Contenido

Introducción

Este documento contesta las preguntas frecuentes sobre el IPX.

Q. ¿Qué tipos SAP hay?

Q. ¿Cuál es el significado del “veneno SAP” en el `comando show ipx traffic`?

A. SAP envenena (o veneno SAP) es una actualización de SAP que es enviada por un dispositivo

IPX. Cuando el dispositivo IPX oye no más un servicio, notifica la red que ese servicio es inalcanzable. Es lo mismo que SAP regular se pone al día salvo que el conteo saltos se fija a 16. Es totalmente normal ver un número no-cero de savias del veneno en la salida del **comando show ipx traffic**. Esto sucede siempre reiniciaron o por alguna razón llegó a ser inalcanzable a un router (la trayectoria a un servicio) o un PC (el servicio sí mismo).

Q. ¿Cómo los routeres Cisco manejan las savias del veneno?

A. Parte 1: 9.1 Administración de SAP del veneno

1. El router recibe un veneno SAP.
2. Si la fuente de veneno SAP hace juego la fuente de SAP Nombre del servidor/los pares del tipo de servidor en la tabla de SAP, el router marca SAP según lo envenenado y fija un temporizador de un minuto. Si los direccionamientos no son lo mismo, se desecha el paquete del veneno. Después de que expire el temporizador de un minuto, la entrada se quita de la tabla del servicio, y un paquete de SAP del veneno se envía el resto de las interfaces.
3. Si el router recibe una actualización de SAP que contiene un NON-veneno métrico dentro del del tiempo correspondido con Nombre del servidor/de los pares del tipo de servidor es "haber envenenado marcado," él borra la entrada del veneno y la substituye por la nueva entrada. Si no se recibe ninguna nueva entrada, el temporizador del veneno expira, y se quita la entrada.

Parte 2: y posterior Administración de SAP del veneno 9.21

y posterior el comportamiento 9.21 se ajusta a la "Especificación del router IPX" de Novell, Inc.

1. El router recibe un veneno SAP.
2. El router marca la entrada según lo envenenado y fija un temporizador de un minuto.
3. El router genera inmediatamente un paquete de SAP del veneno para este servicio hacia fuera el resto de las interfaces.
4. Cuando expira el temporizador de un minuto, y, si el router no ha recibido un nuevo buen métrico para el servicio, el servicio se quita de la tabla.

En ambos casos, cuando un servicio se marca como envenenado, el asociado métrico con él es 16, o inalcanzable, y ningún *consiga el servicio más cercano* o se contesta SAP pregunta los paquetes que contienen este servicio en una respuesta.

Q. ¿Cómo un router Cisco escoge el servidor para incluir en una *respuesta del servidor más cercana del conseguir*?

A. Parte 1: 9.1 Comportamiento

El servidor del tipo pedido con el hopcount más bajo se considera el servidor "más cercano". Si más de un servidor del tipo pedido comparte el hopcount más bajo, primer en la tabla de SAP se elige. Los nuevos servidores del mismo tipo y hopcount que uno que exista ya en la tabla se colocan en la tabla delante de la entrada extant. Esto es una tabla de SAP de la muestra:

Las respuestas *para conseguir las* peticiones *más cercanas del servidor* el tipo 4 contienen la MAGNOLIA. Si un nuevo servidor del tipo 4, también un salto lejos, era docto, la tabla parece esto:

Ahora las respuestas futuras *para conseguir las* peticiones *más cercanas del servidor* el tipo 4 contienen el NEWSERVER en vez de la MAGNOLIA.

Comportamiento 9.21 de la parte 2 y posterior

El servidor del tipo pedido con la ruta más baja métrica se considera el servidor “más cercano”. Si más de un servidor del tipo pedido comparte el métrico más bajo, primer eligen en la tabla de SAP, a menos que el proceso de ordenamiento cíclico GNS de las respuestas GNS se habilite. Los nuevos servidores del mismo tipo y métricos que el que existe ya en la tabla se colocan en la tabla delante de la entrada extant. Si se habilita el ordenamiento cíclico GNS, las contestaciones son equilibradas entre los servidores de ese tipo con la métrica igual de la ruta. Por ejemplo, mire esta tabla de SAP:

Las respuestas *para conseguir las* peticiones *más cercanas del servidor* el tipo 4 contienen la MAGNOLIA. Si un nuevo servidor del tipo 4 con el mismo métrico era docto, la tabla parece esto:

Note que y posterior la tabla 9.21 es por nombre orden clasificada con los tipos del igual costo. Para ver la tabla en las contestaciones de la orden GNS se utilizan, utilizan el comando show ipx server unsort.

```
     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
```

Ahora las respuestas futuras para conseguir las peticiones más cercanas del servidor el tipo 4 contienen el NEWSERVER. Si otro nuevo servidor con el mismo métrico se oye de, la tabla parece esto:

```
     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 orden sin clasificar parece esto:

```
     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
```

El primer pedido GNS el servicio del tipo 4 se contesta con el ANEWSERVER; la segunda petición GNS se contesta con el NEWSERVER; la tercera petición se contesta con la MAGNOLIA; y el cuarto se contesta con el ANEWSERVER.

Q. ¿Cómo el equilibrio de la carga ipx trabaja en el router 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 configuran al router Z con las MAX-trayectorias 2 IPX, y el Routers A y B le llega a la misma red de destino en la misma ruta métrico (el router X), el router Z envía los paquetes a ese destino, que alterna entre las dos trayectorias, con el IPX Slow Switching y la transferencia rápida IPX.

Cuando se habilita el Autonomous Switching o el IPX SSE Switching IPX, el Equilibrio de carga ocurre en a por el bese de destino, como hace con el equilibrio de TCP/IP.

Q. ¿El modo PBURST, que permite que los paquetes múltiples sean excepcionales sin un acuse de recibo, afecta al Equilibrio de carga?

A. Los clientes Novell y los servidores son los únicos dispositivos que están implicados en las negociaciones PBURST/LIPx. Cisco está libre de escoger cualquier trayectoria que piensa es el mejor para el paquete, así pues, si el maximum-path IPX es mayor de uno, los paquetes pueden tomar una diversa trayectoria y llegar fuera de servicio. La estación de destino tiene que ocuparse de reordenar los paquetes. Las versiones anteriores del Netware no manejan los paquetes defectuosos muy bien. Aseegurese le ejecutar las últimas correcciones que se refieren a PBURST/LIPx y a los últimos NLM para el funcionamiento óptimo PBURST/LIPx.

Q. ¿Cómo inundo los broadcasts globales IPX?

A. Parte 1: 9.1 Comportamiento

Cuando los routeres Cisco utilizan los paquetes del “ayudante”, que utilizan la característica del ayudante-direccionamiento, el router adelante que el paquete de broadcast recibió al direccionamiento IPX configurado en el **comando helper-address** en esa interfaz. En el caso de la inundación, la dirección del ayudante es -1.ffff.ffff.ffff en la interfaz receptiva, y el paquete se envía al resto de las interfaces que ejecuten el IPX, con el network number de esa interfaz puesta en el campo de la red de origen del paquete.

Por ejemplo, si su red IPX contiene 10 segmentos de la red IPX, solamente solamente dos de esos segmentos se inundan con el tráfico IPX/NetBIOS, usted configuran a las direcciones de red específicas en el ayudante-direccionamiento.

```
     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
```

En la red distante, usted tiene esta configuración:

```
     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
```

Estos broadcasts se consideran solamente en los segmentos de red 1000, 1011 y las redes entre ellos (el trayecto ruteado entre ellos). Si se utiliza -1.ffff.ffff.ffff (inundación), los broadcasts se envían en los 10 de los segmentos de red.

Soportan a las direcciones del ayudante múltiples para el IPX en la versión 9.1 y más alto.

Parte 2: 9.21 Comportamiento

Aplique el **comando ipx type-20-propagation a** todas las interfaces que necesiten recibir o envíe estos paquetes. Refiera al capítulo 19 de la guía de configuración de los Productos del router para más información sobre los recursos de propagación del Novell NetBIOS/Type-20.

En más nuevas versiones de mantenimiento, el **ayudante tipo 20 del** comando ipx apaga la Administración 9.21 y posterior type-20-propagation de estos paquetes y utiliza el estilo 9.1 de la configuración del ayudante-direccionamiento IPX para remitir estos paquetes.

Q. ¿Cómo prevengo los paquetes inundados de la circulación sin fin a través de mi red?

A. La topología donde ocurre ésta es cuando usted inunda (no ayudante a través de las direcciones dirigidas), y allí es trayectos múltiples de nuevo a la fuente del paquete NETBIOS. Hay casos donde colocación de algunos paquetes de broadcast ocurre. Los guardias pueden ser puestos en el lugar para prevenir los broadcasts adicionales indeseados, que son un tráfico normal de la parte de IPX/NetBIOS:

1. Evite el **comando ipx helper-address -1 ffff ffff ffff**. Siempre que sea posible utilice a las direcciones dirigidas.
2. Configure las ayudante-listas IPX para identificar que los paquetes usted quieren remitido, y utilizan estos comandos global: `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`Por ejemplo, quizás usted quiere solamente los broadcastes del paquete tipos 20 IPX remitidos, y no los broadcasts usados por la versión de shareware original de la condenación del juego de la red. En un sistema IOS 10.2-based, usted puede crear una lista del ayudante que utilice la lista de acceso 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. ¿Cuáles son IPX “señales,” y Cisco los utiliza para calcular el retardo?

A. Una señal es una unidad de a/18o del retardo áspero de segundo largo; hay 18.21 señales en un segundo. Las señales se utilizan para medir cuánto tiempo toma un paquete para alcanzar un destino. El campo de las señales de una ruta de IPX es siempre por lo menos una. Su valor es utilizado por el shell del Netware para determinar cuánto tiempo debe esperar una respuesta de un servidor de archivos y por los routeres NetWare para tomar las decisiones de ruteo.

En 9.1, llevamos la información de las señales en la tabla de ruteo pero no la utilizamos para decidir la mejor ruta a un destino. En lugar, utilizamos el conteo saltos a esa red. Las señales adicionales a agregar a una ruta que pasan con Cisco en 9.1 se basan en la configuración de retraso de interfaz.

En 9.21 y posterior versiones del IOS, las señales son la métrica de ruteo primaria para determinar el mejor trayecto a un destino. Las señales adicionales a agregar a una ruta que pasan a través de un Cisco son determinadas por el “retardo x IPX” configurado para esa interfaz. Por abandono, todas las interfaces LAN tienen valores de las señales de 1, y todas las interfaces de WAN tienen valores de las señales de 6. Para el cálculo dinámico de las señales para las interfaces de WAN, uso IPXWAN, que se soporta en la versión 10.0 y posterior.

Q. ¿Qué el medio del “error de formato” en “el tráfico IPX de la demostración” visualiza?

A. Un error de formato ocurre cuando un router recibe un paquete IPX con un diverso tipo del

encapsulado IPX que la interfaz del router, o cuando la longitud del paquete recibido es más pequeña de 30 bytes o más grande que la unidad máxima de transmisión de interfaz (MTU).

Q. ¿Puede usted explicar el comando " ipx routing "?

A. El direccionamiento en la **encaminamiento del** comando novell **[address]** es solamente relevante para las líneas del serial NON-IPXWAN. Las interfaces con una dirección de hardware de la capa del mac utilizan ese direccionamiento como la dirección de host IPX. Líneas seriales que no tienen una dirección de hardware de la capa del mac utilizar el direccionamiento especificado en el comando " ipx routing ". Si no se especifica ningún direccionamiento en el comando " ipx routing ", el MAC address de la primera interfaz de IEEE se utiliza como la dirección de host. Si no hay interfaces de IEEE en el router o no están encima de cuando se habilita el IPX Routing, el sistema genera un direccionamiento al azar del pseudo-mac para utilizar.

```
    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
```

El IPXWAN utiliza un método distinto para determinar a su dirección de host IPX. Refiera al RFC1634 para los detalles.

Q. ¿Cómo configuro el IPX sobre el Frame Relay?

A. Use estos comandos:

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

Usted tiene que asociar posiblemente un identificador de conexión de link de datos (DLCI) al direccionamiento IPX si el router remoto no soporta el ARP-inverso que este ejemplo asocia al router remoto con un direccionamiento IPX de 100.0000.0c00.1122 a DLCI 123.

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

Q. ¿Qué sobre todo el encapsulado Ethernet del Novell teclea?

A. El ETHERNET_802.3 del tipo de trama es la encapsulación propietaria del Novell. Pusieron los paquetes SPX/IPX directamente dentro de 802.3 tramas; no utilizan 802.2 LLC ni ROMPEN. El resultado es no estándar y puede causar los problemas cuando está mezclado con el tráfico “real” 802.3/.2. Esto se llama “novell-ether del encapsulado de Novell” en la terminología de Cisco.

El ETHERNET_II del tipo de trama es el enmarcar “estándar” del Ethernet II. Los paquetes SPX/IPX se encapsulan en las tramas del Ethernet II con el código 8137 del tipo. Estas tramas son lo mismo que las tramas de Novell a excepción del tipo two-octet cifran/del campo de la longitud de trama. Esto se llama el “encapsulado de Novell ARPA” en la terminología de Cisco.

El ETHERNET_SNAP del tipo de trama, o el Cisco Novell Encapsulation SNAP, es un paquete Ethernet con un encabezado SNAP.

El ETHERNET_802.2 del tipo de trama, o el encapsulado de Novell SAP de Cisco, es la encapsulación real 802.3 con 802.2 LLC. Éste es el nuevo encapsulado predeterminado estándar del Novell en el Netware 3.12 y el Netware 4.x. El encapsulado predeterminado de Cisco para las tramas IPX en los Ethernetes sigue siendo novell-ether, o en la nomenclatura del

ETHERNET_802.3 del Novell.

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

Q. ¿Qué si tengo las porciones de tráfico del Novell en mi red, solamente yo necesitamos dar vuelta encendido a hacer el debug de?

A. Inhabilite el registro a la consola, y el registro a un servidor de Syslog. Utilice estos comandos en configuración de hacer esto:

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

Q. ¿Cómo utilizo una máscara para los números de red IPX en una lista de acceso?

A. En 9.1, no hay máscara para el network number; las máscaras están para las direcciones de origen y de destino. Éste es el sintaxis para la lista de acceso:

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

Para permitir todos los network number que comiencen con 817axxxx (817a0000 - 817affff), usted tiene que teclear adentro todos los network number.

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

En 9.21 y posterior, permitir que todos los network number comiencen con 817axxxx (817a0000 - 817affff) es mucho más fácil debido a las máscaras de la red. Permiten a las máscaras de la red en 900 (listas de acceso ampliadas) y 1000 SAP filtran las listas de acceso. Aquí está el sintaxis para el comando:

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

Aquí tiene un ejemplo:

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

Q. ¿Usted tiene que habilitar el DECNet antes del Novell en los routeres Cisco que funcionan con ambos protocolos?

A. Antes de 8.2, cuando el DECNet fue comenzado en un router, todas las interfaces del router fueron cambiadas de modo que el direccionamiento del nivel del mac bajara dentro del rango de DEC. Esto significó que el DECNet tuvo que ser comenzado antes de cualquier otro protocolo que utilizara el MAC address como parte de su dirección de protocolo (como el Novell y el XNS). 8.2 cambiaron la instrumentación de DECnet de modo que solamente las interfaces que fueron asignadas un coste del DECNet tuvieran su MAC address cambiado. Si usted ejecuta el DECNet y el Novell en lo mismo interconecta, usted necesita comenzar el DECNet primero. Para ser seguro, usted debe comenzar siempre el DECNet primero en un entorno mezclado.

Q. ¿Es Cisco enterado del BIGPACK.NLM y del PBURST.NLM, y ellos se soporta?

A. El Novell nos ha hablado de un módulo cargable de Netware que actúa encendido el fileserver y el más nuevo software de cliente. Al mismo tiempo, este NLM estaba en dos porciones: Modo de ráfaga y soporte grande de la negociación del paquete. Ambas piezas ahora se lían en el mismo PBURST.NLM llamado NLM. El Netware 3.12 y el Netware 4.x tienen PBURST/LIPx incorporado al NOS.

El PBURST.NLM se diseña para compensar un problema con el Netware 3.11 o

clientes/servidores anteriores. Cuando el puesto de trabajo abre una sesión o los attaches a un fileserver, el puesto de trabajo y el servidor deben negociar un valor máximo de tamaño del paquete. Éste es el tamaño de búfer de paquete del puesto de trabajo o el tamaño de búfer de paquete del servidor de archivos, cualquiera es más pequeño. Si hay un router entre el fileserver y el puesto de trabajo, un tamaño predeterminado de 576 bytes se utiliza porque el fileserver no puede determinar si todo el Routers y segmentos en la trayectoria pueden manejar un tamaño de paquetes grande.

La parte de PBurst de LIPx intercepta la petición del tamaño de paquetes de la negociación y duplica el procedimiento arriba exactamente, salvo que ignora el control del router. Después de que LIPx se haya cargado en el fileserver, todos los puestos de trabajo que asocian el uso el tamaño de paquete negociado más grande, sin importar el Routers que interviene. Puesto que no hay control del router, hay una posibilidad de una falla en el establecimiento de la sesión si no configuran a todo el Routers que interviene correctamente.

La ráfaga de paquetes IPX/NCP es totalmente independiente del router Cisco. Las pruebas se han realizado con las versiones actuales de nuestro software, y no se ha observado ningunos problemas. El rendimiento de procesamiento de IPX de punta a punta ha aumentado el uso del Modo de ráfaga, que aumenta el número de paquetes que puedan ser enviados antes de que se requiera un ACK.

Q. ¿Net BIOS Novell los paquetes requieren las ayudante-listas?

A. El NetBios del Novell ejecuta encima el IPX. Las interrogaciones iniciales del NetBios toman la forma de broadcastes locales y, en 9.1, requieren generalmente a una dirección del ayudante alcanzar al servidor de destino. Una vez que han aplicado a una dirección del ayudante a una interfaz, el NetBios se remite al direccionamiento definido en el ayudante-direccionamiento. En 9.21 y posterior, Net BIOS Novell los broadcasts se remiten con el **comando ipx type-20-propagation**.

Q. ¿Cuáles son todos los valores del protocolo posible y del socket para las listas de acceso ampliadas?

A. El router Cisco puede filtrar en CUALQUIER valor en los campos del “protocolo” y del “socket” en la lista de acceso. Aquí están algunos valores reconocidos para estos campos:

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

Q. ¿Cómo grandes son las actualizaciones del RIP y de SAP IPX?

A. El tamaño de un paquete RIP IPX generado por un dispositivo de Cisco es hasta 50 entradas del RIP del octeto ocho más 32 bytes de IPX de arriba (para un total de 432 bytes), más la tara de encapsulación de medio.

El tamaño de un Paquete IPX SAP generado por el router Cisco es hasta siete entradas 64-byte SAP más 32 bytes de IPX de arriba (para un total de 480 bytes), más la tara de encapsulación de medio.

Q. ¿Qué hace medio de las “aplicaciones” en el tabla de IPX Routing?

A. El contador de “usos” asociado a cada ruta se incrementa cada vez que la ruta se elija como la trayectoria para un paquete IPX. No significa necesariamente que ese muchos paquetes se han

enviado con éxito con esa ruta, sólo eso la ruta fue elegida que muchas veces. Es todavía posible después de que el contador de “usos” se incremente para desechar el paquete debido a la talla del MTU excedida para la interfaz de salida, el error de la lista de accesos de salida, una salida de cola completa, el etc.

Q. ¿Qué tipo SAP tengo que permitir que para que el RCONSOLE trabaje?

A. El RCONSOLE envía una “interrogación de general servicios” para los servidores del tipo 0x107. El router Cisco debe ser permitido para anunciar los servidores del tipo 0x107 para que el RCONSOLE trabaje en el PC.

Q. ¿Cómo se implementa el Fast-Switching IPX?

A. El Fast-Switching IPX se basa en la información en el Fastswitch Cache. Las entradas se crean sobre la base de la información derivada del primer Process-Switched Packet a un destino determinado. Cuando el destino está en directamente una red conectada, o los “trayectos máximos IPX” se fijan a 1 (el valor por defecto), puede nunca haber más de una entrada de Fastswitch Cache a un destino determinado.

Cuando los “trayectos máximos” se fijan a un valor más grande de 1, el Routes de igual costo múltiple (a las redes remotas) se puede mantener la tabla de ruteo. En este caso, se crean las entradas de Fastswitch Cache múltiples, también.

En presencia de las entradas de memoria caché múltiple, algoritmo IPX fastswitch es simple: nosotros circulares entre las entradas.

Aquí está la salida de muestra del caché IPX de la demostración:

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

Los paquetes sucesivos destinados para 164.0.0c01.d878 se envían con el TR0, entonces el TR1, entonces el TR0, el etc.

En 9.0 y 8.3, el algoritmo de ordenamiento cíclico es lo mismo, pero el destino de Fastswitch Cache se guarda por la red, no por el host. Parece tan esto:

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

Por lo tanto, usted ve una leve diferencia en la conducta de Fastswitch cuando se habilita la carga a compartir. Los paquetes de entrada sucesivos destinados para una red remota dada son interfaces elegibles enviadas en una modalidad de ordenamiento cíclico, pero los paquetes para un host dado se distribuyen entre las interfaces dependientes sobre la mezcla de tráfico destinada para la red remota.

Q. ¿Hay una manera de controlar qué servidor contesta a la petición GNS?

A. Contestamos a las peticiones GNS en 9.1 con el servidor que aparece en la cima de la tabla del servicio. Para cambiar qué servicio está en la cima de la tabla en 9.1, usted puede cualquier filtro que mantiene hacia fuera totalmente con un Input-sap-filter (entonces nadie puede acceder ese servidor a través de este router), o usted puede definir SAP estático para el servicio que usted quiere aparecer en la cima de la tabla. Para hacer esto, dé a ese SAP estático un conteo saltos más bajo que el servidor que está en la cima de la tabla para ese tipo de servicio, o hacer el servidor que está en la cima del plumón más bajo de la lista en la tabla con SAP estático definido para ese servicio, que hace su conteo saltos más lejos ausente.

En 9.21 y posterior, la mejor manera de controlar qué servidor contesta a una respuesta GNS es utilizar un salida-gns-filtro.

Q. Hace el comando? del “servidor preferido” del Novell's del soporte de Cisco

A. Clase de: utilizan al **comando preferred server** en el cliente como esto:

1. El cliente inicia y envía *Obtener el paquete del servidor más cercano un* broadcast.
2. Si no hay servidor local, el router contesta a esto con el servidor que es top de la lista (en 9.21 y posterior, top de la lista sin ordenar).
3. El cliente entonces envía un pedido del RIP el número de red interno del servidor.
4. El router contesta con los saltos y las señales a la red.
5. El cliente abre a una sesión NCP con el NearestServer.
6. El cliente envía en una búsqueda de bindery al NearestServer para el servidor preferido.
7. El cliente envía un pedido del RIP el servidor preferido.
8. Las desconexiones del cliente del NearestServer y conectan con PreferredServer. **Nota:** Los clientes pueden asociar solamente al Netware los dispositivos OS, y solamente los dispositivos de NetWare pueden contestar a la petición de la búsqueda de bindery. Los routeres Cisco no son dispositivos de NetWare, pero ruteamos los Paquetes NCP al servidor más cercano.

Información Relacionada

- Soporte de la Tecnología
- Soporte de Producto
- Soporte Técnico y Documentación - Cisco Systems