Contenido

Autor: M. Celeste Weidmann / 2019 - Bárbara Carina Yunges

¡Copia este texto!

Dispositivos de Red

Introducción

En esta unidad veremos los dispositivos de red comunes a la mayoría de las redes de computadoras; pero antes de meternos de lleno en las características de los mismos, estudiaremos un poco más la evolución del estándar Ethernet, o IEEE 802.3.

Ethernet

Ethernet es el nombre del estándar más popular para conectar computadores en una Red de Área Local (LAN). Se usa a menudo para conectar computadores individuales a Internet a través de un enrutador, módem ADSL, o dispositivo inalámbrico. Sin embargo, si se conecta un solo computador a Internet, puede que no use Ethernet. Su nombre viene del concepto físico de “éter”, el medio que se suponía, en otros tiempos, que transportaba las ondas luminosas a través del espacio libre. El estándar oficial se denomina IEEE 802.3.

La topología de muchas redes LAN alámbricas está basada en los enlaces de punto a punto. El estándar IEEE 802.3, comúnmente conocido como Ethernet, es hasta ahora el tipo más común de LAN alámbrica.

Existen dos tipos de Ethernet: Ethernet clásica, y Ethernet conmutada. En esta última es donde los dispositivos llamados switches se utilizan para conectar distintas computadoras. Es importante mencionar que, aunque se hace referencia a ambas como Ethernet, son muy diferentes. La Ethernet clásica es la forma original que operaba a tasas de transmisión de 3 a 10 Mbps. La Ethernet conmutada es en lo que se convirtió la Ethernet y opera a 100, 1 000 y 10 000 Mbps,en formas conocidas como Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet. Actualmente, en la práctica sólo se utiliza Ethernet conmutada.

La Ethernet clásica se tendía alrededor del edificio como un solo cable largo al que se conectaban todas las computadora. Primero apareció la Ethernet gruesa, y luego la Ethernet delgada, que se doblaba con más facilidad y las conexiones se realizaban mediante conectores BNC. La Ethernet delgada era mucho más económica y fácil de instalar, pero sólo se podían tender 185 metros por segmento (en vez de los 500 m con la Ethernet gruesa), cada uno de los cuales sólo podía manejar 30 máquinas (en vez de 100). Cada versión de Ethernet tiene una longitud de cable máxima por segmento (es decir, longitud sin amplificar) a través de la cual se propagará la señal. Para permitir redes más grandes, se pueden conectar varios cables mediante repetidores.

Ethernet empezó a evolucionar y a alejarse de la arquitectura de un solo cable extenso de la Ethernet clásica. Los problemas asociados con el hecho de encontrar interrupciones o conexiones flojas condujeron hacia un distinto tipo de patrón de cableado, en donde cada estación cuenta con un cable dedicado que llega a un hub (concentrador) central. Esto es lo que vemos en la mayoría de las oficinas.

Ethernet fue evolucionando a Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet.

La idea básica detrás de Fast Ethernet era simple: mantener todos los formatos, interfaces y reglas de procedimientos anteriores, pero reducir el tiempo de bits de 100 nseg a 10 nseg; todos los sistemas Fast Ethernet utilizan hubs y switches; no se permiten cables con múltiples derivaciones vampiro ni conectores BNC. Soporta cableado de par trenzado

categoría 3 (100Base-T4) y categoría 5 (100Base-TX), como así también fibra óptica (100Base-FX) Cada vez que se implementa un estandar de este tipo, existe una puja por actualizar la tecnología y mantener compatibilidad hacia atrás. Los usuarios empezaron a implementar con rapidez el estándar Fast Ethernet, pero no deseaban tirar las tarjetas Ethernet de 10 Mbps en las computadoras antiguas. Como consecuencia, casi todos los switches Fast Ethernet pueden manejar una mezcla de estaciones de 10 Mbps y 100 Mbps. Para facilitar la actualización, el estándar provee por sí solo un mecanismo llamado autonegociación, el cual permite que dos estaciones negocien de manera automática la velocidad óptima (10 o 100 Mbps) y la duplicidad (half-dúplex o full-dúplex)

En 1999 el IEEE publicó el estandar Gigabit Ethernet o 80.3ab. Gigabit Ethernet soporta dos modos diferentes de funcionamiento: modo full-dúplex y modo half-dúplex. El modo “normal” es el modo full-dúplex, que permite tráfico en ambas direcciones al mismo tiempo. Gigabit Ethernet soporta tanto el cableado de cobre como el de fibra óptica. Para hacer que Ethernet opere a 1000 Mbps a través de cables categoría 5 se necesita una señalización que utilice los cuatro pares trenzados en el cable, y cada par se utiliza en ambas direcciones al mismo tiempo mediante el uso de un procesamiento de señales digitales para separar las señales.

El estandar siguió avanzando hasta "10 Gigabit Ethernet", muy utilizada dentro de los centros e intercambios de datos para conectar enrutadores, switches y servidores de gama alta, así como en las troncales de larga distancia con alto ancho de banda entre las oficinas que permiten la operación de redes de área metropolitana completas, basadas en Ethernet y fibra. Todas las versiones de Ethernet de 10 gigabits soportan sólo la operación full-dúplex. 10GBase-T es la versión que usa cables UTP. Aunque requiere cableado categoría 6a, en distancias más cortas puede usar categorías más bajas (incluyendo la categoría 5) para reutilizar una parte del cableado ya instalado. No es sorpresa que la capa física esté bastante involucrada para llegar a 10 Gbps sobre par trenzado.

Un detalle completo de la evolución del estandar Ethernet se puede encontrar los libros de Tanenbaun.

Dominios de colisión y dominios de difusión

Una colisión en ethernet es el resultado de dos nodos que transmiten de forma simultanea. Las tramas (agrupación lógica de información que se envía a través de un medio de transmisión) chocan y se dañan cuando se encuentran en el medio físico.

Un broadcast es un paquete de datos que se envía a todos los nodos de la red. Los broadcast se identifican a través de una dirección de broadcast (dirección especial que se reserva para enviar un mensaje para todas las estaciones).

Una importante desventaja de las redes Ethernet 802.3 son las colisiones. Las colisiones se producen cuando dos hosts transmiten tramas de forma simultánea. Cuando se produce una colisión, las tramas transmitidas se dañan o se destruyen. Los hosts transmisores detienen la transmisión por un período aleatorio, conforme a las reglas de Ethernet 802.3 de CSMA/CD.

Dado que Ethernet no tiene forma de controlar cuál será el nodo que transmitirá en determinado momento, sabemos que cuando más de un nodo intente obtener acceso a la red, se producirán colisiones. La solución de Ethernet para las colisiones no tiene lugar de manera instantánea. Además, los nodos que estén involucrados en la colisión no podrán dar comienzo a la transmisión hasta que se resuelva el problema. Cuanto mayor sea la cantidad

de nodos que se agreguen a los medios compartidos, mayor será la posibilidad de que se produzcan colisiones.

Dominio de Colisión

El dominio de colisión en ethernet es el área de la red en el que las tramas que han sufrido colisiones se propagan. Los repetidores y los hubs propagan las colisiones. Los switches y los routers no.

El área de red donde se originan las tramas y se producen las colisiones se denomina: dominio de colisiones.

Dominio Broadcast

Dominio de Broadcast es el conjunto de todos los dispositivos que reciben tramas de broadcast, se originan en cualquier dispositivo del conjunto. Los conjuntos de broadcast generalmente están limitados por routers dado que los router no envían tramas de broadcast.

Dispositivos de comunicación

Repetidores, hubs, puentes, switches, enrutadores y puertas de enlace. Todos estos dispositivos son de uso común, aunque difieren en formas sutiles y no tan sutiles. La clave para entender estos dispositivos es tener en cuenta que operan en distintas capas. La capa es importante porque los distintos dispositivos utilizan diferentes piezas de información para decidir cómo van a conmutar.

Repetidores

El término repetidor viene de los primeros días de la comunicación visual, cuando una persona situada en una colina repetía la señal que había recibido de otra persona que se encontraba en la colina anterior. El telégrafo, el teléfono, el microondas y las comunicaciones ópticas emplean repetidores para potenciar sus señales a largas distancias.

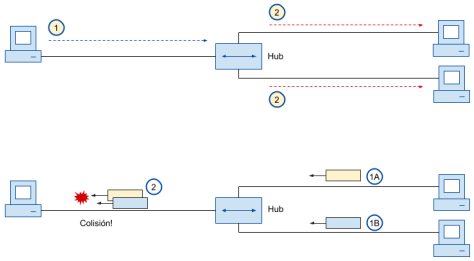
Los repetidores se encuentran en la capa1, capa física, éstos son dispositivos analógicos funcionan con señales de los cables a los que están conectados. Una señal que aparece en un cable se limpia, amplifica y pone en otro cable. Los repetidores no distinguen entre tramas, paquetes o encabezados. Ellos comprenden los símbolos que codifican bits como voltios.

Un repetidor limpia, regenera la señal, y permite extender el área de cobertura de la LAN. Las desventajas al usar un repetidor son el incremento de la colisión, el incremento en el dominio de broadcast, y la incapacidad de realizar cualquier filtrado de tráfico, porque no hacen interpretación de la transmisión.

Concentrador o Hub

Repetidores multipuerto. Los concentradores interconectan dispositivos Ethernet de par trenzado. Funcionan en la capa física (las más baja, la primera). Repiten las señales recibidas por cada puerto hacia el resto de los puertos. Los concentradores pueden, por lo tanto, ser considerados como simples repetidores. Debido a su diseño, sólo uno de los

puertos transmite a la vez con éxito. Si dos dispositivos transmiten al mismo tiempo, las transmisiones se interfieren, y ambos se retiran para tratar de retransmitir los paquetes más tarde. A esto se le conoce como colisión, y cada anfitrión es responsable de detectar las colisiones que se producen durante la transmisión, y de retransmitir sus propios paquetes cuando sea necesario. En un hub, todas las estaciones están en el mismo dominio de colisión. Deben usar el algoritmo CSMA/CD para programar sus transmisiones.



Cuando en un puerto se detectan problemas como: número excesivo de colisiones, algunos concentradores pueden desconectar (segmentar o particionar) ese puerto por un tiempo para limitar su impacto en el resto de la red. Mientras un puerto está segmentado, los dispositivos conectados con ese puerto no pueden comunicarse con el resto de la red. Las redes basadas en concentradores son generalmente más robustas que el Ethernet coaxial (también conocido como 10base2, o ThinNet), donde un dispositivo con problemas puede incapacitar el segmento completo. Pero los concentradores están limitados respecto a su utilidad ya que pueden fácilmente convertirse en puntos de congestionamiento en redes de mucho tránsito.

Los equipos conocidos como hubs son concentradores. Un hub simplemente conecta de manera eléctrica todos los cables que llegan a él, como si estuvieran soldados en conjunto. Un hub tiene varias líneas de entrada que unen de manera eléctrica. Como veíamos en los párrafos anteriores, las tramas que llegan a cualquiera de las líneas se envían por todas las demás. Si dos tramas llegan al mismo tiempo colisionarán, al igual que en un cable coaxial. Todas las líneas que convergen en un hub deben operar a la misma velocidad.

Al igual que los repetidores, los hubs son dispositivos de capa física que no examinan las direcciones de la capa de enlace ni las utilizan de ninguna manera.

Conmutador o Switch

Muchas organizaciones tienen varias redes LAN y desean interconectarlas. ¿No sería conveniente si tan sólo pudiéramos unir las redes LAN para formar una LAN más grande? De hecho, este tipo de redes se puede conectar mediante dispositivos llamados conmutadores o switches; proveen una funcionalidad que va más allá de los hubs de Ethernet clásica y Ethernet para facilitar la unión de varias redes LAN en una red más grande y veloz.

Un conmutador es un dispositivo que funciona de manera muy parecida a un concentrador, pero proporciona una conexión dedicada entre puertos. En lugar de repetir todo el tráfico en cada puerto, el conmutador determina cuáles puertos se están comunicando directamente y los interconecta temporalmente. Los conmutadores proporcionan, en general, mejores

prestaciones que los concentradores, especialmente en redes de mucho tráfico con numerosas computadoras.

Los conmutadores funcionan en la capa de enlace de datos (la segunda capa) puesto que interpretan y actúan sobre las direcciones MAC en los paquetes que reciben. Cuando un paquete llega a un puerto de un conmutador, éste determina la dirección MAC de procedencia, que está asociada a ese puerto. Luego almacena esta información en una tabla MAC interna, y transmite el paquete en el puerto que se corresponda. Si la dirección MAC de destino no aparece en la tabla MAC, el paquete se envía a todas las interfaces conectadas. Cuando llega una trama, el switch extrae la dirección de destino del encabezado y la busca en una tabla para averiguar a dónde debe enviar la trama. En Ethernet, esta dirección es la dirección de destino de 48 bits que se denomina dirección MAC. El switch sólo envía la trama por el puerto en el que se necesita y puede reenviar varias tramas al mismo tiempo. Si el puerto de destino se corresponde con el puerto entrante, el paquete se filtra y no se remite.

Los switches operan en la capa de enlace de datos, por lo que examinan las direcciones de la capa de enlace de datos para reenviar tramas. Como no tienen que examinar el campo de carga útil de las tramas que reenvían, pueden manejar paquetes IP al igual que otros tipos de paquetes. En contraste, los enrutadores examinan las direcciones de los paquetes y realizan su trabajo de enrutamiento con base en ellas, por lo que sólo funcionan con los protocolos para los cuales se diseñaron.

Un switch tiene también las mismas ventajas que un hub. Es fácil agregar o quitar una nueva estación con sólo conectar o desconectar un cable, y es fácil encontrar la mayoría de las fallas, ya que un cable o puerto defectuoso por lo general afectará a una sola estación.

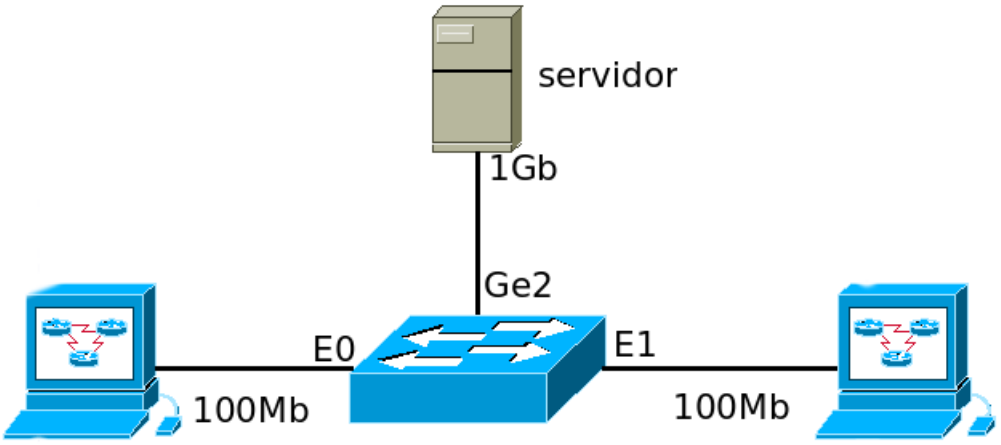
Un switch mejora el desempeño de la red en comparación con un hub de dos maneras. Primero, como no hay colisiones, la capacidad se utiliza con más eficiencia. Segundo y más importante, con un switch se pueden enviar varias tramas al mismo tiempo (por distintas estaciones). Estas tramas llegarán a los puertos del switch y viajarán hacia el plano posterior de éste para enviarlos por los puertos apropiados. No obstante, como se podrían enviar dos tramas al mismo puerto de salida y al mismo tiempo, el switch debe tener un búfer para que pueda poner temporalmente en cola una trama de entrada hasta que se pueda transmitir al puerto de salida. En general, estas mejoras producen una considerable ganancia en el desempeño que no es posible lograr con un hub. Con frecuencia, la velocidad real de transmisión total del sistema se puede incrementar en un orden de magnitud, dependiendo del número de puertos y patrones de tráfico.

El cambio en los puertos por donde se envían las tramas también incluye beneficios de seguridad. La mayoría de las interfaces de LAN tienen un modo promiscuo, en el que todas las tramas se entregan a cada computadora y no sólo las que van dirigidas a ella. En un hub, cualquier computadora conectada puede ver el tráfico transmitido entre todas las demás computadoras. Los espías y los intrusos aman esta característica. En un switch, el tráfico se reenvía sólo a los puertos a los que está destinado. Esta restricción provee un mejor aislamiento, de modo que el tráfico no escape fácilmente y caiga en las manos equivocadas.

Un switch permite "segmentar" la red, dividirla en partes más pequeñas. Un switch aprenden la división de la red, creando tablas de direcciones que contienen: Dirección MAC del dispositivo y la interfaz por la cual lo accede.

Interface	dirección MAC
E0	61:fc:63:c2:45:8c
E1	60:eb:69:c7:15:0c

Los switches ofrecen un desempeño muy superior al de los hubs, además el aislamiento entre los puertos del puente también significa que las líneas de entrada pueden operar a distintas velocidades, e incluso tal vez con distintos tipos de redes. Un ejemplo común es un swithc con puertos que se pueden conectar a redes Ethernet de 10, 100 y 1000 Mbps. Se requiere un búfer dentro del switch para aceptar una trama en un puerto y transmitirla por un puerto distinto. Si las tramas llegan con más rapidez de lo que se pueden retransmitir, el switch se puede quedar sin espacio de búfer y tal vez tenga que empezar a desechar tramas. Por ejemplo, si una red Gigabit Ethernet está transmitiendo bits a una red Ethernet de 10 Mbps a máxima velocidad, el switch tendrá que colocar las tramas en un búfer y ver si no se queda sin memoria. Este problema existe aunque todos los puertos operen a la misma velocidad, ya que tal vez varios puertos envíen tramas a un puerto de destino dado. Es común que los puertos de mayor velocidad en un switch se utilicen para conectar servidores, u otros dispositivos de interconexión como switches o routers.



Todas las instalaciones modernas usan enlaces punto a punto, como los cables de par trenzado, por lo que cada computadora se conecta directamente a un switch y es lógico que tenga muchos puertos.

Cuando un host se conecta a un puerto de switch, el switch crea una conexión dedicada. Esta conexión se considera como un dominio de colisiones individual, dado que el tráfico se mantiene separado de cualquier otro y, por consiguiente, se eliminan las posibilidades de colisión. Los switches reducen las colisiones y permiten una mejor utilización del ancho de

banda en los segmentos de red, ya que ofrecen un ancho de banda dedicado para cada segmento de red. En el caso común en que el cable es full-dúplex, tanto la estación como el puerto pueden enviar una trama en el cable al mismo tiempo, sin preocuparse por los demás puertos y estaciones.

Cuando un switch recibe una trama de broadcast la reenvía a cada uno de sus puertos excepto al puerto entrante en el que el switch recibió esa trama. Cada dispositivo conectado reconoce la trama de broadcast y la procesa. Esto provoca una disminución en la eficacia de la red dado que el ancho de banda se utiliza para propagar el tráfico de broadcast.

Cuando se conectan dos switches, el dominio de broadcast aumenta.

Direcciones MAC

La dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los últimos 24 bits) utilizando el organizationally unique identifier.

Cada dispositivo conectado a una red Ethernet tiene una dirección MAC única asignada por el fabricante de la tarjeta de red. Su función se parece a la de la dirección IP, puesto que sirve como un identificador único que les permite a los dispositivos “hablar” entre sí. Sin embargo, el alcance de una dirección MAC se limita al dominio de difusión que va a estar definido por todos los computadores unidos a través de cables, concentradores y conmutadores, pero sin atravesar enrutadores ni pasarelas de Internet. Las direcciones MAC nunca se usan directamente en la Internet y no son transmitidas entre enrutadores.

VLAN

Las redes VLAN se basan en switches especialmente diseñados para este propósito. Para configurar una red VLAN, el administrador de la red decide cuántas VLAN habrá, qué computadoras habrá en cuál VLAN y cómo se llamarán las VLAN. Para que las VLAN funcionen correctamente, es necesario establecer tablas de configuración en los switches. Estas tablas indican cuáles VLAN se pueden acceder a través de qué puertos.

Las VLAN estáticas también se denominan VLAN basadas en el puerto. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un switch o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el switch.

La definición de múltiples VLAN y el uso de enlaces trunk, frente a las redes LAN interconectadas con un router, es una solución escalable. Si se deciden crear nuevos grupos se pueden acomodar fácilmente las nuevas VLAN haciendo una redistribución de los puertos de los switches

Con las VLAN basadas en puertos, el puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la misma VLAN. Habitualmente es el administrador de

la red el que realiza las asignaciones a la VLAN. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

Los puertos de un switch pueden ser de dos tipos, en lo que respecta a las características VLAN: puertos de acceso y puertos trunk. Un puerto de acceso pertenece únicamente a una VLAN asignada de forma estática. En cambio, un puerto trunk puede ser miembro de múltiples VLAN. Por defecto es miembro de todas, pero la lista de las VLAN permitidas es configurable.

Enrutador o Router

Mientras que los concentradores y los conmutadores proporcionan conectividad para un segmento de una red local, el trabajo de un enrutador es el de remitir paquetes entre diferentes segmentos de la red. Un enrutador normalmente tiene dos o más interfaces físicas de red. Los enrutadores pueden ser dispositivos dedicados de hardware (como por ejemplo los enrutadores Cisco, Huawei o Microtik), o pueden construirse a partir de una computadora estándar con múltiples tarjetas de red y software apropiado.

Un router es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes. Cuando un paquete llega a un enrutador, se quita el encabezado y el terminador de la trama, y se pasa el campo de carga útil de la trama al software de enrutamiento. Este software usa el encabezado del paquete para elegir una línea de salida. En un paquete IP, el encabezado contiene una dirección de 32 bits (IPv4) o 128 bits (IPv6), pero no una dirección IEEE 802 de 48 bits. El software de enrutamiento no ve las direcciones de las tramas y ni siquiera sabe si el paquete llegó por una LAN o por una línea punto a punto.

Un enrutador puede conectar distintos tipos de redes: LAN-LAN, LAN-WAN, LAN-MAN, MAN-WAN, WAN-WAN, inclusive puede conectar diferentes tecnologías (Redes Heterogéneas).

Para lograr sus objetivos, la capa de red debe conocer la topología de la red (es decir, el conjunto de todos los enrutadores y enlaces) y elegir las rutas apropiadas incluso para redes más grandes. También debe tener cuidado al escoger las rutas para no sobrecargar algunas de las líneas de comunicación y los enrutadores, y dejar inactivos a otros. La manera en que cada enrutador toma la decisión de hacia dónde debe enviar el siguiente paquete se le denomina algoritmo de reenvío.

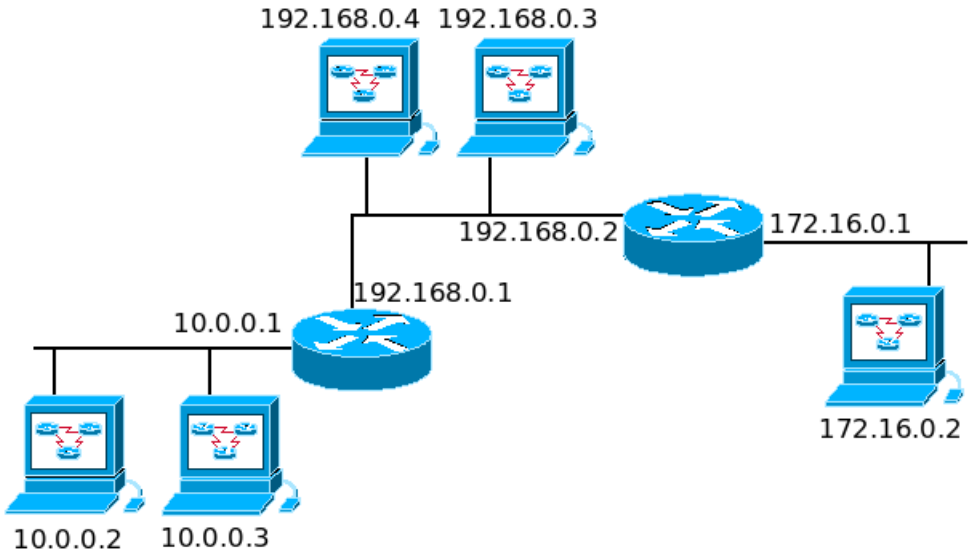
El funcionamiento básico de un enrutador o encaminador consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. Según esta información reenvía los paquetes a otro encaminador o bien al anfitrión final, en una actividad que se denomina 'encaminamiento'. Cada encaminador se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto.

Un router conoce las rutas que tiene directamente conectadas, es decir, las rutas que puede alcanzar directamente en cada puerto del router. Los routers pueden estar configurados de manera estática o dinámica a través de un protocolo de enrutamiento. Las rutas estáticas se

definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso de enrutamiento según los parámetros del administrador. Las rutas estáticas por defecto especifican una puerta de enlace de último recurso, a la que el enrutador debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir, se desconoce; a este puerta de enlace también se la conoce como default gateway.

Los routers toman decisiones para alcanzar el destino final, en base a la red destino y no al host destino. Sólo el Router que está conectado en el mismo segmento IP del host destino, utiliza la información de la parte de host de la dirección IP. Entenderemos mejor esta diferencia entre "red" y "host" destino en las próximas unidades, cuando nos metamos de lleno en direccionamiento ip; a continuación una breve introducción.

Por ejemplo, si la red estuviera estructurada como se muestra en el siguiente gráfico y ambos routers tuvieran definidas rutas estáticas para llegar a todas las redes del gráfico, un paquete que se envía desde el origen: 10.0.0.3 al destino: 172.16.0.2 sigue el siguiente camino: El router que conecta la red 10.0.0.0 y la 192.168.0.0 lo toma, como la red de destino no la tiene directamente conectada, y en su tabla de enrutamiento tiene una ruta estática 172.16.0.0 definida, lo envía hacia el próximo salto que es la interfaz 192.168.0.2. Este segundo router, como la ip destino es una ip de la red que tiene directamente conectada a la interfaz 172.16.0.1 lo envía por dicha interfaz.



Dirección IP

En una red IPv4, la dirección es un número de 32 bits, normalmente escrito como cuatro números de 8 bits expresados en forma decimal y separados por puntos. Ejemplos de direcciones IP son: 10.0.0.1; 192.168.1.1; 172.16.5.23.

Si se enumeraran todas las direcciones IP posibles, estas irían desde 0.0.0.0 hasta 255.255.255.255. Esto arroja un total de más de cuatro mil millones de direcciones IP posibles (255 x 255 x 255 x 255 = 4.228.250.625). Sin embargo, muchas de estas están reservadas para propósitos especiales y no deberían ser asignadas a host. Cada una de las direcciones IP usables, es un identificador exclusivo que diferencia un nodo de red de otro.

Las redes interconectadas deben convenir sobre un plan de direcciones IP. Las direcciones IP deben ser únicas y generalmente no pueden usarse en diferentes puntos de la Internet al mismo tiempo; de lo contrario, los enrutadores no sabrían cuál es la mejor manera de enrutarles los paquetes.

En la unidad 4 veremos con mayor detalle todo lo referente a direccionamiento ip.

En resumen

- Cada interfaz de un Switch separa un dominio de colisión.
- Los Routers separan dominios de colisión por cada interfaz. (El termino dominio de colisión no aplica para interfaces WAN).
- Los Hubs no separan dominios de colisión.
- Las redes LAN modernas con switches y routers, con full duplex en cada enlace, no tienen dominio de colisión.
- En una red LAN moderna con todos switches y routers, incluso sabiendo que full duplex elimina los dominios de colisión, piensa en cada enlace Ethernet como un dominio de colisión separado cuando surga la necesidad de solucionar problemas.

Lecturas recomendadas de la unidad 3

- Redes de Computadoras. Tanenbaum. "Capa física de Ethernet clásica".
- Redes de Computadoras. Tanenbaum. "Ethernet conmutada".
- Redes de Computadoras. Tanenbaum. "Fast Ethernet".
- Redes de Computadoras. Tanenbaum. "Gigabit Ethernet".
- Redes de Computadoras. Tanenbaum. 10 Gigabit Ethernet.
- Redes de Computadoras. Tanenbaum. "Repetidores, hubs, puentes, switches, enrutadores y puertas de enlace (gateways)".
- Redes de Computadoras. Tanenbaum. "Redes LAN virtuales".
- Redes Inalámbricas para países en desarrollo.

Bibliografia

- Redes de Computadoras. Andrew S. Tanenbaum, David J. Wetherall. Capítulo 4.
- Redes Inalámbricas para países en desarrollo. Capítulo 3.
- https://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC
- https://en.wikipedia.org/wiki/Virtual_LAN
- https://es.wikipedia.org/wiki/Router
- https://karimevc.wordpress.com/dominio-de-broadcast-y-colisiones/
- https://ccnadesdecero.com/curso/dominio-de-colision/