TEMA 6

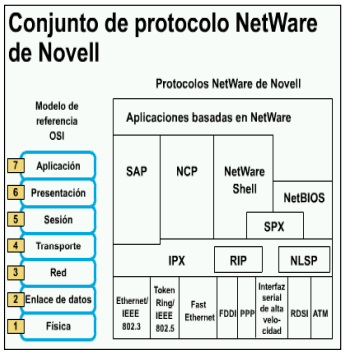
IPX

1

Vista preliminar sobre enrutamiento IPX

2

Netware de Novell



Netware de Novell es un conjunto propietario de protocolos que incluye lo siguiente:

- **IPX, un protocolo de capa 3** no orientado a conexión que no requiere acuse de recibo para cada paquete y define la red y las direcciones de nodo.
- **El protocolo de información de enrutamiento de Novell (RIP),** que es diferente del RIP de IP, facilita el intercambio de información de enrutamiento.
- **El Protocolo de publicación de servicio (SAP)** que permite publicar servicios de red.
- **El Protocolo central de NetWare (NCP)** que permite proporcionar conexiones y aplicaciones cliente a servidor.
- **El Servicio de intercambio de paquete secuenciado (SPX)** para los servicios orientados a conexión de Capa 4.

3

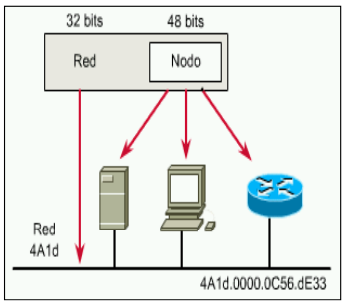
Protocolo IPX

- La dirección es de 80 bits(network.node)
- La dirección MAC de interfaz forma parte de la dirección lógica
- Encapsulamientos múltiples de LAN por interfaz
- El protocolo de enrutamiento por defecto es Novell RIP
- Los servicios de Novell se publican utilizando SAP
- Los clientes de NetWare buscan servidores con paquetes GNS

- IPX es el protocolo NetWare de Capa 3 utilizado para enrutar paquetes a través de redes interconectadas.
- IPX es un protocolo no orientado a conexión (similar a los paquetes IP en las redes TCP/IP) y opera dentro de la misma implementación de red que TCP/IP, siempre y cuando el router sea multiprotocolo.
- Se utiliza en un entorno cliente/servidor

4

Direccionamiento IPX (1/2)



El **direccionamiento** Novell IPX utiliza una dirección en **dos partes**: el número de red y el número de nodo.

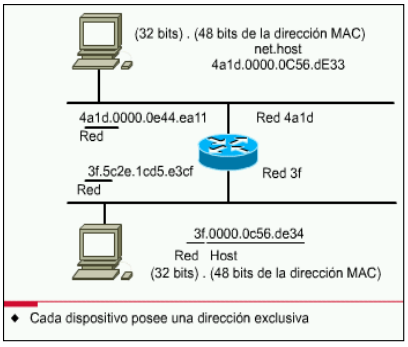
- El número de **red IPX**, asignado por el administrador de red, puede tener una longitud de hasta ocho dígitos hexadecimal
- El número de nodo 12 dígitos hexadecimales, es generalmente la dirección **MAC** para una interfaz de red en el nodo final. Las interfaces seriales utilizan la dirección MAC de la interfaz Ethernet para su dirección de nodo IPX.

RED IPX (32 bits).MAC (48 bits)

- El uso de la dirección MAC en la dirección IPX lógica **elimina** la necesidad de un Protocolo de resolución de direcciones (**ARP**).
- Novell IPX soporta múltiples **redes lógicas** en una interfaz individual (***subinterfaces***); cada red requiere un solo tipo de encapsulamiento.

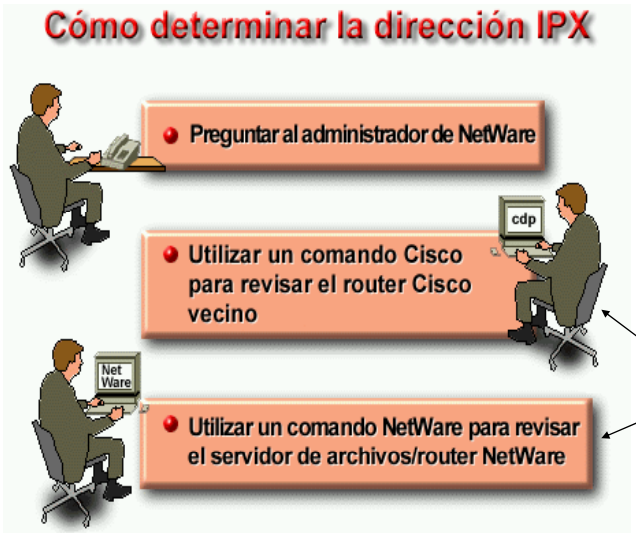
5

Direccionamiento IPX (2/2)



- La figura muestra el nodo 0000.0c56.de33 de IPX en la red 4a1d. Otra dirección de nodo es 0000.0c56.de34 en la red 3f.

6



TELNET a vecino

show protocols
ó
show ipx interface

NOTAS

-No hay que preocuparse de cómo numerar los hosts (uso de las MAC).

-Router no puede tener dos interfaces pertenecientes a la misma red o subredes lógicas(IP, IPX...)

7

Recordemos “show protocols” (Tema 2)

Resultado del comando

```
Router#show protocols
Globalvalues:
Internet Protocol routing is enabled
DECNET routing is enabled
XNS routing is enabled

Vines routing is enabled
AppleTalk routing is enabled
Novell routing is enabled
-- More--
Ethernet0 is up, line protocol is up
Internet address is 183.8.126.2, subnet mask is 255.255.255.128
Decnet cost is 5
XNS address is 3010.aa00.0400.0284
CLNS enabled
Vines metric is 32
AppleTalk address is 3012.93, zone ld-e0
Novell address is 3010.aa00.0400.0284

 - More -
```

8

Encapsulamientos Novell múltiples

Por orden de aparición:

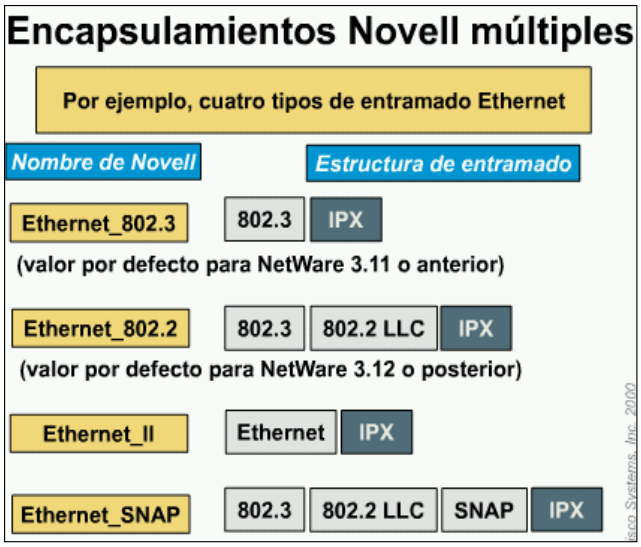
- En 1980 DIX (Xerox, Intel y Digital) lanzaron primero un estándar para Ethernet en 1980, llamado **Ethernet versión I**.
- En 1982, DIX creó **Ethernet II o ARPA** (también denominada Ethernet_II de Novell o Ethernet Versión II) utiliza el encabezado Ethernet Versión II estándar y **se utiliza con TCP/IP**.
- En 1983, Novell creó **Ethernet 802.3** también se denomina Ethernet cruda o sin formato y es la opción por defecto de las **versiones 2 a 3.11 de NetWare**.
- En 1985, IEEE creó **Ethernet 802.2 o SAP** (también denominada Ethernet_802.2 ó 802.3 de Novell) es el formato de trama IEEE estándar, incluyendo un **encabezado ** LLC 802.2**. Con el lanzamiento de **NetWare 3.12 y 4.x**, este encapsulamiento se convirtió en el nuevo formato de trama **estándar de Novell** y también se utiliza para el enrutamiento de OSI.
- **Ethernet SNAP o snap** (también denominada Ethernet_SNAP de Novell o snap) extiende el encabezado IEEE 802.2 agregando un encabezado de **Protocolo de acceso de subred (SNAP)** que proporciona un código de "tipo de encapsulamiento" similar al definido en la especificación de Ethernet Versión II y utilizado con TCP/IP y AppleTalk.

NOTA

Lo más importante que hay que recordar acerca de estas cuatro tipos de tramas es que no son compatibles entre sí. Si un servidor Novell utiliza un entramado 802.3 y se configura un router de Cisco para encapsular utilizando 802.2, estos dos nodos no se podrán comunicar entre sí.

** El LLC contiene campos que identifican puntos de acceso al servicio (SAP)

9



10

Nombres de encapsulamiento para Ethernet, Token Ring y FDDI

Tipo de encapsulamiento	Nombre IPX de Novell	Nombre IOS de Cisco
Ethernet	Ethernet_802.3 Ethernet_802.2 Ethernet_II Ethernet_SNAP	novell-ether sap arpa snap
Token Ring	Token-Ring Token-Ring_SNAP	sap snap
FDDI	FDDI_SNAP FDDI_802.2 FDDI_RAW	snap sap novell-fddi

- El hardware de Cisco y el software Cisco IOS admiten todos los distintos encapsulamientos Ethernet/802.3 utilizados por NetWare.
- El equipo de Cisco puede detectar las diferencias entre estos distintos tipos de paquetes, independientemente de cómo se encapsulan.
- Una sola interfaz LAN soporta múltiples encapsulamientos, permitiendo la coexistencia de nodos más antiguos y más nuevos de NetWare en el mismo segmento LAN, siempre y cuando se puedan configurar ****múltiples redes lógicas**.
- El soporte de encapsulamiento IPX múltiple reduce los gastos del equipo, minimiza la complejidad de la configuración y facilita la migración de un método de encapsulamiento IPX a otro.

*** Las interfaces tendrán varias direcciones IPX con el mismo número de host, pero distintos números de red.*

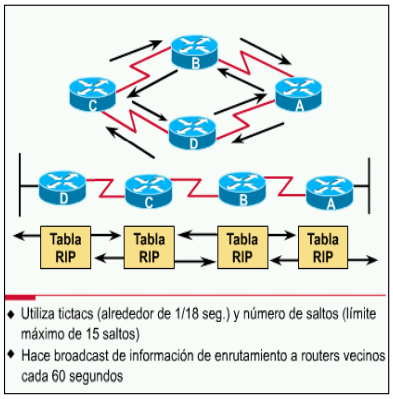
11

Routing en IPX

- RIP de Novell vector distancia
- NLSP Netware Link Service Protocol estado del enlace
- EIGRP (IGRP Mejorado Enhanced de CISCO) incluye módulos para multiprotocolo IP, IPX, AppleTalk,...

12

RIP NOVELL



- tictacs o paso, es el retraso que se espera cuando se usa un longitud concreta.
-Una mejora de enrutamiento es el uso de IGRP mejorado
con soporte para Netware, Appletalk y TCP/IP.

- El RIP Novell es un protocolo de enrutamiento por vector distancia y utiliza dos métricas para tomar decisiones de enrutamiento: **tictacs** (una medida de tiempo) y **número de saltos** (máx 15) (recuento de la cantidad routers que se atraviesan).

  El RIP de Novell verifica sus dos métricas por vector distancia comparando en primer lugar los tictacs en busca de rutas alternativas. Al utilizar los tictacs como métrica se puede obtener una medición más precisa de la velocidad del enlace.
  - Si dos o más rutas poseen el mismo valor de tictacs, el RIP Novell compara el número de saltos.
  - Si dos o más rutas poseen el mismo número de saltos, **el router comparte la carga**.

    Compartir la carga es el uso de dos o más rutas para el enrutamiento de paquetes hacia el mismo destino de forma equitativa entre múltiples routers, a fin de equilibrar el trabajo y mejorar el desempeño de la red.

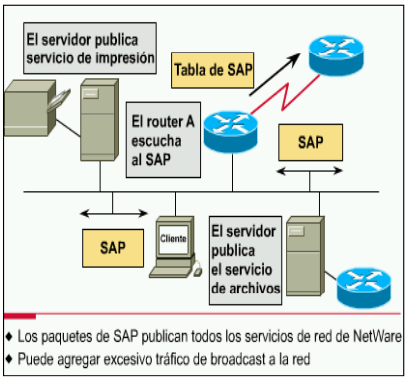
13

Tablas de enrutamiento RIP de Novell

- La tabla de enrutamiento RIP de Novell de un router es distinta de su tabla de enrutamiento IP, ya que **el router mantiene una tabla de enrutamiento para cada protocolo habilitado**.
- Cada router habilitado para IPX **entrega periódicamente copias de su tabla de enrutamiento** RIP de Novell a su vecino más directo. Los routers IPX vecinos **agregan vectores distancia** según se requiera, antes de entregar copias de sus tablas RIP de Novell a sus propios vecinos.
- Un protocolo de **split horizon** (horizonte dividido) con la "mejor información" evita que el vecino realice el broadcast de las tablas RIP de Novell acerca de información IPX nuevamente hacia las redes de las cuales recibió la información.
- El RIP Novell también utiliza un **mecanismo de antigüedad** de la información para manejar las condiciones en las que un router habilitado de IPX entra en colapso sin enviar ningún mensaje preciso a sus vecinos. **Las actualizaciones periódicas reinician el temporizador de antigüedad.**
- Las actualizaciones de la tabla de enrutamiento se envían a **intervalos de 60 segundos**. Esta frecuencia de actualización puede provocar excesivo tráfico en el nivel superior de algunas redes.

14

Protocolo de publicación de servicio (1/5)



- El SAP de NetWare permite que los recursos de red, entre ellos los servidores de archivo y de impresión, publiquen las direcciones y servicios de red que suministran. Cada servicio se identifica con un número, denominado identificador SAP. Las actualizaciones de SAP se envían cada 60 segundos.

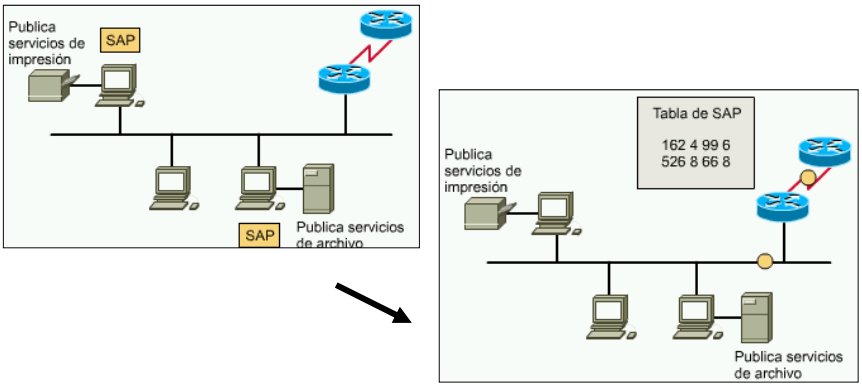
15

Protocolo de publicación de servicio (2/5)

- Los dispositivos de red intermedios, como los routers, escuchan las actualizaciones del SAP y generan una tabla de todos los servicios y direcciones de red asociadas conocidos.
- Cuando un cliente Novell solicita un determinado servicio de red, si se ubica un servidor Netware en el segmento, éste responde a la petición del cliente.
- El router de Cisco no responde a la petición GNS (**GET NEAREST SERVICE**). Si no hay servidores NetWare en la red local, el router de Cisco responde con una dirección de servidor desde su propia tabla SAP. El cliente puede entonces comunicarse directamente con el servicio.
- Todos los servidores de las redes NetWare pueden publicar sus servicios y direcciones. Todas las versiones de NetWare soportan los broadcasts SAP para anunciar y ubicar los servicios de red registrados. Agregar, encontrar y eliminar servicios en la red es un proceso dinámico debido a las publicaciones SAP. Cada servicio SAP es un tipo de objeto identificado por un número.
- Los routers no reenvían difusiones SAP. En vez de hacer esto, construyen sus propias tablas SAP y las reenvían a otros routers.
- El reenvío de estas se produce cada 60 seg. , pero la aceptación o el rechazo se puede controlar mediante las listas de acceso.

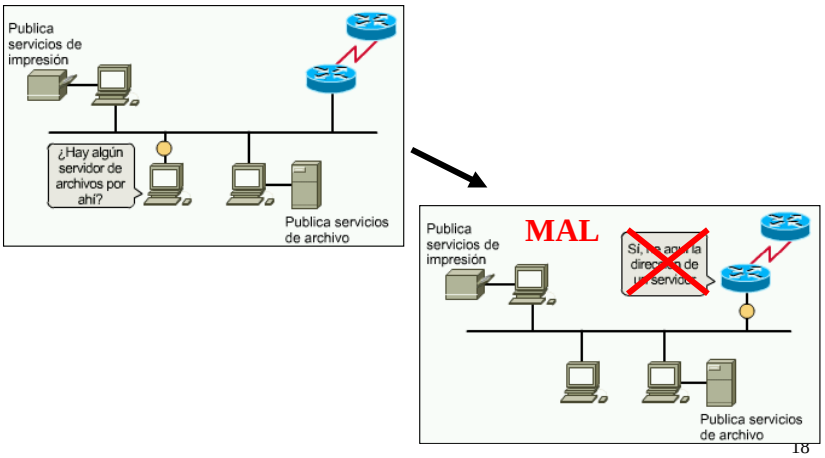
16

Protocolo de publicación de servicio (3/5): Registro de servicios



17

Protocolo de publicación de servicio (4/5)



18

Protocolo de publicación de servicio (5/5)

1) Mediante SAP, los recursos de red como los servidores de archivo o de impresión, pueden publicar sus direcciones y los servicios que ofrecen.

2) Los routers escuchan estos SAPs, y crean una tabla con todos los servicios conocidos y realizan el broadcast de la tabla cada 60 s.

3) Cuando un cliente de Novell desea un determinado servicio, envía una petición.

4) El router responde a esta petición con la dirección de red del dispositivo que ofrece el servicio.

5)Ahora el cliente puede comunicarse con el dispositivo directamente.

Nota: *El software CISCO permite también incrementar el tamaño de los paquetes RIP y SAP (hasta la MTU), con lo cual se reduce el número de paquetes y por tanto se hará un uso más eficiente del ancho de banda.*

19

Uso de nombres en las tablas

- El software Cisco IOS también permite a los administradores de red mostrar las entradas de la tabla SAP por nombre en lugar de por identificador SAP. Al presentar la información de configuración de red en un formato más legible, esta función hace que el mantenimiento de las redes y el diagnóstico de problemas de red sea más fácil.

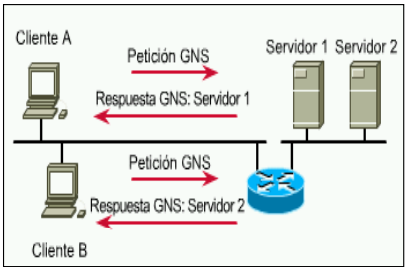
20

Protocolo GNS (1/2)

- Un tipo de publicación SAP es GNS, que permite que un cliente localice rápidamente el servidor más cercano para el inicio de la sesión.
- La interacción cliente/servidor NetWare comienza cuando el cliente enciende su equipo y ejecuta los programas de inicio de cliente. Estos programas utilizan el adaptador de red del cliente en la red e inician la secuencia de conexión para utilizar el shell de NetWare.
- GNS es un broadcast que proviene de un cliente que utiliza SAP. El servidor de archivo NetWare más cercano responde con otro SAP; el tipo de protocolo es GNS. A partir de ese punto, el cliente puede efectuar un login al servidor apuntado, hacer una conexión, establecer el tamaño del paquete, y proceder a utilizar los recursos del servidor.
- Si un servidor NetWare está ubicado en el segmento, responderá al pedido del cliente. El router Cisco no responderá a la solicitud GNS.
- Si no hay servidores NetWare en la red local, el router Cisco responderá con una dirección de servidor de su propia tabla SAP.

21

Protocolo GNS (2/2)



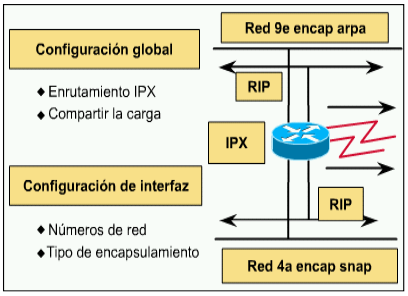
- Al responder a las peticiones GNS, el software Cisco IOS también puede **distribuir los clientes equitativamente** entre los servidores disponibles.
- Por ejemplo, supongamos que los Clientes A y B emiten peticiones GNS. El router Cisco envía una respuesta GNS al Cliente A, pidiéndole que se comunique con el Servidor 1, y una respuesta GNS al Cliente B, pidiéndole que se comunique con el Servidor 2.
- Al brindar **soporte para segmentos LAN sin servidores y distribuir clientes equitativamente** entre los servidores disponibles, el software Cisco IOS **comparte la carga** sobre la base de la red, **mejora la disponibilidad de las aplicaciones** y **minimiza la necesidad de configurar y manejar gran cantidad de servidores locales**, suponiendo que los servidores son idénticos.

22

Configuración del enrutamiento IPX

23

Tareas de configuración de IPX Novell



- Las tareas de configuración IPX globales incluyen lo siguiente:
  - Iniciar el proceso de enrutamiento IPX
  - Habilitar la compartición de carga si resulta necesario para su red.
- Las tareas de configuración IPX de interfaz incluyen lo siguiente:
  - Asignar números de red únicos a cada interfaz. Se pueden asignar múltiples números de red a una interfaz, permitiendo el soporte de distintos tipos de encapsulamiento.
  - Establecer el tipo de encapsulamiento IPX opcional si éste es diferente de la opción por defecto.

24

Comandos de configuración

Router(config)#

ipx routing [node address]

- Habilita el enrutamiento IPX de Novell

(Habilita los servicios RIP y SAP en el router)

Router(config)#

ipx maximum-paths paths

- Configura la acción de compartir la carga en cadena sobre varias rutas con métricas iguales.

(Diseñado para que aumente el rendimiento permitiendo que el router elija entre varias rutas paralelas de coste equivalente. El primer paquete se enviará por la primera ruta, el segundo por la segunda .....) → BALANCE DE CARGA

- El comando **`ipx routing`** habilita el enrutamiento Novell IPX.
  - Si no se especifica ninguna dirección de nodo, el router de Cisco utiliza la dirección MAC de la interfaz.
  - Si un router de Cisco sólo tiene interfaces seriales, se debe especificar una dirección.
- El comando **`ipx maximum-paths`** habilita la opción compartir carga. Es el número máximo de rutas paralelas hacia el destino; la opción por defecto es 1 y el máximo es 512.

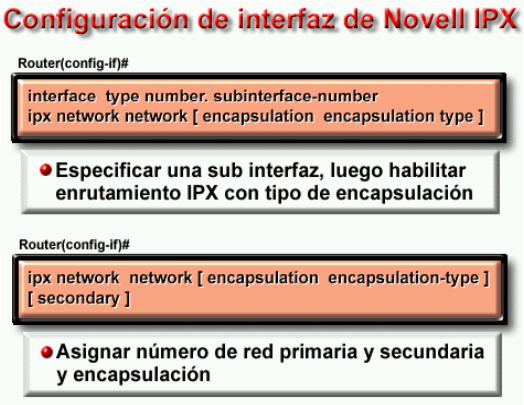
25

Asignación de números de red IPX (1/2)

- Al asignar números de red IPX a las interfaces que soportan múltiples redes IPX, también puede configurar redes IPX primarias y secundarias. La primera red lógica que deberá configurar en una interfaz se considera como **red primaria**. Cualquier red adicional se considera como una **red secundaria**.
- **La asignación del segundo número de red es necesaria si un tipo de encapsulamiento adicional se enlaza a una red individual.**
- Para asignar los números de red a las interfaces que soportan múltiples redes IPX, normalmente se usan **subinterfaces**. Una subinterfaz es un mecanismo que permite que una sola interfaz física brinde soporte para múltiples interfaces o redes lógicas. Es decir que varias interfaces o redes lógicas se pueden asociar con una sola interfaz de hardware. **Cada subinterfaz debe utilizar un encapsulamiento distinto y el encapsulamiento debe coincidir con el de los clientes y servidores que utilizan el mismo número de red**.

26

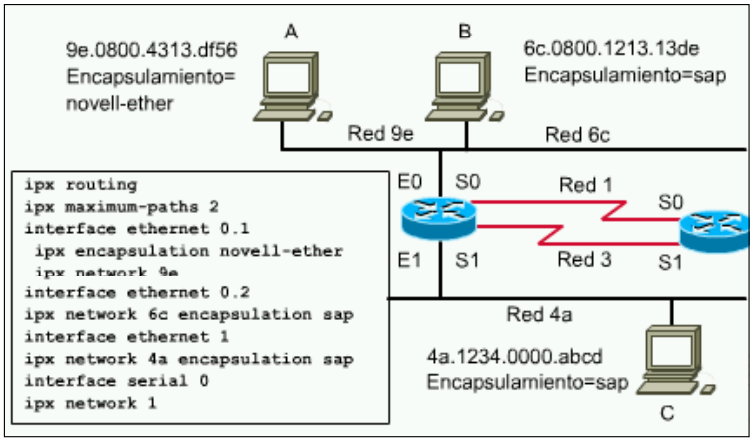
¿¿cómo se hacen subinterfaces???



** Podemos entrar directamente en la subinterface.*
Interface ethernet 0.1
Interface ethernet 0.2
Interface ethernet 1.1
(Config-subif)#

27

Asignación de números de red IPX (2/2)



28

Asignación de números de red IPX a interfaces

Comando	Descripción
`ipx routing`	Selecciona IPX para enrutamiento e inicia RIP de IPX.
`ipx maximum-paths 2`	Permite compartir la carga en rutas métricas paralelas a su destino. La cantidad de rutas paralelas utilizadas se limita a dos.
`interface ethernet 0.1`	Indica la primera subinterfaz en la interfaz E0.
`encapsulation novell-ether`	Especifica que se utiliza el formato de trama exclusivo de Novell en este segmento de red. La palabra clave de Cisco es novell-ether; La terminología de Novell es Ethernet_802.3
`ipx network 9e`	El número de red asignado a la subinterfaz E0.1.
`interface ethernet 0.2`	Indica la segunda subinterfaz en la interfaz E0.
`ipx network 6c`	El número de red asignado a la subinterfaz E0.2.
`encapsulation sap`	Especifica que se utiliza el formato de trama Ethernet 802.2 en este segmento de red. La palabra clave de Cisco es sap.

© Cisco Systems, Inc. 2010

29

Verificación y monitorización del enrutamiento IPX

30

Comandos de control y resolución de problemas de IPX

Comando	Muestra
comandos de control	
`show ipx interface`	Estado y parámetros de IPX.
`show ipx route`	Contenido de la tabla de enrutamiento.
`show ipx servers`	Lista del servidor IPX.
`show ipx traffic`	Cantidad y tipo de paquetes.
Comandos de resolución de problemas.	
`debug ipx routing activity`	Información acerca de los paquetes de actualización RIP
`debug ipx sap`	Información acerca de los paquetes de actualización SAP
`ping`	Información acerca de un nodo específico que puede responder a las peticiones de red.

31

Show ipx interface

```
Router# show ipx interface ethernet 0
Ethernet0 is up, line protocol is up
  IPX address is 3010.aa00.0400.0284 NOVELL_ETHER [up] line-up RIPPQ: 0, SAPPQ: 0
  Delay of this Novell network, in ticks is 1
  IPXWAN processing not enabled on this interface
  IPX SAP update interval is 1 minute(s)
  IPX type 20 propagation packet forwarding is disabled
  Outgoing access list is not set
  IPX Helper access list is not set
  SAP Input filter list is not set
  SAP Output filter list is not set
  SAP Router filter list is not set
  SAP GNS output filter list is not set
  Input filter list is not set
  Output filter list is not set
  Router filter list is not set
  Netbios Input host access list is not set
  Netbios Input bytes access list is not set
  Netbios Output host access list is not set
  Netbios Output bytes access list is not set
  Update time is 60 seconds
  IPX accounting is disabled
  IPX fast switching is configured (enabled)
  IPX SSE switching is disabled
  RIP packets received 1, RIP packets sent 10006
  SAP packets received 1, SAP packets sent 6
```

- *Encapsulación NOVELL_ETHER*
- *[up] line-up. Indica si el enrutamiento IPX está activado o no en la interfaz*
- *RIPPQ: Número de paquetes de la cola RIP*
- *SAPPQ: Número de paquetes de la cola SAP*
- *IPX SAP update interval: Frecuencia de actualizaciones SAP de salida. (***ipx sap-interval***)*
- *Delay of this Novell network in ticks : Valor de tictacks (* **ipx delay***)*
- *Secondary address: Dirección de una red secundaria , si es que la hay.*

El comando show ipx interface muestra el estado de la interfaz IPX y de los parámetros IPX configurados en cada interfaz.

- La primera línea resaltada muestra la dirección IPX, el tipo de encapsulamiento y el estado de la interfaz.
- La segunda área resaltada muestra que no se han establecido los filtros SAP.
- La última línea resaltada muestra que se habilita la conmutación rápida.

32

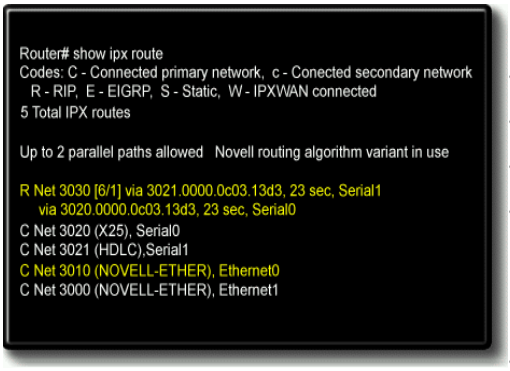
ipx delay

- Puede establecer manualmente la métrica de tictacs para configurar el retardo de tictacs en una interfaz.
- Se utiliza el número de comando ipx delay, donde el número corresponde a la cantidad de tictacs que se asocian a una interfaz. Este comando supera manualmente los siguientes valores por defecto en el router de Cisco:
  - Para las interfaces LAN, 1 tictac
  - Para las interfaces WAN, 6 tictacs

FORMULA nºtic=k/BW

33

Show ipx route



- La R significa que la información se adquirió de la actualización de RIP.
- El número de la red es 3030. La red se encuentra ubicada a una distancia de seis tictacs o un salto.
- El siguiente salto en la ruta es el router 3021.0000.0c03.13d3.
- La información se actualizó hace 23 segundos.
- El router del siguiente salto es una interfaz Serial1 que se puede alcanzar.
- Existe una ruta de métrica igual para un router cuyo siguiente salto es diferente, alcanzable a través de la interfaz Serial 0 (para compartir la carga. Se permiten 2).

La segunda línea resaltada proporciona información acerca de una conexión directa:

- El número de red es 3010.
- El tipo de encapsulamiento es NOVELL-ETHER.
- La C representa la información adquirida de una red primaria directamente conectada.

34

show ipx servers

```
Router>   show ipx servers
Codes: P - Periodic,  I - Incremental,  H - Holddown, S - Static
1 Total IPX Servers

Table ordering is based on routing and server info

Type  Name      Net  Address  Port   Route  Hops Itf
P4    MAXINE  AD33000.0000.1b04.0288:0451 332800/1 2  Et3
```

show ipx servers [**sorted** [*name* | *net* | *type*]] Ordena por nombres, direcciones de red y tipos de dispositivos SAP (es el predeterminado).

Codes: P: La info. Del servidor se conoció a través de las actualizaciones periódicas normales.
I: A través de EIGRP de IPX
H: Se cree que el servidor está caído, y que el router ya no publicará los servicios del servidor
S: El servidor se ha definido estáticamente. Comando ipx sap
Type : Número de servicio SAP (4 = Servidor Archivos Netware)
Route: La métrica o el número de saltos de la ruta a la red
Hops: Número de saltos(publicado por SAP) desde el router hasta la red del servidor.
Itf: La interfaz en la que se descubrió este servidor.

- El comando show ipx servers hace aparecer una lista de los servidores IPX detectados a través de publicaciones SAP.
- El resultado del comando show ipx servers revela la siguiente información:
  - El servicio obtuvo conocimiento acerca del servidor a partir de una actualización SAP.
  - El nombre del servidor, la ubicación de la red, la dirección del dispositivo y el número del socket origen
  - Los tictacs y saltos para la ruta (extraídos de la tabla de enrutamiento)
  - La cantidad de saltos (extraídos del protocolo SAP)
  - La interfaz a través de la cual se alcanza al servidor

35

show ipx traffic

```
Router#show ipx traffic
System Traffic for 2018.0000.0000.0001 System-Name: dtp-18
Rcvd: 23916 total, 13785 format errors, 0 checksum errors, 0 bad hop
count,
    0 packets pitched, 23916 local destinations, 0 multicast
Bcast: 1711 received, 9486 sent
Sent: 16707 generated, 0 forwarded
    0 encapsulations failed, 0 no route
SAP: 6 SAP requests, 6 SAP replies, 2309 servers
    0 SAP Nearest Name requests, 0 replies
    0 SAP General Name requests, 0 replies
    1521 SAP advertisements received, 2212 sent
    0 SAP flash updates sent, 0 SAP format errors
RIP: 6 RIP requests, 6 RIP replies, 2979 routes
    8033 RIP advertisements received, 4300 sent
    154 RIP flash updates sent, 0 RIP format errors
Echo: Rcvd 0 requests, 0 replies
    Sent 0 requests, 0 replies
    0 unknown: 0 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
```

- El comando **show ipx traffic** muestra información acerca del número y tipo de paquetes IPX recibidos y transmitidos por el router.
- En el ejemplo se observa que un alto porcentaje de la cantidad total de paquetes recibidos y enviados fueron publicaciones RIP porque esta muestra se ha tomado de una red laboratorio que esencialmente no tiene tráfico de usuarios.
- Esta pantalla muestra cuanta sobrecarga de tráfico genera IPX.

Rcvd, Sent: descripción de los paquetes recibidos y enviados respectivamente por el router.
Bcast: descripción de los paquetes de difusión recibidos y enviados por el router.
SAP: descripción de paquetes SAP enviados y recibidos por el router
RIP: descripción de paquetes RIP enviados y recibidos por el router
Echo: Descripción de respuestas y peticiones ping recibidas y enviadas por el router.
Watchdog: Descripción de paquetes Watchdog (paquetes que envía un servidor a un cliente después de un cierto periodo de inactividad para comprobar que sigue activo. Si no hay resp. se cierra la conexión) que ha manipulado el router.
Queue lengths: Descripción de los paquetes de salida que hay en los búferes y que esperan ser procesados.

36

Control y administración

- Comandos **debug y ping**, permiten que los administradores de red vean y rastreen prácticamente cualquier aspecto del tráfico de red.
- El soporte de depuración de Cisco puede ser esencial para los administradores de red en el control, administración y resolución de problemas de las redes Novell.
- El comando **debug ipx routing activity** muestra información acerca de los paquetes de actualización de enrutamiento IPX que se transmiten o se reciben.(Un router envía una actualización cada 60 segundos.)
- El comando debug IPX routing activity se debe utilizar con precaución, como cualquier comando debug. Utiliza una gran cantidad de recursos de router y podría provocar el "colapso" del router y de la red.

37

debug ipx routing activity

```
Router# debug ipx routing activity
IPX routing debugging is on
Router#
IPXRIP: positing full update to 3010.ffff.ffff.ffff via Ethernet0 (broadcast)
IPXRIP: positing full update to 3000.ffff.ffff.ffff via Ethernet1 (broadcast)
IPXRIP: positing full update to 3020.ffff.ffff.ffff via Serial0 (broadcast)
IPXRIP: positing full update to 3021.ffff.ffff.ffff via Serial1 (broadcast)
IPXRIP: sending update to 3020.ffff.ffff.ffff via Serial0
IPXRIP: arc=3020.0000.0c03.14d8, dst=3020.ffff.ffff.ffff, packet sent
    network 3021, hops 1, delay 6
    network 3010, hops 1, delay 6
    network 3000, hops 1, delay 6
IPXRIP: sending update to 3021.ffff.ffff.ffff via Serial1
IPXRIP: arc=3021.0000.0c03.14d8, dst=3021.ffff.ffff.ffff, packet sent
    network 3020, hops 1, delay 6
    network 3010, hops 1, delay 6
    network 3000, hops 1, delay 6
IPXRIP: sending update to 3010.ffff.ffff.ffff via Ethernet0
IPXRIP: arc=3010.aa00.0400.0284, dst=3010.ffff.ffff.ffff, packet sent
    network 3030, hops 2, delay 7
    network 3020, hops 1, delay 1
    network 3021, hops 1, delay 1
    network 3000, hops 1, delay 1
IPXRIP: sending update to 3000.ffff.ffff.ffff via Ethernet1
```

- Un router envía una actualización cada 60 segundos. Cada paquete de actualización puede contener hasta 50 entradas. Si hay más de 50 entradas en la tabla de enrutamiento, la actualización incluirá más de un paquete.
- En este ejemplo, el router está enviando actualizaciones pero no las está recibiendo. Las actualizaciones que se reciben de otros routers también aparecerán en este listado.

38

Resolución de problemas para ipx SAP (1/2)

- El comando **`debug ipx sap [events|activity]`** muestra información acerca de los paquetes SAP de IPX que se transmiten o se reciben.
- Se requiere incluir una de las dos opciones [events|activity] al final del comando.
  - La opción Events (eventos) proporciona menos detalles en el resultado del comando, mientras que la de Activity (actividad) más detalles. Al igual que las actualizaciones RIP, estas actualizaciones SAP se envían cada 60 segundos y pueden contener múltiples paquetes. Cada paquete SAP aparece como múltiples líneas en el resultado, incluyendo un mensaje de resumen de paquete y un mensaje de detalle de servicios.

  - Las respuestas SAP pueden ser una de las siguientes:
  - 0x1 -Consulta general
  - 0x2 -Respuesta general
  - 0x3 -petición GNS
  - 0x4 -respuesta GNS

- En cada línea de la respuesta del SAP, aparece la dirección y la distancia del router que responde o del router destino.

39

Resolución de problemas para ipx SAP (2/2)

```
Router# debug ipx sap
IPX SAP debugging is on
Router#
NovellSAP: at 0023F778
I SAP Response type 0x2 len 160 arc:160.0000.0c00.070d dest:160.ffff.ffff.ffff(452)
type 0x4, "HELLO2", 199.0002.0004.0006 (451), 2 hops
type 0x4, "HELLO1", 199.0002.0004.0008 (451), 2 hops
Novell SAP: sending update to 160
NovellSAP: at 00169080
O SAP Update type 0x2 len 96 ssoc; 0x452 dest: 160.ffff.ffff.ffff(452)
Novell: type 0x4 "Magnolia", 42.0000.0000.0000 (451), 2 hops
```

40

Ping ipx privilegiado

- Para analizar la posibilidad de alcanzar el host y la conectividad de red, se utiliza el comando **`ping`** en modo de comando EXEC privilegiado. La sintaxis completa de este comando es:

  `ping [ipx] [network.node]`

  El comando **`ping`** privilegiado proporciona una función **`ping`** completa para usuarios con privilegios de sistema.
  El comando **`ping`** privilegiado funciona solamente con routers Cisco que ejecutan la Versión 8.2 o posterior de IOS. Los dispositivos Novell IPX no responden a este comando.
- No puede hacer ping a un router desde ese mismo router.
- Para interrumpir una sesión **`ping`** , la secuencia es Control-^-X o Control-Mayús 6-X. Se introduce esta opción presionando simultáneamente las teclas Control, Mayús y 6, dejando de presionar y luego presionando la tecla X.

41

Ping a nivel de usuario

- Comparado con el comando **`ping`** privilegiado, el comando ping a nivel de usuario proporciona una función de **ping** básica para los usuarios que no poseen privilegios del sistema.
- Este comando es equivalente a una forma simplificada del comando **`ping`** privilegiado.
- Envía cinco ecos de Cisco IPX de 100 bytes. La sintaxis completa de este comando es:
  `ping [ipx] {{host | address}`

- El comando ping a nivel de usuario sólo funciona con routers de Cisco que ejecutan la Versión 8.2 o posterior de IOS. Los dispositivos Novell IPX no responden a este comando. No puede hacer ping a un router desde ese mismo router. Si el sistema no puede asignar una dirección para un nombre de host, devuelve un mensaje de error de dirección o %Unrecognized host (host irreconocible).

42