quelques services d'être annoncée.

CSCdx73624 - Manquer des sèves IPX

En topologie de relais de trame de hub and spoke, deux rais peuvent ne pas recevoir les sèves de chacun si le nuage BLÊME exécute le RIP et l'IPX EIGRP IPX. Le résultat est une table SAP contradictoire. Comme contournement, RIP IPX de débronchement.

Étapes de dépannage

Si vous observez un problème avec manquer des sèves, utilisez les étapes de dépannage suivantes :

- Si les sèves sont apprises par l'intermédiaire d'un autre rai de Relais de trames, le routeur concentrateur manque-il également les sèves ou seulement le routeur en étoile local ?
- Est-vous de l'utilisation incrémentale ou les mises à jour périodique par SAP ?

- Si vous avez activé des mises à jour régulières, déterminez si le routeur reçoit les mises à jour SAP régénérées. Visualisez les compteurs de SAP en émettant la commande de **show ipx traffic**.

```
System Traffic for 0.0000.0000.0001 System-Name: SAMPLE
 Time since last clear: 00:01:47
 Rcvd: 733 total, 0 format errors, 0 checksum errors, 0 bad hop count,
 4 packets pitched, 733 local destination, 0 multicast
 Bcast: 732 received, 507 sent
 Sent: 529 generated, 456 forwarded
 0 encapsulation failed, 0 no route
 SAP: 0 Total SAP requests, 0 Total SAP replies, 0 servers
```

  - Perdez-vous toutes les sèves d'un serveur particulier ?
  - Y a-t-il des relations entre une panne de lien et les sèves de disparus ? Si les sèves sont perdues après qu'une modification de lien, utilisent les étapes suivantes :Désactivez la journalisation console et activez la mémoire tampon se connectant en émettant la commande de **logging buffered**.Émettez les **événements d'eigrg IPX de débogage** et **mettez au point les** commandes de **voisin d'IPX EIGRP {ID de voisin}**.Transition l'état de lien de l'interface.Si vous détectez les sèves manquantes, attendez au moins cinq minutes pour vérifier que les sèves manquent en effet. Saisissez la sortie du **serveur IPX d'exposition** et **affichez les routecommands IPX les** aux deux les Routeurs de hub and spoke.Émettez la commande de **clear ipx route à l'**extrémité de rai.Émettez les commandes de **serveur** et de **show ipx route IPX d'exposition** de vérifier si toutes les sèves ont été apprises.

Si vous ne pouvez pas résoudre le problème avec les étapes ci-dessus, vous pouvez devoir émettre la commande d'**activité d'ipx sap de débogage**. Des messages de débogage d'exemple sont fournis ci-dessous.

```
3d21h: IPXSAP pv03 from net C4545 rejected, route C0324002 not in table

Oct 19 18:21:05 CDT: IPXEIGRP: SAP from FF16 rejected, route 2200 in table via different
interface
```

Remarque: Assurez que vous comprenez l'incidence de cette commande de **débogage** avant de l'activer, puisqu'elle peut générer un grand nombre de sortie. Pour réduire l'incidence de met au point au routeur, nous recommandons désactiver la journalisation console et activer la mémoire tampon se connectant avec une taille de mémoire tampon suffisante.

Étude de cas #4 : Le show ipx traffic de commande indique des nombreuses erreurs de format

Exemple : La commande est configurée en tant que **trafic IPX lt-4500-3a#show**. La sortie est comme suit :

```
System Traffic for 0.0000.0000.0001 System-Name: dc_gw
Rcvd: 49847808 total, 1974563 format errors, 0 checksum errors,150 bad hop count,
310999 packets pitched, 1067549 local destination, 0 multicast
Bcast: 1072701 received, 1005206 sent
Sent: 2209133 generated, 48465603 forwarded
0 encapsulation failed, 3240 no route
SAP: 2174 SAP requests, 8 SAP replies, 1330 servers
899357 SAP advertisements received, 990129 sent
0 SAP flash updates sent, 535 SAP format errors, last seen from 0.0000.0000.0000
RIP: 91556 RIP requests, 22723 RIP replies, 152 routes
73769 RIP advertisements received, 20433 sent
1475 RIP flash updates sent, 0 RIP format errors
```

```
Echo: Rcvd 0 requests, 0 replies
Sent 0 requests, 0 replies
76 unknown: 76 no socket, 0 filtered, 0 no helper
0 SAPs throttled, freed NDB len 0
Watchdog:
0 packets received, 0 replies spoofed
Queue lengths:
IPX input: 0, SAP 0, RIP 0, GNS 0
SAP throttling length: 0/(no limit), 0 nets pending lost route reply
Delayed process creation: 0
EIGRP: Total received 0, sent 0
Updates received 0, sent 0
Queries received 0, sent 0
Replies received 0, sent 0
SAPs received 0, sent 0
Trace: Rcvd 0 requests, 0 replies
Sent 0 requests, 0 replies
```

Les erreurs de format dans une commande de **show ipx traffic** sont le nombre de mauvais paquets jetés (par exemple, des paquets avec une en-tête corrompue). Ce compteur inclut des paquets IPX reçus pour une encapsulation que le routeur n'est pas configuré.

La plupart des PC sur un réseau automatique-détectent le type de trame d'IPX sur un Anneau à jeton ou le réseau Ethernet en envoyant des demandes GNS de chacun des quatre types de trame possibles. L'interface sur le routeur est dur codée à un type de trame spécifique. Si l'interface sur le routeur reçoit un paquet IPX avec un type de trame différent que ce qui est configuré, le paquet est lâché et le « champ de format » est incrémenté. Par conséquent, les PC configurés pour le type de trame par défaut enregistreront toujours au moins trois erreurs de format sur le routeur contigu de Cisco sur le startup.

Référez-vous aux commandes IPX de Novell pour plus d'informations sur la commande de **show ipx traffic**.

Étude de cas #5 : Les sèves IPX n'apparaissent pas dans la table des serveurs IPX à travers les nuages BLÊMES

Les Routeurs de Cisco à travers un nuage BLÊME afficheront toutes les artères IPX dans la table de routage ipx. Cependant, aucune des sèves IPX n'apparaît dans la table des serveurs IPX. Le codage de ligne AMI ne prend en charge pas des paquets avec une densité élevée de zéros. Le codage de ligne devrait être le codage B8ZS qui, en sentant une densité élevée de zéros, inverser le flux de données pour casser les zéros. Les paquets d'IPX SAP peuvent inclure une structure de données de 11 zéros consécutifs. Par exemple, un serveur de fichiers du type 4 a une adresse IPX d'ABCDEF.0000.0000.0001, qui sera corrompu si le nuage BLÊME ne prend en charge pas la densité nulle élevée. Si le paquet atteint un routeur distant corrompu, il sera lâché. En conséquence, les mises à jour de RIP IPX atteindront les Routeurs distants, mais les paquets d'IPX SAP pas, en raison de la densité nulle élevée.

La solution est de faire placer au fournisseur de service WAN correctement le codage de ligne à B8zs à travers le WAN.

Pour vérifier votre configuration, initiez un ping IP avec un modèle de tous les zéros à travers le nuage BLÊME à 500, 1000 et 1500 octets. Si le ping IP est réussi, le codage de ligne n'est pas une question puisque la haute densité zéro pings de modèle sont réussie.

```
Router#ping Protocol [ip]: Target IP address: 10.10.10.1 Repeat count [5]: Datagram size [100]:
500 Timeout in seconds [2]: Extended commands [n]: y Source address or interface: Type of
```

```
service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]:
0x0000 Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape
sequence to abort. Sending 5, 500-byte ICMP Echoes to 10.10.10.1, timeout is 2 seconds: Packet
has data pattern 0x0000 !!!!! Success rate is 100 percent (5/5) Router#
```

Étude de cas #6 : Les postes de travail ne peuvent pas se connecter à un des serveurs par l'intermédiaire du voisinage réseau

Dans certains cas, les postes de travail peuvent voir tous les serveurs Novell dans un voisinage réseau, mais incapable de se connecter aux serveurs l'uns des par le voisinage réseau. Afin de se relier aux serveurs dans le voisinage réseau à travers des VLAN ou à travers de plusieurs réseaux, les postes de travail de client doivent avoir le client Novell 32 installé ou **activer IPX type-20-propogation** sur les Routeurs correspondants. En outre, chaque network number dans le campus doit être seul à travers le tout le réseau. Utilisez l'outil de PING IPX sur les serveurs Novell et l'outil IPX de PING sur les Routeurs de Cisco pour vérifier la Connectivité à travers le WAN.

Étude de cas #7 : Incapable d'accéder à des ressources en Citrix Winframe utilisant l'IPX à travers des Routeurs de Cisco

Si la sortie de commande du **show ipx servers** prouve qu'il y a plus d'un serveur de Winframe avec le même compte de saut/coutil loin, alors, par défaut seulement SAP de la première entrée sera envoyé au client.

Ce n'est pas un problème pour un serveur Novell, puisque le client recevra le premier SAP, vont au premier serveur, et puis obtiennent réorienté au serveur du choix du client s'il y a un serveur préféré. Winframe n'a pas cette fonctionnalité. Si le client est installé pour le nom du serveur « x », mais obtient SAP pour le nom du serveur « y, » puisque « y » est premier dans la table SAP, alors le client ne se connectera jamais.

La solution est d'ajouter l'**ipx gns-round-robin de** commande comme commande globale sur le routeur avec le plusieurs winframe SAP de la même distance. Le routeur recherche séquentielle par les réponses de SAP et le client obtiendra SAP pour le serveur correct, même si ce n'est pas le premier SAP dans la table SAP du routeur.

Étude de cas #8 : Procédure de connexion lente IPX de Novell

La plupart de cause classique pour la procédure de connexion lente de Novell est une question connue sous le nom de marche d'arborescence. Quand un agent client soumet une demande aux NDS, la demande n'est pas toujours reçue par un Serveur de noms qui est qualifié accomplir la demande. Le Serveur de noms recevant la demande doit trouver un Serveur de noms qui peut accomplir la demande. Plusieurs Serveurs de noms peuvent devoir être contactés avant qu'un serveur qualifié se trouve. Pour trouver les informations, un Serveur de noms initie une recherche jusqu'à ce qu'on trouve une reproduction qui contient les informations désirées. Ce processus s'appelle marche d'arborescence. Tant que les informations de réplication peuvent être accédées à rapidement, la marche d'arborescence n'est pas un problème. Cependant, si les informations de réplication sont seulement disponibles à travers un lien lent, tel qu'un lien WAN, des retards peut se produire. N'importe quelle application qui utilise des NDS peut entraîner l'arborescence marchant, mais la marche d'arborescence peut être réduite avec la bonne conception d'arborescence de NDS.

Problèmes de connexion et résolutions lents communs par site Web de Novell :

```
TID 10051665    Troubleshooting Slow Novell Login Problems

TID 10014302    NW5 client slow logging into IPX server

TID 2950722     Slow NT Login in Pure IP Environment

TID 10020376    The clients are getting a Slow Network Login

TID 10024740    Troubleshooting IP Login Issues

TID 10016768    Login is very slow from specific machines

TID 10021852    Slow login over a WAN link due to Contextless Login
```

Dépannage général

Pour identifier ce qui pose potentiellement le problème de connexion lent, obtenez un tracé de paquets du problème se posant, capturant tous les paquets envoyés à et du poste de travail. Deux tracés de paquets seront nécessaires pour déterminer le problème exactement : un un tracé de paquets du port de serveur et un tracé de paquets différent du poste de travail. En obtenant deux tracés de paquets, il sera très facile de déterminer si le problème est lié aux paquets de baisse de réseau.

Étude de cas #9 : Dépannage des entrées de table corrompues d'IPX SAP

Les entrées d'IPX SAP qui affichent des caractères incorrects, les réseaux fantômes, ou caractères bit-décalés/bit-troqués sont très probablement les entrées corrompues de SAP. Les caractères incorrects témoin incluent (@ ! ~^)). Puisqu'il n'y a aucune somme de contrôle de la couche 3 (L3) dans la trame d'IPX SAP, la corruption des données peut se produire avec des mises à jour d'IPX SAP. Cette corruption ne peut pas sont provoqué par par la corruption de la couche 2 (L2) parce que le CRC sur la trame L2 serait non valide et le routeur relâcherait la trame. Des sèves corrompues IPX sont toujours provoquées par le matériel défectueux. Trouver la source des SAP altérés par IPX est assez simple en utilisant l'exclusivité de RIP IPX ; Simplement compte de saut d'utilisation pour trouver la source. Avec l'IPX EIGRP, le dépannage est plus difficile, cependant.

Avec des chemins redondants et une topologie faite une boucle utilisant l'IPX EIGRP, une entrée de point d'accès de service altéré peut rester pour toujours, ne chronométrant pas même lorsque le périphérique d'origine a été arrêté. La raison pour laquelle les sèves ne disparaîtront pas d'un environnement mélangé EIGRP et de RIP est due au fait que quand vous avez des chemins parallèles par un réseau, le RIP et l'EIGRP passeront les entrées de SAP dans les deux sens. Ce comportement empêchera les sèves de chronométrer jamais. Quand l'EIGRP reçoit des mises à jour des Routeurs deux ou plus différents des mises à jour SAP, l'EIGRP passera les mises à jour de nouveau dans le RIP de l'EIGRP si l'entrée de RIP part. L'EIGRP préservera également le compte de saut de RIP, qui rend identifiant la source plus difficile.

La condition de bouclage décrite ci-dessus effectue seulement SAP, pas des artères. C'est parce que SAP toujours indiquera l'artère la plus courte et ne note pas des boucles de routage. SAP n'est pas un protocole de routage. Retirer l'EIGRP dans le chemin entier permettra aux points d'accès de service altéré pour vieillir.

Dû le comportement de l'IPX EIGRP et des entrées de table corrompues d'IPX SAP de dépannage, utilisent les procédures de dépannage suivantes dans l'isolement des SAP altérés par IPX en utilisant l'IPX EIGRP :

1. Pendant une fenêtre de panne de réseau, IPX EIGRP de débronchement et RIP d'utilisation pour identifier exactement la source des entrées de point d'accès de service altéré. Puisque les utilisations de RIP sautent à cloche-pied compte dans le chemin réseau, la détermination de la source ou de l'origine devrait être assez simple. Le dépannage de cette manière suppose que les renommées corrompues doivent être générées pendant la fenêtre de temps d'arrêt. Puisque la corruption d'IPX SAP est due au matériel, le problème peut se poser fréquemment et seulement ne pas se poser au hasard des périodes. Sans points d'accès de service altéré actuellement étant générés dans le réseau, il n'y aura aucune manière de déterminer la source. Tous les points d'accès de service altéré coincés dans la table EIGRP partiront une fois que l'EIGRP est retiré.
2. Trouvez une source commune ou une origine des points d'accès de service altéré. Si là une origine commune aux sèves, il peut être simple pour isoler la question et ne doit pas exécuter en tant que dépannage intrusif comme dans l'étape 1.Tous les points d'accès de service altéré sont provoqué par par le matériel défectueux quelque part dans le réseau. Ceci inclut n'importe quel routeur, Commutateurs L3, serveurs exécutant IPX (pas simplement serveurs Novell), et postes de travail exécutant l'IPX. Jusqu'à présent, Cisco n'a jamais fait contribuer un problème logiciel IOS pour corrompre des sèves IPX.
3. Àtravail-autour des sèves corrompues IPX affectant la connexion réseau, configurez les filtres IPX comprenant des filtres GNS, des filtres GGS, et des filtres de SAP pour passer seulement les serveurs valides dans le réseau. En outre, ajoutant l'**ipx sap follow-route-path de** commande réduira le nombre de points d'accès de service altéré. C'est parce que quand la commande d'**ipx sap follow-route-path** est utilisée, le routeur interviewe des services individuels (sèves) dans les mises à jour SAP. Le routeur regarde le numéro du réseau de destination de chaque entrée de SAP. Si l'interface de réception est l'une des meilleures interfaces pour atteindre le réseau de destination de SAP, cette entrée de SAP est reçue. Autrement, l'entrée de SAP est jetée. Si un routeur reçoit des points d'accès de service altéré, il est probable l'artère peut être corrompu aussi bien.

Étude de cas #10 : La liste de serveur de la commande non triée de show ipx servers peut afficher des serveurs en panne

Dans certains cas, quand la recherche séquentielle IPX GNS est configurée, le routeur peut éprouver une question qui peut causer un service de métrique peu élevée d'être déplacée dans la table au delà du plus bas groupe métrique de services. Ceci fera sembler la table SAP en panne. C'est comportement connu, et n'importe quel effet secondaire de ce comportement peut être résolu à l'aide des filtres de sortie GNS pour permettre seulement aux serveurs spécifiques pour répondre à GNS.

Si vous rencontrez ces problèmes, visualisez l'erreur de programmation suivante et l'améliorez à une version de logiciel qui n'éprouve pas ces questions.

CSCds54733 - sortie non triée de show ipx servers n'est pas en règle

La sortie de l'ordre **non trié de serveur IPX d'exposition** affiche une table SAP qui n'est pas en règle. Tandis que la table est dans cet état, les réponses GNS SAP peuvent ne pas fournir le service le plus proche comme elles devraient. La table misordered résulte d'activer la recherche séquentielle GNS. Comme contournement, recherche séquentielle du débronchement GNS en n'émettant l'aucune commande d'ipx gns-round-robin.

Études de cas IP du Novell 5.X

Étude de cas #1 : Configuration de routeur Cisco de base requise pour que les clients ouvrent une session au réseau IP de Novell à travers des limites du réseau

Par défaut, les clients IP de Novell découvrent des Services IP par l'intermédiaire de la Multidiffusion. À moins qu'une autre méthode soit configurée, les clients IP tenteront de découvrir le serveur par l'emplacement Protocol (SLP) de service qui utilise IGMP (multifusion). Par défaut, les Routeurs IOS n'expédieront pas des paquets de multidiffusion.

La solution de base de routeur est d'activer la commande d'**ip multicast-routing** globalement et d'activer la commande de dense-**mode d'ip pim** sous chaque VLAN respectif ou interface physique.

Exemple de configuration :

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
boot system bootflash:c6msfc-js-mz.120-7.XE1.bin
boot bootldr bootflash:c6msfc-boot-mz.120-7.XE1
!
ip subnet-zero
no ip domain-lookup
!
ip multicast-routing
ip dvmrp route-limit 20000
ip cef
cns event-service server
!
!
!
interface Vlan1
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
ip pim dense-mode
!
interface Vlan11
ip address 10.1.2.1 255.255.255.0
no ip directed-broadcast
ip pim dense-mode
!
interface Vlan12
ip address 10.1.3.1 255.255.255.0
no ip directed-broadcast
ip pim dense-mode
!
ip classless
no ip http server
!
!
!
line con 0
```

```
transport input none
line vty 0 4
login
transport input lat pad mop telnet rlogin udptn nasi
!
end
Router#
```

Il y a deux autres méthodes par lesquelles les postes de travail de client peuvent accéder au Novell 5.0 ressources à travers des limites du réseau sans nécessité d'activer le mutlicast-routage.

Configuration Novell #1 (document de Novell : 2944038)

Ajoutez le nom du serveur et les entrées d'adresse IP dans le fichier de NWHost sur le poste de travail. Le fichier NWHOST se trouve sur le poste de travail dans le répertoire Novell\Client32 sur des postes de travail de Win95 et de Win98. Il a les échantillons il est facile suivre que.

Sur un poste de travail NT, au lieu de NWHost, le client utilise le fichier hôte standard TCP/IP de Microsoft. Éditez le fichier hôte pour ajouter le nom du serveur et l'adresse. Le chemin à ce fichier est Winnt/System32/Drivers/Etc/Hosts.

Configuration Novell #2 (de document 2944038 de Novell)

Chargement SLPDA.NLM sur le serveur de NetWare 5. Ceci définit le serveur comme agent de répertoire. Ajoutez l'adresse IP du serveur exécutant le SLPDA.NLM sous des propriétés du client, onglet d'emplacement de service, liste d'agent de répertoire. Cliquez sur en fonction la case à côté de la case d'agent de répertoire étiquetée « charge statique. » L'agent directoy statique étant défini, le client pas Multidiffusion pour un agent de répertoire, mais enverra un unicast à l'agent de répertoire spécifié.

Pour un aperçu de SLP (emplacement Protocol de service) et un examen des agents de répertoire, voir le tid 2943614 chez support.novell.com

Étude de cas #2 : L'activation du Protocole IP Multicast dans le réseau de production apporte les réseaux vers le bas existants IPX

Les réseaux peuvent experiennce une perte de connectivité IPX soudaine et complète pour le PC client.

Ceci peut se produire parce que le logiciel client 3.x de NetWare de Novell préférera l'IP pour la couche réseau Protocol au-dessus de l'IPX par défaut. Par conséquent, si un serveur réservé à l'IP du Novell 5.X non configuré correctement pour la procédure de connexion et la multidiffusion IP de NetWare de Novell dans le réseau est activé, toutes les machines cliente préféreront la connexion au serveur du Novell 5.X. Si le serveur du Novell 5.X ne se rend pas correctement compte des ressources en réseau existant, les clients ne pourront pas accéder aux ressources existantes.

Pour résoudre ce problème, configurez le Protocole IP Multicast conduisant pour exclure SLP ou pour configurer les serveurs de NetWare 5.X de Novell correctement.

Étude de cas #3 : Pourquoi l'IP de Novell ne fonctionne-t-il pas par s'exécuter de routeur de Cisco NAT ?

Les réalisations NAT traduisent des adresses IP dans des en-têtes de paquet et les circonstances spéciales recherchent la partie données du paquet et traduisent des références incluses d'adresses IP. Cependant, le logiciel NAT en cours de Cisco ne traduit pas des références incluses IP de Novell pour des NDS ou SLP dans les parties données du paquet IP. En conséquence, les périphériques dans le réseau public essayeront d'entrer en contact avec des ressources par l'intermédiaire des adresses privées non-traduites. Puisque les réseaux publics ne pourront pas aux réseaux privés, les connexions échoueront. La solution alternative pour créer des connexions IP de Novell par NAT est d'utiliser une solution VPN.

Le pour en savoir plus, voient TID 2948010 chez support.novell.com

Étude de cas #4 : Procédure de connexion lente IP de Novell

Le dépannage lent de procédure de connexion IP de Novell est identique que la procédure de connexion lente IPX. Voir l'étude de cas #8 sous des études de cas IPX de Novell.

Questions relatives à la configuration communes

Pourquoi est-ce que je ne peux pas configurer plus de 200 réseaux IPX sur mon routeur ?

Un routeur de Cisco peut manipuler plus de 200 réseaux IPX dans sa table de routage, par exemple, mais vous ne pouvez pas configurer plus de 200 interfaces IPX sur un routeur (utilisant la **commande réseau IPX**). La limite seulement a été atteinte récemment maintenant que nous avons des Commutateurs de la couche 3 qui peuvent fournir ce nombre d'interfaces. Ce nombre est codé en dur dans l'IOS et ne sera pas probablement changé. Les Commutateurs de la couche 3 peuvent implémenter plus de 200 interfaces parce que la plupart des fonctions de commutation sont manipulées par quelques ASIC spécialisés qui débarquent le processeur principal en ce qui concerne le trafic IP. Les interfaces IPX ont besoin beaucoup plus de puissance CPU d'effectuer le processus RIP/SAP, et obtenir même près de la limite en cours peut être essentiel.

Pourquoi est-ce que je ne peux pas cingler un hôte de Novell de mon routeur ?

Un routeur de Cisco implémente deux types de ping IPX :

- Ping IPX de Cisco : c'est le protocole propriétaire par défaut de Cisco qu'un routeur l'utilisera quand vous tentez de cingler une adresse IPX.
- Ping IPX de Novell : c'est le seul que les serveurs Novell peuvent exécuter, et il n'est pas compatible avec l'implémentation de Cisco.

Vous pouvez employer le ping IPX de Cisco pour tester la Connectivité entre les périphériques de Cisco configurés pour l'IPX. Si vous voulez cingler un serveur Novell, vous devez configurer le routeur pour envoyer le ping IPX de Novell, utilisant le Novell d'ipx ping-default de commande de configuration globale

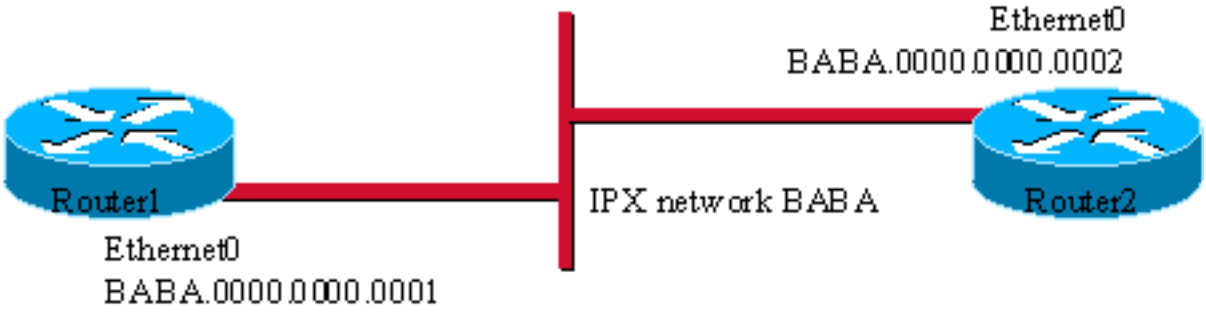
Vous pouvez également émettre une **commande ping étendue IPX** et sélectionner l'option standard d'écho de Novell.

Le serveur Novell doit faire charger le responder pour répondre à un écho de Novell (ping). Pour cingler d'un serveur Novell, on doit également charger IPXPING.NLM sur le serveur. Nous avons observé, dans le test occasionnel, cela :

- Les serveurs de NetWare 3.x, les serveurs de NetWare 4.0x, les clients NETX, les clients VLM (v.1.20a), et le client de MS pour NetWare ne répondent pas aux pings de Novell.
- NetWare 4.10 serveurs, radar de moyenne puissance v3.x de NetWare, client 32, et client DOS/Win95 de MS répondent aux pings de Novell.

Naturellement, le ping peut également échouer pour d'autres raisons qu'une non-concordance dans le type de protocole de ping. Le succès du ping dépend également de la table de routage ipx (il doit y a une artère à l'adresse de destination), l'intégrité de la liaison (pertes de paquets), filtrant, et ainsi de suite. Instructions à se souvenir en utilisant le ping :

- Quand le cinglement d'un serveur est possible, assurez-vous que toutes les questions de connectivité IPX ont été abordées.
- Quand le ping manque, sur le dessus de tous les problèmes de connectivité possibles (d'un problème complexe de routage ipx à un problème de fonctionnalité de lien), souvenez-vous qu'il peut y a un problème simple avec le serveur ne mettant pas en application la fonctionnalité de ping IPX. Il signifie que, malheureusement, il n'y a souvent rien à beaucoup conclure quand un ping IPX à un serveur manque.



Dans cet exemple, nous avons deux Routeurs directement connectés par l'intermédiaire de leur interface Ethernet sur le BABA de réseau IPX. De router1, si nous cinglons l'interface router2, de routeur les utilisations d'abord par défaut, protocole propriétaire de Cisco :

```
router1#ping ipx baba.0.0.2 Type escape sequence to abort. Sending 5, 100-byte IPX cisco Echoes
to BABA.0000.0000.0002, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-
trip min/avg/max = 4/6/8 ms
```

Nous pouvons forcer le protocole de ping de Novell utilisant la **commande ping étendue** :

```
router1#ping ipx Target IPX address: baba.0.0.2 Repeat count [5]: Datagram size [100]: Timeout
in seconds [2]: Verbose [n]: Novell Standard Echo [n]: y Type escape sequence to abort. Sending
5, 100-byte IPX Novell Echoes to BABA.0000.0000.0002, timeout is 2 seconds: !!!!! Success rate
is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

L'autre possibilité est de placer le protocole par défaut de ping pour être le Novell un :

```
router1#conf t Enter configuration commands, one per line. End with CNTL/Z. router1(config)#ipx
ping-default novell router1(config)#^Z 2w1d: %SYS-5-CONFIG_I: Configured from console by console
router1#ping ipx baba.0.0.2 Type escape sequence to abort. Sending 5, 100-byte IPX Novell Echoes
to BABA.0000.0000.0002, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-
trip min/avg/max = 4/6/12 ms router1#
```

Changer le type de ping au Novell est seulement important quand vous tentez de cingler un protocole courant de Novell d'hôte. Manquer pour cingler un hôte de Novell ne signifie pas nécessairement que la Connectivité à cet hôte est cassée (non tous les hôtes de Novell répondent au ping de Novell). Le cinglement d'un routeur est une bonne manière de connectivité IPX de test à lui.

Pourquoi est-ce que je ne peux pas configurer le routage ipx ?

Vous devez avoir le logiciel correct IOS pour configurer le routage ipx.

Très souvent, un routeur est livré avec un logiciel par défaut dans l'éclair et ce logiciel par défaut peut ne pas prendre en charge l'IPX (même si vous avez payé un permis la prise en charge d'IPX). Vous alors devez promouvoir votre routeur au logiciel que vous êtes autorisé pour. La prise en charge d'IPX est généralement une partie du jeu de fonctionnalités de poste de travail, qui est souvent identifié avec un « d » dans le nom d'image :

```
c6sup-ds-mz.121-1.E2.bin
```

Voir le ce jeu de fonctionnalités de poste de travail comme ensemble de caractéristiques minimal comprenant la prise en charge d'IPX. Ensemble de caractéristiques de « entreprise » (identifié avec « j » au lieu du du « d » ci-dessus), qui inclut le jeu de fonctionnalités de poste de travail, naturellement, prendra en charge également l'IPX. Vérifiez les notes de version d'IOS pour les caractéristiques précises disponibles dans l'IOS que vous vous exécutez.

Quelle est la commande d'ipx pad-process-switched-packets ?

Cette commande est utilisée pour contrôler si des paquets d'impair-longueur sont complétés, ainsi être envoyé comme paquets d'égal-longueur sur une interface. La commande d'**ipx pad-process-switched-packets** affecte des paquets commutés par processus seulement, ainsi vous devez désactiver la commutation rapide avant que la commande d'**ipx pad-process-switched-packets** ait n'importe quel effet. La commande était due nécessaire à quelques hôtes IPX qui ont rejeté les paquets Ethernet qui ne sont pas complétés. Certaines topologies peuvent avoir comme conséquence de tels paquets étant expédiés sur un réseau Ethernet distant. Dans des conditions spécifiques, compléter sur des medias intermédiaires peut être utilisé comme contournement provisoire pour ce problème.

Cette commande est activée par défaut. Cependant, la spécification de gestionnaire d'Ethernets de Novell indique que des paquets IPX devraient « evenized » par le périphérique de envoi. C'est dû aux périphériques hérités qui ont eu des problèmes avec les paquets impairs de longueur et ne devraient pas être une question de nos jours, mais la condition requise persiste.

Un périphérique non suivant la condition requise existante de Novell pourrait produire les paquets impairs de longueur. Les paquets impairs pourraient également résulter en conduisant d'une encapsulation IPX à une autre encapsulation différente IPX. Quelques encapsulations ont la longueur différente et un changement de l'encapsulation peut produire un paquet impair de longueur.

Les Routeurs de Cisco prennent en charge-ils la caractéristique d'extension de paquet IPX pour courber l'encombrement de réseau en envoyant de plus grands paquets de mise à jour RIP/SAP ?

C'est une caractéristique prise en charge. Par défaut, un paquet RIP IPX contient 25 artères et un paquet d'IPX SAP contient 7 sèves. Le nombre d'artères et de sèves par paquet de RIP et de SAP peut être changé en changeant la longueur de paquet respective de mise à jour. Voir la documentation sur l'**ipx sap-max-packetsize** et l'**ipx rip-max-packetsize** dans la référence de commande IOS pour plus de détails.

En dépit de configurer tous les serveurs Novell et Routeurs pour l'IP seulement, je

vois toujours des vues IPX sur des tracés de renifleur. Pourquoi cela ?

Le logiciel 3.x de client Novell par défaut enverra des trames pour l'IP et l'IPX lors du démarrage afin d'essayer d'ouvrir une session au réseau Novell indépendamment de la configuration réseau. La solution est de désactiver manuellement tous les protocoles IPX relatif aux PC de client.

Pourquoi activant l'IPX EIGRP sur une interface VLAN désactive IPX MLS pour cette interface respective ?

Le MLS IPX est désactivé avec l'IPX EIGRP puisque la transmission entre les domaines de RIP et EIGRP exige des traductions des champs spécifiques dans la partie données (transmettez le contrôle) de paquets d'artère. Une interface de routeur IPX quand activé pour RIP/NLSP, aura le nombre maximum de sauts de 16. Quand un routeur est sur la borne d'un routing domain NLSP/RIP et EIGRP, l'interface est configurée avec l'EIGRP et le NLSP/RIP. Il est nécessaire d'enlever le soutien MLS de cette interface si le saut maximum est configuré pour être 16 ou moins parce que dans ce cas, la valeur du contrôle de transmission (comité technique) sera traduite au lieu de l'incrémentation par 1 quand un paquet traverse d'un routing domain à l'autre. Le MLS-SE n'a pas la connaissance au sujet du protocole de routage étant utilisé et le matériel MLS ne pourra pas réécrire le champ du contrôle de transmission (comité technique) correctement.

Des « mls IPX seront désactivés sur le <vlan_id> de VLAN dû message d'**eigrp à utilisation »** apparaît seulement si les maximum-sauts IPX est placés à 16 quand l'IPX EIGRP est configuré. Pour toutes autres valeurs (17-254) pas un tel message d'avertissement est affiché. IPX MLS fonctionne bien pour la valeur de saut de 16 bien qu'il y ait un avertissement.

La commande d'augmenter la valeur du contrôle de transmission (comité technique) au-dessus de 16 est **value> de <max_hops IPX MAXIMUM-HOPS**

Il n'y a aucun inconvénient/avantage spécifiques en augmentant le compte de saut.

Problèmes de connectivité communs

Compréhension du processus de connexion de client IPX

Comment est-ce qu'un client se connecte à un réseau Novell ?

Si un client doit localiser un serveur dans une arborescence spécifique de serveur de répertoire la plus proche (NDS), le client annoncera un type 3 de SAP pour le type de service 0278 obtiennent la demande de service d'annuaire la plus proche (GNDs). N'importe quel serveur de NDS (configuré pour répondre aux demandes GNS et de GNDs) situé sur le même segment conduit que le client répondra avec le nom de l'arborescence de NDS qu'elle appartient à et de son numéro IPX interne. Le client vérifiera le nom d'arborescence dans la réponse contre le nom d'arborescence du lequel elle a besoin (selon ce que le client a placé en tant que son arborescence préférée). Si c'est l'arborescence correcte le client annoncera une demande de RIP d'une artère au numéro IPX interne a fourni dans la réponse. Le serveur répondra disant que c'est l'artère à ce numéro IPX interne. Le client unicast une demande d'établir une connexion à ce serveur et de commencer la procédure d'authentification. Si le serveur sur le segment local n'est pas un serveur de NDS qu'il ne répondra pas à la demande initiale de GNDs parce qu'il peut seulement fournir le type de service 0004, non 0278. Aucun serveur de NDS qui ne tiennent pas

des reproductions de NDS ne répondra à la demande. Si aucune des réponses ne contient le nom correct d'arborescence de NDS, le client émettra un type 1 de SAP pour la demande du type de service 0278 (GGDS). Tous les serveurs de NDS situés sur le même segment conduit répondront avec une liste des services, indépendamment de l'établissement de REPLY TO GET NEAREST SERVER. Le client lira toutes les réponses au GGDS recherchant le nom correct d'arborescence de NDS. Une fois qu'il trouve une entrée pour l'arborescence correcte, il tentera d'établir une connexion à ce serveur. Le client tentera d'établir une connexion à la première entrée qui contient le nom correct d'arborescence, pas le plus proche puisque ceci une requête de service général, la requête de service non la plus proche. Si le client demande un serveur de façonnage (ou le client a seulement un positionnement préféré de serveur dans sa configuration de client) que le même processus aura lieu, seulement le type de service de la demande sera 0004 au lieu de 0278. Supplémentaire, si le serveur a le REPLY TO GET NEAREST SERVER réglé à OUTRE de puis le serveur ne répondra pas aux demandes GNS (type de service 0004) ou de GNDs (type de service 0278)

Organigramme pour la procédure de connexion de client Novell

NDS (Novell 4.11)

1. Lors du démarrage, le client enverra une demande de GNDs. Si le client est configuré à l'automatique détectez le type de trame, le client enverra quatre GNDSs, un pour chaque type de trame.
2. Tous les serveurs locaux (ou Routeurs de Cisco si segment sans serveur) répondront avec une réponse de GNDs.Le client utilisera la première réponse de GNDs si les plusieurs serveurs ou les Routeurs répondent à la demande de GNDs. La réponse de GNDs contiendra le nom du numéro de réseau interne et de l'arborescence du serveur respectif.
3. Si la réponse de GNDs a l'arborescence correcte, le client émettra une demande de RIP du numéro IPX interne fourni dans la réponse de GNDs.

Comment est-ce qu'un routeur de Cisco sélectionne le serveur pour inclure dans une réponse de GetNearestServer (GNS) ?

Le serveur IPX d'exposition de commande non trié affichera dans d'abord placent le nom du serveur qui sera utilisé pour répondre à la prochaine demande GNS. Dans la version de logiciel 9.21 ou ultérieures, employez l'ipx gns-round-robin de commande pour activer l'Équilibrage de charge des réponses aux demandes GNS parmi des services de la mesure égale. La manière que les serveurs sont commandés est décrite dans le document suivant : Comment les serveurs sont-ils triés ?

Avec quoi est-elle la séquence de connexion de client et/ou sans serveur préféré ?

Pour l'ordre de connexion sans serveur préféré, émettez les étapes suivantes :

1. Service de découverte (requête et réponse GNS)
2. Artère de découverte à entretenir (requête et réponse de RIP)
3. Établissez le rapport au serveur le plus proche
4. Obtenez les informations de serveur de fichiers
5. Négociez la taille de mémoire tampon
6. Effacez la connexion précédente

7. Obtenez la date et l'heure de serveur de fichiers

Pour l'ordre de connexion avec le serveur préféré, émettez les étapes suivantes :

1. Service de découverte (requête et réponse GNS)
2. Artère de découverte à entretenir (requête et réponse de RIP)
3. Établissez le rapport au serveur le plus proche
4. Obtenez les informations de serveur de fichiers
5. Négociez la taille de mémoire tampon
6. Lisez la valeur d'une propriété de « a préféré le serveur » enregistré dans le serveur le plus proche
7. Artère de découverte au serveur préféré
8. Créez la connexion au serveur préféré
9. Get a préféré les informations du serveur de fichiers du serveur
10. Négociez la taille de mémoire tampon
11. Effacez la connexion de service avec le serveur le plus proche
12. Effacez la connexion précédente avec le serveur préféré
13. Obtenez la date du serveur et le temps de fichier

Ceci exige toujours la requête/réponse GNS du serveur le plus proche, mais il ne se termine pas l'ordre de connexion avec le serveur le plus proche. Il utilise le serveur le plus proche pour apprendre comment arriver au serveur préféré. Une fois l'artère au serveur préféré est apprise, elle détruit la connexion avec le serveur le plus proche et répète l'ordre de connexion avec le serveur préféré.

Comment filtrez-vous des réponses aux demandes GNS ou GGS ?

Il est utile de contrôler le mécanisme des utilisations d'un routeur de répondre à une demande du client GNS. Afin de répondre à un client, l'IOS sélectionne un des serveurs connus par le routeur. L'IOS fournit une manière d'empêcher quelques serveurs dans cette liste d'être utilisé, utilisant la commande IOS :

ipx output-gns-filter {access-list-number|nom}

Cette commande, une fois appliquée à une interface, s'assurera que le routeur fournit seulement aux clients un serveur le plus proche appariant la liste d'accès spécifiée.

Connecter des clients au réseau

Pourquoi est-ce que je ne peux pas connecter mon client une fois directement relié à un commutateur ?

Les questions qui peuvent résulter de cette configuration sont amplement décrites dans le document suivant utilisant Portfast et d'autres commandes de réparer des connectivités au démarrage de la station de travail.

Fondamentalement, si vous avez un PC connecté directement à un port sur le commutateur de Catalyst, assurez-vous que vous faites activer la fonctionnalité PortFast. Pour le placer avec le CatOS, utilisez la commande :

```
set spantree portfast enable <module/port>
```

Supplémentaire, si vous avez la jonction et les modules capables de acheminement (par exemple, WS-X5225R sur le Catalyst 5000 et tous modules du Catalyst 6000 sont jonction/acheminement capable) vous doivent s'assurer que vous les avez arrêtés manuellement, utilisant les commandes suivantes :

```
set trunk <module/port> off set port channel <module/port-range> off
```

Du logiciel 5.2 sur la famille du Catalyst 4000/5000 et de 5.4 sur la famille du Catalyst 6000, ces trois commandes peuvent être empaquetées dans une commande macro simple :

```
set port host <module/port>
```

Y a-t-il des questions de permis ou de serveur qui affecteront la connexion ?

La première chose qu'un client Novell se connectant fait est d'envoyer une demande GNS (obtenez le serveur le plus proche). Cette demande est répondue par un serveur ou un routeur. Les essais de client puis à connecter utilisant le serveur spécifié dans la réponse. Il y a deux problèmes courants qui peuvent mener à une panne de la connexion :

- Le serveur contacté ne répond pas à GNS. Si le numéro de réseau interne du serveur le plus proche n'a pas 0000.0000.0001 ans, alors c'est probablement un serveur NT qui ignorera GNS.
- Le serveur contacté s'exécute sous peu des permis. Seulement un nombre limité de clients pourrait se connecter, des tentatives supplémentaires manquent.

Dans des les deux cas, si un routeur de Cisco est impliqué, vérifiez quel serveur est donné au client utilisant l'unsort de serveur IPX d'exposition de commande. Vous pouvez alors utiliser la commande d'ipx output-gns-filter de filtrer les serveurs qui ne devraient pas être donnés comme réponse.

Y aura-t-il se connecter de problèmes devant reproduire l'IPX ou les adresses MAC ?

Normalement, toutes les adresses IPX dans le réseau devraient être différentes, car une adresse MAC fait partie de elles. Cependant, il y a beaucoup de cas où l'utilisateur peut coder en dur une adresse MAC, dans ce cas, grande attention de paiement à l'unicité de cette adresse. En outre, faites attention très à ne pas reproduire une adresse IPX en coupant-collant la configuration d'un routeur à l'autre par exemple. C'est extrêmement important pour les interfaces WAN qui utilisent l'adresse MAC définie dans la commande de **routage ipx**. Dans l'exemple suivant, le routeur A et les configurations B ont été reproduits. L'administrateur réseau a changé le réseau IPX sur le chaque des interfaces mais a oublié de mettre à jour la ligne de **routage ipx**, qui est identique dans les deux configurations.

Une interface série n'a pas sa propre adresse MAC. Le routeur utilisera l'adresse MAC spécifiée dans la commande de **routage ipx** d'établir l'adresse IPX de ses interfaces série. Dans ce cas, le

routeur A et le routeur B auront le précis la même adresse IPX AAA.0000.0C14.11E1. Naturellement, il y a beaucoup d'autres manières de tomber dans le problème d'adresse en double. Le TAC voit beaucoup de problèmes de connectivité provoqués par l'adressage en double, fasse attention ainsi très en assignant un réseau IPX ou une adresse MAC.

Sur une liaison donnée :

- Tous les serveurs et Routeurs doivent être configurés avec de seuls numéros de réseau IPX pour une encapsulation donnée.
- Toutes les adresses MAC doivent être seules.

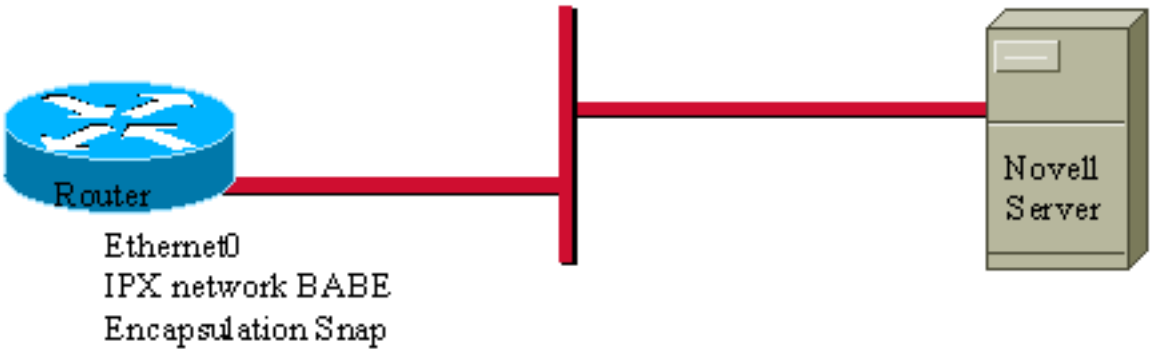
Visionnement des serveurs et des services

Pourquoi est-ce que je ne peux pas accéder à un serveur/service spécifiques ?

Si un client essaye d'accéder à un serveur par un routeur de Cisco, utilisez l'ordre de serveur IPX d'exposition sur le routeur :

Si le serveur/service que vous recherchez est parmi ceux répertoriés quand vous émettez le serveur IPX d'exposition de commande, et là n'est aucune liste d'accès dans la configuration qui casserait la Connectivité, alors le routeur très probablement pas la cause du problème. Si vous ne voyez pas le service sur le routeur, assurez-vous que le réseau IPX du serveur apparaît dans la table de routage. Émettez une commande de show ipx route d'afficher la table de routage ipx. Un service ne sera pas annoncé si le routeur n'a pas une artère au réseau correspondant.

Si le serveur est directement relié au routeur mais n'apparaît pas toujours quand le **serveur IPX d'exposition** est émis, soyez sûr que vous avez configuré le **même réseau IPX** avec la même **encapsulation IPX** sur le serveur et sur le routeur.



Dans cet exemple, soyez sûr que le serveur Novell est configuré avec le protocole SNAP d'encapsulation et que l'adresse IPX est BÉBÉ. Si l'encapsulation est erronée, des paquets envoyés par le serveur seront jetés par le routeur. Si les réseaux IPX ne s'assortissent pas, le serveur affichera un message d'erreur indiquant cette non-concordance.

Sur le routeur, le show ipx traffic de commande fournira quelques informations utiles, malheureusement pour le périphérique entier, pas pour une interface spécifique. Attention de paiement au champ de « erreur de format ». Il sera incrémenté chaque fois que le routeur reçoit un paquet avec l'encapsulation fausse. Si ce compteur augmente, vous êtes très pour avoir une erreur de correspondance d'encapsulation.

Le show ipx interface de commande [<interface>] fournit les détails associés par IPX pour une interface spécifique. Il récapitule le type d'encapsulation, l'adresse IPX, et la liste d'accès configurée pour l'interface. Serveur de pour le dépannage/visibilité de service, il est utile de vérifier qu'une interface spécifique reçoit le RIP et les mises à jour SAP d'un voisin. C'est possible utilisant cette commande.

Pourquoi est-ce que je ne peux pas accéder à un serveur IPX par RConsole ?

Tandis que le RIP et l'EIGRP diffusent l'information réseau, SAP diffuse l'information. Chaque paquet d'IPX SAP généré par un routeur de Cisco peut porter jusqu'à sept entrées 64-byte SAP plus 32 octets de temps système IPX (pour un total de 480 octets), en plus de l'encapsulation de medias supplémentaire. Quand ils sont portés à l'intérieur des paquets EIGRP, les paquets d'IPX SAP se composent d'une en-tête standard EIGRP avec une valeur d'Opcode de 6, suivie de la charge utile standard d'un paquet standard d'IPX SAP sans en-tête IPX d'original.

Dans un échange typique de paquet de SAP, un client de NetWare annoncera une requête de SAP pour localiser un serveur de répertoire, comme indiqué par le champ de type de serveur de SAP (voir le Novell SAP entretenir la liste). Les paquets de réponse de SAP contiennent l'adresse IPX interne des serveurs qui offrent des services d'annuaire. Le client envoie alors une émission de RIP pour localiser le chemin à l'adresse IPX interne du serveur.

Les étapes suivantes établissent une connexion RCONSOLE :

1. Le client de RConsole annonce une demande de SAP recherchant un serveur. Spécifiquement, RConsole envoie une requête de services généraux pour des serveurs du type 0x107. On doit permettre au le routeur de Cisco pour annoncer des serveurs du type 0x107 pour que RConsole travaille sur le PC. Le client envoie une demande de SAP de consultation de serveur quoiqu'elle soit actuellement connectée dans un serveur.S'il y a un serveur sur le segment, il répond au client.Si les clients IPX sont sur un segment sans serveur, le routeur sélectionne la première entrée de SAP dans sa liste non triée pour répondre à la demande GNS des clients IPX. Dans certains cas, la première entrée de SAP dans le routeur est le serveur faux. Émettez l'ordre **non trié de serveur IPX d'exposition** de capturer ceci. Comme contournement, créez une liste d'accès de SAP pour bloquer ce serveur et pour l'appliquer comme filtre GNS.
2. Le client envoie une demande de RIP de l'adresse IPX interne du premier serveur qui a répondu.
3. Une fois que le client apprend le moyen le plus rapide d'arriver au serveur, il lui envoie un paquet de demandes de connexion SPX.

Si vous ne pouvez pas établir un rapport de RConsole à un serveur NetWare particulier, employez les étapes suivantes pour déterminer si la cause est un problème de réseau ou une question de serveur :

- Pouvez-vous voir des serveurs ? Quelques serveurs ? Serveurs qui sont locaux ? Serveurs qui sont à travers le WAN ?
- L'autre trafic IPX est-il affecté ?
- Queest-ce que la table des serveurs IPX ressemble à dans le routeur le plus proche ?
- Voyez-vous l'ID de réseau interne du serveur dans la table du routage ipx du routeur ?
- Indiquez le réseau IPX que vous provenez et le serveur dans lequel vous essayez à RConsole :**show versionaffichez le passageaffichez le serveur IPXshow ipx route**
- Est-vous NetWare de utilisation 4.11 ou NetWare 5 ? Est-ce IP de Novell ? Pouvez-vous

cingler le serveur de NetWare 5 ? En d'autres termes, essai à connecter par l'IP contre de nom. Si oui, des DN n'est pas résolus.

Dans certains cas, une base de données corrompue sur un serveur pose des problèmes de connexion SPX, en particulier car la base de données corrompue est expédiée à d'autres serveurs. Souvent, vous pouvez réparer ce problème en exécutant l'utilitaire de réparation DS. Cependant, si la réparation DS ne restaure pas la base de données, une réinitialisation du serveur peut être exigée. Si vous ne pouvez pas établir un rapport de RConsole utilisant le numéro de réseau interne, le problème est avec le serveur NetWare.

Le Novell édite également des conseils techniques en ligne dans une base de connaissances. Le conseil suivant peut être utile à dépanner des questions de RConsole de la perspective des serveurs IPX. Ce conseil est donné comme ressource pour des clients de Cisco.

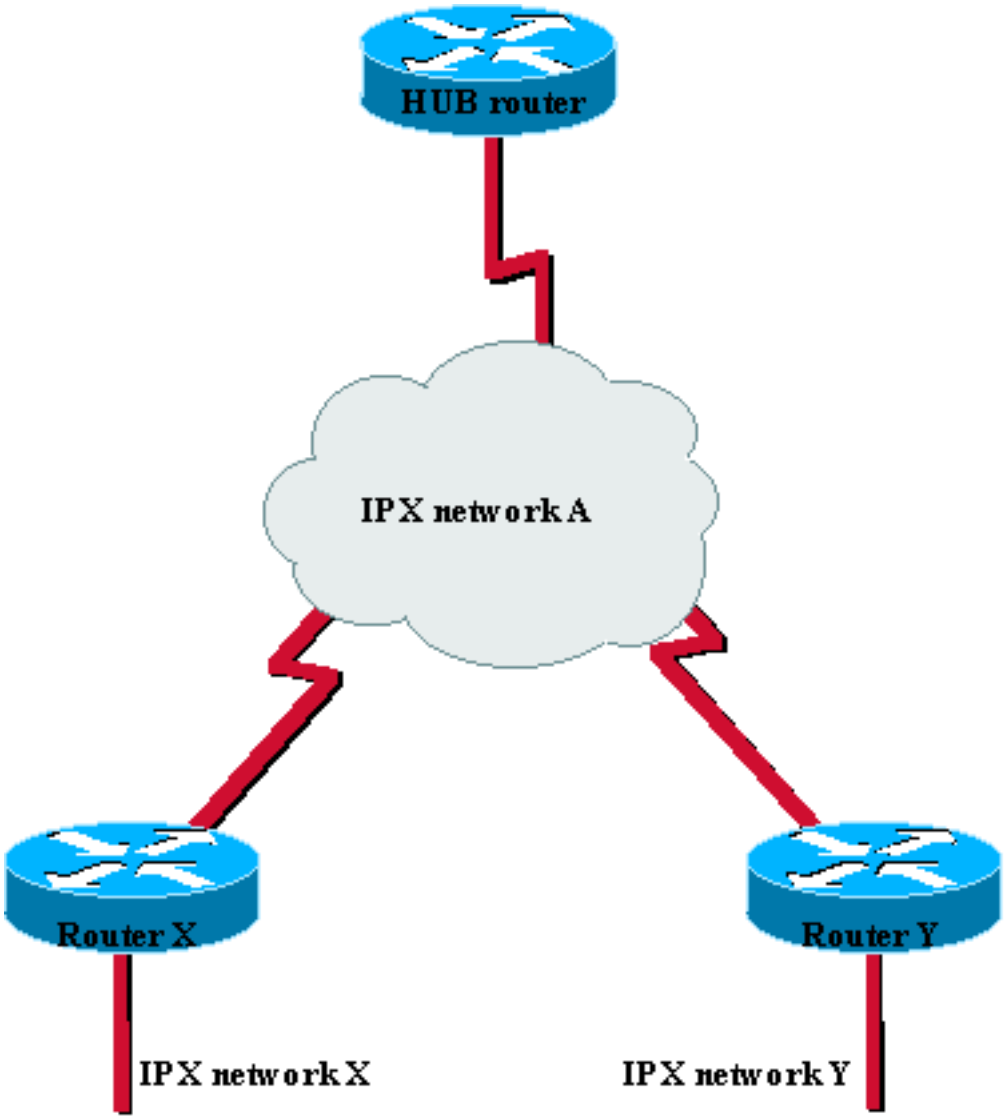
Le « SPX RCONSOLE -4.10-112 établissent la connexion n'a pas établi une connexion au serveur désiré. »

1. Le REMOTE.NLM est-il chargé sur le serveur ? RSPX.NLM est-il chargé ?
2. Avez-vous vérifié le DS et veillé lui est sain et est-ce que ce tout synchronise ?
3. Les erreurs mettent en boîte sont provoqué par par un routeur qui filtre le RConsole SAP. Le type 0107 de SAP est le RConsole SAP, et ne doit pas être filtré si RConsole est de fonctionner correctement.
4. Une mauvaise carte NIC peut interdire le client d'établir la connexion SPX.
5. Assurez l'absolu que tous vos numéros de réseau IPX sont seuls. C'est le raison numéro un pourquoi RConsole échoue, mais parfois le plus difficile de dépanner.
6. Forcez le type de trame sur le client au lieu de à autodétection le type de trame.

Contournement

Àl'écran de RConsole, l'**Institut central des statistiques de** presse et introduisent le numéro de réseau interne IPX du serveur de cible. Le numéro de réseau interne IPX du serveur peut être trouvé en tapant le **CONFIG à la** console de serveur. Si écrire manuellement le numéro de réseau interne IPX permet à RConsole pour fonctionner, il pourrait signifier que la table de socket IPX sur ce serveur a été dépassée. Augmentez la taille de table de socket IPX de maximum : **INETCFG - > protocoles - > IPX - paramètres >IPX/SPX - taille de table de socket IPX de >Maximum**. Le par défaut est 1200. Augmentez cette valeur à 2400 au commencement. Le serveur doit être redémarré afin de remettre à l'état initial cette taille de table.

[Pourquoi est-ce que je ne vois pas tous mes serveurs dans une topologie de hub and spoke ?]



Dans le diagramme ci-dessus, nous avons un routeur concentrateur connecté par l'intermédiaire d'une interface point-à-multipoint à plusieurs autres. C'est les réseaux de hub and spoke typiques de Relais de trames. Tous les Routeurs sont connectés dans les mêmes routeurs en étoile du réseau A. IPX annoncent leur réseau local X et Y au hub, mais vous ne voyez pas le réseau Y dans la table de routage du routeur X (et pareillement vous ne voyez pas X dans routeur Y la table). Ce problème est directement lié au fractionnement-horizon. Le RIP n'annonce pas une artère sur l'interface où il a appris de lui. Fondamentalement, le routeur concentrateur renseigné sur le réseau X sur son interface WAN serial0, connectée au réseau A, et à lui n'annoncera jamais le dos X sur serial0. Routeur Y, également connecté par l'intermédiaire de serial0 au routeur concentrateur, n'entendra jamais parler du réseau X.

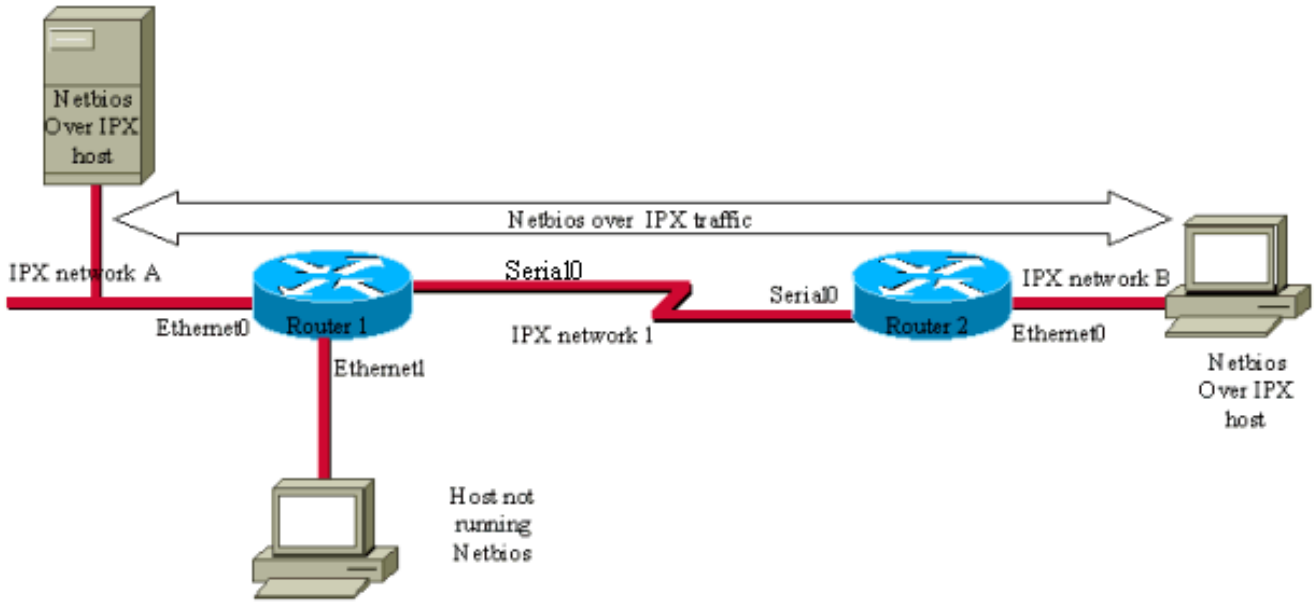
Les caractéristiques de Novell ne permettent pas le fractionnement-horizon à désactiver pour le RIP, tellement là sont deux contournements principaux disponibles avec des Routeurs de Cisco :

- Remplacez l'interface point-à-multipoint par plusieurs interfaces point par point. Ceci peut être fait en créant plusieurs sous-interfaces sur le routeur concentrateur serial0. Le problème est que vous devez assigner un network number différent pour chaque lien point par point créé, qui signifie un changement du système d'adressage et d'une augmentation de la taille de table de routage.
- Remplacez le RIP par l'IPX EIGRP. Ce dernier protocole de routage permet la suppression du fractionnement-horizon (utilisant la commande aucun ipx split-horizon eigrp) et l'exécute mieux sur des liaisons WAN lentes (mises à jour incrémentielles, et ainsi de suite). Le seul

inconvénient est que tous les Routeurs doivent être Cisco sur le WAN.

Pourquoi Netbios au-dessus d'IPX ne va-il pas par mon routeur ?

Ceci se produit parce que Netbios au-dessus d'IPX se fonde sur le type de diffusion 20 paquets IPX, cela ne doivent pas être expédiés par un routeur. Afin de faire expédier ces paquets spécifiques par un routeur, configurez la commande d'ipx type-20-propagation sur chaque interface qui propagera le trafic de Netbios :



Configuration du routeur 1	Configuration de Router2
ipx routing 0000.0000.0001 ! interface Ethernet0 ipx network A ipx type-20-propagation ! interface Ethernet1 ipx network C ! interface Serial0 ipx network 1 ipx type-20-propagation	ipx routing 0000.0000.0002 ! interface Ethernet0 ipx network B ipx type-20-propagation ! interface Serial0 ipx network 1 ipx type-20-propagation

Cette configuration inclut seulement la cloison appropriée IPX. Dans cet exemple, hébergez A et l'hôte B exécutent Netbios au-dessus d'IPX. Le routeur 1 et le Router2 ont une configuration très de base IPX. **L'ipx type-20-propagation de** commande a été ajouté sur l'interface chaque qui est censée transmettre par relais Netbios au-dessus du trafic IPX. En cela le respect, des Ethernet 1 d'interface du routeur 1 n'a pas besoin de lui, car il n'y a aucun hôte de Netbios sur le segment d'Ethernets.

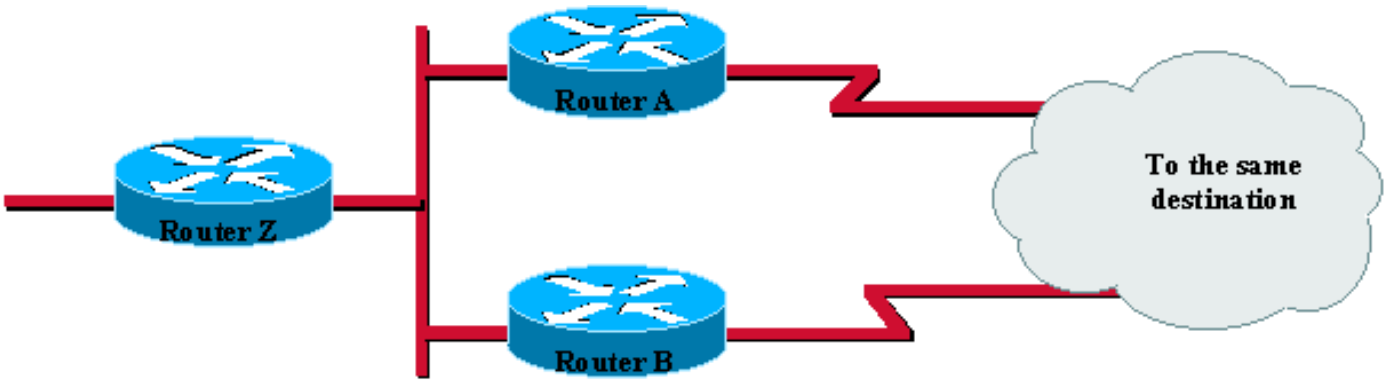
Notez que la commande type-20-propagation, bien qu'obligatoire, aura une incidence des performances sur votre réseau.

Problèmes de performance

Utilisation de mémoire pour des routes RIP et des sèves

IOS	10.0, 10.2	10.3 et en haut
Artère	180 octets pour chaque artère, ajoutent 50 octets pour chaque chemin supplémentaire si maximum-chemin > 1	160 octets pour chaque artère, ajoutent 70 octets pour chaque ajout si maximum-chemin > 1
SAP	200 octets pour chaque SAP, ajoutent 4030 octets pour chaque type de SAP	200 octets pour chaque SAP, ajoutent 4030 octets pour chaque type de SAP, et ajoutent 50 octets pour chaque chemin supplémentaire

Équilibrage de charge IPX sur le routeur de Cisco



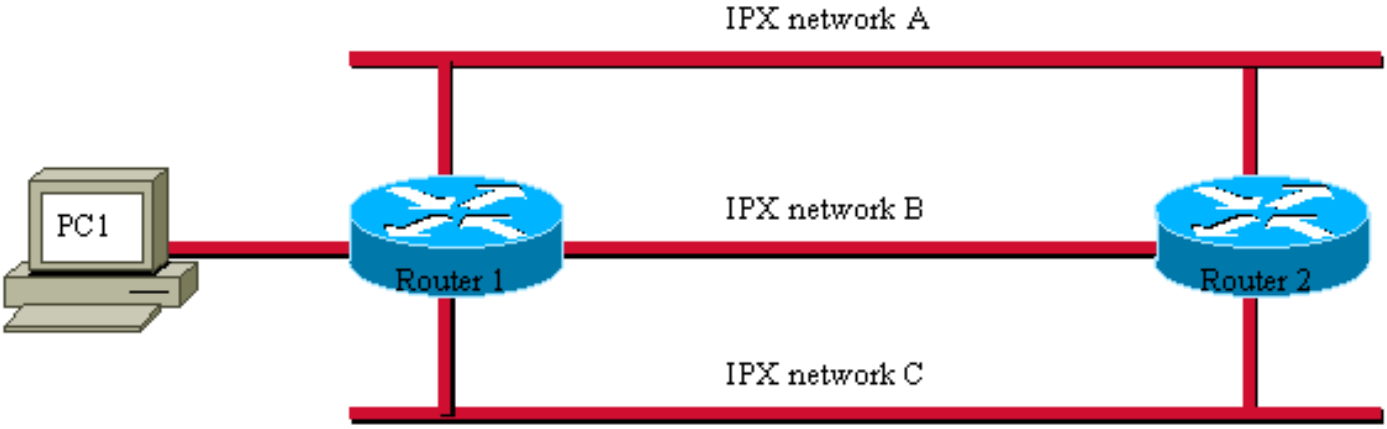
Si le routeur Z est configuré avec l'ipx maximum-paths 2 de commande et les Routeurs A et B vous obtiennent au même réseau de destination dans le même nombre de sauts, le routeur Z enverra alors chaque paquet à la destination au routeur A et B d'une permutation circulaire, avec la lent-commutation et la commutation rapide.

Faites attention que dans ce cas particulier, si vous équilibrez la charge au-dessus des chemins de bande passante inégale et vous faites activer le pburst, les paquets en panne peuvent résulter. De plus nouvelles versions de Netware devraient manipuler ce des versions de Netware meilleur que plus anciennes, mais il vaut d'essayer d'enlever l'Équilibrage de charge ou le pburst quand

vous dépannez un problème de performance dans cette configuration. Depuis IOS 11.1, vous pouvez également activer le par-hôte chargement-partageant utilisant l'ipx per-host-load-share de commande. chargement-partager de Par-hôte transmet le trafic à travers le multiple, des chemins de coût égal tout en garantissant que les paquets pour un hôte d'extrémité donné prend toujours le même chemin.

Mauvais fonctionnement quand type-20-propagation est activé

L'IP helpering sur un routeur n'est pas recommandé dans un réseau, mais la commande d'**ipx type-20-propagation** n'est pas également recommandée, en ce qui concerne la charge de la circulation. Avec une commande d'**aide IP**, le routeur prend un paquet d'émission et le transforme en paquet monodiffusion (ou diffusion dirigée) afin de l'expédier sur le prochain segment. Avec la commande d'**ipx type-20-propagation**, le routeur prend une émission et en avant elle en tant qu'émission. Le paquet de type 20 contient une liste de tous les réseaux déjà intervenus et le routeur ne l'expédiera de retour jamais sur un réseau apparaissant dans cette liste.



Assumons l'ipx type-20-propagation de commande est activé sur chaque interface, avec trois segments entre le routeur 1 et 2 (une configuration commune avec du Catalyst 5000 et RSM connecté ensemble par un trunkof 20 VLAN, par exemple).

1. PC1 émet une émission type-20.
2. Le routeur 1 obtient lui et en avant une copie sur chaque segment A B et C (avec liste de segment D).
3. Le Router2 obtient trois copies et en avant chacun d'eux (la liste de segment est le DA pour le premier DB pour le deuxième C.C pour le tiers) aux deux autres segments faisant 6 copie davantage du paquet (le DA est envoient à B et C, DB à A et au C, C.C à A et B).
4. Le routeur 1 obtient ces six copies (LIMANDE, CNA, DBA, DBC, DCA, bloc de contrôle de données) et expédie tous au dernier segment qui ne l'a pas vu.
5. Le routeur 1 obtient les six paquets (DABC, DACB, DBAC, DBCA, DCAB, DCBA) et les relâche tous car ils ont le tout croisé tous les segments.

Avec cet exemple nous pouvons voir que chaque émission génèrera 15 paquets supplémentaires entre les deux Routeurs. Avec quatre liens (VLAN) entre deux Routeurs vous avez 64 paquets. Avec cinq liens entre deux Routeurs vous avez 325 paquets, et ainsi de suite. Par conséquent, utilisant cette commande entraînera un nombre accru de paquets, qui peuvent ralentir ou arrêter votre réseau.

Pour améliorer la situation, utilisez les commandes suivantes :

- ipx type-20-input-checks `Do additional input checks on type 20 propagation packets` ipx type-20-output-checks `Do additional output checks on type 20 propagation packets`

Quand ceux-ci sont configurés, nous nous assurons que le type 20 est livré dedans sur une interface qui est une route primaire de nouveau à la source. S'il n'est pas, nous relâchons le paquet. Quand nous allons envoyer un paquet, nous vérifions si le réseau/interface que nous l'envoyons à n'est pas une route de retour vers la source de ce paquet de type 20, ou bien nous la relâchons. C'est en plus des huit sauts vérifiant les boucles qui les appels de spécification du routeur IPX pour que nous fassent avec le type 20s.

Configuration de liste d'accès

Filtrage d'une plage des réseaux IPX

La liste d'accès étendue par IPX te permet pour filtrer une plage des réseaux. Par exemple, vous pouvez avoir un grand réseau IPX. Tous les réseaux IPX commencent par et. Les réseaux n'ont pas besoin d'aller à quelques Routeurs, ainsi j'ai filtré chacun utilisant les commandes suivantes :

```
interface Serial0


     ipx output-network-filter 805


     !


     access-list 805 deny  A43C0100


     access-list 805 deny  A43C0101


     access-list 805 deny  A43C0102


     .
     .
     .
```

Cette liste d'accès continue pour 120 lignes. Comment est-ce que je peux filtrer les réseaux IPX qui commencent par A43 ?

Essai utilisant la commande suivante :

```
access-list 905 deny any A4300000.0000.0000.0000 FFFFF.FFFF.FFFF.FFFF
```

Soyez incluent sure une ligne pour permettre les artères que vous voulez. **Le n'importe quel** mot clé représentera « tous les protocoles » et est un argument exigé. Les travaux de masque selon le même principe que le masque de masque IP. Les bits d'hôte doivent être spécifiés, autrement

vous n'aurez pas l'option de masque. Vous pouvez utiliser la liste d'accès étendue par IPX de toutes les mêmes manières que vous pouvez utiliser la version standard. Si vous utilisez des services de lien de NetWare Protocol (NLSP) en tant que votre protocole de routage, vous devrez utiliser de plusieurs zones ainsi vous pouvez filtrer des artères sur les bornes de zone.

Débogage

En visualisant la sortie des paquets IPX d'un debug quelques paquets sont marqués en tant que « mauvais paquet. » Pourquoi sont ces paquets marqués en tant que « mauvais paquet ? »

Exemple :

```
IPX: unable to forward, no helper A0000001.0000.0000.0001(455)to B0000001.ffff.ffff.ffff(455)
typ 4IPX: Fa0/0:A000000.0000.0000.0001->B00000001.ffff.ffff.ffff ln=173 tc=01, bad pkt
```

Ceci peut se produire parce que le socket 455 est le numéro de prise de Netbios et l'adresse de destination de couche de MAC du paquet est émission. Ce paquet sera lâché par le routeur par défaut à moins qu'**IPX type-20-propogation** ou un **ipx helper-address** soit configuré. Voir la documentation sur activer type-20-propogation pour plus de détails sur expédier à ceux-ci Netbios au-dessus des diffusions dirigées IPX.

Informations connexes

- Protocoles de poste de travail
- Support et documentation techniques - Cisco Systems