CAPÍTULO 5. ETHERNET

Ethernet funciona en la capa de enlace de datos y en la capa física. Los estándares del protocolo Ethernet definen muchos aspectos de la comunicación en red, incluido el formato, el tamaño, la temporización y la codificación de las tramas. Los estándares de Ethernet definen los protocolos de capa 2 (OSI) y las tecnologías de capa 1 (OSI).

En este capítulo, se analizan las características y el funcionamiento de Ethernet en cuanto a su evolución desde una tecnología de medios compartidos de comunicación de datos basada en contienda hasta convertirse en la actual tecnología de dúplex completo de gran ancho de banda.

5.1.1.1 Encapsulamiento de Ethernet

Ethernet es la tecnología LAN más utilizada hoy en día. Ethernet funciona en la capa de enlace de datos y en la capa física y admite los siguientes anchos de banda de datos:

- 10 Mb/s
- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10 000 Mb/s (10 Gb/s)
- 40 000 Mb/s (40 Gb/s)
- 100 000 Mb/s (100 Gb/s)

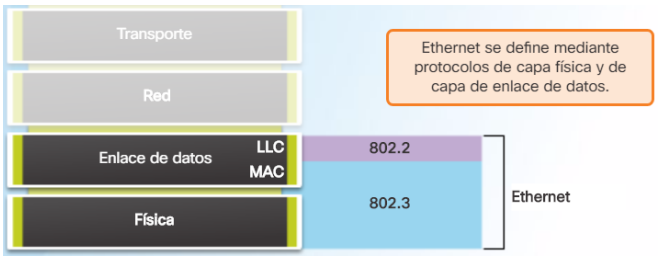
Ethernet depende de ambas subcapas individuales de la capa de enlace de datos para funcionar: la subcapa de control de enlace lógico (LLC) y la subcapa MAC.

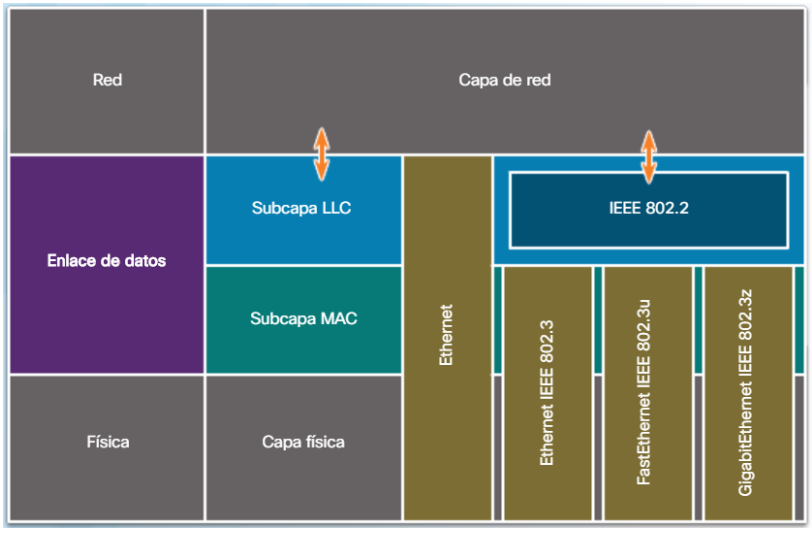
Subcapa LLC

La subcapa LLC de Ethernet maneja la comunicación entre las capas superiores (agregando información de control) e inferiores (ayudando a su distribución). En una computadora, el LLC se puede considerar el software del controlador de la NIC. El controlador de la NIC es un programa que interactúa directamente con el hardware de la NIC para trasladar los datos entre la subcapa MAC y los medios físicos.

Subcapa MAC

La subcapa MAC es la subcapa inferior de la capa de enlace de datos y se implementa mediante hardware, generalmente, en la NIC de la computadora.





5.1.1.2 Subcapa MAC

Como se muestra en la ilustración, la subcapa MAC de Ethernet tiene dos tareas principales:

- Encapsulamiento de datos
- Control de acceso al medio

Encapsulamiento de datos

El proceso de encapsulamiento de datos incluye el armado de tramas antes de la transmisión y el desarmado de tramas en el momento de la recepción. Para armar la trama, la capa MAC agrega un encabezado y un tráiler a la PDU de la capa de red.

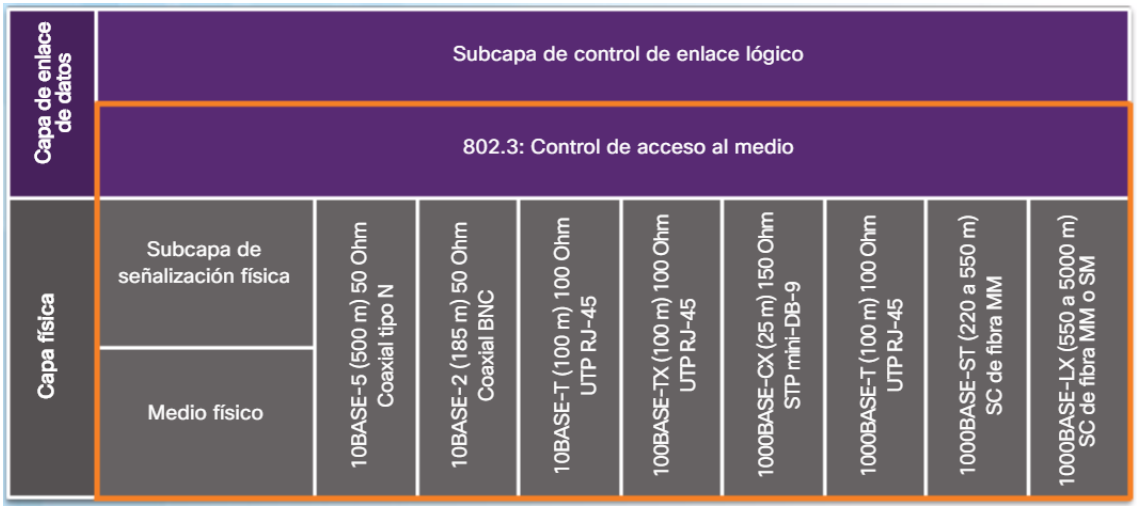
El encapsulamiento de datos proporciona tres funciones principales:

- **Delimitación de tramas:** Estos bits delimitadores proporcionan sincronización entre los nodos de transmisión y de recepción.
- **Direccionamiento.**
- **Detección de errores**.

Control de acceso al medio

La segunda tarea de la subcapa MAC es el control de acceso al medio. El control de acceso al medio es responsable de colocar las tramas en los medios y de quitarlas de ellos. Esta subcapa se comunica directamente con la capa física y se encarga además de la recuperación de medios.

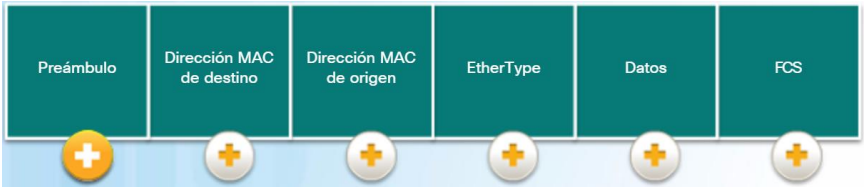
La topología lógica subyacente de Ethernet es un bus de acceso múltiple, por lo que todos los nodos (dispositivos) de un único segmento de red comparten el medio. Ethernet es un método de red de contienda. En un método de contienda, cualquier dispositivo puede intentar transmitir datos a través del medio compartido siempre que tenga datos que enviar. Para detectar y resolver colisiones, se utiliza el proceso CSMA/CD en las LAN Ethernet de dúplex medio. Las LAN Ethernet actuales utilizan switches de dúplex completo, que permiten que varios dispositivos envíen y reciban datos en simultáneo y sin colisiones.



5.1.1.4 Campos de trama de Ethernet

El tamaño mínimo de trama de Ethernet es de 64 bytes, y el máximo es de 1518 bytes. 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 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 y, por lo tanto, se consideran no válidas.



Campos "Preámbulo" y "Delimitador de inicio de trama"

Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD), también llamado "inicio de trama" (1 byte), se utilizan para la sincronización entre los dispositivos emisores y receptores. Estos ocho primeros bytes de la trama se utilizan para captar la atención de los nodos receptores. Básicamente, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.

Campo Dirección MAC de destino

Este campo de 6 bytes es el identificador del destinatario deseado. Como recordará, la capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama está dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama. Puede ser una dirección de unidifusión, de multidifusión o de difusión.

Campo Dirección MAC de origen

Este campo de 6 bytes identifica la NIC o la interfaz de origen de la trama. Debe ser una dirección de unidifusión.

Campo EtherType

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.

Campo de datos

Este campo (de 46 a 1500 bytes) contiene los datos encapsulados de una capa superior, que es una PDU de capa 3 o, más comúnmente, un paquete IPv4. Todas las tramas deben tener, al menos, 64 bytes de longitud. Si se encapsula un paquete pequeño, se utilizan bits adicionales (llamados "relleno") para aumentar el tamaño de la trama al tamaño mínimo.

Campo Secuencia de verificación de trama

El campo Secuencia de verificación de trama (FCS) (4 bytes) se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (CRC). El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama. Un cambio en los datos podría ser consecuencia de una interrupción de las señales eléctricas que representan los bits.

5.1.2.2 Dirección MAC: Identidad de Ethernet

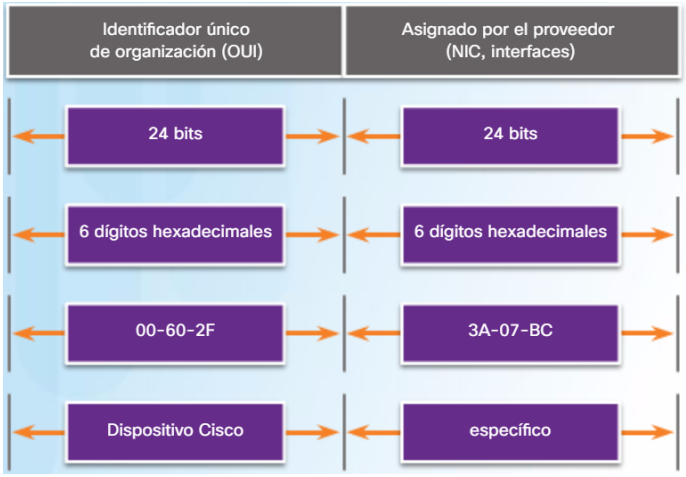
Una dirección MAC de Ethernet es un valor binario de 48 bits expresado como 12 dígitos hexadecimales. Las normas establecidas por el IEEE obligan a los proveedores de dispositivos Ethernet a registrarse en el IEEE. El IEEE asigna al proveedor un código de 3 bytes (24 bits), llamado "identificador único de organización (OUI)".

El IEEE requiere que un proveedor siga dos sencillas reglas, como se muestra en la ilustración:

- Todas las direcciones MAC asignadas a una NIC o a otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor como los tres primeros bytes.

- Todas las direcciones MAC con el mismo OUI deben tener asignado un valor único en los tres últimos bytes.

Nota: es posible que existan direcciones MAC duplicadas debido a errores de fabricación o en algunos métodos de implementación de máquinas virtuales. En cualquier caso, será necesario modificar la dirección MAC con una nueva NIC o en el software.



5.1.2.3 Procesamiento de tramas

A menudo, la dirección MAC se conoce como "dirección física (BIA)" porque, históricamente, esta dirección se graba de manera física en la memoria de solo lectura (ROM) de la NIC. Es decir que la dirección está codificada en el chip de la ROM de manera permanente.

Nota: en las NIC y los sistemas operativos de PC 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 arranca, lo primero que hace la NIC es copiar la dirección MAC de la ROM a la RAM. Cuando un dispositivo reenvía un mensaje a una red Ethernet, la información del encabezado contiene las direcciones MAC de origen y de destino.

Cuando una NIC recibe una trama de Ethernet, examina la dirección MAC de destino para ver si coincide con la dirección MAC física del dispositivo 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 Ethernet también aceptan tramas si la dirección MAC de destino es un grupo de difusión o de multidifusión del cual es miembro el host.

5.1.2.4 Representaciones de la dirección MAC

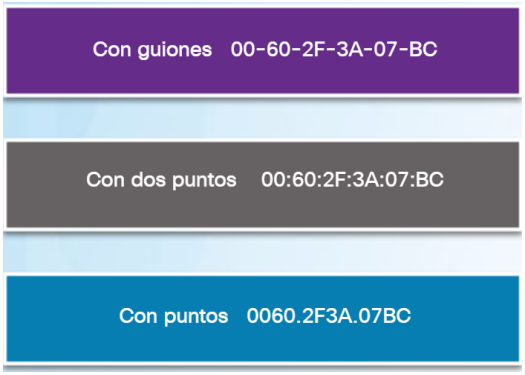
En un host de Windows, se puede utilizar el comando **ipconfig /all** para identificar la dirección MAC de un adaptador Ethernet. Según el dispositivo y el sistema operativo, puede ver varias representaciones de direcciones MAC

```
C:\>ipconfig/all

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Intel(R) Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-18-DE-DD-A7-B2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::449f:c2:de06:ebad%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, June 01, 2015 11:19:48 AM
   Lease Expires . . . . . . . . . . : Thursday, June 04, 2015 11:19:49 PM
   Default Gateway . . . . . . . . . : 10.10.10.1
   DHCP Server . . . . . . . . . . . : 10.10.10.1
   DNS Servers . . . . . . . . . . . : 10.10.10.1
```

Tipos de representación de la dirección MAC



5.1.2.5 Dirección MAC de unidifusión

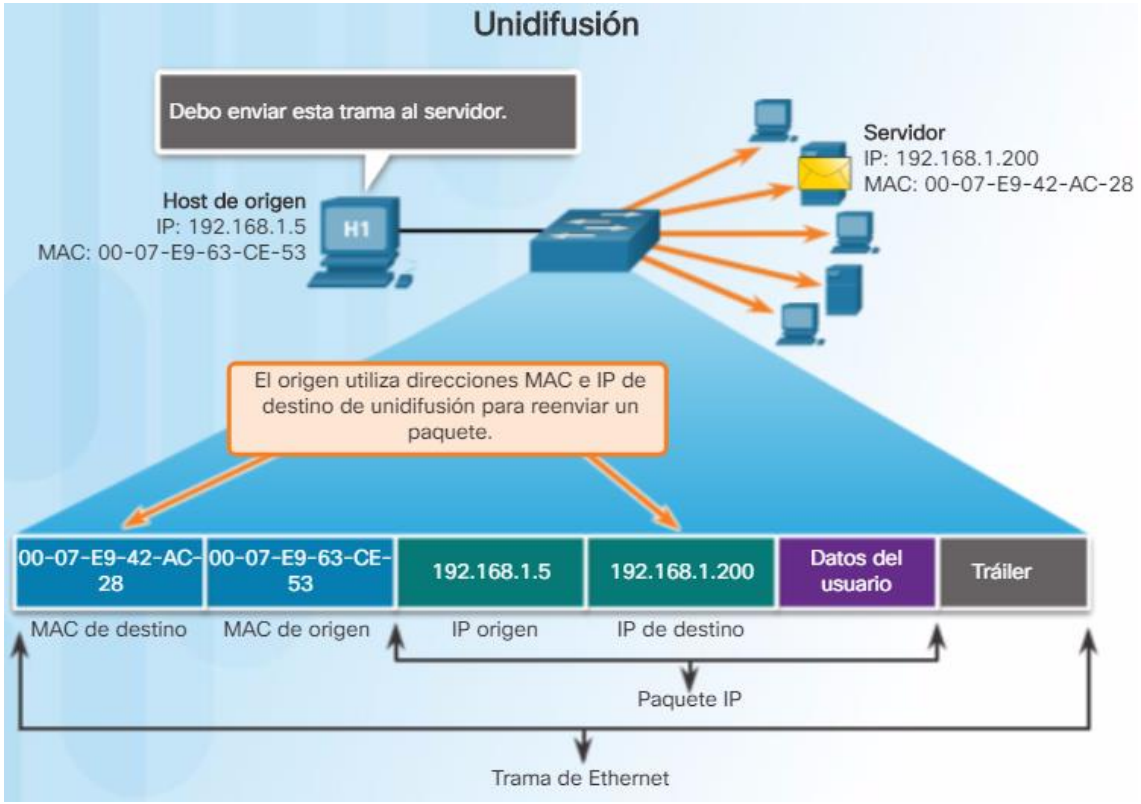
En Ethernet, se utilizan diferentes direcciones MAC para las comunicaciones de unidifusión, difusión y multidifusión de capa 2.

Una dirección MAC de unidifusión es la dirección única utilizada cuando se envía una trama desde un único dispositivo transmisor hacia un único dispositivo receptor.

En el ejemplo, un host con la dirección IPv4 192.168.1.5 (origen) solicita una página web del servidor en la dirección IPv4 de unidifusión 192.168.1.200. Para que un paquete de unidifusión 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.

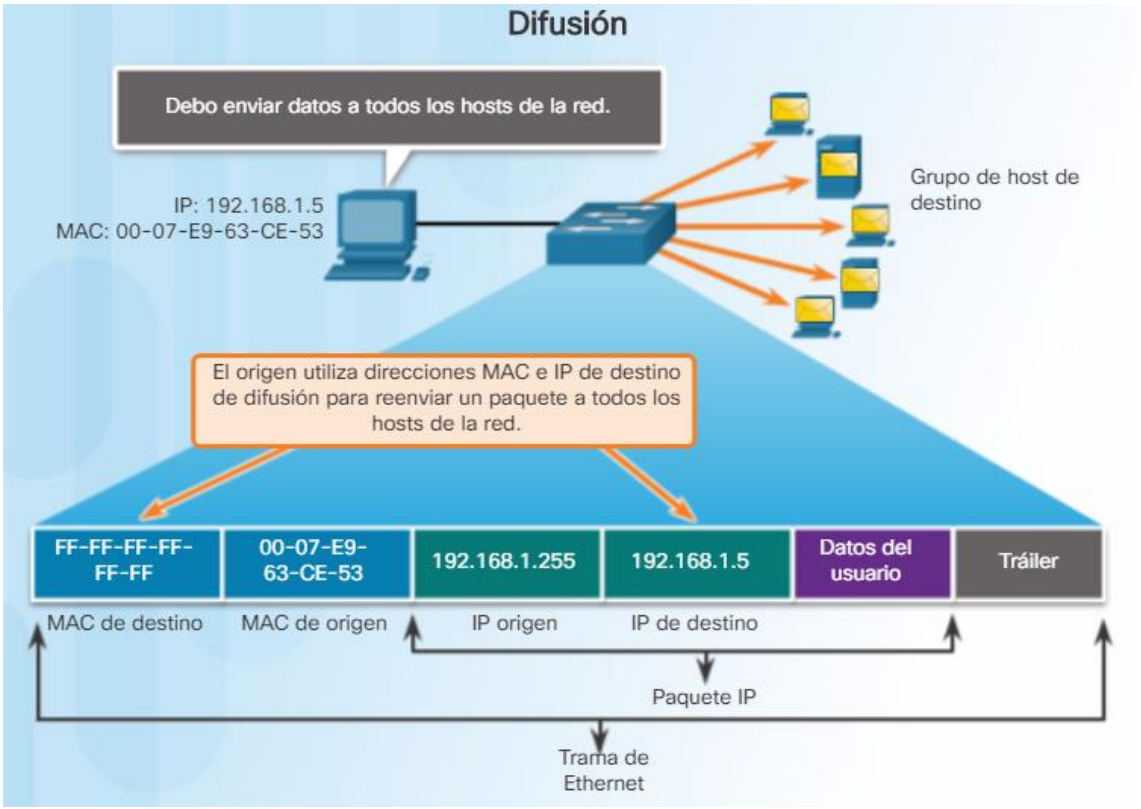
El proceso que un host de origen utiliza para determinar la dirección MAC de destino se conoce como “protocolo de resolución de direcciones (ARP)”. El ARP se analiza más adelante en este capítulo.

Aunque la dirección MAC de destino puede ser una dirección de unidifusión, difusión o multidifusión, la dirección MAC de origen siempre debe ser de unidifusión.



5.1.2.6 Dirección MAC de difusión

Los paquetes de difusión tienen una dirección IPv4 de destino que contiene solo números uno (1) en la porción de host. Esta numeración en la dirección significa que todos los hosts de esa red lal (dominio de difusión) recibirán y procesarán el paquete. Muchos protocolos de red, como DHCP y ARP, utilizan la difusión.

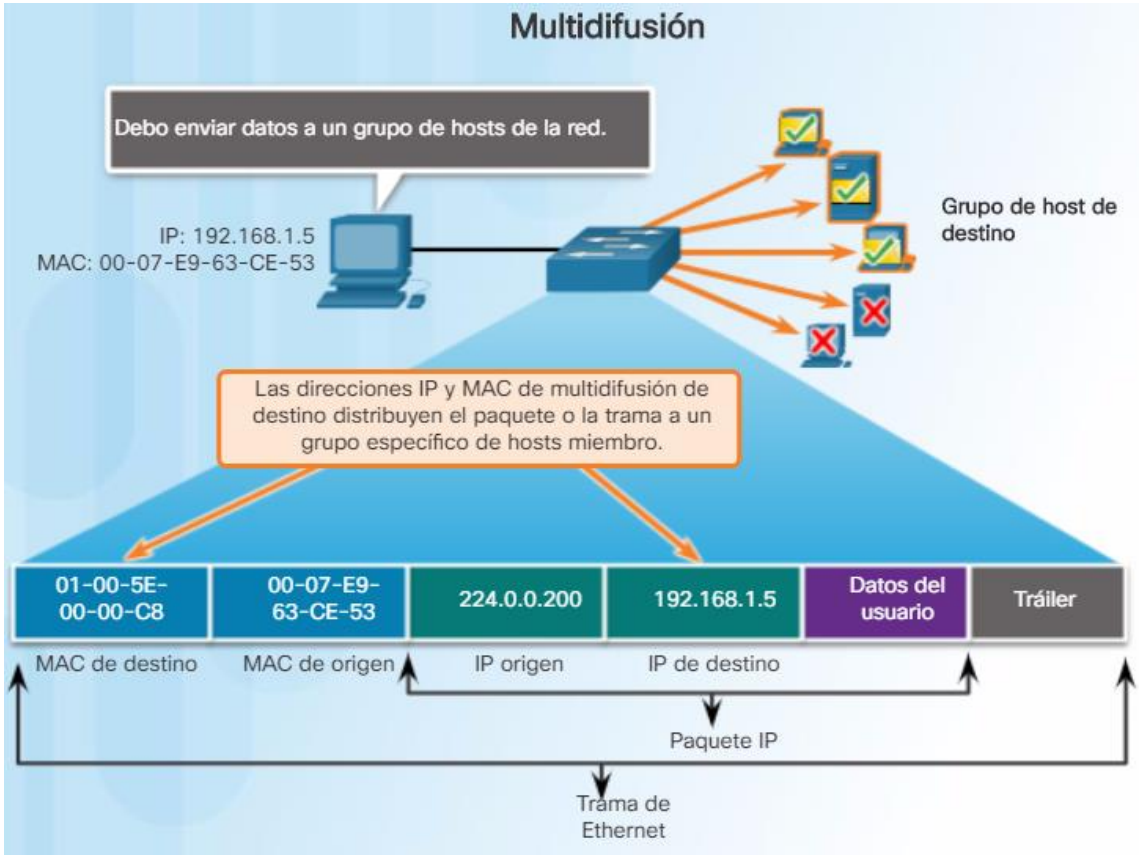


5.1.2.7 Dirección MAC de multidifusión

Las direcciones de multidifusión le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Una dirección IP de grupo de multidifusión se asigna a los dispositivos que pertenecen a un grupo de multidifusión. El intervalo de direcciones IPv4 de multidifusión va de 224.0.0.0 a 239.255.255.255. El rango de direcciones de multidifusión IPv6 comienza con FF00::/8. Debido a que las direcciones de multidifusión 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 unidifusión.

Al igual que con las direcciones de unidifusión y de difusión, la dirección IP de multidifusión requiere una dirección MAC de multidifusión correspondiente para poder enviar tramas en una red local. La dirección de multidifusión MAC relacionada con una dirección de multidifusión IPv4 es un valor especial que comienza con 01-00-5E en formato hexadecimal. La porción restante de la dirección MAC de multidifusión se crea convirtiendo en seis caracteres hexadecimales los 23 bits inferiores de la dirección IP del grupo de multidifusión. Para una dirección IPv6, la dirección de multidifusión MAC comienza con 33-33.

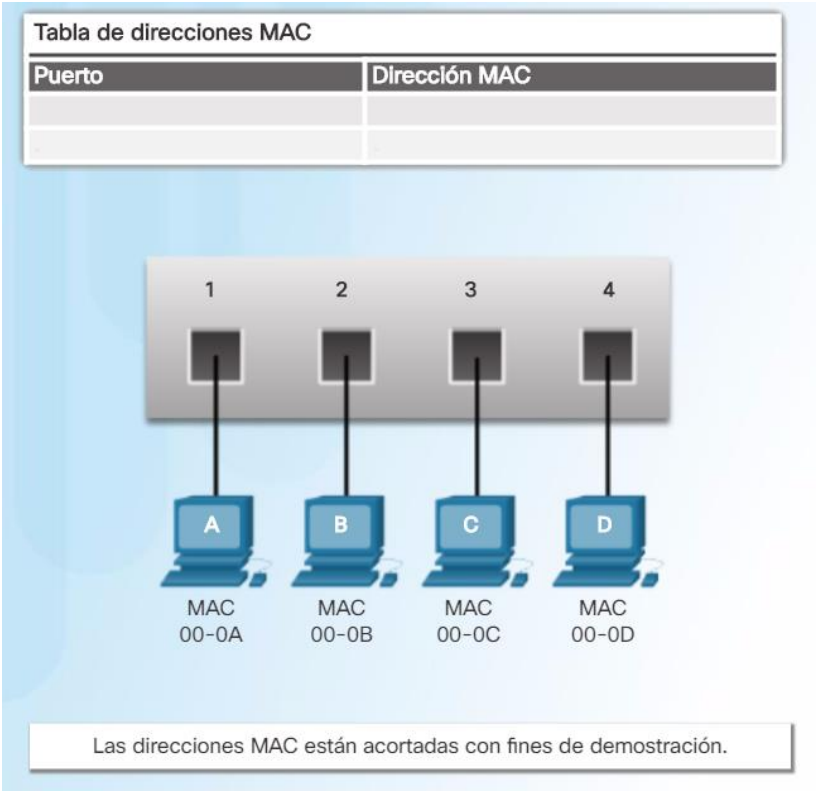
Un ejemplo, como se muestra en la animación, es la dirección hexadecimal de multidifusión 01-00-5E-00-00-C8. El último byte (u 8 bits) de la dirección IPv4 224.0.0.200 es el valor decimal 200. La forma más fácil de ver el equivalente hexadecimal es convertirlo en binario con un espacio cada 4 bits: 200 (decimal) = 1100 1000 (binario). Con la tabla de conversión que se presentó antes, podemos convertirlo en hexadecimal: 1100 1000 (binario) = 0xC8 (hexadecimal).



5.2.1.1 Nociones básicas de switches

Un switch Ethernet de capa 2 utiliza direcciones MAC para tomar decisiones de reenvío. Desconoce por completo qué protocolo se transmite en la porción de datos de la trama. Un switch Ethernet consulta una tabla de direcciones MAC para tomar una decisión de reenvío para cada trama. Cuando un switch se inicia por primera vez, todavía no conoce las direcciones MAC de los dispositivos conectados.

Nota: a veces, la tabla de direcciones MAC se conoce como “tabla de memoria de contenido direccionable (CAM)”.



5.2.1.2 Obtención de direcciones MAC

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.

El siguiente proceso se realiza para cada trama de Ethernet que ingresa a un switch.

Aprendizaje: 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. En la figura 1, la PC-A está enviando una trama de Ethernet a la PC-D. El switch agrega a la tabla la dirección MAC de la PC-A.

- 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.

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.

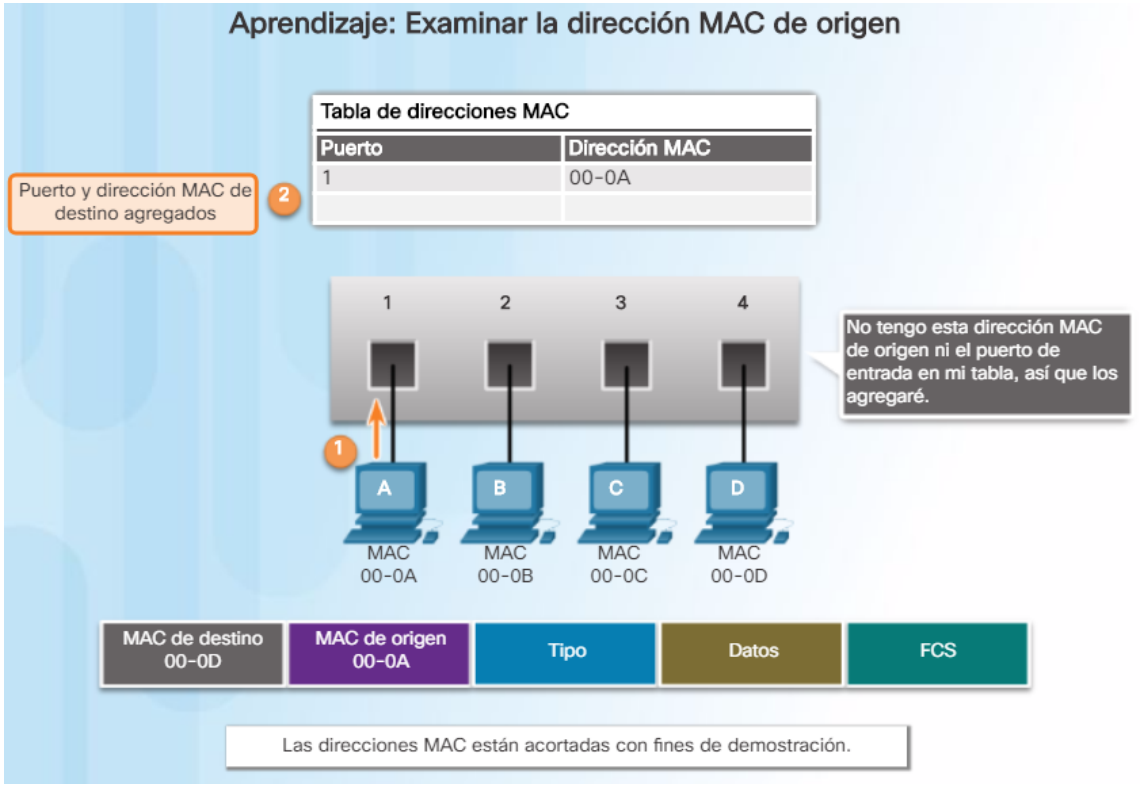
Reenvío: Examinar la dirección MAC de destino

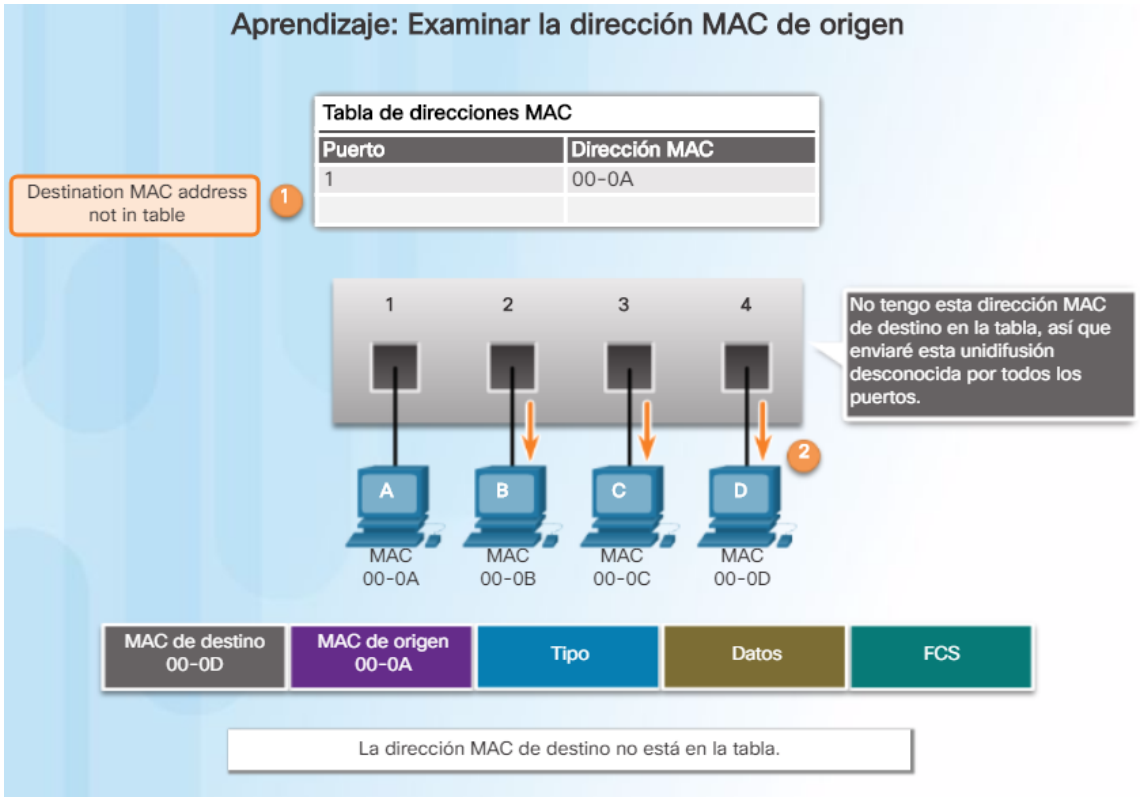
A continuación, si la dirección MAC de destino es una dirección de unidifusión, el switch busca una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC.

- Si la dirección MAC de destino está en la tabla, reenvía la trama por el puerto especificado.

- Si la dirección MAC de destino no está en la tabla, el switch reenvía la trama por todos los puertos, excepto el de entrada. Esto se conoce como “unidifusión desconocida”. Como se muestra en la figura 2, el switch no tiene la dirección MAC de destino de la PC-D en la tabla, por lo que envía la trama por todos los puertos, excepto el 1.

Nota: si la dirección MAC de destino es de difusión o de multidifusión, la trama también se envía por todos los puertos, excepto el de entrada.





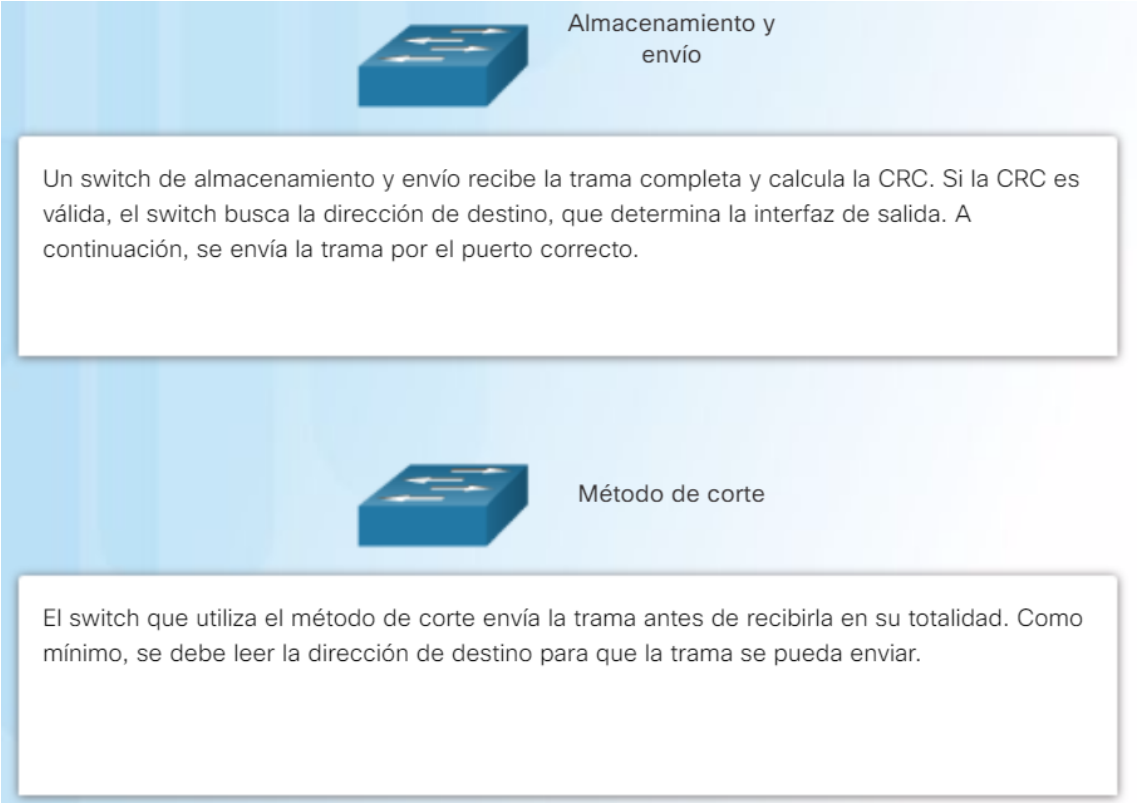
Cuando un dispositivo tiene una dirección IP ubicada en una red remota, la trama de Ethernet no se puede enviar directamente al dispositivo de destino. En cambio, la trama de Ethernet se envía a la dirección MAC del gateway predeterminado: el router.

5.2.2.1 Métodos de reenvío de tramas de los swiches Cisco

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
- Switching por método de corte

El switching de almacenamiento y envío 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.



5.2.2.2 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 reúne en el búfer solo la información suficiente de la trama como para leer la dirección MAC de destino y 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 no lleva a cabo ninguna verificación de errores en la trama.

A continuación, se presentan dos variantes del switching por método de corte:

- **Switching de reenvío rápido:** este método ofrece el nivel de latencia más bajo. El switching de envío rápido reenvía el paquete inmediatamente después de leer la dirección de destino. Como el switching de reenvío rápido comienza a reenviar el paquete antes de recibirlo por completo, es posible que, a veces, los paquetes se distribuyan con errores. En el modo de reenvío rápido, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. El switching de envío rápido 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 switching libre de fragmentos se puede ver como un punto medio entre el switching de almacenamiento y envío, y el switching por método de corte. El motivo por el que el switching libre de fragmentos 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.

Algunos switches están configurados para realizar el switching por método de corte en cada puerto hasta alcanzar un umbral de errores definido por el usuario y, luego, cambiar automáticamente al switching de almacenamiento y envío. Si el índice de error está por debajo del umbral, el puerto vuelve automáticamente al switching por método de corte.

5.2.2.3 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. El almacenamiento en búfer también se puede utilizar cuando el puerto de destino está ocupado debido a una congestión. En este caso, el switch almacena la trama hasta que se pueda transmitir.

Como se muestra en la ilustración, existen dos métodos de almacenamiento en búfer de memoria: memoria basada en puerto y memoria compartida.

Búfer de memoria basada en puerto

En el búfer de memoria basada en puerto, las tramas se almacenan en colas conectadas a puertos de entrada y de salida específicos. Una trama se transmite al puerto de salida una vez que todas las que están delante de ella en la cola se hayan transmitido correctamente. Es posible que una sola trama demore la transmisión de todas las tramas almacenadas en la memoria debido al tráfico del puerto de destino. Esta demora se produce aunque las demás tramas se puedan transmitir a puertos de destino abiertos.

Búfer de memoria compartida

El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch. La cantidad de memoria de búfer que requiere un puerto se asigna de forma dinámica. Las tramas que están en el búfer se enlazan de forma dinámica al puerto de destino. Esto permite que se pueda recibir el paquete por un puerto y que se pueda transmitir por otro, sin necesidad de colocarlo en otra cola.

El switch conserva un mapa de enlaces de trama a puerto que indica adónde debe transmitirse el paquete. El enlace se elimina del mapa una vez que la trama se transmite correctamente. La cantidad de tramas almacenadas en el búfer está limitada por el tamaño del búfer de memoria en su totalidad y no se limita a un solo búfer de puerto. Esto permite que se transmitan tramas más grandes y que se descarte una menor cantidad de ellas. Esto es de especial importancia para el switching asimétrico. El switching asimétrico permite diferentes índices de datos en diferentes puertos. Esto permite dedicar un mayor ancho de banda a ciertos puertos, como a un puerto conectado a un servidor.

5.2.3.1 Configuración de dúplex y velocidad

Dos de los parámetros más básicos de un switch son el ancho de banda y los parámetros de 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.

Existen dos tipos de parámetros de dúplex utilizados para las comunicaciones en una red Ethernet: dúplex medio y dúplex completo.

- Dúplex completo: ambos extremos de la conexión pueden enviar y recibir datos simultáneamente.

- Dúplex medio: 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 NIC, que permite que dos dispositivos intercambien automáticamente información sobre velocidad y funcionalidades de dúplex. El switch y el dispositivo conectado seleccionan el modo de mayor rendimiento. Si ambos dispositivos tienen la funcionalidad, se selecciona dúplex completo, junto con el ancho de banda común más alto.

Nota: de manera predeterminada, la mayoría de los switches Cisco y NIC Ethernet utilizan la autonegociación para la configuración de velocidad y dúplex. Los puertos Gigabit Ethernet solamente funcionan en dúplex completo.

Incompatibilidad de dúplex

Una de las causas más comunes de problemas de rendimiento en enlaces Ethernet de 10 o 100 Mb/s ocurre cuando un puerto del enlace funciona en dúplex medio, mientras el otro puerto funciona en dúplex completo, como se muestra en la figura 2. Esto sucede cuando uno o ambos puertos de un enlace se restablecen, y el proceso de autonegociación no configura ambos participantes del enlace de la misma manera. 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.

5.2.3.2 MDIX automática

Además de tener la configuración de dúplex correcta, también es necesario tener definido el tipo de cable correcto para cada puerto. Anteriormente, las conexiones entre dispositivos específicos, como switch a switch, switch a router, switch a host y router a host, requerían el uso de tipos de cable específicos (cruzado o directo). En la actualidad, la mayoría de los dispositivos de switch permiten que el comando mdix auto interface configuration en la CLI active la función de interfaz cruzada dependiente del medio (MDIX) automática.

Cuando se activa la función de MDIX automática, el switch detecta el tipo de cable conectado al puerto y configura las interfaces de manera adecuada. 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.

5.3.1.1 Destino en la misma red

Hay dos direcciones primarias asignadas a un dispositivo en una LAN Ethernet:

- **Dirección física (dirección MAC):** se utiliza para comunicaciones de NIC Ethernet a NIC Ethernet en la misma red.

- **Dirección lógica (dirección IP):** se utiliza para enviar el paquete del origen inicial al destino final.

Las direcciones IP se utilizan para identificar la dirección del origen inicial y del destino final. La dirección IP de destino puede estar en la misma red IP que la de origen o en una red remota.

Nota: la mayoría de las aplicaciones utilizan el sistema de nombres de dominio (DNS) para determinar la dirección IP cuando se les indica un nombre de dominio, como “www.cisco.com”. El DNS se analiza en detalle en otro capítulo.

5.3.1.2 Red remota de destino

Cuando la dirección IP de destino está en una red remota, la dirección MAC de destino es la dirección del gateway predeterminado del host (la NIC del router) como se muestra en la ilustración.

Cuando el router recibe una trama de Ethernet, desencapsula la información de capa 2. Por medio de la dirección IP de destino, determina el dispositivo del siguiente salto y encapsula el paquete IP en una nueva trama de enlace de datos para la interfaz de salida. Junto con cada enlace en una ruta, se encapsula un paquete IP en una trama específica para la tecnología de enlace de datos particular relacionada con ese enlace, como Ethernet. Si el dispositivo del siguiente salto es el destino final, la dirección MAC de destino es la de la NIC Ethernet del dispositivo.

¿Cómo se asocian las direcciones IPv4 de los paquetes IPv4 en un flujo de datos con las direcciones MAC en cada enlace a lo largo de la ruta hacia el destino? Esto se realiza mediante un proceso llamado “protocolo de resolución de direcciones (ARP)”.

5.3.2.1 Introducción ARP

Recuerde que cada dispositivo que tiene una dirección IP en una red Ethernet también tiene una dirección MAC Ethernet. Cuando un dispositivo envía una trama de Ethernet, esta contiene estas dos direcciones:

- **Dirección MAC de destino:** la dirección MAC de la NIC Ethernet, que es la dirección del destino final o del router.
- **Dirección MAC de origen:** la dirección MAC de la NIC Ethernet del remitente.

Para determinar la dirección MAC de destino, el dispositivo utiliza ARP. ARP proporciona dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantenimiento de una tabla de asignaciones

5.3.2.2 Funciones del ARP

Cuando se envía un paquete a la capa de enlace de datos para encapsularlo en una trama de Ethernet, el dispositivo consulta una tabla en su memoria para encontrar la dirección MAC que está asignada a la dirección IPv4. Esta tabla se denomina “tabla ARP” o “caché ARP”. La tabla ARP se almacena en la RAM del dispositivo.

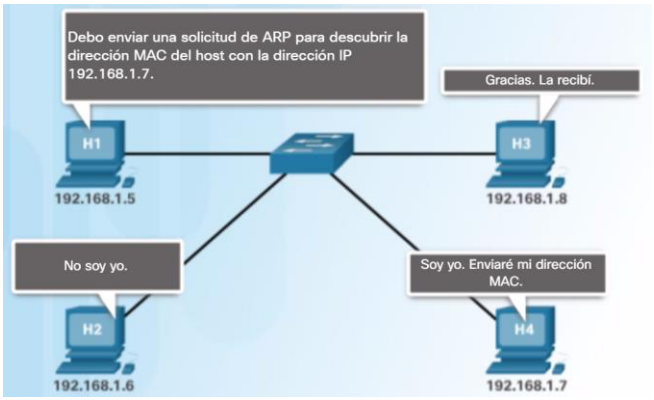
El dispositivo emisor busca en su tabla ARP la dirección IPv4 de destino y la dirección MAC correspondiente.

- Si la dirección IPv4 de destino del paquete está en la misma red que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 de destino en la tabla ARP.
- Si la dirección IPv4 de destino está en una red diferente que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 del gateway predeterminado.

En ambos casos, se realiza una búsqueda de la dirección IPv4 y la dirección MAC correspondiente para el dispositivo.

En cada entrada o fila de la tabla ARP, se enlaza una dirección IPv4 con una dirección MAC. Llamamos “asignación” a la relación entre dos valores; simplemente, se refiere a que puede localizar una dirección IPv4 en la tabla y averiguar la dirección MAC correspondiente. La tabla ARP almacena temporalmente (en caché) la asignación para los dispositivos de la LAN.

Si el dispositivo localiza la dirección IPv4, se utiliza la dirección MAC correspondiente como la dirección MAC de destino de la trama. Si no se encuentra ninguna entrada, el dispositivo envía una solicitud de ARP.



5.3.2.3 Solicitud de ARP (Vídeo)

Una solicitud de ARP se envía cuando un dispositivo necesita asociar una dirección MAC a una dirección IPv4 y no tiene una entrada para la dirección IPv4 en su tabla ARP.

Los mensajes de ARP se encapsulan directamente dentro de una trama de Ethernet. No se utiliza un encabezado de IPv4. El mensaje de solicitud de ARP incluye lo siguiente:

- **Dirección IPv4 objetivo:** esta es la dirección IPv4 que requiere una dirección MAC correspondiente.

- **Dirección MAC objetivo:** esta es la dirección MAC desconocida; en el mensaje de solicitud de ARP, está vacía.

La solicitud de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:

- **Dirección MAC de destino:** esta es una dirección de difusión que requiere que todas las NIC Ethernet de la LAN acepten y procesen la solicitud de ARP.

- **Dirección MAC de origen:** este es el remitente de la dirección MAC de la solicitud de ARP.

- **Tipo:** los mensajes de ARP tienen un campo de tipo de 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

Como las solicitudes de ARP son de difusión, el switch las envía por todos los puertos, excepto el de recepción. Todas las NIC Ethernet de la LAN procesan difusiones. Cada dispositivo debe procesar la solicitud de ARP para ver si la dirección IPv4 objetivo coincide con la suya. Un router no reenvía difusiones por otras interfaces.

5.3.2.4 Respuesta ARP (Vídeo)

Solamente el dispositivo que tiene la dirección IPv4 asociada con la dirección IPv4 objetivo de la solicitud de ARP envía una respuesta de ARP. El mensaje de respuesta de ARP incluye lo siguiente:

- **Dirección IPv4 del remitente:** esta es la dirección IPv4 del dispositivo cuya dirección MAC se solicitó.

- **Dirección MAC del remitente:** esta es la dirección MAC que el remitente solicita por medio de la solicitud de ARP.

La respuesta de ARP se encapsula en una trama de Ethernet con la siguiente información de encabezado:

- **Dirección MAC de destino:** es la dirección MAC del remitente de la solicitud de ARP.

- **Dirección MAC de origen:** este es el remitente de la dirección MAC de la respuesta de ARP.

- **Tipo:** los mensajes de ARP tienen un campo de tipo de 0x806. Esto informa a la NIC receptora que la porción de datos de la trama se debe enviar al proceso ARP.

Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no se puede crear una trama.

Las entradas de la tabla ARP tienen marcas de tiempo. Si un dispositivo no recibe una trama de un dispositivo determinado antes de que caduque la marca horaria, la entrada para este dispositivo se elimina de la tabla ARP.

Además, se pueden introducir entradas estáticas de asignaciones en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP no caducan con el tiempo y se deben eliminar de forma manual.

Nota: IPv6 utiliza un proceso similar al ARP para IPv4 llamado “detección de vecinos (ND o NDP) ICMPv6”. IPv6 utiliza mensajes de solicitud de vecino y de anuncio de vecino similares a las solicitudes y respuestas de ARP de IPv4.

5.3.2.5 El ARP en la comunicación remota

Cuando la dirección IPv4 de destino no está en la misma red que la dirección IPv4 de origen, el dispositivo de origen debe enviar la trama al gateway predeterminado, es decir a la interfaz del router local.

La dirección IPv4 de la dirección del gateway predeterminado se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IPv4 de destino con la propia para determinar si ambas están ubicadas en la misma red de capa 3. Si el host de destino no está en la misma red, el origen busca en la tabla ARP una entrada que contenga la dirección IPv4 del gateway predeterminado. Si no existe una entrada, utiliza el proceso ARP para determinar la dirección MAC del gateway predeterminado.

5.3.2.6 Eliminación de entradas de una tabla ARP

Para cada dispositivo, un temporizador de memoria caché ARP elimina las entradas de ARP que no se hayan utilizado durante un período especificado. El temporizador varía según el sistema operativo del dispositivo. Por ejemplo, algunos sistemas operativos Windows almacenan entradas de ARP en la memoria caché durante dos minutos, como se muestra en la ilustración.

También se pueden utilizar comandos para eliminar de manera manual todas las entradas de la tabla ARP o algunas de ellas. Después de eliminar una entrada, el proceso de envío de una solicitud de ARP y de recepción de una respuesta de ARP debe ocurrir nuevamente para que se introduzca la asignación en la tabla ARP.

5.3.2.7 Tablas ARP

En un router Cisco, se utiliza el comando **show ip arp** para visualizar la tabla ARP, como se muestra en la figura 1.

En una PC con Windows 7, se utiliza el comando **arp –a** para visualizar la tabla ARP, como se muestra en la figura 2.

```
Router# show ip arp
                     Age
Protocol  Address        (min)  Hardware Addr    Type   Interface
Internet  172.16.233.229   -    0000.0c59.f892   ARPA   Ethernet0/0
Internet  172.16.233.218   -    0000.0c07.ac00   ARPA   Ethernet0/0
Internet  172.16.168.11    -    0000.0c63.1300   ARPA   Ethernet0/0
Internet  172.16.168.254   9    0000.0c36.6965   ARPA   Ethernet0/0
```

```
C:\> arp -a

Interface: 192.168.1.67 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.254         64-0f-29-0d-36-91     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.82.253.91 --- 0x10
  Internet Address      Physical Address      Type
  10.82.253.92          64-0f-29-0d-36-91     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

5.3.3.2 Suplantación de ARP

En algunos casos, el uso de ARP puede ocasionar un riesgo de seguridad potencial conocido como “suplantación de ARP” o “envenenamiento ARP”. Esta es una técnica utilizada por un atacante para responder a una solicitud de ARP de una dirección IPv4 que pertenece a otro dispositivo, como el gateway predeterminado, como se muestra en la ilustración. El atacante envía una respuesta de ARP con su propia dirección MAC. El receptor de la respuesta de ARP agrega la dirección MAC incorrecta a la tabla ARP y envía estos paquetes al atacante.

Los switches de nivel empresarial incluyen técnicas de mitigación conocidas como “inspección dinámica de ARP (DAI)”. La DAI excede el ámbito de este curso.