Contenu

Introduction

Ce document apporte des réponses pour des forums aux questions au sujet d'IPX.

Q. Quel SAP tape sont là ?

Q. Quelle est la signification du « poison SAP » dans la commande de `show ipx traffic` ?

A. Un poison de SAP (ou poison SAP) est une mise à jour SAP qui est envoyée par un

périphérique IPX. Quand le périphérique IPX n'entend plus un service, il informe le réseau que ce service est inaccessible. C'est pareil comme mise à jour SAP régulière sauf que le compte de saut est placé à 16. Il est complètement normal de voir un nombre différent de zéro de sèves de poison dans la sortie de commande de **show ipx traffic**. Ceci se produit lorsqu'un routeur (le chemin à un service) ou un PC (le service lui-même) a été redémarré ou est pour quelque raison devenu inaccessible.

Q. Comment les Routeurs de Cisco manipulent-ils des sèves de poison ?

A. Partie : 9.1 Gestion de SAP de poison

1. Le routeur reçoit un poison SAP.
2. Si la source du poison SAP apparie la source de paires de nom du serveur de SAP/type de serveur dans la table SAP, le routeur marque SAP comme empoisonné et place un temporisateur d'one-minute. Si les adresses ne sont pas identiques, le paquet de poison est jeté. Après one-minute le temporisateur expire, l'entrée est retirée de la table de service, et un paquet de SAP de poison est envoyé toutes autres interfaces.
3. Si le routeur reçoit une mise à jour SAP qui contient une mesure de non-poison dans le temps par paires appariées de nom du serveur/type de serveur est marquée « empoisonné, » il supprime l'entrée de poison et la remplace par la nouvelle entrée. Si aucune nouvelle entrée n'est reçue, le temporisateur de poison expire, et l'entrée est retirée.

Partie : 9.21 et plus défunte Gestion de SAP de poison

9.21 et comportement postérieur se conforme à la « spécification du routeur IPX » de Novell, Inc.

1. Le routeur reçoit un poison SAP.
2. Le routeur marque l'entrée comme empoisonné et place un temporisateur d'one-minute.
3. Le routeur génère immédiatement un paquet de SAP de poison pour ce service toutes autres interfaces.
4. Quand le temporisateur d'one-minute expire, et, si le routeur n'a pas reçu une nouvelle bonne mesure pour le service, le service est enlevé de la table.

Dans des les deux cas, quand un service est marqué en tant qu'empoisonné, la mesure associée avec elle est 16, ou inaccessible, et aucun *obtenez le service le plus proche* ou des paquets de requête de SAP sont répondus qui contiennent ce service dans une réponse.

Q. Comment est-ce qu'un routeur de Cisco sélectionne le serveur pour inclure dans une réponse de *serveur la plus proche d'obtenir* ?

A. Partie : 9.1 Comportement

Le serveur du type prié avec le plus bas hopcount est considéré le serveur « le plus proche ». Si plus d'un serveur du type prié partage le plus bas hopcount, le premier dans la table SAP est choisi. Les nouveaux serveurs de la même chose tapent et le hopcount en tant qu'un qui existe déjà dans la table sont placés dans la table en avant de l'entrée extant. C'est une table SAP témoin :

Les réponses *pour obtenir les* demandes *les plus proches de serveur du* type 4 contiennent la MAGNOLIA. Si un nouveau serveur du type 4, aussi un saut loin, était appris, la table ressemble à ceci :

Les réponses maintenant futures *pour obtenir les* demandes *les plus proches de serveur du* type 4 contiennent NEWSERVER au lieu de la MAGNOLIA.

Partie 9.21 et plus défunt comportement

Le serveur du type prié avec la plus basse mesure d'artère est considéré le serveur « le plus proche ». Si plus d'un serveur du type prié partage la plus basse mesure, le premier dans la table SAP est choisi, à moins que le traitement de recherche séquentielle GNS des réponses GNS soit activé. Les nouveaux serveurs de la même chose tapent et la mesure en tant que celle qui existe déjà dans la table sont placées dans la table en avant de l'entrée extant. Si la recherche séquentielle GNS est activée, les réponses sont équilibrées parmi les serveurs de ce type avec des mesures égales d'artère. Par exemple, regardez cette table SAP :

Les réponses *pour obtenir les* demandes *les plus proches de serveur du* type 4 contiennent la MAGNOLIA. Si un nouveau serveur du type 4 avec la même mesure était appris, la table ressemble à ceci :

Notez que les 9.21 et la table postérieure est de nom commande triée avec les types de coût égal. Afin de voir la table dans les réponses de la commande GNS sont utilisés, utilisent l'**unsort de serveur IPX d'exposition de** commande.

```
     router>show ipx server unsort      Codes: S - Static, I - Incremental, P - Periodic, H -
Holddown     2 Total IPX Servers     Table ordering is based on routing and server info
Type   Name            Net Address       Port   Route  Hops    Itf    P      4     NEWSERVER
AA.0000.0000.0001::0451   3/02     2    Et1    P      4     MAGNOLIA
42.0000.0000.0001::0451   3/02     2    Et2
```

Les réponses maintenant futures pour obtenir les demandes les plus proches de serveur du type 4 contiennent NEWSERVER. Si un autre nouveau serveur avec la même mesure est entendu de, la table ressemble à ceci :

```
     router>show ipx server unsort      Codes: S - Static, I - Incremental, P - Periodic, H -
Holddown     2 Total IPX Servers     Table ordering is based on routing and server info
Type   Name            Net Address       Port   Route  Hops    Itf    P      4     NEWSERVER
AA.0000.0000.0001::0451   3/02     2    Et1    P      4     MAGNOLIA
42.0000.0000.0001::0451   3/02     2    Et2
```

La commande non triée ressemble à ceci :

```
     router>show ipx server unsort      Codes: S - Static, I - Incremental, P - Periodic, H -
Holddown     2 Total IPX Servers     Table ordering is based on routing and server info
Type   Name            Net Address       Port   Route  Hops    Itf    P      4     NEWSERVER
AA.0000.0000.0001::0451   3/02     2    Et1    P      4     MAGNOLIA
42.0000.0000.0001::0451   3/02     2    Et2
```

La première demande GNS du service du type 4 est répondue avec ANEWSERVER ; la deuxième demande GNS est répondue avec NEWSERVER ; la troisième demande est répondue avec la MAGNOLIA ; et le quatrième est répondu avec ANEWSERVER.

Q. Comment l'Équilibrage de charge IPX travaille-t-il au routeur de Cisco ?


```
     router>show ipx server unsort      Codes: S - Static, I - Incremental, P - Periodic, H -
Holddown     2 Total IPX Servers     Table ordering is based on routing and server info
Type   Name            Net Address       Port   Route  Hops    Itf    P      4     NEWSERVER
AA.0000.0000.0001::0451   3/02     2    Et1    P      4     MAGNOLIA
42.0000.0000.0001::0451   3/02     2    Et2
```


A. Si le routeur Z est configuré avec le **max-paths 2 IPX**, et les Routeurs A et B vous obtiendront au même réseau de destination dans la même mesure d'artère (le routeur X), le routeur Z envoie

des paquets à cette destination, qui alterne entre les deux chemins, avec la commutation lente IPX et la commutation rapide IPX. Quand la commutation autonome IPX ou la commutation IPX SSE sont activées, l'Équilibrage de charge a lieu sur a par base de destination, comme il fait avec l'équilibrage TCP/IP.

Q. Est-ce que mode PBURST, qui permet à des plusieurs paquets pour être exceptionnel sans accusé de réception, affecte l'Équilibrage de charge ?

A. Les clients Novell et les serveurs sont les seuls périphériques qui sont impliqués dans des négociations PBURST/LIPx. Cisco est libre de sélectionner Qu'est ce que chemin qu'il pense est le meilleur pour le paquet, ainsi, si le maximum-chemin IPX est plus grand qu'un, les paquets peuvent prendre un différent chemin et arriver en panne. La gare de destination doit traiter commander à nouveau des paquets. Des versions plus anciennes de NetWare ne manipulent pas des paquets en panne très bien. Assurez-vous que vous exécutez les derniers correctifs qui concernent PBURST/LIPx et le plus défunt NLMs pour la représentation optimale PBURST/LIPx.

Q. Comment est-ce que j'inonde des émissions globales IPX ?

A. Partie : 9.1 Comportement

Quand les Routeurs de Cisco utilisent les paquets de « aide », qui utilisent la caractéristique de helper-address, le routeur en avant que le paquet d'émission a reçu à l'adresse IPX configurée dans la commande de **helper-address** sur cette interface. Dans le cas de l'inondation, l'adresse auxiliaire est -1.ffff.ffff.ffff sur l'interface réceptive, et le paquet est envoyé à toutes autres interfaces qui exécutent l'IPX, avec le network number de cette interface placée dans le domaine de réseau de source du paquet.

Deux par exemple, si votre réseau IPX contient 10 segments de réseau IPX, mais seulement de ces segments sont inondés avec le trafic IPX/NetBIOS, vous configurent les adresses réseau spécifiques sur le helper-address.

```
     router>show ipx server unsort     Codes: S - Static, I - Incremental, P - Periodic, H -
Holddown     2 Total IPX Servers     Table ordering is based on routing and server info
Type   Name            Net Address       Port   Route  Hops    Itf    P      4     NEWSERVER
AA.0000.0000.0001::0451   3/02     2    Et1    P      4     MAGNOLIA
42.0000.0000.0001::0451   3/02     2    Et2
```

Sur le réseau distant, vous avez cette configuration :

```
     router>show ipx server unsort     Codes: S - Static, I - Incremental, P - Periodic, H -
Holddown     2 Total IPX Servers     Table ordering is based on routing and server info
Type   Name            Net Address       Port   Route  Hops    Itf    P      4     NEWSERVER
AA.0000.0000.0001::0451   3/02     2    Et1    P      4     MAGNOLIA
42.0000.0000.0001::0451   3/02     2    Et2
```

Ces émissions sont vues seulement sur des segments de réseau 1000, 1011 et les réseaux entre eux (le chemin conduit entre eux). Si -1.ffff.ffff.ffff (inondation) est utilisé, des émissions sont envoyées sur chacun des 10 des segments de réseau.

De plusieurs adresses auxiliaires pour l'IPX sont prises en charge dans la version 9.1 et plus élevé.

Partie : 9.21 Comportement

Appliquez-vous la commande d'**ipx type-20-propagation à** toutes les interfaces qui doivent recevoir

ou envoyez ces paquets. Référez-vous au chapitre 19 du guide de configuration de produits pour routeur pour plus d'informations sur des équipements de propagation du Novell NetBIOS/Type-20.

Dans de plus nouvelles releases de maintenance, l'**aide IPX type-20 de** commande arrête les 9.21 et la Gestion postérieure type-20-propagation de ces paquets et emploie le style 9.1 de la configuration d'ipx helper-address afin d'expédier ces paquets.

Q. Comment est-ce que j'empêche les paquets inondés de la circulation sans fin par mon réseau ?

A. La topologie où ceci se produit est quand vous inondez (pas aide par des adresses dirigées), et là est des plusieurs chemins de nouveau à la source du paquet de NETBIOS. Il y a des cas où bouclage de quelques paquets d'émission se produisent. Des protections peuvent être mises en place pour empêcher les émissions supplémentaires non désirées, qui sont une partie du trafic normal IPX/NetBIOS :

1. Évitez la commande de l'**ipx helper-address -1.ffff.ffff.ffff**. Toutes les fois qu'adresses dirigées par utilisation possible.
2. Configurez les aide-listes IPX pour l'identifier que les paquets vous veulent expédié, et utilisent ces commandes globales : `router>`**`show ipx server unsort`** `Codes: S - Static, I - Incremental, P - Periodic, H - Holddown 2 Total IPX Servers Table ordering is based on routing and server info Type Name Net Address Port Route Hops Itf P 4 NEWSERVER AA.0000.0000.0001::0451 3/02 2 Et1 P 4 MAGNOLIA 42.0000.0000.0001::0451 3/02 2 Et2`Par exemple, peut-être vous voulez seulement des émissions de paquet de type 20 IPX expédiées, et pas les émissions utilisées par la version d'origine de shareware du sort malheureux de jeu de réseau. Sur un système IOS 10.2-based, vous pouvez créer une liste d'aide qui utilise la liste d'accès 901 : `router>`**`show ipx server unsort`** `Codes: S - Static, I - Incremental, P - Periodic, H - Holddown 2 Total IPX Servers Table ordering is based on routing and server info Type Name Net Address Port Route Hops Itf P 4 NEWSERVER AA.0000.0000.0001::0451 3/02 2 Et1 P 4 MAGNOLIA 42.0000.0000.0001::0451 3/02 2 Et2`

Q. Quel est IPX « coutils, » et Cisco les emploie-t-il pour calculer le retard ?

A. Un coutil est une unité de 1/18th de retard rudement du deuxième long ; il y a 18.21 coutils dans une seconde. Des coutils sont utilisés pour mesurer combien de temps il prend un paquet pour atteindre une destination. Le champ de coutils d'une artère IPX est toujours au moins une. Sa valeur est utilisée par le shell de NetWare pour déterminer combien de temps elle doit attendre une réponse d'un serveur de fichiers et des Routeurs de NetWare pour prendre des décisions de routage.

Dans 9.1, nous diffusons les informations de coutils dans la table de routage mais ne les employons pas pour décider la meilleure route à une destination. Au lieu de cela, nous utilisons le compte de saut à ce réseau. Les coutils supplémentaires à ajouter à une artère qui passent par Cisco dans 9.1 sont basés sur la configuration de retard d'interface.

Dans 9.21 et des releases postérieures IOS, les coutils sont la mesure primaire de routage pour déterminer le meilleur chemin à une destination. Les coutils supplémentaires à ajouter à une artère qui passent par Cisco sont déterminés par le « ipx delay X » configuré pour cette interface. Par défaut, toutes les interfaces de RÉSEAU LOCAL ont des valeurs de coutils de 1, et toutes les interfaces WAN ont des valeurs de coutils de 6. Pour le calcul dynamique des coutils pour des

interfaces WAN, utilisation IPXWAN, qui est prise en charge dans la version 10.0 et ultérieures.

Q. Que le moyen de « erreur de format » dans le « show ipx traffic » affiche-t-il ?

A. Une erreur de format se produit quand un routeur reçoit un paquet IPX avec un type d'encapsulation différent IPX que l'interface du routeur, ou quand la longueur du paquet reçu est plus petite que 30 octets ou plus grande que l'unité de transfert maximale de l'interface (MTU).

Q. Pouvez-vous expliquer la commande de « routage ipx » ?

A. L'adresse dans le **Routage Novell de** commande **[adresse]** est seulement appropriée pour des lignes série de non-IPXWAN. Les interfaces avec une adresse de matériel de couche de MAC utilisent cette adresse comme host address IPX. Les lignes série qui n'ont pas une utilisation d'adresse de matériel de couche de MAC l'adresse ont spécifié dans la commande de « routage ipx ». Si aucune adresse n'est spécifiée dans la commande de « routage ipx », le MAC address de la première interface d'IEEE est utilisé comme host address. S'il n'y a aucune interface d'IEEE sur le routeur ou ils ne sont pas vers le haut de quand le routage ipx est activé, le système génère une adresse aléatoire de pseudo-MAC pour l'utiliser.

```
     router>show ipx server unsort     Codes: S - Static, I - Incremental, P - Periodic, H -
Holddown     2 Total IPX Servers     Table ordering is based on routing and server info
Type   Name            Net Address       Port   Route  Hops    Itf    P      4     NEWSERVER
AA.0000.0000.0001::0451   3/02     2    Et1    P      4     MAGNOLIA
42.0000.0000.0001::0451   3/02     2    Et2
```

IPXWAN emploie une différente méthode pour déterminer son host address IPX. Référez-vous à RFC1634 pour des détails.

Q. Comment est-ce que je configure l'IPX au-dessus du Relais de trames ?

A. Utilisez les commandes suivantes :

```
     int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Vous probablement devez tracer un identificateur de connexion de liaison de données (DLCI) à l'adresse IPX si le routeur distant ne prend en charge pas l'ARP inverse que cet exemple trace le routeur distant avec une adresse IPX de 100.0000.0c00.1122 à DLCI 123.

```
     int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Q. Que diriez-vous de toute l'encapsulation Ethernet de Novell tape ?

A. Le type ETHERNET_802.3 de vue est l'encapsulation de propriété industrielle du Novell. Ils ont mis des paquets SPX/IPX directement à moins de 802.3 trames ; ils n'utilisent pas LLC 802.2 ou SE CASSENT. Le résultat est non standard et peut poser des problèmes une fois mélangé au « vrai » trafic 802.3/.2. Ceci s'appelle le « Novell-Ether d'encapsulation Novell » en terminologie de Cisco.

Le type ETHERNET_II de vue est encadrement « standard » d'Ethernet II. Les paquets SPX/IPX sont encapsulés dans des trames d'Ethernet II avec le code 8137 de type. Ces trames sont identiques que les trames de Novell excepté le champ de code de type de deux-octet/longueur de trame. Ceci s'appelle la « encapsulation Novell ARPA » en terminologie de Cisco.

Le type ETHERNET_SNAP de vue, ou le SNAP d'encapsulation Novell de Cisco, est un paquet Ethernet avec une en-tête SNAP.

Le type ETHERNET_802.2 de vue, ou l'encapsulation Novell SAP de Cisco, est la vraie encapsulation 802.3 avec LLC 802.2. C'est la nouvelle encapsulation de par défaut de norme du Novell dans NetWare 3.12 et NetWare 4.x. L'encapsulation par défaut de Cisco des trames IPX sur des Ethernets est toujours Novell-Ether, ou dans la nomenclature du Novell ETHERNET_802.3.

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Q. Que si j'ai un bon nombre de trafic de Novell sur mon réseau, mais moi devons activer l'élimination des imperfections ?

A. Désactivez se connecter à la console, et connectez-vous à un serveur de Syslog. Utilisez ces commandes dans la configuration de faire ceci :

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Q. Comment est-ce que j'utilise un masque pour des numéros de réseau IPX dans une liste d'accès ?

A. Dans 9.1, il n'y a aucun masque pour le network number ; les masques sont pour la source et les adresses de destination. C'est la syntaxe pour la liste d'accès :

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Afin de permettre tous les network number qui commencent par 817axxxx (817a0000 - 817affff), vous devez saisir tous les network number.

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

En 9.21 et plus tard, il est beaucoup plus facile de permettre à tous les network number pour commencer par 817axxxx (817a0000 - 817affff) en raison des masques de réseau. On permet des masques de réseau sur 900 (des listes d'accès étendues) et 1000 Listes d'accès de filtre de SAP. Voici la syntaxe pour la commande :

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Voici un exemple :

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Q. Devez-vous activer le DECNet avant Novell sur les Routeurs de Cisco qui exécutent les deux protocoles ?

A. Avant 8.2, quand le DECNet a été commencé sur un routeur, toutes les interfaces du routeur ont été changées de sorte que l'adresse de niveau de MAC ait fait partie de la marge de DEC. Ceci a signifié que le DECNet a dû être commencé avant que n'importe quel autre protocole qui a utilisé le MAC address en tant qu'élément de son adresse de protocole (comme le Novell et le XNS). 8.2 ont changé l'implémentation de DECNet de sorte que seulement les interfaces qui ont été assignées un decnet cost aient eu leur MAC address changé. Si vous exécutez le DECNet et le Novell sur la même interface, vous devez commencer le DECNet d'abord. Afin d'être sûr, vous devez toujours commencer le DECNet d'abord dans un environnement mixte.

Q. Est-ce que Cisco averti de BIGPACK.NLM et de PBURST.NLM, et ils est-il sont pris en charge ?

A. Le Novell nous a indiqué au sujet d'un module chargeable de NetWare qui traite le serveur de fichiers et le logiciel client plus nouveau. En même temps, ce NLM était dans deux parts : Mode

rafale et grand support de négociation de paquet. Les deux pièces sont maintenant empaquetées dans le même PBURST.NLM appelé par NLM. NetWare 3.12 et NetWare 4.x ont PBURST/LIPx construit dans les no.

PBURST.NLM est conçu pour compenser un problème avec NetWare 3.11 ou de premiers clients/serveurs. Quand le poste de travail ouvre une session ou se relie à un serveur de fichiers, le serveur et station de travail doit négocier une valeur de taille de paquet maximale. C'est la taille de tampon de paquets du poste de travail ou la taille de tampon de paquets du serveur de fichiers, celui qui est plus petit. S'il y a un routeur entre le serveur de fichiers et le poste de travail, une taille par défaut de 576 octets est utilisée parce que le serveur de fichiers ne peut pas déterminer si tous les Routeurs et segments dans le chemin peuvent manipuler une grande longueur de paquet.

La pièce de LIPx de PBurst intercepte la demande de longueur de paquet de négociation et reproduit la procédure ci-dessus exactement, sauf qu'elle ignore le contrôle de routeur. Après que LIPx ait été chargé sur le serveur de fichiers, tous les postes de travail qui relient l'utilisation la plus grande longueur de paquet négociée, indépendamment des Routeurs qui interviennent. Puisqu'il n'y a aucun contrôle de routeur, il y a une possibilité d'une panne d'établissement de session si tous les Routeurs qui interviennent ne sont pas correctement configurés.

Le Packet Burst IPX/NCP est complètement indépendant du routeur de Cisco. Des essais ont été réalisés avec les versions en cours de notre logiciel, et aucun problème n'a été observé. L'ipx throughput de bout en bout a augmenté l'utilisation du mode rafale, qui augmente le nombre de paquets qui peuvent être envoyés avant qu'un ACK soit exigé.

Q. Les paquets de Novell NetBIOS exigent-ils des aide-listes ?

A. Le Netbios du Novell exécute plus de l'IPX. Les requêtes initiales de Netbios généralement prennent la forme des diffusions locales et, dans 9.1, exigent d'une adresse auxiliaire d'atteindre le serveur de cible. Une fois qu'une adresse auxiliaire a été appliquée à une interface, Netbios est expédié à l'adresse définie dans le helper-address. En 9.21 et plus tard, des émissions de Novell NetBIOS sont expédiées avec la commande d'**ipx type-20-propagation**.

Q. Quelles sont toutes les valeurs possibles de protocole et de socket pour des listes d'accès étendues ?

A. Le routeur de Cisco peut filtrer sur N'IMPORTE QUELLE valeur dans les domaines de « protocole » et de « socket » dans la liste d'accès. Voici quelques valeurs réputées pour ces champs :

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Q. Combien grand sont le RIP et les mises à jour SAP IPX ?

A. La taille d'un paquet RIP IPX généré par un périphérique de Cisco est jusqu'à 50 entrées de RIP de huit-octet plus 32 octets d'IPX de supplémentaire (pour un total de 432 octets), plus l'encapsulation de medias supplémentaire.

La taille d'un paquet d'IPX SAP généré par le routeur de Cisco est jusqu'à sept entrées 64-byte SAP plus 32 octets d'IPX de supplémentaire (pour un total de 480 octets), plus l'encapsulation de medias supplémentaire.

Q. Que le moyen de « utilisations » dans le routage ipx ajourne-t-il ?

A. Le compteur de « utilisations » associé avec chaque artère est incrémenté chaque fois que l'artère est choisi comme chemin pour un paquet IPX. Il ne signifie pas nécessairement que ce beaucoup de paquets ont été avec succès envoyés avec cette artère, seulement cela l'artère a été choisi qui beaucoup de fois. Il est encore possible après que le compteur de « utilisations » soit incrémenté pour jeter le paquet dû à la taille dépassée de MTU pour l'interface de sortie, la panne de liste d'accès de sortie, une file d'attente de sortie complète, etc.

Q. À quel type de SAP est-ce que je dois permettre pour que RCONSOLE travaille-t-il ?

A. 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.

Q. Comment la commutation rapide IPX est-elle mise en application ?

A. La commutation rapide IPX est basée sur les informations dans le cache de fastswitch. Des entrées sont créées ont basé sur les informations dérivées du premier paquet commuté par processus à une destination donnée. Quand la destination est sur directement un réseau connecté, ou « des chemins maximum IPX » est placés à 1 (le par défaut), il peut jamais ne y avoir plus d'une entrée de cache de fastswitch à une destination donnée.

Quand « des chemins maximum » est placés à une valeur plus grande que 1, de plusieurs artères de coût égal (aux réseaux distants) peuvent être maintenues dans la table de routage. Dans ce cas, le plusieurs cache entries de fastswitch est créé, aussi bien.

En présence du plusieurs cache entries, l'algorithme de fastswitch IPX est simple : nous circulaires entre les entrées.

Voici la sortie témoin du **show ipx cache** :

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

Des paquets successifs destinés pour 164.0.0c01.d878 sont envoyés par TR0, puis TR1, puis TR0, etc.

Dans 9.0 et 8.3, l'algorithme de recherche séquentielle est identique, mais la destination de cache de fastswitch est gardée par réseau, pas par hôte. Ainsi il ressemble à ceci :

```
int serial 0     encap frame-relay     ipx network 100     frame-relay inverse-arp ipx DLCI
```

En conséquence, vous voyez une légère différence dans le comportement de fastswitch quand partager de chargement est activé. Les paquets entrant successifs destinés pour un réseau distant donné sont les interfaces éligibles envoyées sur une base circulaire, mais les paquets pour un hôte donné sont distribués entre les interfaces dépendantes sur le mélange du trafic destiné pour le réseau distant.

Q. Y a-t-il une manière de contrôler quel serveur répond à la demande GNS ?

A. Nous répondons à des demandes GNS dans 9.1 avec le serveur qui apparaît en haut de la table de service. Afin de changer quel service est en haut de la table dans 9.1, vous pouvez l'un

ou l'autre de filtre qui entretiennent complètement avec un entrée-SAP-filtre (alors personne ne peut accéder à ce serveur par ce routeur), ou vous pouvez définir SAP statique pour le service que vous voulez apparaître en haut de la table. Afin de faire ceci, donnez que SAP statique un compte inférieur de saut que le serveur qui est en haut de la table pour ce type de service, ou faire le serveur qui est en haut du bas inférieur de liste dans la table avec SAP statique défini pour ce service, qui fait son saut compter plus loin loin.

En 9.21 et plus tard, la meilleure manière de contrôler quel serveur répond une réponse GNS est d'utiliser un sortie-gns-filtre.

Q. Fait Cisco prennent en charge le serveur « préféré » du Novell commandent ?

A. Tri de : l'ordre **préféré de serveur** sur le client est utilisé comme ceci :

1. Le client démarre et envoie à un *obtenir l'*émission de paquet de *serveur la plus proche*.
2. S'il n'y a aucun serveur local, le routeur répond à ceci avec le serveur qui est haut de la liste (en 9.21 et plus tard, dessus de la liste non triée).
3. Le client envoie alors une demande de RIP du numéro de réseau interne du serveur.
4. Le routeur répond avec les sauts et les coutils au réseau.
5. Le client ouvre une session de NCP avec le NearestServer.
6. Le client introduit une consultation de façonnage au NearestServer pour le serveur préféré.
7. Le client envoie une demande de RIP du serveur préféré.
8. Les démonter de client de NearestServer et se connecte à PreferredServer. **Remarque:** Les clients peuvent seulement se relier aux périphériques de SYSTÈME D'EXPLOITATION de NetWare, et seulement les périphériques de NetWare peuvent répondre à la demande de consultation de façonnage. Les Routeurs de Cisco ne sont pas des périphériques de NetWare, mais nous conduisons les paquets NCP au serveur le plus proche.

Informations connexes

- Assistance technique sur la technologie
- Assistance sur les produits
- Support et documentation techniques - Cisco Systems