

7.0 Introducción

Desplázate para empezar

7.0.1 ¿Por qué debería tomar este módulo?

¡Bienvenido a Ethernet Switching!

Si planea convertirse en administrador de red o arquitecto de red, definitivamente necesitará saber acerca de la Ethernet Switching y Ethernet. Las dos tecnologías LAN más destacadas que se utilizan hoy en día son Ethernet y WLAN. Ethernet admite anchos de banda de hasta 100 Gbps, lo que explica su popularidad. Este módulo contiene un laboratorio que utiliza Wireshark en el que puede ver tramas Ethernet y otro laboratorio donde ver direcciones MAC de dispositivos de red. También hay algunos vídeos instructivos para ayudarle a comprender mejor Ethernet. Para cuando haya terminado este módulo, usted también podría crear una red conmutada que use Ethernet!

7.0.2 ¿Qué aprenderé en este módulo?

Título del módulo: □ Switching Ethernet

Objetivos del módulo: Explique cómo funciona Ethernet en una red switched.

Título del tema	Objetivo del tema
Trama de Ethernet	Explique la forma en que las subcapas de Ethernet se relacionan con los campos de trama.
Dirección MAC de Ethernet	Describa la dirección MAC de Ethernet.
La tabla de direcciones MAC	Explique la forma en que un switch arma su tabla de direcciones MAC y reenvía las tramas.
Velocidades y métodos de reenvío del switch	Describa los métodos de reenvío de switch y la configuración de puertos disponibles para los puertos de switch en la capa 2 puertos de switch.

7.1.1 Encapsulamiento de Ethernet

Este módulo comienza con una discusión de la tecnología Ethernet incluyendo una explicación de la subcapa MAC y los campos de trama Ethernet.

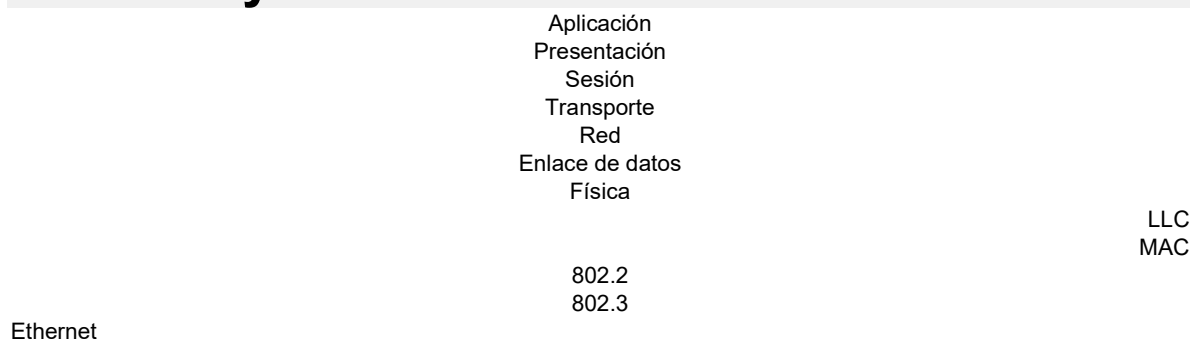
Ethernet es una de las dos tecnologías LAN utilizadas hoy en día, siendo la otra LAN inalámbricas (WLAN). Ethernet utiliza comunicaciones por cable, incluyendo pares trenzados, enlaces de fibra óptica y cables coaxiales.

Ethernet funciona en la capa de enlace de datos y en la capa física. Es una familia de tecnologías de red definidas en los estándares IEEE 802.2 y 802.3. Ethernet soporta los siguientes anchos de banda de datos:

- 10 Mbps
- 100 Mbps
- 1000 Mbps (1 Gbps)
- 10.000 Mbps (10 Gbps)
- 40,000 Mbps (40 Gbps)
- 100,000 Mbps (100 Gbps)

Como se muestra en la figura, los estándares de Ethernet definen tanto los protocolos de Capa 2 como las tecnologías de Capa 1.

Ethernet y el modelo OSI



Ethernet se define mediante protocolos de capa física y de capa de enlace de datos.

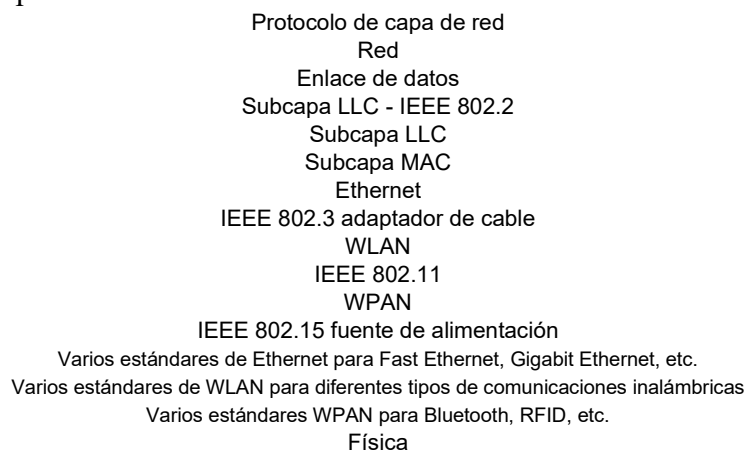
7.1.2 Subcapas de enlace de datos

Los protocolos IEEE 802 LAN/MAN, incluyendo Ethernet, utilizan las dos subcapas independientes siguientes de la capa de enlace de datos para operar. Son el Control de enlace lógico (LLC) y el Control de acceso a medios (MAC), como se muestra en la figura.

Recuerde que LLC y MAC tienen los siguientes roles en la capa de enlace de datos:

- **Subcapa LLC** - Esta subcapa IEEE 802.2 se comunica entre el software de red en las capas superiores y el hardware del dispositivo en las capas inferiores. Coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama. Esta información permite que múltiples protocolos de Capa 3, como IPv4 e IPv6, utilicen la misma interfaz de red y medios.
- **Subcapa MAC** - Esta subcapa (IEEE 802.3, 802.11 o 802.15, por ejemplo) se implementa en hardware y es responsable de la encapsulación de datos y control de acceso a medios. Proporciona direccionamiento de capa de enlace de datos y está integrado con varias tecnologías de capa física.

El diagrama muestra la red OSI, el vínculo de datos y las capas físicas. También muestra las subcapas de capa de enlace de datos LLC y MAC y varios protocolos LAN/WAN. En la parte superior del diagrama se encuentra la capa de red y el protocolo de capa de red. Debajo de eso está la capa de enlace de datos y sus subcapas. La subcapa superior es la subcapa LLC como se especifica en IEEE 802.2. A continuación se muestra la subcapa MAC con tres columnas que representan diferentes tipos de tecnologías de red. La primera columna es Ethernet IEEE 802.3 en la parte superior de la subcapa MAC. Debajo de esto hay varios estándares Ethernet para Fast Ethernet, Gigabit Ethernet, etc. que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI. La siguiente columna es WLAN IEEE 802.11 en la parte superior de la subcapa MAC. Debajo de esto se encuentran los diversos estándares WLAN para diferentes tipos de comunicaciones inalámbricas que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI. La última columna es WPAN IEEE 802.15 en la parte superior de la subcapa MAC. Debajo de esto hay varios estándares WPAN para Bluetooth, RFID, etc. que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI.



7.1.3 Subcapa MAC

La subcapa MAC es responsable de la encapsulación de datos y el acceso a los medios.

Encapsulación de datos

La encapsulación de datos IEEE 802.3 incluye lo siguiente:

- **Trama de Ethernet** - Esta es la estructura interna de la trama Ethernet.
- **Direccionamiento Ethernet** - la trama Ethernet incluye una dirección MAC de origen y destino para entregar la trama Ethernet de NIC Ethernet a NIC Ethernet en la misma LAN.
- **Detección de errores Ethernet** - La trama Ethernet incluye un avance de secuencia de verificación de trama (FCS) utilizado para la detección de errores.

Accediendo a los medios

Como se muestra en la figura, la subcapa MAC IEEE 802.3 incluye las especificaciones para diferentes estándares de comunicaciones Ethernet sobre varios tipos de medios, incluyendo cobre y fibra.

Estándares Ethernet en la subcapa MAC

El diagrama muestra varios estándares Ethernet en la subcapa MAC. En la parte superior del diagrama se encuentra la capa de red y el protocolo de capa de red. Debajo de eso está la capa de enlace de datos y sus subcapas. La subcapa superior es la subcapa IEEE 802.2 LLC. La siguiente es la subcapa MAC Ethernet IEEE 802.3. Debajo hay cinco columnas con varios estándares Ethernet y tipos de medios que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI. De izquierda a derecha, las columnas son: IEEE 802.3u Fast Ethernet; IEEE 802.3z Gigabit Ethernet sobre fibra; IEEE 802.3ab Gigabit Ethernet sobre cobre; IEEE 802.3ae 10 Gigabit Ethernet sobre fibra; y Etc.

Ethernet IEEE 802.3
IEEE 802.3z
Gigabit Ethernet
por Fibra
IEEE 802.3ab
Gigabit Ethernet
por Cobre

Fast Ethernet IEEE 802.3u
Protocolo de capa de red
Red
Enlace de datos
Subcapa LLC-IEEE 802.2
Subcapa LLC
Física
Subcapa MAC
Etc.
IEEE 802.3ae
10 Gigabit Ethernet
por Fibra

Recuerde que Ethernet heredado utiliza una topología de bus o hubs, es un medio compartido, medio dúplex. Ethernet a través de un medio medio dúplex utiliza un método de acceso basado en contención, detección de accesos múltiples/detección de colisiones (CSMA/CD) Esto garantiza que sólo un dispositivo esté transmitiendo a la vez. CSMA/CD permite que varios dispositivos compartan el mismo medio medio dúplex, detectando una colisión cuando más de un dispositivo intenta transmitir simultáneamente. También proporciona un algoritmo de retroceso para la retransmisión.

Las LAN Ethernet de hoy utilizan switches que funcionan en dúplex completo. Las comunicaciones dúplex completo con switches Ethernet no requieren control de acceso a través de CSMA/CD.

7.1.4 Campos de trama de Ethernet

El tamaño mínimo de trama de Ethernet es de 64 bytes, y el máximo es de 1518 bytes. Esto incluye todos los bytes del campo de dirección MAC de destino a través del campo de secuencia de verificación de trama (FCS). El campo preámbulo no se incluye al describir el tamaño de una trama.

Cualquier trama de menos de 64 bytes de longitud se considera un fragmento de colisión o una trama corta, y es descartada automáticamente por las estaciones receptoras. Las tramas de más de 1500 bytes de datos se consideran “jumbos” o tramas bebés gigantes.

Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas. Ellas se consideran inválidas. Las tramas jumbo suelen ser compatibles con la mayoría de los switches y NIC Fast Ethernet y Gigabit Ethernet.

La figura muestra cada campo en la trama Ethernet. Consulte la tabla para obtener más información sobre la función de cada campo.

Campos de trama en internet

El diagrama muestra los campos de una trama Ethernet. De izquierda a derecha, los campos y su longitud son: Preámbulo y SFD, 8 bytes; Dirección MAC de destino, 6 bytes; Dirección MAC de origen, 6 bytes; Tipo/longitud, 2 bytes; datos, 45 - 1500 bytes; y FCS, 4 bytes. Excluyendo el primer campo, el número total de bytes en los campos restantes está entre 64 y 1518.

FCS
Datos
Tipo/Longitud
Dirección MAC de origen
Preámbulo y SFD
Dirección MAC de destino
8 bytes
6 bytes
6 bytes
2 bytes

46 a 1500 bytes
4 bytes
64-1518 octetos

Ethernet Frame Fields Detail

Campo	Descripción
Campos Preámbulo y Delimitador de inicio de trama	El Preámbulo (7 bytes) y el Delimitador de tramas de inicio (SFD), también llamado Inicio de Trama (1 byte), los campos se utilizan para la sincronización entre el envío y recepción de dispositivos. Estos primeros ocho bytes de trama son utilizados para llamar la atención de los nodos receptores. Esencialmente, los primeros cuantos bytes le dicen a los receptores que se preparen para recibir una nueva trama.
Campo Dirección MAC de destino	Este campo de 6 bytes es el identificador del destinatario deseado. Como usted recordará, esta dirección es utilizada por la capa 2 para ayudar a los dispositivos en determinar si una trama está dirigido a ellos. La dirección en la trama es comparada con la dirección MAC en el dispositivo. Si hay una coincidencia, el acepta la trama. Puede ser unicast, multicast o broadcast dirección.
Campo Dirección MAC de origen	Este campo de 6 bytes identifica la NIC o la interfaz de origen de la trama
Tipo/Longitud	Este campo de 2 bytes identifica el protocolo de capa superior encapsulado en la trama de Ethernet. Los valores comunes son, en hexadecimal, 0x800 para IPv4, 0x86DD para IPv6 y 0x806 para ARP. Nota: También puede ver este campo denominado como EtherType, Type o Length.
Campo de datos	Este campo (46 - 1500 bytes) contiene los datos encapsulados de una capa superior, que es una PDU genérica de Capa 3, o más comúnmente, un IPv4 paquete. Todas las tramas deben tener, al menos, 64 bytes de longitud. Si un paquete pequeño es encapsulado, bits adicionales llamados padding se utilizan para aumentar el tamaño de la trama a este tamaño mínimo.
Campo Secuencia de verificación de trama	El campo Secuencia de verificación de trama (FCS) (4 bytes) se usa para detectar errores en una trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo de envío incluye los resultados de un CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar por errores. Si los cálculos coinciden, significa que no se produjo ningún error. Cálculos que no coinciden son una indicación de que los datos han cambiado; por lo tanto, la trama se descarta. Un cambio en los datos podría ser el resultado de una interrupción de las señales eléctricas que representan los bits.

7.2 Dirección MAC de Ethernet

Desplázate para empezar

7.2.1 Dirección MAC y hexadecimal

En redes, las direcciones IPv4 se representan utilizando el sistema de números de base decimal diez y el sistema de números base binaria 2. Las direcciones IPv6 y las direcciones Ethernet se representan utilizando el sistema de número de dieciséis base hexadecimal. Para entender hexadecimal, primero debe estar muy familiarizado con binario y decimal.

El sistema de numeración hexadecimal usa los números del 0 al 9 y las letras de la A a la F.

Una dirección MAC Ethernet consta de un valor binario de 48 bits. Hexadecimal se utiliza para identificar una dirección Ethernet porque un solo dígito hexadecimal representa cuatro bits binarios. Por lo tanto, una dirección MAC Ethernet de 48 bits se puede expresar utilizando sólo 12 valores hexadecimales.

La figura compara los valores decimales y hexadecimales equivalentes para el binario 0000 a 1111.

Equivalentes decimales y binarios a los valores hexadecimales del 0 al F

La figura es de tres columnas que muestran los equivalentes decimales y hexadecimales de los números binarios seleccionados de 4 bits. De izquierda a derecha, los encabezados de columna son: decimal, binario y hexadecimal. Cada columna tiene 16 filas debajo del encabezado.

01534567891011121314210000111100110100010101100111100010011010101111001101110001000010F3456789ABCDE21

Decimal

Binario

Hexadecimal

Dado que 8 bits (un byte) es un método de agrupación binaria común, los números binarios del 00000000 al 11111111 se pueden representar en hexadecimal como el rango del 00 al FF, como se muestra en la figura.

Equivalentes decimales, binarios y hexadecimales seleccionados

La figura es de tres columnas que muestran los equivalentes decimales y hexadecimales de los números binarios seleccionados de 8 bits. De izquierda a derecha, los encabezados de columna son: decimal, binario y hexadecimal. Cada columna tiene 18 filas debajo del encabezado.

02553571015321281922022402181664640000 00001111 11110000 00110000 01010000
01110000 10100000 11110010 00001000 00001100 00001100 10101111 00000000 00100000
00010000 10000001 00000100 00000000 01100000
010000FF0305070A0F2080C0CAF002010810400604

Decimal

Binario

Hexadecimal

Cuando se usa hexadecimal, los ceros iniciales siempre se muestran para completar la representación de 8 bits. Por ejemplo, en la tabla, el valor binario 0000 1010 se muestra en hexadecimal como 0A.

Los números hexadecimales suelen ser representados por el valor precedido por **0x** (por ejemplo, 0x73) para distinguir entre valores decimales y hexadecimales en la documentación.

El hexadecimal también puede estar representado por un subíndice 16, o el número hexadecimal seguido de una H (por ejemplo, 73H).

Es posible que tenga que convertir entre valores decimales y hexadecimales. Si es necesario realizar dichas conversiones, generalmente, es más fácil convertir el valor decimal o hexadecimal a un valor binario y, a continuación, convertir ese valor binario a un valor decimal o hexadecimal, según corresponda.

7.2.2 Dirección MAC de Ethernet

En una LAN Ethernet, cada dispositivo de red está conectado a los mismos medios compartidos. La dirección MAC se utiliza para identificar los dispositivos físicos de origen y destino (NIC) en el segmento de red local. El direccionamiento MAC proporciona un método para la identificación del dispositivo en la capa de enlace de datos del modelo OSI.

Una dirección MAC Ethernet es una dirección de 48 bits expresada con 12 dígitos hexadecimales, como se muestra en la figura. Debido a que un byte equivale a 8 bits, también podemos decir que una dirección MAC tiene 6 bytes de longitud.

El diagrama muestra que la dirección MAC se compone de 48 bits en total. Estos 48 bits se pueden dividir en doce grupos de 4 bits, o 12 dígitos hexadecimales. Combinando dos dígitos hexadecimales juntos hace un byte, por lo tanto, los 48 bits también son equivalentes a 6 bytes.

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111

Byte

Byte

Byte

Byte

Byte

Byte

= 6 bytes

Hex

Hex

Hex

Hex

Hex

Hex

Hex

Hex

Hex

Asignado por el proveedor

Hex

Por ejemplo, suponga que Cisco necesita asignar una dirección MAC única a un nuevo dispositivo. El IEEE ha asignado a Cisco un OUI de **00-60-2F**. Cisco configuraría entonces el dispositivo con un código de proveedor único como **3A-07-BC**. Por lo tanto, la dirección MAC Ethernet de ese dispositivo sería **00-60-2F-3A-07-BC**.

Es responsabilidad del proveedor asegurarse de que ninguno de sus dispositivos tenga asignada la misma dirección MAC. Sin embargo, es posible que existan direcciones MAC duplicadas debido a errores cometidos durante la fabricación, errores cometidos en algunos métodos de implementación de máquinas virtuales o modificaciones realizadas con una de varias herramientas de software. En cualquier caso, será necesario modificar la dirección MAC con una nueva NIC o realizar modificaciones a través del software.

7.2.3 Procesamiento de tramas

A veces, la dirección MAC se conoce como una dirección grabada (BIA) porque la dirección está codificada en la memoria de solo lectura (ROM) en la NIC. Es decir que la dirección está codificada en el chip de la ROM de manera permanente.

Nota: En los sistemas operativos de PC y NIC modernos, es posible cambiar la dirección MAC en el software. Esto es útil cuando se intenta acceder a una red filtrada por BIA. En consecuencia, el filtrado o el control de tráfico basado en la dirección MAC ya no son tan seguros.

Cuando la computadora se inicia, la NIC copia su dirección MAC de la ROM a la RAM. Cuando un dispositivo reenvía un mensaje a una red Ethernet, el encabezado Ethernet incluye estos:

- **Dirección MAC de origen** - Esta es la dirección MAC de la NIC del dispositivo origen.
- **Dirección MAC de destino** - Esta es la dirección MAC de la NIC del dispositivo de destino.

En la animación, haga clic en Reproducir para ver el proceso de reenvío de tramas.

La animación tiene una topología que consiste en un switch con vínculos a cuatro equipos host etiquetados, H1, H2, H3 y H4. H1 dice que necesito enviar información a H3. Aparece una trama en la pantalla de la PC y una vista ampliada de la trama aparece encima de la PC. La trama consiste en el direccionamiento de trama y los datos. La dirección de destino

CC:CC:CC:CC:CC:CC:CC, la dirección de origen AA:AA:AA:AA:AA:AA y la parte de datos de la trama está encapsulada. La trama de H1 se reenvía a el software. A continuación, el switch reenvía la trama fuera de cada interfaz, excepto la interfaz conectada a H1. Cuando H2 y H4 reciben la trama y dicen que esto no está dirigido a mí. Lo ignoraré. Cuando H3 recibe la trama, dice Esto es mío.

Esto no está dirigido a mí. Lo ignoraré.

Esto no está dirigido a mí. Lo ignoraré.

Esto es mío.

Necesito enviar información a H3.

Dirección de destino

Dirección de origen

CC:CC:CC:CC:CC:CC

AA:AA:AA:AA:AA:AA

Datos encapsulados

Direccionamiento de tramas

play_circle_filled

Cuando una NIC recibe una trama de Ethernet, examina la dirección MAC de destino para ver si coincide con la dirección MAC física que está almacenada en la RAM. Si no hay coincidencia, el dispositivo descarta la trama. Si hay coincidencia, envía la trama a las capas OSI, donde ocurre el proceso de desencapsulamiento.

Nota: Las NIC de Ethernet también aceptarán tramas si la dirección MAC de destino es una transmisión o un grupo multicast del que es miembro el host.

Cualquier dispositivo que sea la origen o destino de una trama Ethernet, tendrá una NIC Ethernet y, por lo tanto, una dirección MAC. Esto incluye estaciones de trabajo, servidores, impresoras, dispositivos móviles y routers.

7.2.4 Dirección MAC de unicast

En Ethernet, se utilizan diferentes direcciones MAC para las comunicaciones de unicast, broadcast y multicast de capa 2.

Una dirección MAC de unicast es la dirección única que se utiliza cuando se envía una trama desde un único dispositivo de transmisión a un único dispositivo de destino.

Haga clic en Reproducir en la animación para ver cómo se procesa una trama de unicast. En este ejemplo, la dirección MAC de destino y la dirección IP de destino son unicast.

La animación muestra un host con dirección IPv4 192.168.1.5 (origen) solicitando una página web de un servidor IPv4 unicast. dirección 192.168.1.200. La animación tiene una topología que consiste en un equipo host llamado H1 vinculado a un switch. El switch tiene conexiones a otros tres equipos host y dos servidores. En la parte inferior de la animación hay una vista ampliada de un ethernet trama La trama consiste en el MAC 00-07-E9-42-AC-28 de destino, MAC 00-07-E9-63-CE-53 de origen, IP 192.168.1.5, dirección IP de destino 192.168.1.200, datos de usuario y remolque. La parte del paquete IP de la trama es la IP de origen, dirección IP de destino y datos del usuario. En la animación, H1 dice que necesito enviar la trama al servidor. Se envía una trama de H1 al switch. A continuación, el switch reenvía la trama al servidor con la IP y MAC que coinciden con la IP de destino y la dirección MAC

Servidor

IP: 192.168.1.200

MAC: 00-07-E9-42-AC-28

Host de Origen

IP: 192.168.1.5

MAC: 00-07-E9-63-CE-53

00-07-E9-42-AC-28

00-07-E9-63-CE-53

192.168.1.5

192.168.1.200

Datos del usuario

Cola

MAC de destino

MAC de origen

IP de origen

IP de destino

Paquete IP

Trama de Ethernet

play_circle_filled

En el ejemplo de la animación, un host con la dirección IPv4 192.168.1.5 (origen) solicita una página web del servidor en la dirección IPv4 unicast 192.168.1.200. Para que un paquete de unicast se envíe y se reciba, la dirección IP de destino debe estar incluida en el encabezado del paquete IP. Además, el encabezado de la trama de Ethernet también debe contener una dirección MAC de destino correspondiente. Las direcciones IP y MAC se combinan para la distribución de datos a un host de destino específico.

El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv4 se conoce como Protocolo de resolución de direcciones (ARP). El proceso que utiliza un host de origen para determinar la dirección MAC de destino asociada con una dirección IPv6 se conoce como Neighbor Discovery (ND).

Nota: La dirección MAC de origen siempre debe unicast.

7.2.5 Dirección MAC broadcast

Cada dispositivo de la LAN Ethernet recibe y procesa una trama de broadcast Ethernet. Las características de una transmisión Ethernet son las siguientes:

- Tiene una dirección MAC de destino de FF-FF-FF-FF-FF-FF en hexadecimal (48 unidades en binario).
- Está inundado todos los puertos del switch Ethernet excepto el puerto entrante.
- No es reenviado por un router.

Si los datos encapsulados son un paquete broadcast IPv4, esto significa que el paquete contiene una dirección IPv4 de destino que tiene todos los (1s) en la parte del host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de broadcast) recibirán y procesarán el paquete.

Haga clic en Reproducir en la animación para ver cómo se procesa un trama de broadcast. En este ejemplo, la dirección MAC de destino y la dirección IP de destino son ambas broadcasts.

La animación muestra un host de origen que envía un paquete broadcast IPv4 a todos los dispositivos en su red. La animación tiene una topología que consiste en una PC host llamada H1 vinculada a un switch. El switch tiene conexiones a otros tres equipos host y dos servidores. En la parte inferior de la animación hay una vista ampliada de una trama de ethernet. La trama consiste en el destino MAC FF-FF-FF-FF-FF-FF, origen MAC 00-07-E9-63-CE-53, origen IP 192.168.1.5, dirección IP de destino 192.168.1.255, usuario datos y tráiler. La parte del paquete IP de la trama es la IP de origen, la dirección IP de destino y los datos del usuario. En la animación, H1 dice que necesito enviar datos a todos los hosts en la red. Se envía una trama desde H1 al switch. El switch luego reenvía la trama a todas sus interfaces excepto la conectada a H1. Los otros tres hosts de PC y los dos servidores reciben las tramas.

**Grupode
host de destino**

Host de Origen
IP: 192.168.1.5
MAC: 00-07-E9-63-CE-53

FF-FF-FF-FF-FF-FF

00-07-E9-63-CE-53

192.168.1.5

192.168.1.255

Datos del usuario

Cola

MAC de destino

MAC de origen
IP de origen
IP de destino
Paquete IP
Trama de Ethernet

play_circle_filled

Como se muestra en la animación, el host de origen envía un paquete broadcast IPv4 a todos los dispositivos de la red. La dirección IPv4 de destino es una dirección broadcast: 192.168.1.255. Cuando el paquete de broadcast IPv4 se encapsula en la trama de Ethernet, la dirección MAC de destino es la dirección MAC de difusión FF-FF-FF-FF-FF-FF en hexadecimal (48 números uno en binario).

DHCP para IPv4 es un ejemplo de protocolo que utiliza direcciones de broadcast Ethernet e IPv4.

Sin embargo, no todas las transmisiones Ethernet llevan un paquete de broadcast IPv4. Por ejemplo, las solicitudes ARP no utilizan IPv4, pero el mensaje ARP se envía como un broadcast Ethernet.

7.2.6 Dirección MAC de multicast

Una trama de multicast de Ethernet es recibida y procesada por un grupo de dispositivos en la LAN de Ethernet que pertenecen al mismo grupo de multicast. Las características de una multicast Ethernet son las siguientes:

- Hay una dirección MAC de destino 01-00-5E cuando los datos encapsulados son un paquete de multicast IPv4 y una dirección MAC de destino de 33-33 cuando los datos encapsulados son un paquete de multicast IPv6.
- Existen otras direcciones MAC de destino de multicast reservadas para cuando los datos encapsulados no son IP, como Spanning Tree Protocol (STP) y Link Layer Discovery Protocol (LLDP).
- Se inundan todos los puertos del switch Ethernet excepto el puerto entrante, a menos que el switch esté configurado para la indagación de multicast.
- No es reenviado por un router, a menos que el router esté configurado para enrutar paquetes de multicast.

Si los datos encapsulados son un paquete de multicast IP, a los dispositivos que pertenecen a un grupo de multicast se les asigna una dirección IP de grupo de multicast. El rango de direcciones de multicast IPv4 es 224.0.0.0 a 239.255.255.255. El rango de direcciones de multicast IPv6 comienza con ff00 :: / 8. Debido a que las direcciones de multicast representan un grupo de direcciones (a veces denominado grupo de hosts), solo se pueden utilizar como el destino de un paquete. El origen siempre tiene una dirección de unicast.

Al igual que con las direcciones de unicast y broadcast, la dirección IP de multicast requiere una dirección MAC de multicast correspondiente para entregar tramas en una red local. La dirección MAC de multicast está asociada a la dirección de multicast IPv4 o IPv6 y utiliza la información de direccionamiento de dicha dirección.

Haga clic en Reproducir en la animación para ver cómo se procesa un trama de multicast. En este ejemplo, la dirección MAC de destino y la dirección IP de destino son ambas multicast.

La animación muestra un host de origen que envía una trama de multicast a los dispositivos que pertenecen al grupo de multicast. La animación tiene una topología que consiste en un equipo host llamado H1 vinculado a un switch. El switch tiene conexiones a otros tres equipos host y dos servidores. En la parte inferior de la animación hay una vista ampliada de una trama de ethernet. La trama consiste en el destino MAC 01-00-5E-00-00-C8, origen MAC 00-07-E9-63-CE-53, origen IP 192.168.1.5, dirección IP de destino 224.0.0.200, usuario datos y tráiler. La parte del paquete IP de la trama es la IP de origen, la dirección IP de destino y los datos del usuario. En la animación, H1 dice que necesito enviar datos a todos los hosts en la red. Se envía una trama desde H1 al switch. El switch luego reenvía la trama a solo los dispositivos del grupo de multicast. Dos de los tres hosts de PC y un servidor reciben el trama de multicast.

7.3 Tabla de direcciones MAC

Desplázate para empezar

7.3.1 Fundamentos de switches

Ahora que sabe todo acerca de las direcciones MAC Ethernet, es hora de hablar sobre cómo un switch utiliza estas direcciones para reenviar (o descartar) tramas a otros dispositivos de una red. Si un switch acaba de reenviar cada trama que recibió todos los puertos, su red estaría tan congestionada que probablemente se detendría por completo.

Un switch Ethernet de capa 2 usa direcciones MAC de capa 2 para tomar decisiones de reenvío. No tiene conocimiento de los datos (protocolo) que se transportan en la porción de datos de la trama, como un paquete IPv4, un mensaje ARP o un paquete IPv6 ND. El switch toma sus decisiones de reenvío basándose únicamente en las direcciones MAC Ethernet de capa 2.

Un switch Ethernet examina su tabla de direcciones MAC para tomar una decisión de reenvío para cada trama, a diferencia de los hubs Ethernet heredados que repiten bits en todos los puertos excepto el puerto entrante. En la ilustración, se acaba de encender el switch de cuatro puertos. La tabla muestra la tabla de direcciones MAC que aún no ha aprendido las direcciones MAC para las cuatro PC conectadas.

Nota: Las direcciones MAC se acortan a lo largo de este tema con fines de demostración.

El diagrama muestra cuatro hosts, junto con sus direcciones MAC asociadas, conectados a los puertos 1 - 4 de un switch. La tabla de direcciones MAC que asigna puertos a direcciones MAC está vacía actualmente.

ABCD1234



MAC
00-0A

MAC
00-0B

MAC
00-0C

MAC
00-0D

La tabla de direcciones MAC del switch está vacía.

Nota: En ocasiones, la tabla de direcciones MAC se denomina tabla de memoria de contenido direccionable (CAM). Aunque el término “tabla CAM” es bastante común, en este curso nos referiremos a ella como “tabla de direcciones MAC”.

7.3.2 Switch, Aprendiendo y Reenviando

El switch arma la tabla de direcciones MAC de manera dinámica después de examinar la dirección MAC de origen de las tramas recibidas en un puerto. El switch reenvía las tramas después de buscar una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC.

Haga clic en los botones Aprender y Reenviar para obtener una ilustración y una explicación de este proceso.

Aprender

Reenviar

Examinar la dirección MAC de Origen

Se revisa cada trama que ingresa a un switch para obtener información nueva. Esto se realiza examinando la dirección MAC de origen de la trama y el número de puerto por el que ingresó al switch. Si la dirección MAC de origen no existe, se la agrega a la tabla, junto con el número de puerto de entrada. Si la dirección MAC de origen existe, el switch

actualiza el temporizador de actualización para esa entrada. De manera predeterminada, la mayoría de los switches Ethernet guardan una entrada en la tabla durante cinco minutos.

En la figura, por ejemplo, la PC-A está enviando una trama Ethernet a la PC-D. La tabla muestra que el switch agrega la dirección MAC para PC-A a la tabla de direcciones MAC.

Nota: Si la dirección MAC de origen existe en la tabla, pero en un puerto diferente, el switch la trata como una entrada nueva. La entrada se reemplaza con la misma dirección MAC, pero con el número de puerto más actual.

Cuatro hosts, A - D, están conectados a un switch en los puertos 1 - 4. El host A con dirección MAC 00-0A (simplificado en este ejemplo) está conectado al switch en el puerto 1. El host A envía una trama con una dirección MAC de destino de 00-0D. La dirección MAC de origen de la trama es 00-0A, El switch asigna el puerto 1 a la dirección MAC 00-0A en su tabla de direcciones MAC.

ABCD1234

MAC
00-0A

MAC
00-0B

MAC
00-0C

MAC
00-0D

MAC de destino
00-0D

MAC de origen
00-0A

Tipo

Datos

FCS

1. PC-A envía una trama Ethernet.
2. El switch agrega el número de puerto y la dirección MAC para PC-A a la tabla de direcciones MAC.

7.3.3 Filtrado de tramas

A medida que un switch recibe tramas de diferentes dispositivos, puede completar la tabla de direcciones MAC examinando la dirección MAC de cada trama. Cuando la tabla de direcciones MAC del switch contiene la dirección MAC de destino, puede filtrar la trama y reenviar un solo puerto.

Haga clic en cada botón para obtener una ilustración y una explicación de cómo un switch filtra tramas.

PC-D a Switch

Switch a PC-A

PC-A a Switch a PC-D

En la figura, PC-D responde a PC-A. El switch ve la dirección MAC de PC-D en la trama entrante en el puerto 4. A continuación, el switch coloca la dirección MAC de PC-D en la tabla de direcciones MAC asociada con el puerto 4.

Cuatro hosts, A - D, están conectados a un switch en los puertos 1 - 4. El host D con dirección MAC 00-0D está conectado al switch en el puerto 4. El host D envía una trama con una dirección MAC de destino de 00-0A y un MAC de origen de 00-0D. El switch asigna el puerto 4 a la dirección MAC 00-0D en su tabla de direcciones MAC.

ABCD1234

MAC
00-0A

MAC
00-0B

MAC
00-0C

MAC
00-0D

MAC de destino
00-0A

MAC de origen
00-0D

Tipo

Datos

FCS

El switch agrega el número de puerto y la dirección MAC para PC-D a su tabla de direcciones MAC.

7.3.4 Video - Tablas de direcciones MAC en switches conectados

Un switch puede tener muchas direcciones MAC asociadas a un solo puerto. Esto es común cuando el switch está conectado a otro switch. El switch tiene una entrada independiente en

la tabla de direcciones MAC para cada trama recibida con una dirección MAC de origen diferente.

Haga clic en Reproducir en la figura para ver una demostración de cómo dos switches conectados crean tablas de direcciones MAC.

7.3.5 Video - Envío de una trama al gateway predeterminado

Cuando un dispositivo tiene una dirección IP ubicada en una red remota, la trama de Ethernet no se puede enviar directamente al dispositivo de destino. En cambio, la trama de Ethernet se envía a la dirección MAC del gateway predeterminado: el router.

En la ilustración, haga clic en Reproducir para ver una demostración de cómo la PC-A se comunica con el gateway predeterminado.

Nota: En el vídeo, el paquete IP que se envía de la PC-A al destino en una red remota tiene como dirección IP de origen la de la PC-A y como dirección IP de destino, la del host remoto. El paquete IP de retorno tiene la dirección IP de origen del host remoto, y la dirección IP de destino es la de la PC A.

TRANSCRIPCION:

- 00:01- [Instructor] En este vídeo,
- 00:02PC-A enviará un paquete a Internet
- 00:06porque la dirección IP de destino está en otra red.
- 00:10Entonces, en este caso, la dirección MAC de origen es la de la PC-A,
- 00:14la dirección MAC de destino es la del router de 00-0D.
- 00:20Entonces, la trama de Ethernet se envía al switch S1.
- 00:24Switch S1 recibe la trama,
- 00:26examina la dirección MAC de origen,
- 00:28que se encuentra en su tabla de direcciones MAC.
- 00:31Por lo tanto, simplemente actualiza el temporizador de cinco minutos.
- 00:35Examina la dirección MAC de destino,
- 00:38y porque esa dirección MAC de destino no esta
- 00:40en la tabla de direcciones MAC del switch S1,
- 00:43lo satura por todos los puertos.
- 00:46La PC-B recibe la trama de Ethernet,
- 00:49y ya que la dirección MAC de destino
- 00:51no coincide con su propia dirección MAC,
- 00:53no acepta el resto de la trama.
- 00:57El switch S2 recibe la trama de Ethernet,
- 01:00examina la dirección MAC de origen,
- 01:03que está en su tabla de direcciones MAC ,
- 01:05así que también simplemente actualiza el temporizador de cinco minutos.

- 01:09 Examina la dirección MAC de destino de la trama,
- 01:13 que no está en su tabla de direcciones MAC ,
- 01:15 entonces satura todos los puertos.
- 01:19 PC-C obtiene la trama de Ethernet,
- 01:23 y ya que la dirección MAC de destino
- 01:24 no coincide con su propia dirección MAC,
- 01:28 no acepta el resto de la trama de Ethernet.
- 01:31 El router recibe la trama de Ethernet,
- 01:34 y ya que la dirección MAC de destino
- 01:36 coincide con su propia dirección MAC,
- 01:38 acepta el resto de la trama.
- 01:41 Ahora veremos la trama de Ethernet
- 01:43 que viene del router a la PC-A.
- 01:47 La dirección IP de origen es la dirección IP
- 01:50 del dispositivo en una red remota.
- 01:55 La dirección MAC de origen es la del router en 00-0D,
- 02:00 y la dirección MAC de destino es la de la PC-A.
- 02:05 La trama se envía al switch S2.
- 02:08 S2 lo recibe, examina la dirección MAC de origen,
- 02:11 que no está en su tabla de direcciones MAC, por lo que la agrega.
- 02:16 Luego examina la dirección MAC de destino,
- 02:19 que está en su tabla de direcciones MAC ,
- 02:21 así que la reenvía al puerto 1.
- 02:25 S1 recibe la trama de Ethernet,
- 02:28 examina la dirección MAC de origen,
- 02:29 que no está en su tabla de direcciones MAC ,
- 02:32 entonces la agrega a su tabla de direcciones MAC.
- 02:35 Examina la dirección MAC de destino,
- 02:38 que está en su tabla de direcciones MAC ,
- 02:41 por lo que continúa y solo la reenvía al puerto 1
- 02:44 hacia PC-A.
- 02:47 La PC-A examina la dirección MAC de destino,
- 02:51 y ya que es una coincidencia,
- 02:52 acepta el resto de la trama.

7.4 Velocidades y métodos de reenvío del switch

Desplázate para empezar

7.4.1 Métodos de reenvío de tramas de los switches Cisco

Como aprendió en el tema anterior, los modificadores utilizan sus tablas de direcciones MAC para determinar qué puerto utilizar para reenviar tramas. Con los switches Cisco, en

realidad hay dos métodos de reenvío de tramas y hay buenas razones para usar uno en lugar del otro, dependiendo de la situación.

Los switches utilizan uno de los siguientes métodos de reenvío para el switching de datos entre puertos de la red:

- **Switching de almacenamiento y envío** - Este método de reenvío de trama recibe la trama completa y calcula el CRC. La CRC utiliza una fórmula matemática basada en la cantidad de bits (números uno) de la trama para determinar si esta tiene algún error. Si la CRC es válida, el switch busca la dirección de destino, que determina la interfaz de salida. Luego, la trama se reenvía desde el puerto correcto.
- **Switching por método de corte** - Este método de reenvío de tramas reenvía la trama antes de que se reciba por completo. Como mínimo, se debe leer la dirección de destino para que la trama se pueda enviar.

Una gran ventaja de store-and-forward switching, es que determina si una trama tiene errores antes de propagarla. Cuando se detecta un error en la trama, el switch la descarta. El proceso de descarte de las tramas con errores reduce el ancho de banda consumido por datos dañados. Store-and-forward switching se requiere para el análisis de calidad de servicio (QoS) en las redes convergentes, donde se necesita una clasificación de la trama para decidir el orden de prioridad del tráfico. Por ejemplo, los flujos de datos de voz sobre IP deben tener prioridad sobre el tráfico de navegación web.

Haga clic en Reproducir en la animación para ver una demostración del proceso de store-and-forward

La animación se muestra como host de origen enviando un trama a un switch cut-through. La animación tiene una topología que consiste en un host de origen vinculado a un switch. El tiene un vínculo a un host de destino y un servidor. En la animación, el host de origen reenvía un trama al switch. El switch recibe la trama y mira su tabla de switching para determinar qué interfaz desea reenviar la trama. El switch luego envía la trama al host de destino.

Origen

Destino

Dirección de destino

Dirección de origen

Datos

CRC

play_circle_filled

7.4.2 Switching por método de corte

En este tipo de switching, el switch actúa sobre los datos apenas los recibe, incluso si la transmisión aún no se completó. El switch almacena la cantidad suficiente de trama como para leer la dirección MAC de destino para que pueda determinar a qué puerto debe reenviar los datos. La dirección MAC de destino se encuentra en los primeros 6 bytes de la trama después del preámbulo. El switch busca la dirección MAC de destino en la tabla de switching, determina el puerto de la interfaz de salida y reenvía la trama a su destino mediante el puerto de switch designado. El switch no lleva a cabo ninguna verificación de errores en la trama.

Reproduzca la animación para ver una demostración del proceso cut-through switching.

La animación se muestra como host de origen enviando un trama a un switch de store-and-forward. El switch calcula el CRC y, si es válido envía la trama al host de destino. La animación tiene una topología que consiste en un host de origen vinculado a un switch. El switch tiene un vínculo a un host de destino y un servidor. En la animación, el host de origen muestra el contenido de la trama consistente en una dirección de destino, dirección de origen, datos y CRC. La trama se reenvía al switch desde el host de origen. El switch recibe la trama y calcula el CRC en la trama. El CRC en el paquete es 435869123 y el CRC calculado es 435869123, ambos coincidentes. El switch dice que la Trama es buena y luego mira su tabla de switching para determinar a qué interfaz reenviar la trama. A continuación, el switch envía la trama al host de destino.

Origen

Destino

play_circle_filled

A continuación, se presentan dos variantes del cut-through switching:

- **Switching de reenvío rápido** - Este método ofrece el nivel de latencia más bajo. Fast-forward switching reenvía el paquete inmediatamente después de leer la dirección de destino. Como el fast-forward switching comienza a reenviar el paquete antes de recibirlo por completo, es posible que, a veces, los paquetes se distribuyan con errores. Esto ocurre con poca frecuencia y la NIC de destino descarta el paquete defectuoso al recibirlo. En el modo de fast-forward, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. El fast-forward switching es el método de corte típico.
- **Switching libre de fragmentos** - En este método, el switch almacena los primeros 64 bytes de la trama antes de reenviarla. El fragment-free switching se puede ver como un punto medio entre el store-and-forward switching y el fast-forward switching. El motivo por el que el fragment-free switching almacena solamente los primeros 64 bytes de la trama es que la mayoría de los errores y las colisiones de la red se producen en esos primeros 64 bytes. El fragment-free switching intenta mejorar el fast-forward switching al realizar una pequeña verificación de errores en los 64 bytes de la trama para asegurar que no haya ocurrido una colisión antes de reenviarla. Este método de fragment-free switching es un punto medio entre la alta latencia y la alta

integridad del store-and-forward switching, y la baja latencia y la baja integridad del fast-forward switching.

Algunos switches están configurados para realizar el cut-through switching en cada puerto hasta alcanzar un umbral de errores definido por el usuario y, luego, cambiar automáticamente al store-and-forward. Si el índice de error está por debajo del umbral, el puerto vuelve automáticamente al cut-through switching.

7.4.3 Almacenamiento en búfer de memoria en los switches

Un switch Ethernet puede usar una técnica de almacenamiento en búfer para almacenar tramas antes de enviarlas. También se puede utilizar el almacenamiento en búfer cuando el puerto de destino está ocupado debido a la congestión. El switch almacena la trama hasta que se pueda transmitir.

Como se muestra en la tabla, hay dos métodos de almacenamiento en memoria intermedia:

Memory Buffering Methods

El almacenamiento en búfer de memoria compartida también da como resultado la capacidad de almacenar tramas más grandes con potencialmente menos tramas descartadas. Esto es importante con la conmutación asimétrica, que permite diferentes velocidades de datos en diferentes puertos, como cuando se conecta un servidor a un puerto de switch de 10 Gbps y PC a puertos de 1 Gbps.

7.4.4 Configuración de dúplex y velocidad

Dos de las configuraciones más básicas en un switch son el ancho de banda (a veces denominado "velocidad") y la configuración dúplex para cada puerto de switch individual. Es fundamental que los parámetros de dúplex y de ancho de banda coincidan entre el puerto de switch y los dispositivos conectados, como una computadora u otro switch.

Se utilizan dos tipos de parámetros dúplex para las comunicaciones en una red Ethernet:

- **Dúplex completo** - Ambos extremos de la conexión pueden enviar y recibir datos simultáneamente.
- **Semidúplex** - Solo uno de los extremos de la conexión puede enviar datos por vez.

La autonegociación es una función optativa que se encuentra en la mayoría de los switches Ethernet y NICs. Permite que dos dispositivos negocien automáticamente las mejores capacidades de velocidad y dúplex. Si ambos dispositivos tienen la funcionalidad, se selecciona dúplex completo, junto con el ancho de banda común más alto.

En la figura, la NIC Ethernet para PC-A puede funcionar en duplex completo o medio duplex, y en 10 Mbps o 100 Mbps.

S2PC A

Dúplex

Velocidad

Dúplex

Velocidad

Completo

Medio

Completo

Medio

100 Mbps

10 Mbps

100 Mbps

10 Mbps

1000 Mbps

Puerto 1

Autonegociación

Autonegociación

La PC-A está conectada al switch S1 en el puerto 1, que puede operar en duplex completo o medio duplex, y en 10 Mbps, 100 Mbps o 1000 Mbps (1 Gbps). Si ambos dispositivos utilizan la autonegociación, el modo de funcionamiento será en dúplex completo y a 100 Mb/s.

Nota: La mayoría de los switches de Cisco y las NIC de Ethernet tienen por defecto la negociación automática para velocidad y dúplex. Los puertos Gigabit Ethernet solamente funcionan en dúplex completo.

La falta de coincidencia dúplex es una de las causas más comunes de problemas de rendimiento en enlaces Ethernet de 10/100 Mbps. Ocurre cuando un puerto en el enlace opera en medio duplex mientras que el otro puerto opera en duplex completo, como se muestra en la figura.

El switch S1 está conectado al switch S2. S1 funciona en dúplex completo y S2 funciona en medio dúplex. Un texto sobre S1 dice: Yo soy dúplex completo para que pueda enviar

cuando quiera. Un texto sobre S2: Yo soy medio dúplex, así que solo puedo enviar cuando el enlace está despejado, ¡pero también estoy recibiendo muchas colisiones! El gráfico muestra ambos switches que envían datos al mismo tiempo que han dado lugar a una colisión.

S1S2

Medio dúplex

Dúplex completo

Soy medio dúplex, así que solamente puedo enviar elementos cuando el enlace está libre, pero también estoy recibiendo muchas colisiones.

Soy full dúplex, así que puedo enviar cuando quiera.

El S2 experimentará colisiones continuamente porque el S1 no deja de enviar tramas cada vez que tiene algo que enviar.

La falta de coincidencia dúplex se produce cuando se restablecen uno o ambos puertos en un enlace, y el proceso de negociación automática no da como resultado que ambos socios del enlace tengan la misma configuración. También puede ocurrir cuando los usuarios reconfiguran un lado del enlace y olvidan reconfigurar el otro. Ambos lados de un enlace deben tener activada la autonegociación, o bien ambos deben tenerla desactivada. La práctica recomendada es configurar ambos puertos del switch Ethernet como dúplex completo.

7.4.5 Auto-MDIX (MDIX automático)

Las conexiones entre dispositivos requerían el uso de un cable cruzado o directo. El tipo de cable requerido dependía del tipo de dispositivos de interconexión.

Por ejemplo, la figura identifica el tipo de cable correcto necesario para interconectar dispositivos de switch a switch, switch a router, switch a host o router a host. Se utiliza un cable cruzado cuando se conectan dispositivos similares, y un cable directo para conectarse a dispositivos diferentes.

Nota: Una conexión directa entre un router y un host requiere una conexión cruzada.

El diagrama muestra el tipo de cable correcto que se debe utilizar al conectar varios tipos de dispositivos de red juntos. De arriba a abajo, los dispositivos y tipos de cable son: switch a switch es un cable cruzado; switch a router es un cable directo; switch a host es un cable directo; y router a host es un cable cruzado.

Cable de conexión cruzada

Cable directo

Cable directo

Cable de conexión cruzada

Actualmente, la mayor parte de los dispositivos admiten la característica interfaz cruzada automática dependiente del medio (auto-MDIX). Cuando está habilitado, el switch detecta automáticamente el tipo de cable conectado al puerto y configura las interfaces en consecuencia. Por lo tanto, se puede utilizar un cable directo o cruzado para realizar la conexión con un puerto 10/100/1000 de cobre situado en el switch, independientemente del tipo de dispositivo que esté en el otro extremo de la conexión.

La función auto-MDIX está habilitada de manera predeterminada en los switches que ejecutan Cisco IOS Release 12.2 (18) SE o posterior. Sin embargo, la característica podría estar deshabilitada. Por esta razón, siempre debe utilizar el tipo de cable correcto y no confiar en la función Auto-MDIX. Auto-MDIX se puede volver a habilitar mediante el comando **mdix auto** de configuración de interfaz.

7.5 Módulo de Práctica y Prueba

Desplázate para empezar

7.5.1 ¿Qué aprendió en este módulo?

Trama Ethernet

Ethernet funciona en la capa de enlace de datos y en la capa física. Los estándares de Ethernet definen los protocolos de capa 2 y las tecnologías de capa 1. Ethernet utiliza las subcapas LLC y MAC de la capa de enlace de datos para operar. La encapsulación de datos incluye lo siguiente: trama Ethernet, direccionamiento Ethernet y detección de errores Ethernet. Las LAN Ethernet utilizan switches que funcionan en dúplex completo. Los campos de trama Ethernet son: delimitador de trama de preámbulo y inicio, dirección MAC de destino, dirección MAC de origen, EtherType, datos y FCS.

Dirección MAC Ethernet

El sistema de números binarios usa los dígitos 0 y 1. Decimal usa de 0 a 9. Hexadecimal utiliza de 0 a 9 y las letras A a F. La dirección MAC se utiliza para identificar los dispositivos físicos de origen y destino (NIC) en el segmento de red local. El direccionamiento MAC proporciona un método para la identificación del dispositivo en la capa de enlace de datos del modelo OSI. Una dirección MAC de Ethernet es una dirección de 48 bits expresada con 12 dígitos hexadecimales o 6 bytes. Una dirección MAC Ethernet consta de un código OUI de proveedor hexadecimal 6 seguido de un valor asignado de proveedor hexadecimal 6. Cuando un dispositivo reenvía un mensaje a una red Ethernet, el encabezado Ethernet incluye las direcciones MAC de origen y destino. En Ethernet, se utilizan diferentes direcciones MAC para las comunicaciones de unicast, broadcast y multicast de capa 2.

La tabla de direcciones MAC

Un switch Ethernet de capa 2 toma sus decisiones de reenvío basándose únicamente en las direcciones MAC Ethernet de capa 2. El switch arma la tabla de direcciones MAC de manera dinámica después de examinar la dirección MAC de origen de las tramas recibidas en un puerto. El switch reenvía las tramas después de buscar una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC. A medida que un switch recibe tramas de diferentes dispositivos, puede completar la tabla de direcciones MAC examinando la dirección MAC de cada trama. Cuando la tabla de direcciones MAC del switch contiene la dirección MAC de destino, puede filtrar la trama y reenviar un solo puerto.

Métodos de reenvío y velocidad del switch

Los switches utilizan uno de los siguientes métodos de reenvío para cambiar datos entre puertos de red: store-and-forward switching o cut-through switching. Dos variantes de cut-through switching son fast-forward y fragment-free. Dos métodos de almacenamiento en búfer de memoria son la memoria basada en puertos y la memoria compartida. Hay dos tipos de configuraciones dúplex utilizadas para las comunicaciones en una red Ethernet: dúplex completo y medio dúplex. La autonegociación es una función optativa que se encuentra en la mayoría de los switches Ethernet y NICs. Permite que dos dispositivos negocien automáticamente las mejores capacidades de velocidad y dúplex. Si ambos dispositivos tienen la funcionalidad, se selecciona dúplex completo, junto con el ancho de banda común más alto. Actualmente, la mayor parte de los dispositivos admiten la característica interfaz cruzada automática dependiente del medio (auto-MDIX). Cuando está habilitado, el switch detecta automáticamente el tipo de cable conectado al puerto y configura las interfaces en consecuencia.