UD3. Ethernet

Índice

Introducción

La capa física de OSI proporciona los medios de transporte de los bits que conforman una trama de la capa de enlace de datos a través de los medios de red.

En la actualidad, Ethernet es la tecnología LAN predominante en el mundo. 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 de red, incluidos el formato y el tamaño de la trama, la temporización y la codificación. Cuando se envían mensajes entre hosts a través de una red Ethernet, los hosts asignan un formato a los mensajes según la configuración de trama que especifican los estándares. Las tramas también se conocen como unidades de datos de protocolo (PDU).

Dado que Ethernet se compone de estándares en estas capas inferiores, es probable que sea más sencillo de entender con referencia al modelo OSI. El modelo OSI separa las funcionalidades de direccionamiento, entramado y acceso a los medios de la capa de enlace de datos de los estándares de la capa física de los medios. Los estándares de Ethernet definen los protocolos de Capa 2 y las tecnologías de Capa 1. Si bien las especificaciones de Ethernet admiten diferentes medios, anchos de banda y otras variaciones de Capa 1 y 2, el formato de trama básico y el esquema de direcciones son los mismos para todas las variedades de Ethernet.

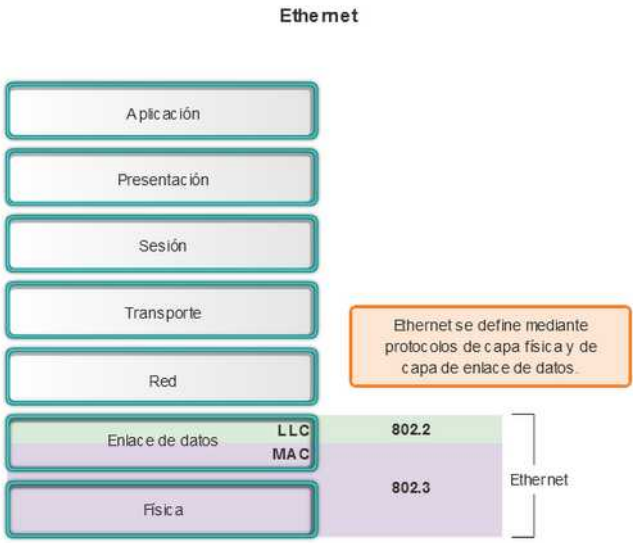
Este capítulo analiza las características y el funcionamiento de la Ethernet en términos de su evolución desde una tecnología de medios compartidos de comunicación de datos basada en contenciones hasta convertirse en la actual tecnología full-duplex de gran ancho de banda.

Protocolo Ethernet

Funcionamiento de Ethernet

Ethernet es la tecnología LAN más ampliamente utilizada en la actualidad.

Ethernet funciona en la capa de enlace de datos y en la capa física. Se trata de una familia de tecnologías de red que se definen en los estándares IEEE 802.2 y 802.3. Ethernet admite los anchos de banda de datos siguientes:



- 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)

Como se muestra, los estándares de Ethernet definen tanto los protocolos de capa 2 como las tecnologías de capa 1. En lo que respecta a los

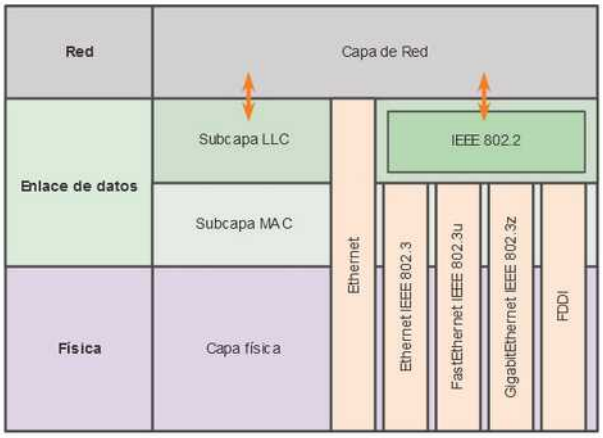
protocolos de capa 2, al igual que sucede con todos los estándares IEEE 802, Ethernet depende de las dos subcapas separadas de la capa de enlace de datos para funcionar: la subcapa de control de enlace lógico (LLC) y la subcapa MAC.

Subcapa LLC

La subcapa LLC de Ethernet se ocupa de la comunicación entre las capas superiores y las capas inferiores. Generalmente, esta comunicación se produce entre el software de red y el hardware del dispositivo. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino. El LLC se utiliza para comunicarse con las capas superiores de la aplicación y para la transición del paquete a las capas inferiores para su entrega.

El LLC se implementa en software, y su implementación no depende del hardware. En un PC, el LLC se puede considerar el controlador de la NIC. El controlador de la NIC es un programa que interactúa directamente con el hardware de la NIC para transmitir los datos entre la subcapa MAC y los medios físicos.

Subcapa MAC

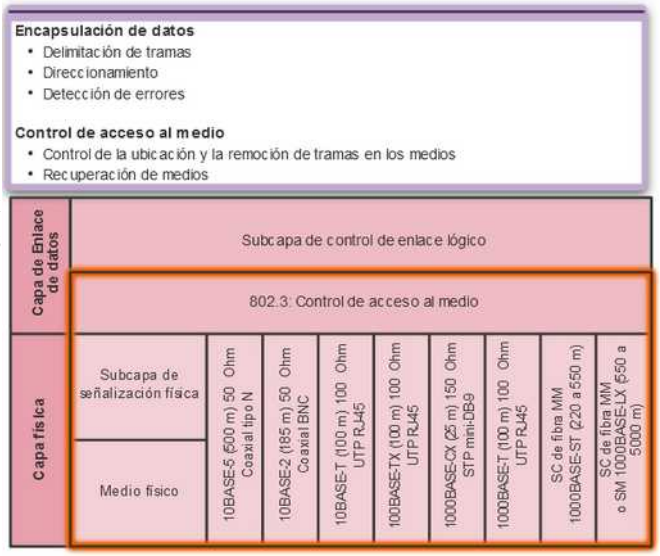


La MAC constituye la subcapa inferior de la capa de enlace de datos. La MAC se implementa mediante hardware, por lo general, en la NIC de la PC. Los detalles se especifican en los estándares IEEE 802.3.

En la figura se enumeran los estándares IEEE de Ethernet comunes.

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

- Encapsulación de datos
- Control de acceso al medio



Encapsulación de datos

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el desarmado de la trama en el momento en que se la recibe. Cuando se forma la trama, la capa MAC agrega un encabezado y un tráiler o cola a la PDU de la capa de red.

La encapsulación de datos proporciona tres funciones principales:

- **Delimitación de tramas**: el proceso de entramado proporciona delimitadores importantes que se utilizan para identificar un grupo de bits que componen una trama. Este proceso ofrece una sincronización entre los nodos transmisores y receptores.
- **Direccionamiento**: el proceso de encapsulación también proporciona direccionamiento de la capa de enlace de datos. Cada encabezado Ethernet agregado a la trama contiene la dirección física (dirección MAC) que permite que la trama se envíe a un nodo de destino.
- **Detección de errores**: cada trama de Ethernet contiene un tráiler con una comprobación de redundancia cíclica (CRC) del contenido de la trama. Una vez que se recibe una trama, el nodo receptor crea una CRC para compararla con la de la trama. Si estos dos cálculos de CRC coinciden, puede asumirse que la trama se recibió sin errores.

La utilización de tramas facilita la transmisión de bits a medida que se colocan en los medios y la agrupación de bits en el nodo receptor.

Control de acceso al medio

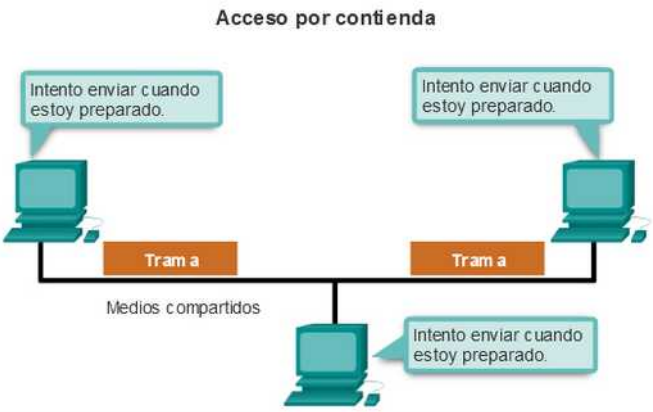
La segunda responsabilidad de la subcapa MAC es el control de acceso al medio. El control de acceso al medio es responsable de la ubicación y la remoción de tramas en los medios. Como su nombre lo indica, controla el acceso a los medios. Esta subcapa se comunica directamente con la capa física.

La topología lógica subyacente de Ethernet es de bus de multiacceso; por lo tanto, todos los nodos (dispositivos) en un mismo segmento de red comparten el medio. Ethernet es un método de red de contienda. Recuerde que en un método por contienda, o método no determinista, cualquier dispositivo puede intentar transmitir datos a través del medio compartido siempre que tenga datos para enviar. Sin embargo, tal como sucede si dos personas intentan hablar al mismo tiempo, si hay varios dispositivos en un único medio que intentan reenviar datos simultáneamente, los datos colisionan, lo que provoca que estos se dañen y no se puedan utilizar. Por este motivo, Ethernet proporciona un método para controlar la forma en que los nodos comparten el acceso mediante el uso de una tecnología de acceso múltiple por detección de portadora (CSMA).

CSMA

En primera instancia, el proceso de CSMA se utiliza para detectar si los medios transportan una señal. Si se detecta una señal portadora en el medio desde otro nodo, quiere decir que otro dispositivo está transmitiendo. Cuando un dispositivo está intentando transmitir y nota que el medio está ocupado, esperará e intentará después de un período de tiempo corto. Si no se detecta una señal portadora, el dispositivo transmite sus datos. Es posible que el proceso CSMA falle si dos dispositivos transmiten al mismo tiempo. A esto se le denomina colisión de datos. Si esto ocurre, los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.

Los métodos de control de acceso al medio por contienda no requieren mecanismos para llevar la cuenta de a quién le corresponde acceder al medio; por lo tanto, no tienen la sobrecarga de los métodos de acceso controlado. Sin embargo, los sistemas por contención no escalan bien bajo un uso intensivo de los medios. A medida que el uso y el número de nodos aumenta, la probabilidad de acceder a los medios con éxito sin una colisión disminuye. Además, los mecanismos de recuperación que se requieren para corregir errores debidos a esas colisiones disminuyen aún más el rendimiento.



Método	Características	Ejemplo
Acceso por contienda	• Las estaciones pueden transmitir en cualquier momento. • Existen colisiones. • Existen mecanismos para resolver problemas de contienda. • CSMA/CD para redes Ethernet • CSMA/CA para redes inalámbricas	• Ethernet • Acceso inalámbrico

Como se muestra en la ilustración, el CSMA se suele implementar junto con un método para resolver la contienda de los medios. Los dos métodos comúnmente utilizados son:

CSMA/Detección de colisión

Con el método CSMA/Detección de colisión **(CSMA/CD),** el dispositivo controla los medios para detectar la presencia de una señal de datos. Si no hay una señal de datos, que indica que el medio está libre, el dispositivo transmite los datos. Si luego se detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. Las formas tradicionales de Ethernet se desarrollaron para utilizar este método.

La incorporación a gran escala de tecnologías conmutadas en las redes modernas reemplazó ampliamente la necesidad original de implementación de CSMA/CD en redes de área local. Hoy en día, casi todas las conexiones por cable entre dispositivos en una LAN son conexiones full-duplex, es decir, un mismo dispositivo puede enviar y recibir información simultáneamente. Esto significa que, si bien las redes Ethernet se diseñan con tecnología CSMA/CD, con los dispositivos intermediarios actuales no se producen colisiones y los procesos utilizados por el CSMA/CD son realmente innecesarios.

Sin embargo, todavía se deben tener en cuenta las colisiones en conexiones inalámbricas en entornos LAN. Los dispositivos LAN inalámbricos utilizan el método de acceso al medio CSMA/Prevención de colisiones (CSMA/CA).

CSMA/Prevención de colisiones

Con el método CSMA/CA, el dispositivo analiza los medios para detectar la presencia de una señal de datos. Si el medio está libre, el dispositivo envía una notificación a través del medio, sobre su intención de utilizarlo. El dispositivo luego envía los datos. Las tecnologías de red inalámbricas 802.11 utilizan este método.

Estándares

EEE 802.3 fue el primer intento para estandarizar ethernet. Aunque hubo un campo de la cabecera que se definió de forma diferente, posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y los de 10, 40 y 100 Gigabits Ethernet), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).

Los estándares de este grupo no reflejan necesariamente lo que se usa en la práctica, aunque a diferencia de otros grupos este suele estar cerca de la realidad.

Nombre	Medio	Distancia máx	Estándar
Ethernet (10 Mbps)			
10BASE5	Coaxial grueso	500 m	802.3
10BASE2	Coaxial fino	185 m	802.3a
10BASE-T	Par trenzado cat. 3 o 5	100 m	802.3i
10BASE-FL	MMF 850 nm	2 km	802.3j
FastEthernet (100 Mbps)			
100BASE-TX	Par trenzado cat. 5	100 m	802.3u
100BASE-FX	MMF 1310 nm	2 km	
GigabitEthernet (1000 Mbps)			
1000BASE-T	Par trenzado >= cat. 5	100 m	802.3ab
1000BASE-SX	MMF 850 nm	550 m	802.3z
1000BASE-LX	MMF y SMF 1310 nm	10 km	
10 GigabitEthernet (10 Gbps)			
10GBASE-T	Par trenzado >= cat 6	100 m	802.3an
10GBASE-SR	MMF 850 nm	400 m	802.3ae
10GBASE-LR	SMF	10 Km	
40 GigabitEthernet (40 Gbps)			
40GBASE-SR4	MMF	125 m	802.3ba
40GBASE-LR4	SMF	10 km	
100 GigabitEthernet (100 Gbps)			
100GBASE-SR10	MMF	125 m	802.3ba
100GBASE-LR4	SMF	10 km	

Siglas

MMF: Fibra multimodo (Multi Mode Fiber)
SMF: Fibra monomodo (Single Mode Fiber)
SR: Corto alcance (Short Range)
LR: Largo alcance (Long Range)

La alimentación a través de Ethernet (Power over Ethernet, PoE)

Es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo cable que se utiliza para la conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones del dispositivo alimentado y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

Power over Ethernet se regula en la norma **IEEE 802.3af**, y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos preexistentes que no sean compatibles. Esta característica permite a los usuarios mezclar en la red con total libertad y seguridad dispositivos preexistentes con dispositivos compatibles con PoE.

Actualmente existen en el mercado varios dispositivos de red como switches o hubs que soportan esta tecnología. Para implementar PoE en una red que no se dispone de dispositivos que la soporten directamente se usa una unidad base (con conectores RJ45 de entrada y de salida) con un adaptador de alimentación para recoger la electricidad y una unidad terminal (también con conectores RJ45) con un cable de alimentación para que el dispositivo final obtenga la energía necesaria para su funcionamiento.

Ventajas

- PoE es una fuente de alimentación inteligente: Los dispositivos se pueden apagar o reiniciar desde un lugar remoto usando los protocolos existentes, como el Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol).
- PoE simplifica y abarata la creación de un suministro eléctrico altamente robusto para los sistemas: La centralización de la alimentación a través de concentradores (hubs) PoE significa que los sistemas basados en PoE se pueden enchufar al Sistema de alimentación ininterrumpida (SAI) central, que ya se emplea en la mayor parte de las redes informáticas formadas por más de uno o dos PC, y en caso de corte de electricidad, podrá seguir funcionando sin problemas.
- Los dispositivos se instalan fácilmente allí donde pueda colocarse un cable LAN, y no existen las limitaciones debidas a la proximidad de una base de alimentación (dependiendo la longitud del cable se deberá utilizar una fuente de alimentación de mayor voltaje debido a la caída del mismo, a mayor longitud mayor perdida de voltaje, superando los 25 metros de cableado aproximadamente).
- Un único juego de cables para conectar el dispositivo Ethernet y suministrarle alimentación, lo que simplifica la instalación y ahorra espacio.
- La instalación no supone gasto de tiempo ni de dinero ya que no es necesario realizar un nuevo cableado.
- PoE dificulta enormemente cortar o destrozar el cableado: Generalmente el cableado se encuentra unido a bandejas en los huecos del techo o detrás de conductos de plástico de muy difícil acceso. Cualquier corte de estos cables resultará obvio al momento para quien pase por el lugar y, por supuesto, para los usuarios de los ordenadores que serán incapaces de proseguir con su trabajo.

Desventajas

- Ausencia de estándares tecnológicos para la interoperabilidad de equipos.
- Para poder usar **PoE**, todos los dispositivos de Red (Hub/Switch, Cámaras IP, Puntos de Acceso,…) deben ser compatibles con esta norma.

El estándar original IEEE 802.3af-2003 de PoE proporciona hasta **15,4 W** de potencia de CC (mínimo 44 V DC y 350 mA) para cada dispositivo. Sólo se aseguran 12,95 W en el dispositivo puesto que cierta energía se disipa en el cable.

El estandar actualizado IEEE 802.3af-2009 de PoE también conocido como **PoE+** o PoE plus, proporciona hasta **25,5 W** de potencia. Algunos vendedores han anunciado productos que dicen ser compatibles con el estándar 802.3af y ofrecen hasta 51 W de potencia en un solo cable utilizando los cuatro pares del cable de categoría 5.

Comparativa PoE y PoE+

Propiedad	802.3af (802.3at Tipo1)	802.3at Tipo 2
Potencia en el origen	15.40 W	34.20 W
Potencia para dispositivo final	12.95 W	25.50 W
Voltaje en el origen	44.0–57.0 V	50.0–57.0 V
Voltaje para el dispositivo final	37.0–57.0 V	42.5–57.0 V
Intensidad máxima	350 mA	600 mA
Resistencia máxima del cable	20 Ω (Categoría 3)	12.5 Ω (Categoría 5)

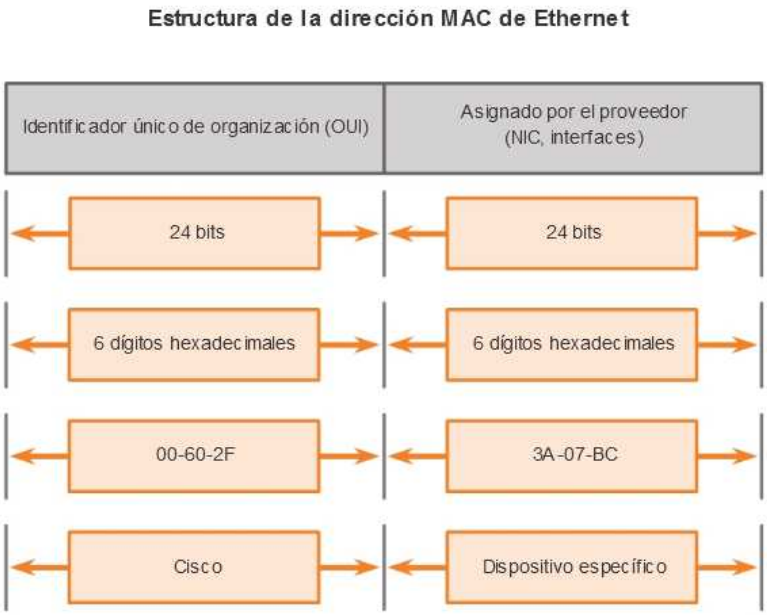
La dirección MAC

Como se indicó anteriormente, la topología lógica subyacente de Ethernet es de bus de multiacceso. Cada dispositivo de red está conectado a los mismos medios compartidos, y todos los nodos reciben todas las tramas que se transmiten. El problema es que si todos los dispositivos reciben cada trama, ¿cómo puede determinar cada dispositivo si es el receptor previsto sin la sobrecarga de tener que procesar y desencapsular la trama para obtener la dirección IP? Esta cuestión se vuelve aún más problemática en redes con alto volumen de tráfico donde se reenvían muchas tramas.

Para evitar la sobrecarga excesiva relacionada con el procesamiento de cada trama, se creó un identificador único denominado “dirección MAC” que identifica los nodos de origen y de destino reales dentro de una red Ethernet. Sin importar qué variedad de Ethernet se utilice, el direccionamiento MAC proporciona un método para la identificación de dispositivos en el nivel inferior del modelo OSI. Como recordará, el direccionamiento MAC se agrega como parte de una PDU de capa 2. Una dirección MAC de Ethernet es un valor binario de 48 bits expresado como 12 dígitos hexadecimales (4 bits por dígito hexadecimal).

Estructura de la dirección MAC

Las direcciones MAC deben ser únicas en el mundo. El valor de la dirección MAC es el resultado directo de las normas implementadas por el IEEE para proveedores con el objetivo de garantizar direcciones únicas para cada dispositivo Ethernet. Las normas establecidas por el IEEE obligan a los proveedores de dispositivos Ethernet a registrarse en el IEEE. El IEEE le asigna al proveedor un código de 3 bytes (24 bits), denominado “Identificador único de organización” (OUI).



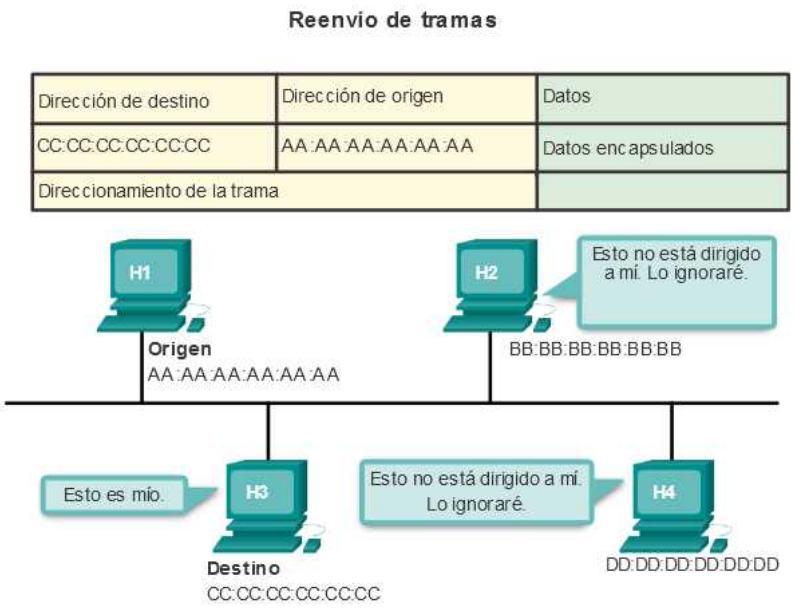
El IEEE requiere que un proveedor siga dos reglas sencillas, como se muestra en la ilustración:

- Todas las direcciones MAC asignadas a una NIC u otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor como los 3 primeros bytes.
- Se les debe asignar un valor exclusivo (código del fabricante o número de serie) a todas las direcciones MAC con el mismo OUI (Identificador exclusivo de organización) en los últimos 3 bytes.

La dirección MAC suele denominarse “dirección física” (BIA) porque, históricamente, se graba en la ROM (memoria de solo lectura) de la NIC. Esto significa que la dirección se codifica en el chip de la ROM de manera permanente pero en los sistemas operativos de PC y en las NIC modernos, es posible cambiar la dirección MAC mediante software. Esto es útil cuando se trata de acceder a una red que filtra sobre la base de la BIA. Esto quiere decir que el filtrado o control del tráfico sobre la base de la dirección MAC ya no es tan seguro como antes.

Las direcciones MAC se asignan a estaciones de trabajo, servidores, impresoras, switches y routers, es decir, a cualquier dispositivo que debe originar o recibir datos en una red. Todos los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC. Diferentes fabricantes de hardware y software pueden representar las direcciones MAC en distintos formatos hexadecimales. Los formatos de las direcciones pueden ser similares a los siguientes:

- 00-05-9A-3C-78-00
- 00:05:9A:3C:78:00
- 0005.9A3C.7800



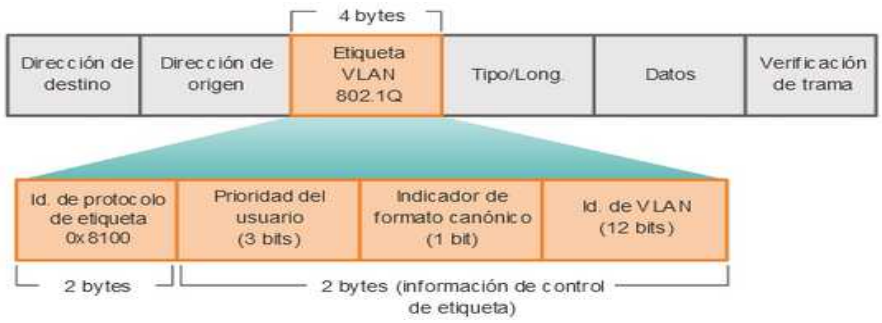
Cuando se inicia la PC, lo primero que hace la NIC es copiar la dirección MAC del ROM en la RAM. Cuando un dispositivo reenvía un mensaje a una red Ethernet, adjunta al paquete la información del encabezado. La información del encabezado contiene la dirección MAC de origen y destino. El dispositivo de origen envía los datos a través de la red.

Cada NIC en la red revisa la información en la subcapa MAC para ver si la dirección MAC de destino que está en la trama coincide con la dirección MAC física del dispositivo almacenada en la RAM. Si no hay coincidencia, el dispositivo descarta la trama. Cuando la trama llega al destino en que la MAC de la NIC coincide con la MAC de destino de la trama, la NIC pasa la trama a las capas OSI, donde se lleva a cabo el proceso de desencapsulación.

Tanto el estándar Ethernet II como el IEEE 802.3 definen el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes.

Cualquier trama con menos de 64 bytes de longitud se considera un "fragmento de colisión" o "runt frame" y las estaciones receptoras la descartan automáticamente.

El estándar IEEE 802.3ac, publicado en 1998, amplió el tamaño de trama máximo permitido a 1522 bytes. Se aumentó el tamaño de la trama para que se adapte a una tecnología denominada Red de área local virtual (VLAN). Las VLAN se crean dentro de una red conmutada y se estudiarán más tarde. Además, muchas tecnologías de calidad de servicio (QoS) hacen uso del campo Prioridad del usuario para implementar diversos niveles de servicio, como el servicio de prioridad para el tráfico de voz. En la ilustración, se muestran los campos contenidos en la etiqueta VLAN 802.1Q.



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.

Atributos de la trama de Ethernet

Los campos principales de la trama de Ethernet son los siguientes:

- **Campos Preámbulo y Delimitador de inicio de trama:** los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD), también conocido como “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 previsto. Como recordará, la Capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama viene dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.
- **Campo Dirección MAC de origen:** este campo de 6 bytes identifica la NIC o la interfaz que origina la trama.
- **Campo Longitud**: para todos los estándares IEEE 802.3 anteriores a 1997, el campo Longitud define la longitud exacta del campo de datos de la trama. Esto se utiliza posteriormente como parte de la FCS para garantizar que el mensaje se reciba adecuadamente. Por lo demás, el propósito del campo es describir qué protocolo de capa superior está presente. Si el valor de los dos octetos es igual o mayor que 0x0600 hexadecimal o 1536 decimal, el contenido del campo Datos se decodifica según el protocolo EtherType indicado. Por otro lado, si el valor es igual o menor que el hexadecimal de 0x05DC o el decimal de 1500, el campo Longitud se está utilizando para indicar el uso del formato de trama de IEEE 802.3. Así se diferencian las tramas de Ethernet II y 802.3.
- **Campo Datos**: este campo (de 46 a 1500 bytes) contiene los datos encapsulados de una capa superior, que es una PDU de capa 3 genérica 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 conocidos como “relleno” para incrementar el tamaño de la trama al tamaño mínimo.
- **Campo Secuencia de verificación de trama (FCS):** este campo de 4 bytes se utiliza para detectar errores en una trama. Utiliza una comprobación de redundancia cíclica (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 resultado de una interrupción de las señales eléctricas que representan los bits.

MAC de Ethernet

En un host de Windows, el comando **ipconfig /all** se puede utilizar para identificar la dirección MAC de un adaptador de Ethernet. Observe que la pantalla indica que la dirección física (dirección MAC) de la PC es 00-18-DE-C7-F3-FB

Según el dispositivo y el sistema operativo, verá distintas representaciones de las direcciones MAC, como se muestra en la figura 2. Los routers y switches Cisco utilizan la forma XXXX.XXXX.XXXX, donde "X" representa un carácter hexadecimal.

Con guiones: 00-60-2F-3A-07-BC

Con dos puntos: 00:60:2F:3A:07:BC

Con puntos: 0060.2F3A.07BC

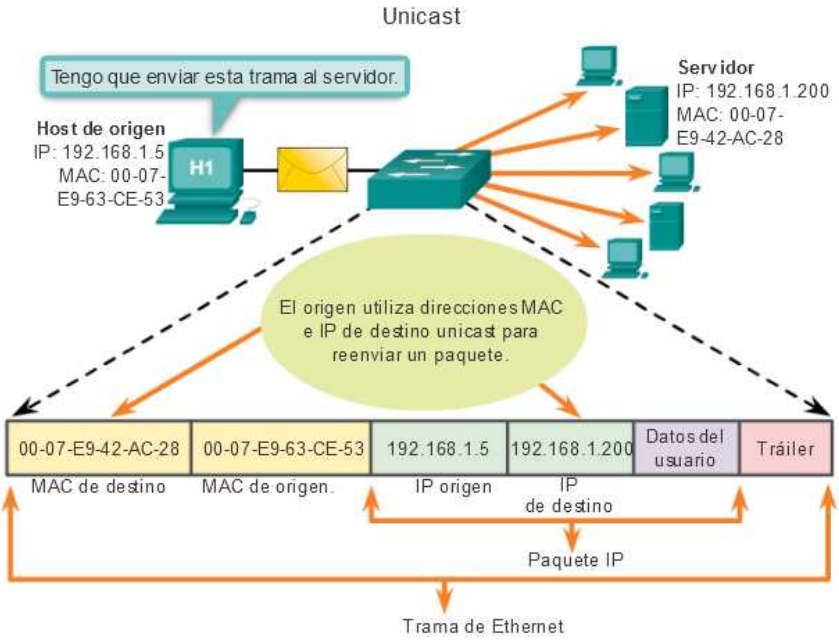
```
C:\>ipconfig/all

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Intel(R) Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-18-DE-C7-F3-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.67(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, November 26, 2012 12:14:48 PM
   Lease Expires . . . . . . . . . . : Saturday, December 01, 2012 12:15:02 AM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DNS Servers . . . . . . . . . . . : 192.168.1.254
```

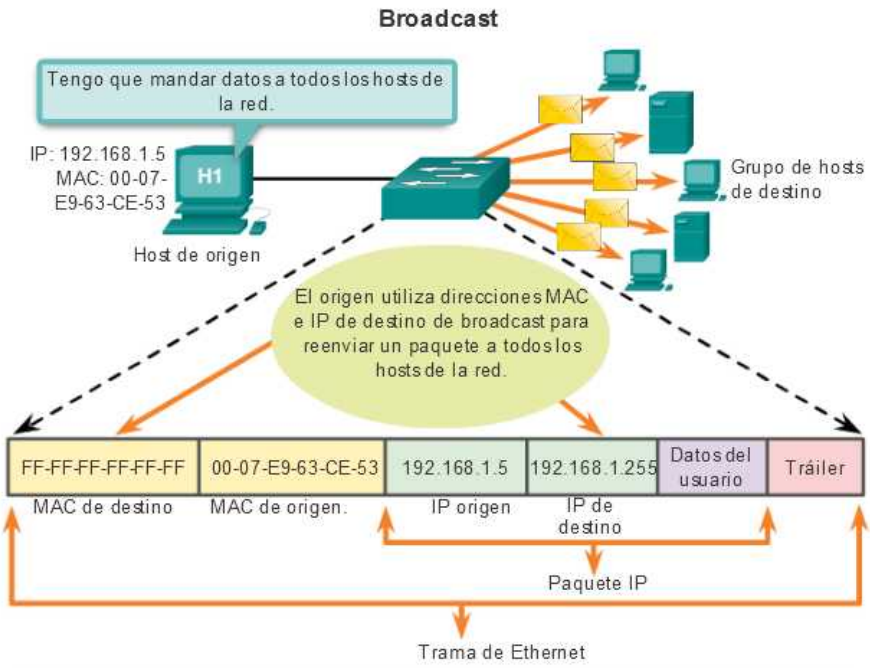
En Ethernet se utilizan distintas direcciones MAC para las comunicaciones unicast, broadcast y multicast de capa 2.

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



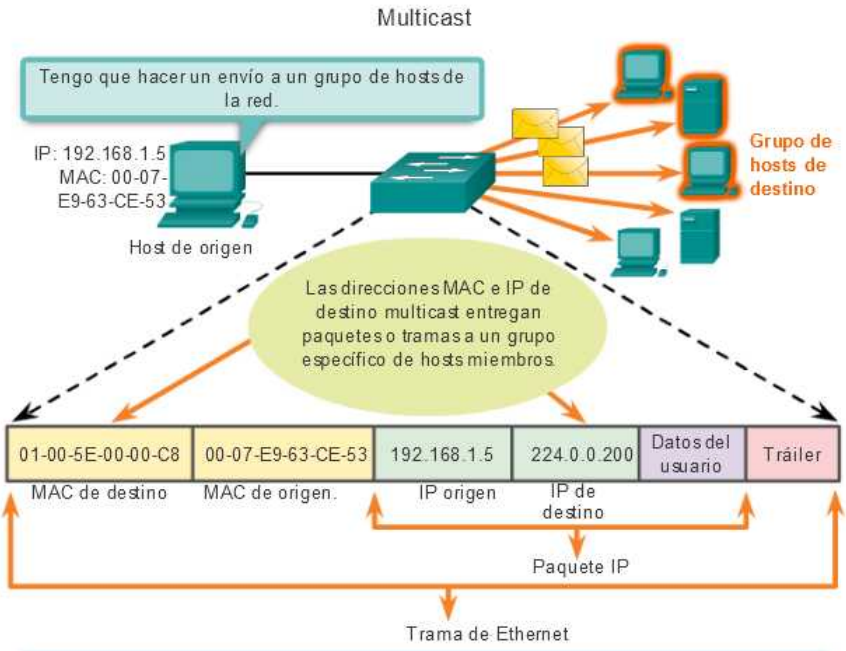
En el ejemplo que se muestra en la figura, un host con una dirección IP 192.168.1.5 (origen) solicita una página web del servidor en la dirección IP 192.168.1.200. Para que un paquete unicast sea enviado y recibido, la dirección IP de destino debe estar incluida en el encabezado del paquete IP. Además, 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 entrega de datos a un host de destino específico.

Los paquetes de **broadcast** contienen una dirección IP 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 local (dominio de broadcast) recibirán y procesarán el paquete. Muchos protocolos de red, como DHCP y el protocolo de resolución de direcciones (ARP), utilizan broadcasts. Más adelante en este capítulo se analizará cómo el ARP utiliza los broadcasts para asignar direcciones de Capa 2 a direcciones de Capa 3.



Como se muestra en la figura, una dirección IP de broadcast para una red requiere una dirección MAC de broadcast correspondiente en la trama de Ethernet. En las redes Ethernet, la dirección MAC de broadcast está compuesta por 48 unos, que se muestran como el valor hexadecimal FF-FF-FF-FF-FF-FF.

Las direcciones **multicast** le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Una dirección IP de grupo multicast se asigna a los dispositivos que pertenecen a un grupo multicast. El rango de direcciones IPv4 multicast va de 224.0.0.0 a 239.255.255.255. Debido a que las direcciones multicast representan un grupo de direcciones, sólo pueden utilizarse como el destino de un paquete. El origen siempre tendrá una dirección unicast.



Las direcciones multicast se pueden utilizar en juegos remotos, donde muchos jugadores se conectan de forma remota pero juegan al mismo juego; también se pueden utilizar en situaciones de educación a distancia donde muchos estudiantes se conectan a la misma clase.

Al igual que con las direcciones unicast y de broadcast, la dirección IP multicast requiere una dirección MAC multicast correspondiente para poder enviar tramas en una red local. La dirección MAC multicast es un valor especial que comienza con 01-00-5E en hexadecimal. La porción restante de la dirección MAC multicast se crea mediante la conversión de los 23 bits inferiores de la dirección IP del grupo multicast en 6 caracteres hexadecimales.

Un ejemplo de esto es la dirección hexadecimal multicast 01-00-5E-00-00-C8 de la figura.

MAC e IP

Existen dos direcciones principales asignadas a un dispositivo host:

- Dirección física (dirección MAC)
- Dirección lógica (dirección IP)

Tanto la dirección MAC como la dirección IP operan juntas para identificar un dispositivo en la red. El proceso de utilizar la dirección MAC y la dirección IP para encontrar una PC es similar al proceso de utilizar el nombre y la dirección de una persona para enviarle una carta.

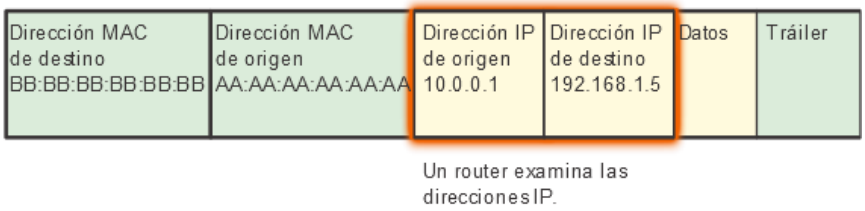
El nombre de una persona generalmente no cambia. Por otro lado, la dirección de una persona indica dónde vive esa persona y puede cambiar.

La dirección MAC en un host, como los nombres de las personas, no cambia; se asigna físicamente a la NIC del host y se conoce como “dirección física”. La dirección física es siempre la misma, independientemente del lugar en donde se encuentre el host.

La dirección IP es similar a la dirección de una persona. Esta dirección está basada en la ubicación real del host. Con esta dirección, la trama puede determinar la ubicación adonde se deben enviar las tramas. La dirección IP, o dirección de red, se conoce como “dirección lógica” porque se asigna de forma lógica. Un administrador de red asigna esta dirección a cada host sobre la base de la red local a la que el host está conectado. En la ilustración, se muestra la naturaleza jerárquica de la localización de una persona sobre la base de una dirección “lógica”. Haga clic en cada grupo para ver cómo se filtra la dirección.

Para que una computadora pueda comunicarse en una red jerárquica, se necesitan tanto la dirección MAC física como la dirección IP lógica, de la misma manera en la que se necesitan el nombre y la dirección de una persona para poder enviarle una carta.

Un dispositivo de origen envía un paquete sobre la base de una dirección IP. El servicio de nombres de dominios (DNS), en el que una dirección IP se asocia a un nombre de dominio, es una de las formas más comunes en que un dispositivo de origen determina la dirección IP de un dispositivo de destino. Por ejemplo, www.cisco.com equivale a 209.165.200.225. Esta dirección IP envía el paquete a la ubicación de red del dispositivo de destino.



Los routers utilizan esta dirección IP para determinar el mejor camino para llegar a destino.

Entonces, en resumen, el direccionamiento IP determina el comportamiento de extremo a extremo de un paquete IP.

Sin embargo, en cada enlace de la ruta, se encapsula un paquete IP en una trama específica de la tecnología de enlace de datos particular relacionada con ese enlace, como Ethernet. Los dispositivos finales en una red Ethernet no aceptan ni procesan

tramas según las direcciones IP. Por el contrario, las tramas se aceptan y procesan según las direcciones MAC.

En las redes Ethernet, las direcciones MAC se utilizan para identificar, en un nivel inferior, los hosts de origen y destino. Cuando un host de una red Ethernet se comunica, envía tramas que contienen su propia dirección MAC como origen y la dirección MAC del destinatario previsto como destino. Todos los hosts que reciben la trama leerán la dirección MAC de destino. El host procesa el mensaje solo si la dirección MAC de destino coincide con la dirección MAC configurada en su NIC.

MAC estática y dinámica

Una MAC estática es la que ha sido introducida en la CAM o Tabla de direcciones MAC de un switch a mano (tecleando un comando)

Una MAC dinámica es aquella que ha sido aprendida por el switch (normalmente vía peticiones y respuestas ARP) mirando las direcciones origen de las tramas que atraviesan sus puertos.

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

Protocolo de resolución de direcciones

ARP

Recuerde que cada nodo de una red IP tiene tanto una dirección MAC como una dirección IP. Para enviar datos, el nodo debe utilizar ambas direcciones. El nodo debe utilizar sus propias direcciones MAC e IP en los campos de origen y debe proporcionar una dirección MAC y una dirección IP para el destino. Mientras que una capa OSI superior proporciona la dirección IP del destino, pero el nodo de envío necesita encontrar la dirección MAC del destino para un enlace de Ethernet determinado. Ese es el propósito del protocolo ARP.

El protocolo ARP se basa en determinados tipos de mensajes Ethernet de broadcast y unicast, denominados “solicitudes ARP” y “respuestas ARP”.

El protocolo ARP ofrece dos funciones básicas:

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

Resolución de direcciones IPv4 a direcciones MAC

Para que una trama se coloque en los medios de la LAN, debe contar con una dirección MAC de destino. Cuando se envía un paquete a la capa de enlace de datos para que se encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de enlace de datos asignada a la dirección IPv4 de destino. Esta tabla se denomina tabla ARP o caché ARP. La tabla ARP se almacena en la RAM del dispositivo.

Cada entrada o fila de la tabla ARP vincula una dirección IP a una dirección MAC. La relación entre los dos valores se denomina mapa, que simplemente significa que usted puede localizar una dirección IP en la tabla y descubrir la dirección MAC correspondiente. En la tabla ARP, se guardan temporalmente (en caché) las asignaciones de los dispositivos en la LAN local.

Para comenzar el proceso, un nodo transmisor intenta localizar la dirección MAC asignada a un destino IPv4. Si se encuentra este mapa en la tabla, el nodo utiliza la dirección MAC como MAC de destino en la trama que encapsula el paquete IPv4. La trama se codifica entonces en los medios de la red.

Mantenimiento de la tabla ARP

La tabla ARP se mantiene dinámicamente. Existen dos maneras en las que un dispositivo puede reunir direcciones MAC. Una es monitorear el tráfico que se produce en el segmento de la red local. A medida que un nodo recibe tramas de los medios, puede registrar las direcciones IP y MAC de origen como mapeos en la tabla ARP. A medida que las tramas se transmiten en la red, el dispositivo completa la tabla ARP con los pares de direcciones.

Un dispositivo también puede obtener pares de direcciones mediante el envío de una solicitud de ARP, como se muestra en la ilustración. Una solicitud de ARP es un broadcast de capa 2 que se transmite a todos los dispositivos en la LAN Ethernet. La solicitud de ARP contiene la dirección IP del host de destino y la dirección MAC de broadcast, FFFF.FFFF.FFFF. Dado que se trata de un

broadcast, todos los nodos en la LAN Ethernet reciben y examinan el contenido. El nodo cuya dirección IP coincide con la dirección IP en la solicitud de ARP responde. La respuesta es una trama de unicast que incluye la dirección MAC que corresponde a la dirección IP en la solicitud. Esta respuesta se utiliza para crear una entrada nueva en la tabla ARP del nodo de envío.

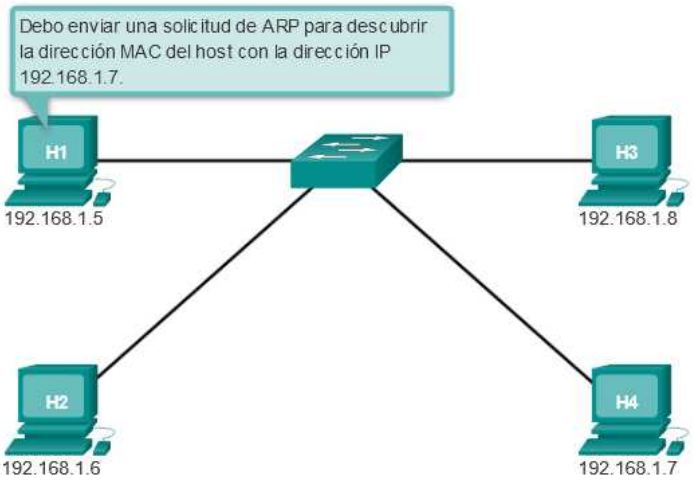
Las entradas en la tabla ARP tienen una marca de hora similar a la de las entradas de la tabla MAC en los switches. Si un dispositivo no recibe una trama de un dispositivo determinado antes de que caduque la marca horaria, la entrada para ese dispositivo se elimina de la tabla ARP.

Además, pueden ingresarse 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 deben eliminarse en forma manual.

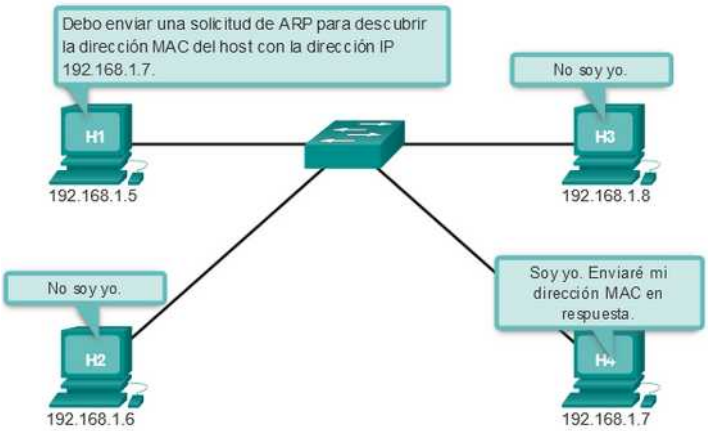
Creación de la trama

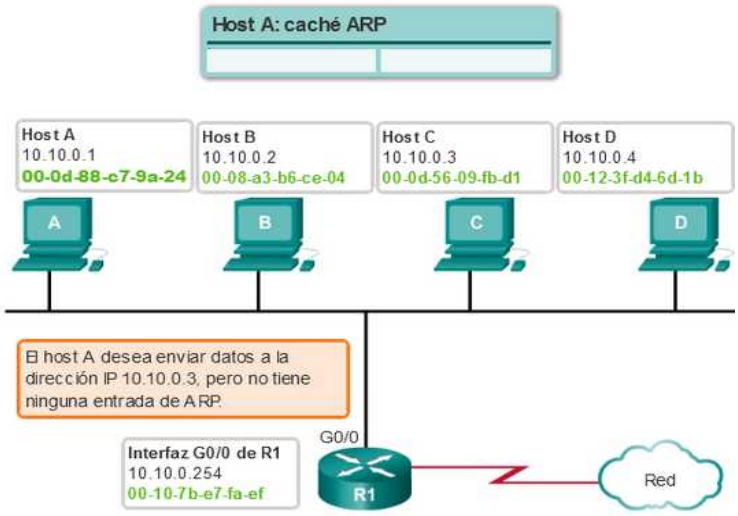
¿Qué hace un nodo cuando debe crear una trama y la caché ARP no contiene una asignación de una dirección IP hacia una dirección MAC de destino? Genera una solicitud de ARP.

Cuando el ARP recibe una solicitud para mapear una dirección IPv4 a una dirección MAC, busca el mapa almacenado en su tabla ARP. Si no encuentra la entrada, la encapsulación del paquete IPv4 no se realiza y los procesos de Capa 2 notifican al ARP que necesita un mapa. Los procesos ARP envían entonces un paquete de solicitud de ARP para descubrir la dirección MAC del dispositivo de destino de la red local. Si un dispositivo que recibe la solicitud tiene la dirección IP de destino, responde con una respuesta de ARP. Se crea un mapa en la tabla ARP. Los paquetes para esa dirección IPv4 pueden ahora encapsularse en tramas.



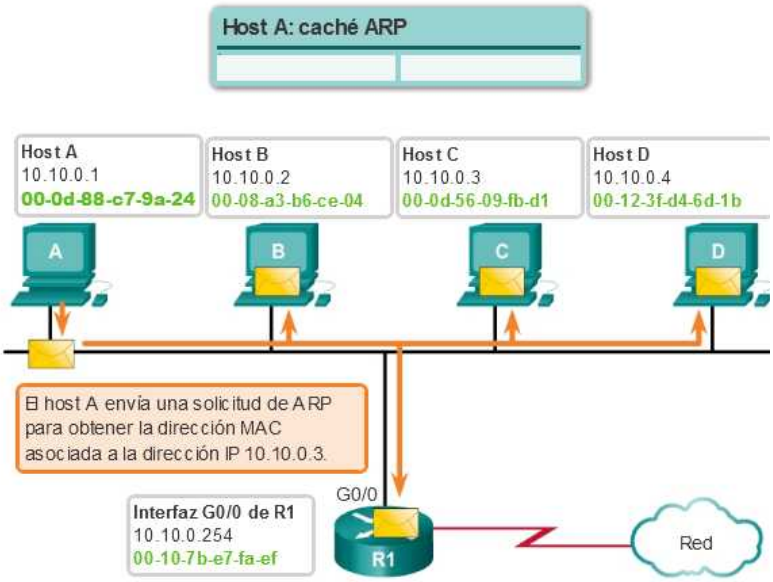
Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no puede crearse una trama. Esta falla de encapsulación se informa a las capas superiores del dispositivo. Si el dispositivo es un dispositivo intermediario, como por ejemplo, un router, las capas superiores pueden optar por responder al host de origen con un error en un paquete ICMPv4.





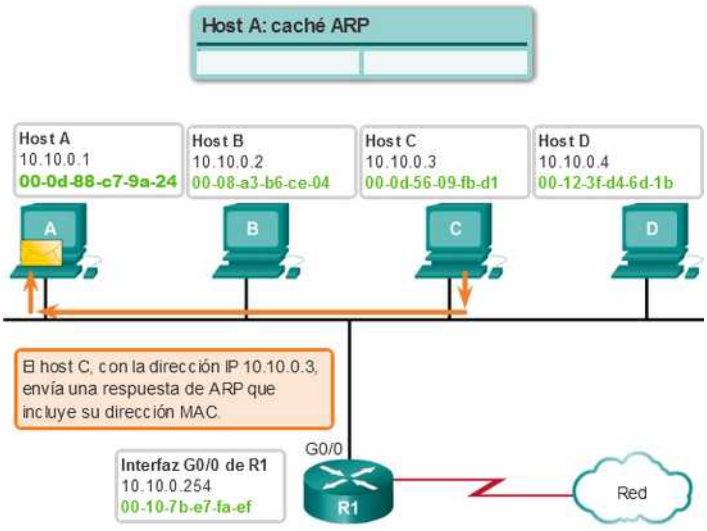
Todas las tramas deben enviarse a un nodo de un segmento de red local.

Si el host IPv4 de destino se encuentra en la red local, la trama utilizará la dirección MAC de este dispositivo como la dirección MAC de destino.

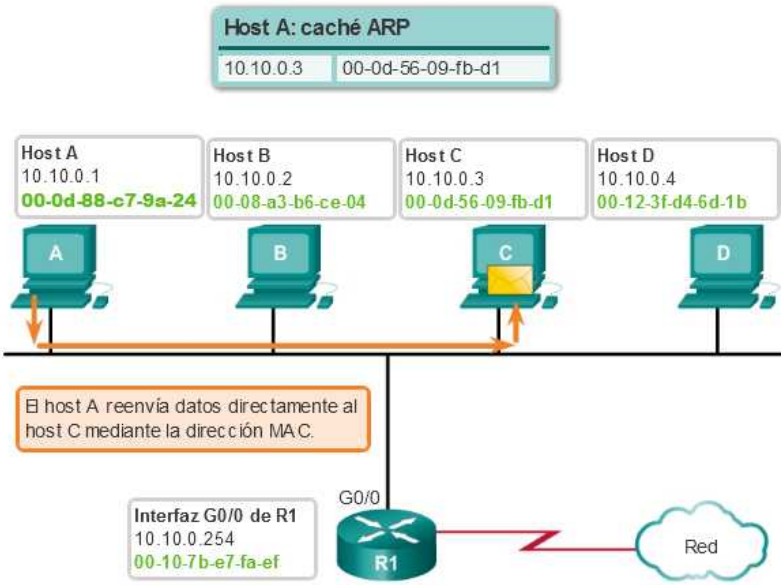


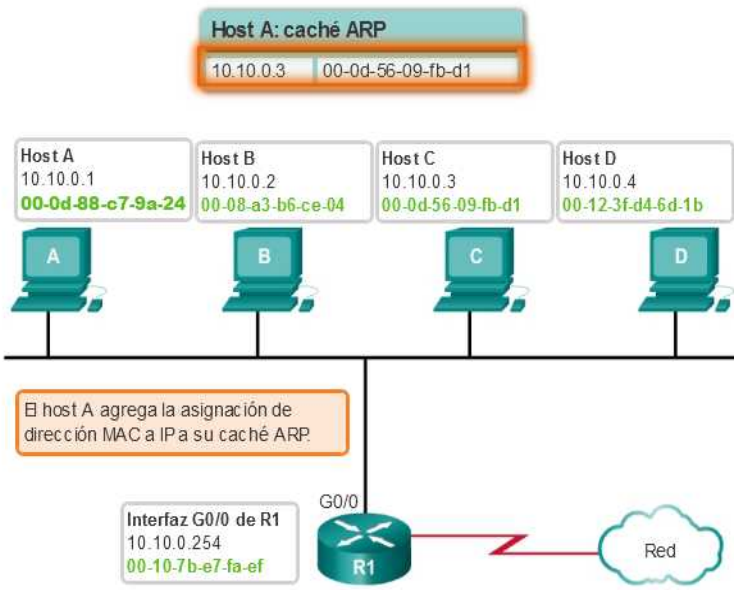
Reenvío de datos con información de dirección MAC

Respuesta de ARP con información de MAC

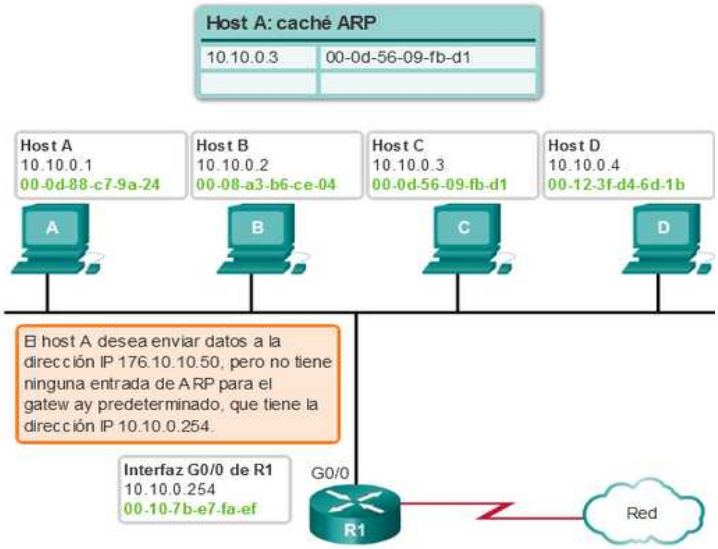


Agregado de asignación de MAC a IP en el caché ARP





El proceso de ARP: comunicación de forma remota

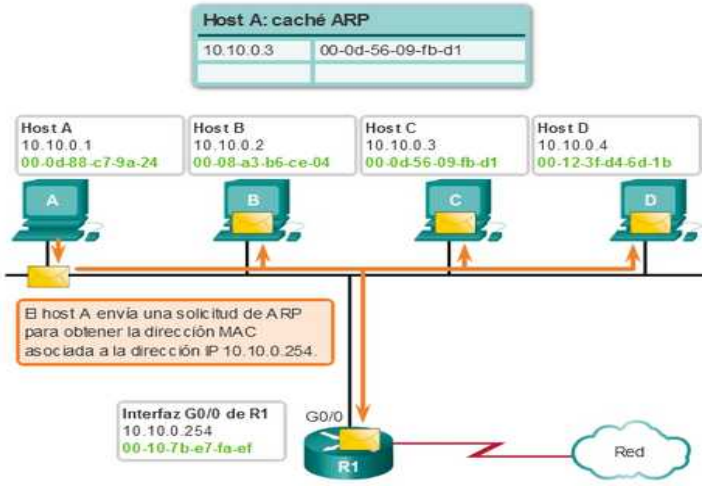


Si el host IPv4 de destino no se encuentra en la red local, el nodo de origen necesita enviar la trama a la interfaz del router. **El nodo de origen utilizará la dirección MAC del gateway como dirección de destino para las tramas que contengan un paquete IPv4 dirigido a hosts que se encuentren en otras redes.**

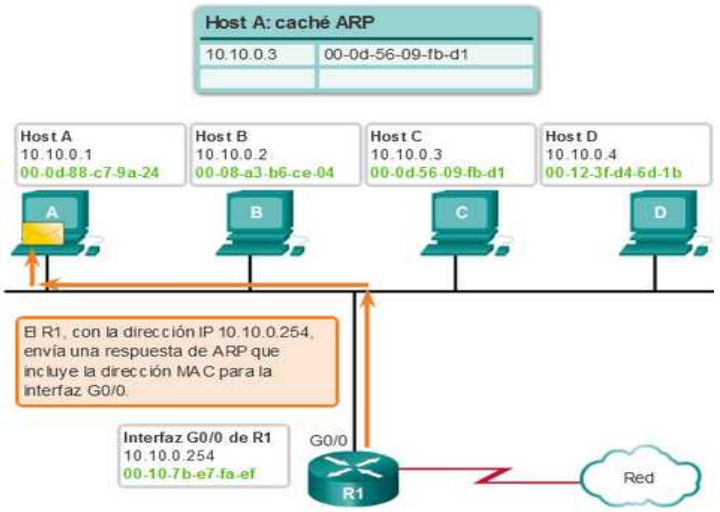
La dirección de gateway de la interfaz del router se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IP de destino con su propia dirección IP para determinar si las dos direcciones IP se encuentran en la misma red de Capa 3. Si el host receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del router que sirve de gateway.

En caso de que la entrada de gateway no se encuentre en la tabla, el proceso de ARP normal enviará una solicitud de ARP para recuperar la dirección MAC asociada con la dirección IP de la interfaz del router.

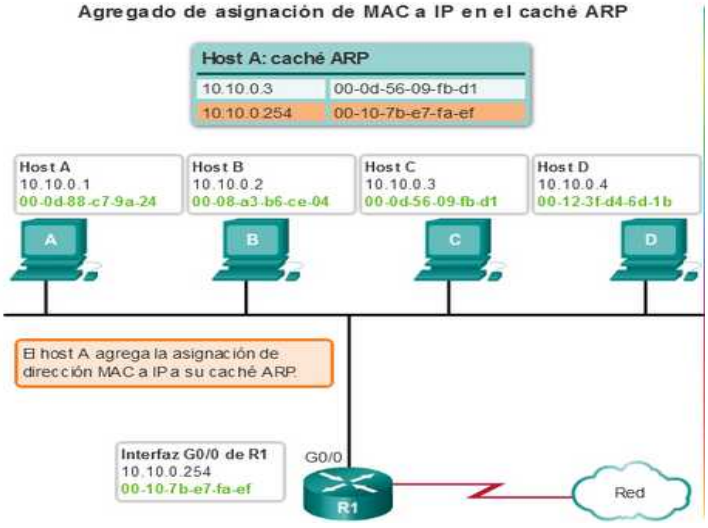
Transmisión de una solicitud de ARP



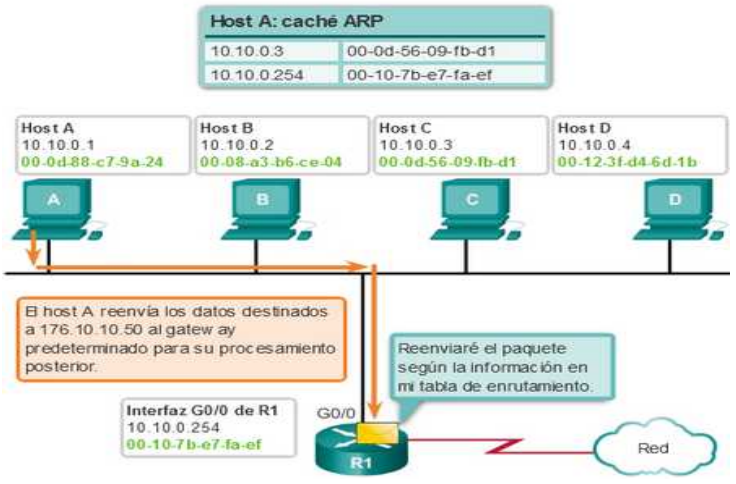
Respuesta de ARP con información de MAC



Agregado de asignación de MAC a IP en el caché ARP



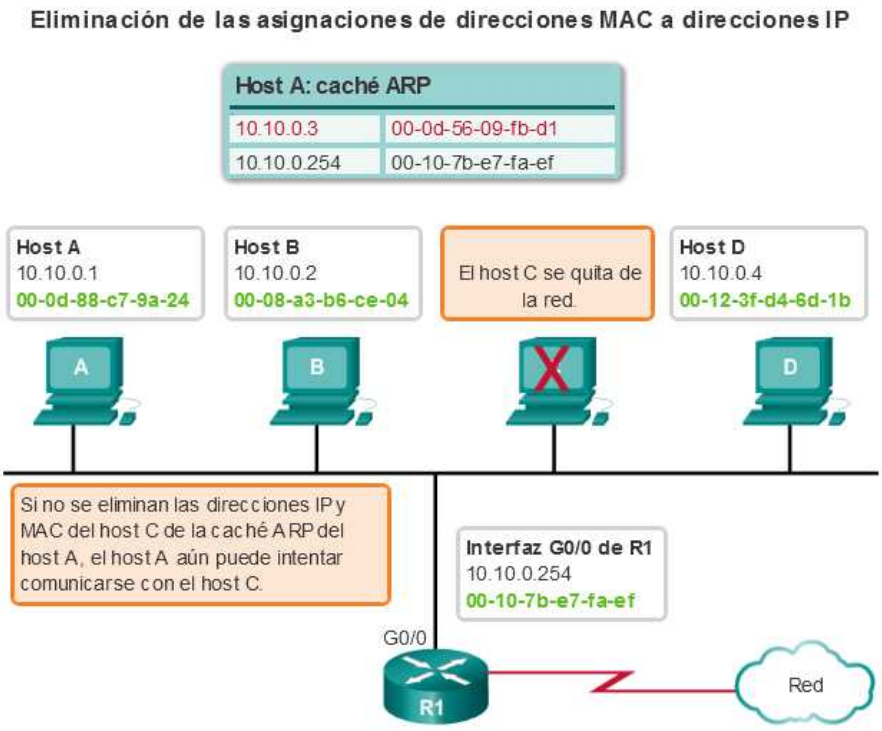
Reenvío de datos con información de dirección MAC



Para cada dispositivo, un temporizador de caché ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado. Los tiempos difieren dependiendo del dispositivo y su sistema operativo. Por ejemplo: algunos sistemas operativos de Windows almacenan las entradas de caché ARP por 2 minutos. Si la entrada se utiliza nuevamente durante ese tiempo, el temporizador ARP para esa entrada se extiende a 10 minutos.

También pueden utilizarse comandos para eliminar manualmente todas o algunas de las entradas de la tabla ARP. Después de eliminar una entrada, el proceso para enviar una solicitud de ARP y recibir una respuesta de ARP debe ocurrir nuevamente para ingresar la asignación en la tabla ARP.

Cada dispositivo tiene un comando específico del sistema operativo para eliminar el contenido de la caché ARP. Estos comandos de ninguna manera invocan la ejecución de ARP, sino que, simplemente, eliminan las entradas de la tabla ARP. El dispositivo integra el servicio ARP dentro del protocolo IPv4 y lo implementa. Su funcionamiento es transparente para aplicaciones y usuarios de capa superior.



Como se muestra en la ilustración, a veces es necesario eliminar una entrada de tabla ARP.

En un router Cisco, se utiliza el comando **show ip arp** para mostrar la tabla ARP

```
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
```

En un PC se utiliza el comando **arp -a** para mostrar la tabla ARP

```
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
```

Problemas de ARP

En la ilustración, se muestran dos problemas potenciales con el protocolo ARP.

Sobrecarga en los medios

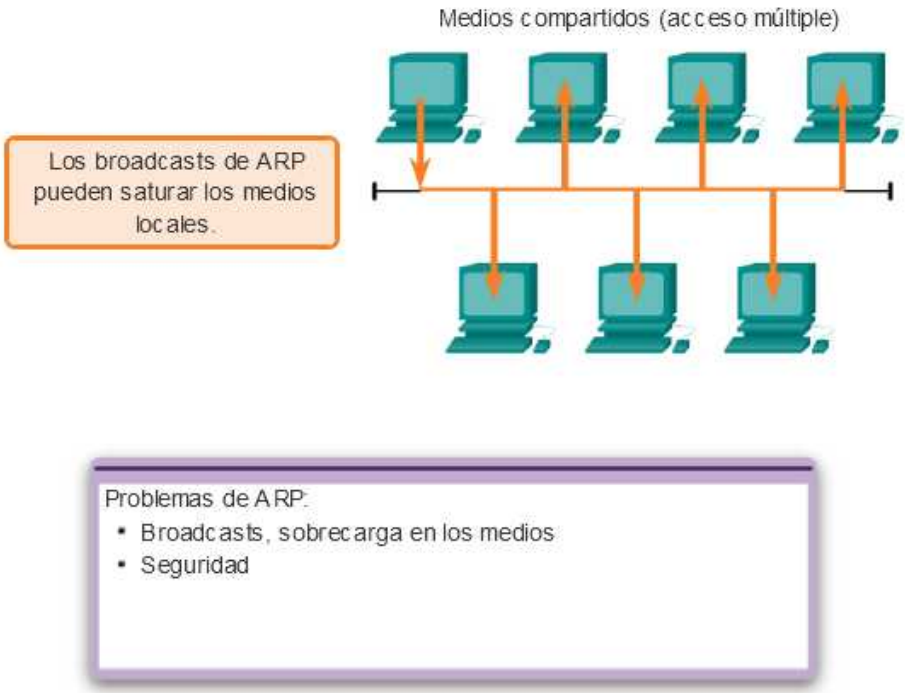
Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de broadcast. En una red comercial típica, estos broadcasts tendrían probablemente un impacto mínimo en el rendimiento de la red. Sin embargo, si un gran número de dispositivos se encendiera y todos comenzaran a acceder a los servicios de la red al mismo tiempo, podría haber una disminución del rendimiento durante un período de tiempo breve. Por ejemplo, si todos los estudiantes de una práctica de laboratorio inician sesión en computadoras del aula e intentan acceder a Internet al mismo tiempo, podría haber demoras. Sin embargo, una vez que los dispositivos envían los broadcasts de ARP iniciales y que aprenden las direcciones MAC necesarias, se minimizará todo impacto en la red.

Seguridad

En algunos casos, el uso del ARP puede ocasionar un riesgo potencial de seguridad. La suplantación o el envenenamiento ARP es una técnica que utiliza un atacante para introducir una asociación de direcciones MAC incorrecta en una red emitiendo respuestas ARP falsas. El individuo falsifica la dirección MAC de un dispositivo y de esta manera las tramas pueden enviarse a la dirección equivocada.

Configurar manualmente asociaciones ARP estáticas es una manera de impedir la suplantación de identidad de ARP.

Las direcciones MAC autorizadas pueden configurarse en algunos dispositivos de red para que limiten el acceso a la red para sólo los dispositivos indicados.Los switches modernos pueden mitigar los problemas de broadcast y de seguridad relacionados con ARP. Los switches Cisco admiten varias tecnologías de seguridad diseñadas específicamente para mitigar problemas de Ethernet relacionados con los broadcasts, en general, y con ARP, en particular.



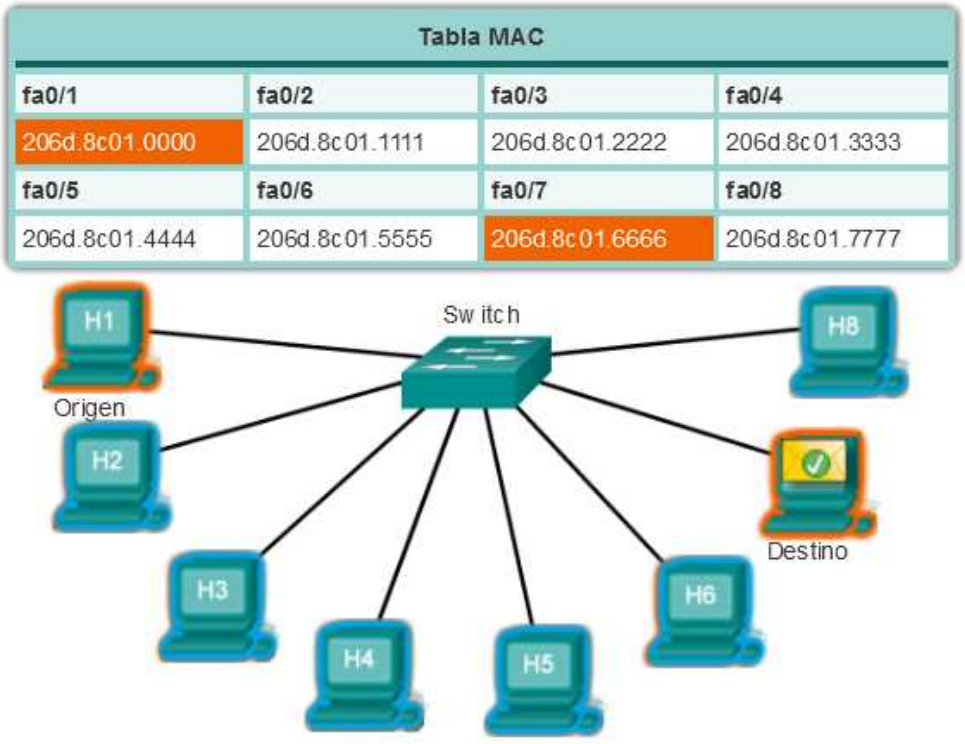
Los mensajes ARP falsos pueden proporcionar una dirección MAC incorrecta que luego toma control de las tramas que utilizan esa dirección (proceso denominado "suplantación").

Switches LAN

Conmutación

Recuerde que la topología lógica de una red Ethernet es un bus de multiacceso en el que todos los dispositivos comparten el acceso al mismo medio. Esta topología lógica determina la forma en que los hosts de la red ven y procesan las tramas enviadas y recibidas en la red. Sin embargo, en la actualidad, la topología física de la mayor parte de las redes Ethernet es en estrella y en estrella extendida. Esto significa que, en la mayoría de las redes Ethernet, los dispositivos finales se suelen conectar a un switch LAN de capa 2 de forma punto a punto.

Los switches LAN de capa 2 llevan a cabo los procesos de conmutación y filtrado basándose solamente en la dirección MAC de la capa de enlace de datos (capa 2) del modelo OSI. El switch es completamente transparente para los protocolos de red y las aplicaciones de usuario. Los switches de capa 2 crean una **tabla de direcciones MAC** que utilizan para tomar decisiones de reenvío. Los switches de capa 2 dependen de los routers para pasar datos entre subredes IP independientes.



Los switches emplean direcciones MAC para dirigir las comunicaciones de red a través de su estructura al puerto correspondiente hasta el nodo de destino. La estructura del switch son los circuitos integrados y la programación de máquina adjunta que permite controlar las rutas de datos a través del switch. El switch debe primero saber qué nodos existen en cada uno de sus puertos para poder definir cuál será el puerto que utilizará para transmitir una trama unicast.

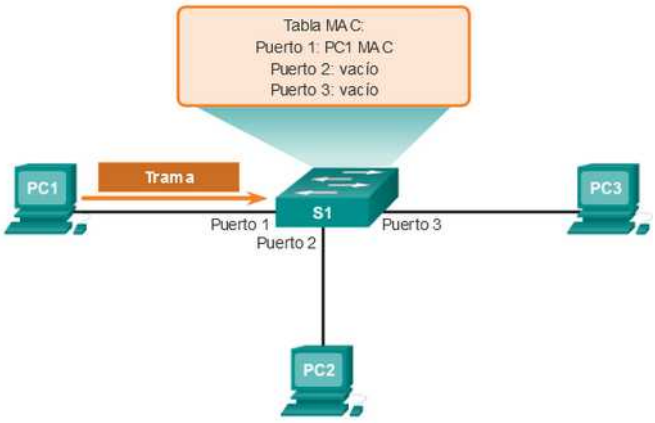
El switch determina cómo manejar las tramas de datos entrantes mediante una tabla de direcciones MAC. El switch genera su tabla de direcciones MAC grabando las direcciones MAC de los nodos que se encuentran conectados en cada uno de sus puertos. Una vez que la dirección MAC de un nodo específico en un puerto determinado queda registrada en la tabla de direcciones, el switch ya sabe enviar el tráfico destinado a ese nodo específico desde el puerto asignado a dicho nodo para posteriores transmisiones.

Cuando un switch recibe una trama de datos entrantes y la dirección MAC de destino no figura en la tabla, éste reenvía la trama a todos los puertos excepto al que la recibió en primer lugar. Cuando el nodo de destino responde, el switch registra la dirección MAC de éste en la tabla de direcciones del

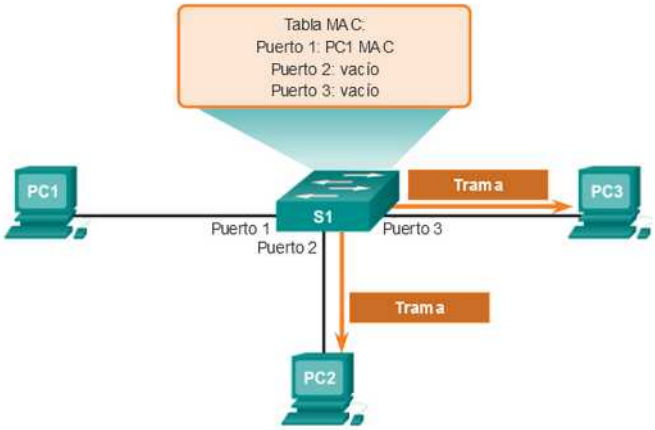
campo dirección de origen de la trama. En las redes que cuentan con varios switches interconectados, las tablas de direcciones MAC registran varias direcciones MAC para los puertos que conectan los switches que reflejan los nodos de destino. Generalmente, los puertos de los switches que se utilizan para interconectar dos switches cuentan con varias direcciones MAC registradas en la tabla de direcciones.

Paso 1. El switch recibe una trama de broadcast de la PC1 en el Puerto 1.

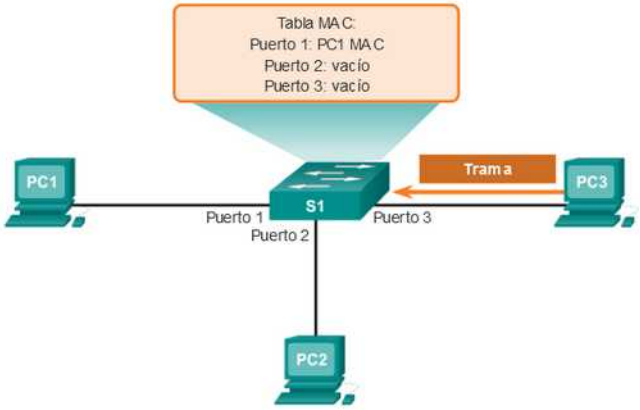
Paso 2. El switch ingresa la dirección MAC de origen y el puerto del switch que recibió la trama en la tabla de direcciones.



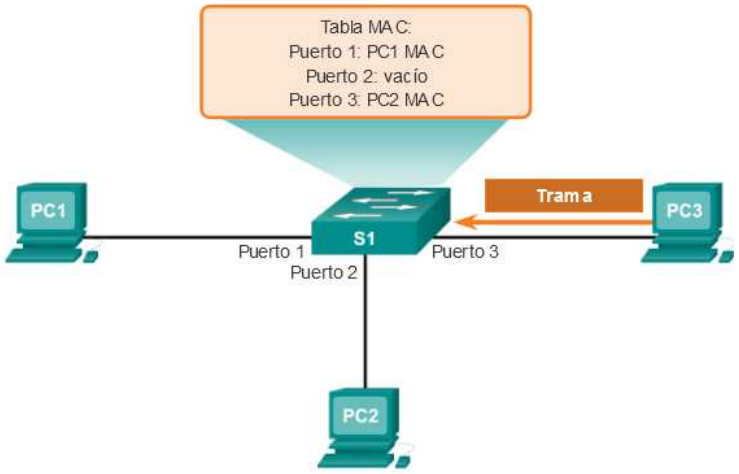
Paso 3. Dado que la dirección de destino es broadcast, el switch satura todos los puertos enviando la trama, excepto el puerto que la recibió.



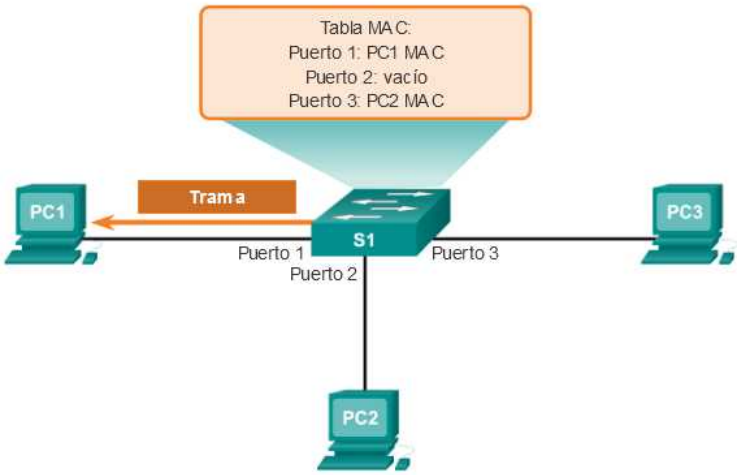
Paso 4. El dispositivo de destino (PC3) responde al broadcast con una trama de unicast dirigida al PC1.



Paso 5. El switch introduce en la tabla de direcciones la dirección MAC de origen del PC3 y el número del puerto de switch que recibió la trama. En la tabla de direcciones MAC pueden encontrarse la dirección de destino de la trama y su puerto asociado.



Paso 6. Ahora el switch puede enviar tramas entre los dispositivos de origen y destino sin saturar el tráfico, ya que cuenta con entradas en la tabla de direcciones que identifican a los puertos asociados.



Si bien los switches son transparentes para los protocolos de red y las aplicaciones de usuario, pueden funcionar en modos diferentes que pueden tener tanto efectos positivos como negativos al reenviar tramas de Ethernet en una red. Una de las configuraciones más básicas de un switch es la configuración de dúplex de cada puerto individual conectado a cada dispositivo host. Los puertos en los switches debe estar configurados para coincidir con la configuración de dúplex del tipo de medio. Existen dos tipos de configuraciones de dúplex que se utilizan para las comunicaciones en una red Ethernet: half duplex y full duplex.

Half duplex

La comunicación half-duplex se basa en un flujo de datos unidireccional en el que el envío y la recepción de datos no se producen al mismo tiempo. Esto es similar a la función de las radios de dos vías o dos walki-talkies en donde una sola persona puede hablar a la vez. Si una persona habla mientras lo hace la otra, se produce una colisión. Por ello, la comunicación half-duplex implementa el CSMA/CD con el objeto de reducir las posibilidades de que se produzcan colisiones y detectarlas en caso de que se presenten. Las comunicaciones half-duplex presentan problemas de funcionamiento debido a la constante espera, ya que el flujo de datos sólo se produce en una dirección a la vez. Las

conexiones half-duplex suelen verse en los dispositivos de hardware más antiguos, como los hubs. Los nodos que están conectados a los hubs y que comparten su conexión con un puerto de un switch deben funcionar en el modo half-duplex porque las computadoras finales deben tener la capacidad de detectar las colisiones. Los nodos pueden funcionar en el modo half-duplex si la tarjeta NIC no puede configurarse para hacerlo en full duplex. En este caso, el puerto del switch también adopta el modo half-duplex predeterminado. Debido a estas limitaciones, la comunicación full-duplex ha reemplazado a la half duplex en los elementos de hardware más modernos.

Full duplex

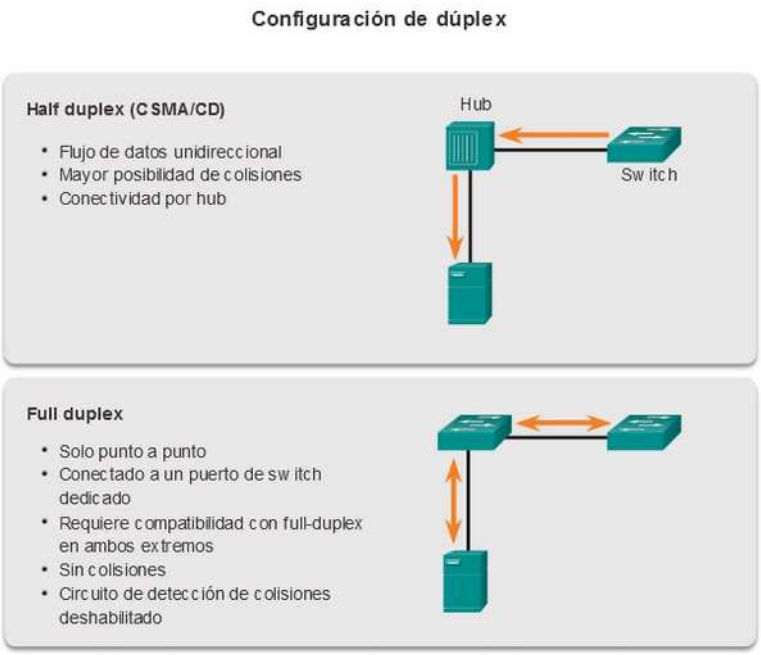
En las comunicaciones full-duplex el flujo de datos es bidireccional, por lo tanto la información puede enviarse y recibirse al mismo tiempo. La capacidad bidireccional mejora el rendimiento, dado que reduce el tiempo de espera entre las transmisiones. Actualmente, la mayoría de las tarjetas NIC Ethernet, Fast Ethernet y Gigabit Ethernet disponibles en el mercado proporciona capacidad full-duplex. En el modo full-duplex, el circuito de detección de colisiones se encuentra desactivado. Las tramas enviadas por los dos nodos finales conectados no pueden colisionar, dado que éstos utilizan dos circuitos independientes en el cable de la red. Cada conexión full-duplex utiliza un solo puerto. Las conexiones full-duplex requieren un switch que admita esta modalidad o bien una conexión directa entre dos nodos compatibles con el modo full duplex. Los nodos que se conecten directamente al puerto de un switch dedicado con tarjetas NIC capaces de admitir full duplex deben conectarse a puertos que estén configurados para funcionar en el modo full-duplex.

La figura muestra los dos parámetros dúplex que están disponibles en los equipos de red modernos.

Los switches Cisco Catalyst admiten tres configuraciones dúplex:

- La opción full establece el modo full-duplex.
- La opción half establece el modo half-duplex.
- La opción auto establece el modo autonegociación de dúplex. Cuando este modo se encuentra habilitado, los dos puertos se comunican para decidir el mejor modo de funcionamiento.

Para los puertos 10/100/1000 y Fast Ethernet la opción predeterminada es auto. Para los puertos 100BASE-FX, la opción predeterminada es full. Los puertos 10/100/1000 funcionan tanto en el modo half-duplex como en el full-duplex cuando se establecen en 10 ó 100 Mb/s, pero sólo funcionan en el modo full-duplex cuando se establecen en 1000 Mb/s.



Además de tener la configuración de dúplex correcta, también es necesario tener el tipo de cable adecuado definido para cada puerto. Antes, las conexiones entre dispositivos específicos, como las conexiones switch a switch, switch a router, switch a host y router a host, requerían el uso de tipos de cables específicos (de conexión cruzada o de conexión directa). Ahora, en cambio, la mayoría de los dispositivos de switch admiten el comando de configuración de interfaz **mdix auto** en la CLI para habilitar la característica automática de conexión cruzada de interfaz dependiente del medio (MDIX automática o auto-MDIX).

Al habilitar la función auto-MDIX, el switch detecta el tipo de cable que se requiere para las conexiones Ethernet de cobre y, conforme a ello, configura las interfaces. Por lo tanto, se puede utilizar un cable de conexión directa o cruzada 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 se habilita de manera predeterminada en los switches que ejecutan el software Cisco IOS, versión 12.2(18)SE o posterior. En el caso de las versiones existentes entre Cisco IOS, versión 12.1(14)EA1 y 12.2(18)SE, la función auto-MDIX se encuentra deshabilitada de manera predeterminada.

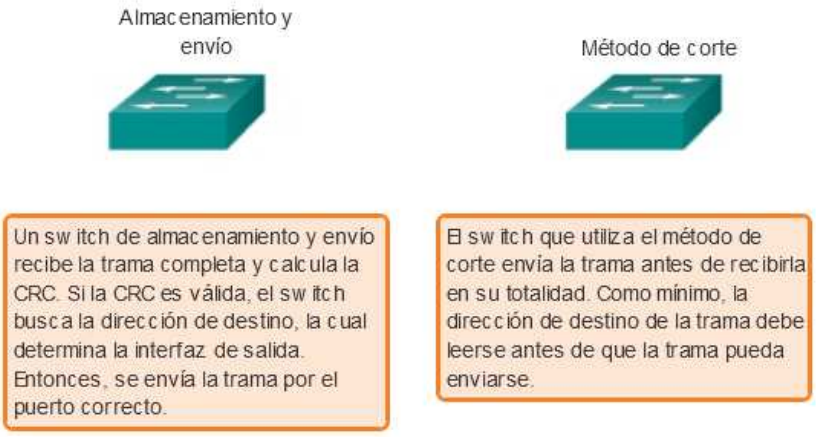
Anteriormente, los switches solían utilizar uno de los siguientes métodos de reenvío para conmutar datos entre los puertos de la red:

- Conmutación por almacenamiento y envío
- Conmutación por método de corte

Conmutación por almacenamiento y envío

En este tipo de conmutación, cuando el switch recibe la trama la almacena en los búferes de datos hasta recibir la trama en su totalidad. Durante el proceso de almacenamiento, el switch analiza la trama para buscar información acerca de su destino. En este proceso, el switch también lleva a cabo una verificación de errores utilizando la porción del tráiler de comprobación de redundancia cíclica (CRC) de la trama de Ethernet.

La CRC utiliza una fórmula matemática, basada en la cantidad de bits (1) de la trama, para determinar si ésta tiene algún error. Después de confirmar la integridad de la trama, ésta se envía desde el puerto correspondiente hasta su destino. Cuando se detecta un error en la trama, el switch la descarta. El proceso de descarte de las tramas con errores reduce la cantidad de ancho de banda consumido por datos dañados. La conmutación por almacenamiento y envío se requiere para el análisis de calidad de servicio (QoS) en las redes convergentes, en 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 exploración Web.



El método de almacenamiento y envío es el único método de reenvío que se utiliza en los modelos actuales de los switches Cisco Catalyst.

Conmutación por método de corte

En este tipo de conmutación, el switch actúa sobre los datos apenas los recibe, incluso si la transmisión aún no se ha completado. El switch recopila en el búfer sólo la información suficiente de la trama como para leer la dirección MAC de destino y así 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 su tabla de conmutación, 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. Dado que el switch no tiene que esperar que la trama se almacene de manera completa en el búfer y que no realiza ninguna verificación de errores, la conmutación por método de corte es más rápida que la de almacenamiento y envío. No obstante, al no llevar a cabo ninguna verificación de errores, el switch reenvía tramas dañadas a través de la red. Las tramas dañadas consumen ancho de banda mientras se reenvían. Al final, la NIC de destino descarta las tramas dañadas.

A continuación, se presentan dos variantes de la conmutación por método de corte:

- **Conmutación por envío rápido:** este tipo de conmutación ofrece el nivel más bajo de latencia. La conmutación por envío rápido reenvía el paquete inmediatamente después de leer la dirección de destino. Como la conmutación por envío rápido comienza a reenviar el paquete antes de haberlo recibido en forma completa, es probable que a veces los paquetes se entreguen con errores. Esto ocurre con poca frecuencia y el adaptador de red de destino descarta los paquetes defectuosos en el momento de su recepción. En el modo de envío rápido, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. La conmutación por envío rápido es el típico método de corte.
- **Conmutación libre de fragmentos:** en este método, el switch almacena los primeros 64 bytes de la trama antes de hacer el reenvío. Este tipo de conmutación se puede definir como un punto intermedio entre la conmutación por almacenamiento y envío y la conmutación por método de corte. El motivo por el cual la conmutación libre de fragmentos almacena sólo 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 método de conmutación libre de fragmentos intenta mejorar la conmutación por envío rápido mediante una pequeña verificación de errores en los primeros 64 bytes de la trama, a fin de asegurar que no se hayan producido colisiones antes de reenviar la trama. La conmutación libre de fragmentos es un punto intermedio entre el alto nivel de latencia y la gran integridad que ofrece la conmutación por almacenamiento y envío, y el bajo nivel de latencia y la integridad reducida que brinda la conmutación por envío rápido.

Algunos switches se configuran para realizar una conmutación por método de corte por puerto hasta llegar a un umbral de error definido por el usuario y luego cambian la conmutación al modo de almacenamiento y envío. Si el índice de error está por debajo del umbral, el puerto vuelve automáticamente a la conmutación por método de corte.

Según lo analizado, un switch examina parte de un paquete, o su totalidad, antes de reenviarlo al host de destino. Un switch Ethernet puede usar una técnica de bufferes para almacenar tramas antes de enviarlas. El almacenamiento en buffers también puede utilizarse cuando el puerto de destino está ocupado debido a una congestión. El switch almacena la trama hasta el momento en que pueda transmitirse.

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

Búfer de memoria basada en puerto

En el búfer de memoria basado 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 tramas que están delante de ella en la cola se hayan transmitido con éxito. Es posible que una sola trama retarde la transmisión de todas las tramas almacenadas en la memoria debido al tráfico del puerto de destino. Este retraso se produce aunque las demás tramas puedan transmitirse a puertos de destino abiertos.

Almacenamiento en 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 en el búfer se vinculan de forma dinámica al puerto de destino. Esto permite que se pueda recibir el paquete por un puerto y se pueda transmitir por otro puerto, sin tener que colocarlo en otra cola.

Memoria basada en puerto	En el búfer de memoria basado en puerto, las tramas se almacenan en colas conectadas a puertos de entrada y de salida específicos.
Memoria compartida	El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch.

El switch conserva un mapa de enlaces de trama a puerto que indica dónde debe transmitirse el paquete. El enlace del mapa se elimina una vez que la trama se ha transmitido con éxito. La cantidad de tramas almacenadas en el búfer se encuentra limitada por el tamaño del búfer de memoria en su totalidad y no se limita a un solo búfer de puerto. Esto permite la transmisión de tramas más amplias y que se descarte una menor cantidad de ellas. Esto es muy importante para la conmutación asimétrica. La conmutación asimétrica permite diferentes velocidades de datos en diferentes puertos. Esto permite que se dedique más ancho de banda a ciertos puertos, como un puerto conectado a un servidor.

Las líneas de productos de switches Cisco se utilizan a gran escala en todo el mundo, en gran parte debido a la flexibilidad que proporcionan para opciones complementarias. Cisco IOS no solo tiene el conjunto más completo de características disponibles en relación con cualquier otro sistema operativo de red, sino que además el IOS está diseñado a la medida de cada dispositivo de red de Cisco, en especial, los switches.

Factores de forma del switch

Switches de configuración fija
Las características y opciones se limitan a las que vienen originalmente con el switch.

Switches de configuración modular
El bastidor admite tarjetas de línea que contienen puertos.

Switches de configuración apilable
Los switches apilables, que se conectan mediante un cable especial, funcionan eficazmente como si fuesen un switch grande.

Fija o modular

Las líneas de productos de switches Cisco se utilizan a gran escala en todo el mundo, en gran parte debido a la flexibilidad que proporcionan para opciones complementarias. Cisco IOS no solo tiene el conjunto más completo de características disponibles en relación con cualquier otro sistema operativo de red, sino que además el IOS está diseñado a la medida de cada dispositivo de red de Cisco, en especial, los switches.

Para ilustrar las opciones disponibles, que son realmente demasiadas para enumerarlas aquí, nos enfocamos en los switches Catalyst 3560. Los switches Catalyst 3560 tienen puertos de factor de forma conectable pequeño (SFP) que admiten una cantidad de módulos de transceptor SFP. Aquí se presenta una lista de los módulos SFP admitidos en uno o más tipos de switches 3560:

Módulos SFP Fast Ethernet:

- 100BASE-FX (fibra óptica multimodo [MMF]) para 2 km
- 100BASE-LX10 (fibra óptica monomodo [SMF]) para 2 km
- 100BASE-BX10 (SMF) para 10 km
- 100BASE-EX (SMF) para 40 km
- 100BASE-ZX (SMF) para 80 km

Módulos SFP Gigabit Ethernet:

- 1000BASE-SX de 50/62,5 µm (MMF), hasta 550/220 m
- 1000BASE-LX/LH (SMF/MMF), hasta 10 km/0,550 km, respectivamente
- 1000BASE-ZX (SMF), hasta 70 km
- 1000BASE-BX10-D y 1000BASE-BX10-U (SMF), hasta 10 km
- 1000BASE-T (transceptor de hilos de cobre)

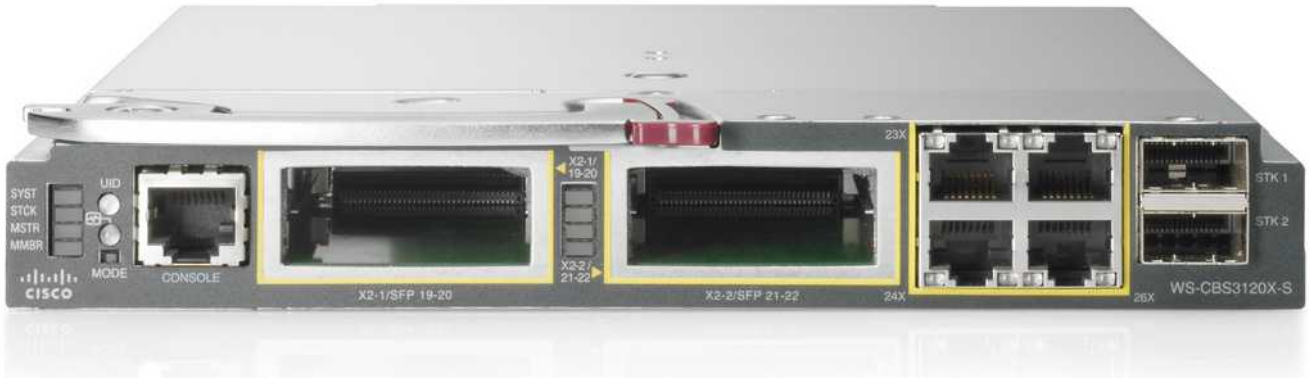
Módulos SFP de 10 Gigabit Ethernet:

- 10G-SR (MMF), hasta 400 m
- 10G-SR-X (MMF), hasta 400 m (admiten un intervalo de temperatura extendido)
- 10G-LRM (MMF), hasta 220 m
- FET-10G (MMF), hasta 100 m (para uplinks de estructura Nexus)
- 10G-LR (SMF), hasta 10 km
- 10G-LR-X (SMF), hasta 10 km (admiten un intervalo de temperatura extendido)
- 10G-ER (SMF), hasta 40 km
- 10G-ZR (SMF), hasta 80 km
- Cable de conductores axiales retorcidos (transceptor de hilos de cobre), hasta 10 m
- Fibra óptica activa, hasta 10 m (para conexiones entre bastidores e intrabastidor)

Los módulos 40 Gigabit Ethernet y 100 Gigabit Ethernet son compatibles con los dispositivos Cisco de alta gama, como Catalyst 6500, el router CRS, el router de la serie ASR 9000 y el switch de la serie Nexus 7000.

switches modulares

Los switches modulares están diseñados con ranuras que permiten insertar tarjetas en linea que le proporcionan nuevas funcionalidades, de tal forma que es posible agregar mas puertos Fast Ethernet, Modems o puertos de conexión Gigabit Ethernet, claro está que el switch en cuestión solo soporta un número y modelos determinados de tarjetas.



Transceptores SFP

Un transceptor es un dispositivo que cuenta con **un transmisor y un receptor** que comparten parte de la circuitería o se encuentran dentro de la misma caja.

El módulo de factor de forma pequeño (SFP: **Small Form-factor Pluggable**) es un transceptor (en inglés transceiver) modular óptico de intercambio dinámico para conectar dos equipos de telecomunicaciones, normalmente switches o routers…

Los módulos **SFP** fueron desarrollados para velocidades de **1 Gbit/s**. No todos son ópticos (los hay de cobre) y los hay de muchos más tipos que 1000BaseSX ó 1000BaseLX (como por ejemplo, hay SFP de 1000BaseT, 1000BaseZX, SONET/SDH).

El transceptor SFP no ha sido estandarizado por ningún organismo de normalización oficial, sino que se especifica mediante un acuerdo multi-fuente entre fabricantes competidores. SFP fue diseñado después de la interfaz GBIC, y permite una mayor densidad de puertos (número de transceptores por cm a lo largo del borde de una placa) que el GBIC, que es la razón por la SFP también se conoce como mini-GBIC.

La versión mejorada de Small Form Factor Pluggable (**SFP+**) admite velocidades de datos de hasta **10 Gbit/s**. La especificación SFP+ se publicó el 9 de mayo de 2006, y la versión 4.1 fue publicada el 6 de julio de 2009. SFP+ soporta 10 Gigabit Ethernet y 8 Gbit/s en redes Fibre Channel (usadas comúnmente en redes Storage Area Networks (SAN)). Es un formato popular de la industria con el apoyo de muchos fabricantes de componentes de red.

Transceptores CFP

El módulo de factor de forma C (**CFP: C Form-factor Pluggable**) es un transceptor para la transmisión de señales digitales de alta velocidad. La C indica la letra latina C para expresar el número 100 (centum), ya que el estándar fue desarrollado principalmente para sistemas Ethernet 100 Gigabit.

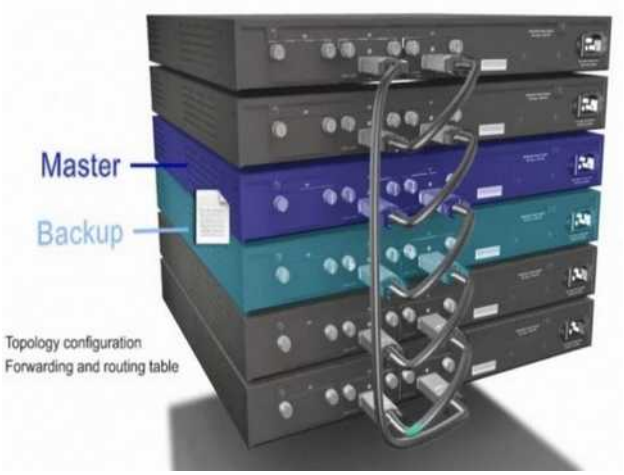
El transceptor CFP se especifica mediante un acuerdo multi-fuente entre fabricantes competidores. El CFP fue diseñado posteriormente a la interface SFP, pero es significativamente más rápido para soportar **40 y 100 Gbit/s**.

Switch apliable

A esta configuración de switch se les conoce como en stack o stackwise. Se trata de conectar con cables de alta velocidad varios switches, el objetivo es obtener tolerancia a fallos, ofreciendo una configuración redundante.

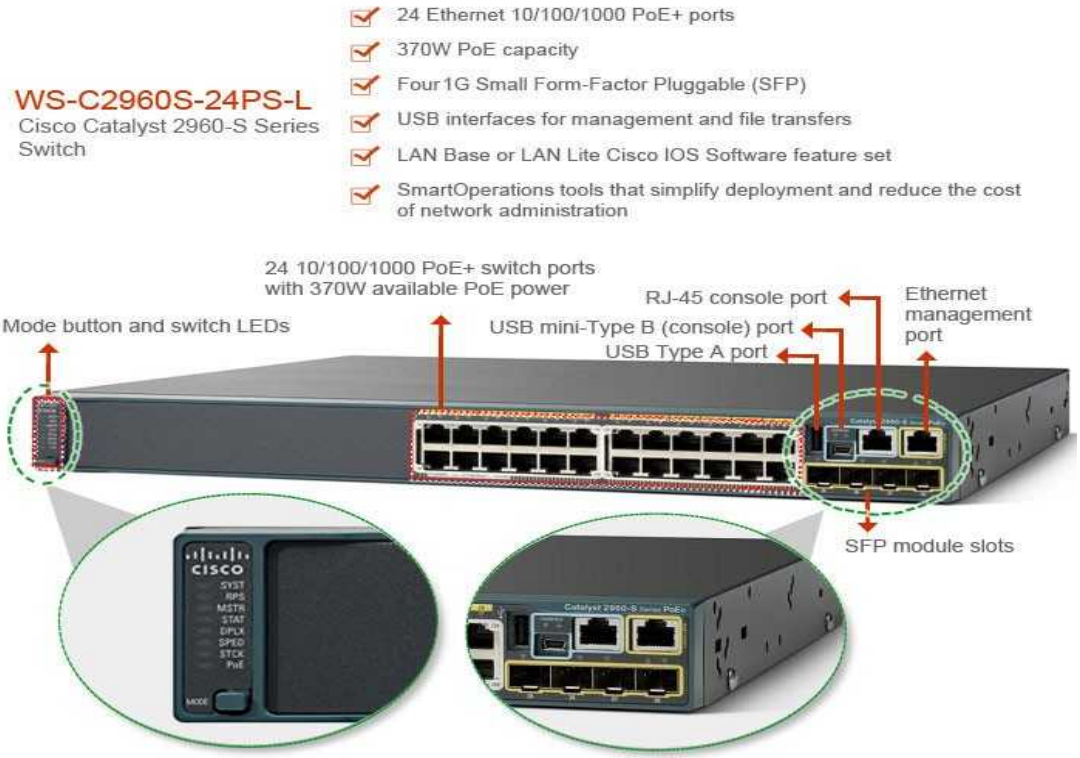
Un grupo de switches (stack) puede apilarse (uniéndolos con enlaces de alta velocidad) y comportarse como un único switch con la capacidad de puertos de la suma de todos ellos. Por ejemplo 12 swiches de 48 puertos cada uno, equivalen a un switch de 576 puertos.

Los enlaces que unen los switch del stack pueden alcanzar los 20 Gbps.



Dentro de la pila (stack) existe un switch maestro y otro de respaldo (backup). El switch Master y el Backup se sincronizan constantemente para tener la misma configuración Si el Master falla, el Backup se convierte en el nuevo Master y otro switch del stack toma el rol de Backup.

Los switches de configuración apilable se pueden interconectar mediante un cable especial que proporciona un rendimiento de ancho de banda alto entre los switches. La tecnología Cisco StackWise permite la interconexión de hasta nueve switches. Los switches se pueden apilar unos sobre otros con cables que conectan los switches en forma de cadena margarita. Los switches apilados operan con efectividad como un switch único más grande. Los switches apilables son convenientes cuando la tolerancia a fallas y la disponibilidad de ancho de banda son críticas y resulta costoso implementar un switch modular. El uso de conexiones cruzadas hace que la red pueda recuperarse rápidamente si falla un switch único. Los switches apilables usan un puerto especial para las interconexiones. Muchos switches apilables Cisco también admiten la tecnología StackPower, que permite compartir la alimentación entre los miembros de la pila.



El puerto de consola

Algunos switches (además de los routers) disponen de un puerto especial, denominado **Console Port**. Este puerto es muy importante pues permite realizar la configuración del dispositivo a través de él de forma directa. **Es necesario un cable rollover**.

El cable Rollover (también conocido como cable de consola Cisco o cable Yost) es un tipo de cable de módem nulo que se utiliza a menudo para conectar un terminal de ordenador al puerto de consola del switch o router. Este cable es generalmente plano (y tiene un color azul claro) para ayudar a distinguirlo de otros tipos de cableado de red.

Se pone el nombre de rollover debido a las patillas en un extremo se invierten de el otro.

Port security

Es una característica de los switches Cisco que nos permite retener las direcciones MAC conectadas a un puerto y permitir solamente esas direcciones MAC registradas comunicarse a través de ese puerto del switch.

Nos permite:

- Restringir el acceso a los puertos del switch según la MAC.
- Restringir el número de MACs por puerto en el switch.
- Reaccionar de diferentes maneras a violaciones de las restricciones anteriores.
- Establecer la duración de las **asociaciones MAC-Puerto**.

Si un dispositivo **con otra dirección MAC** intenta comunicarse a través de un puerto de la LAN, **port-security deshabilitará el puerto**.

Port mirroring (Puerto espejo)

Es una función que tienen los switches para copiar todo el tráfico de un puerto específico a otro puerto. Esta función generalmente se utiliza para atrapar todo el tráfico de una red y poder analizarlo (con herramientas como **wireshark** por ejemplo).

El puerto espejo en un sistema de switch **Cisco** generalmente se refiere a un Analizador de Puertos del switch (**Switched Port Analyzer: SPAN**) algunas otras marcas usan otros nombres para esto, tal como Roving Analysis Port (RAP) en los switches 3Com.

MACsec

Media Access Control de Seguridad (MACsec) es una tecnología de seguridad estándar de la industria que proporciona una comunicación segura para todo el tráfico en enlaces Ethernet. MACsec proporciona seguridad de punto a punto de enlaces Ethernet entre nodos conectados directamente-y es capaz de identificar y prevenir la mayoría de las amenazas a la seguridad, incluida la denegación

de servicio, intrusión, man-in-the-middle, enmascaramiento, las escuchas telefónicas pasivo, y los ataques de reproducción. MACsec está estandarizado en IEEE 802.1AE.

Una vez que un enlace punto a punto Ethernet ha habilitado MACsec, todo el tráfico que atraviesa el enlace es asegurado mediante el uso de controles de **integridad de datos y cifrado si se desea**.

Las comprobaciones de integridad de datos verifican la integridad de los datos en ambos lados del enlace asegurado Ethernet. MACsec añade una cabecera de 8 bytes y una cola de 16 bytes a todas las tramas Ethernet que atraviesan el enlace, y la cabecera y la cola son revisados por la interfaz de recepción para asegurar que los datos no se vieron comprometidos al atravesar el enlace. Si la comprobación de integridad de datos detecta algo irregular sobre el tráfico , el tráfico se desecha.

MACsec también se puede utilizar para cifrar todo el tráfico en el enlace Ethernet. El cifrado utilizado por MACsec asegura que los datos de la trama Ethernet no pueden ser vistos por cualquier persona al monitorear el tráfico en el enlace. El cifrado MACsec es opcional y configurable por el usuario.

CDP

CDP (**Cisco Discovery Protocol**, 'protocolo de descubrimiento de Cisco', es un **protocolo de red propietario** de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos. Es utilizado para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP. CDP también puede ser usado para realizar encaminamiento bajo demanda (ODR, On-Demand Routing), que es un método para incluir información de encaminamiento en anuncios CDP, de forma que los protocolos de encaminamiento dinámico no necesiten ser usados en redes simples.

Los dispositivos Cisco envían anuncios a la dirección de destino de multidifusión. Los anuncios CDP (si está soportados y configurados en el IOS) se envían por defecto cada 60 segundos en las interfaces que soportan cabeceras SNAP, incluyendo Ethernet, Frame Relay y ATM. Cada dispositivo Cisco que soporta CDP almacena la información recibida de otros dispositivos en una tabla que puede consultarse usando el comando show cdp neighbor. La información de la tabla CDP se refresca cada vez que se recibe un anuncio y la información de un dispositivo se descarta tras tres anuncios no recibidos por su parte (tras 180 segundos usando el intervalo de anuncio por defecto).

La información contenida en los anuncios CDP varía con el tipo de dispositivo y la versión del sistema operativo que corra. Dicha información incluye la versión del sistema operativo, el nombre de equipo, todas la direcciones de todos los protocolos configurados en el puerto al que se envía la trama CDP (por ejemplo, la dirección IP), el identificador del puerto desde el que se envía el anuncio, el tipo y modelo de dispositivo, la configuración duplex/simplex, el dominio VTP, la VLAN nativa, el consumo energético (para dispositivos PoE) y demás información específica del dispositivo. El protocolo está habilitado por defecto en todos las interfaces de los equipos CISCO. Para deshabilitarlo de forma global se utiliza el comando **no cdp run** en modo enable y para deshabilitarlo en una interfaz concreta se utiliza el comando **no cdp enable** en la configuración de dicha interfaz o rango de interfaces. **Es recomendable desactivarlo en las interfaces hacia los PC's por motivos de seguirdad**

CDP es un protocolo exclusivo de Cisco que se ejecuta en la capa de enlace de datos. Debido a que el protocolo CDP funciona en la capa de enlace de datos, es posible que dos o más dispositivos de red Cisco obtengan información de los demás incluso si no hay conectividad de capa 3. En situaciones de detección de redes, la dirección IP del vecino con CDP suele ser la única información necesaria para conectarse a ese dispositivo mediante Telnet.

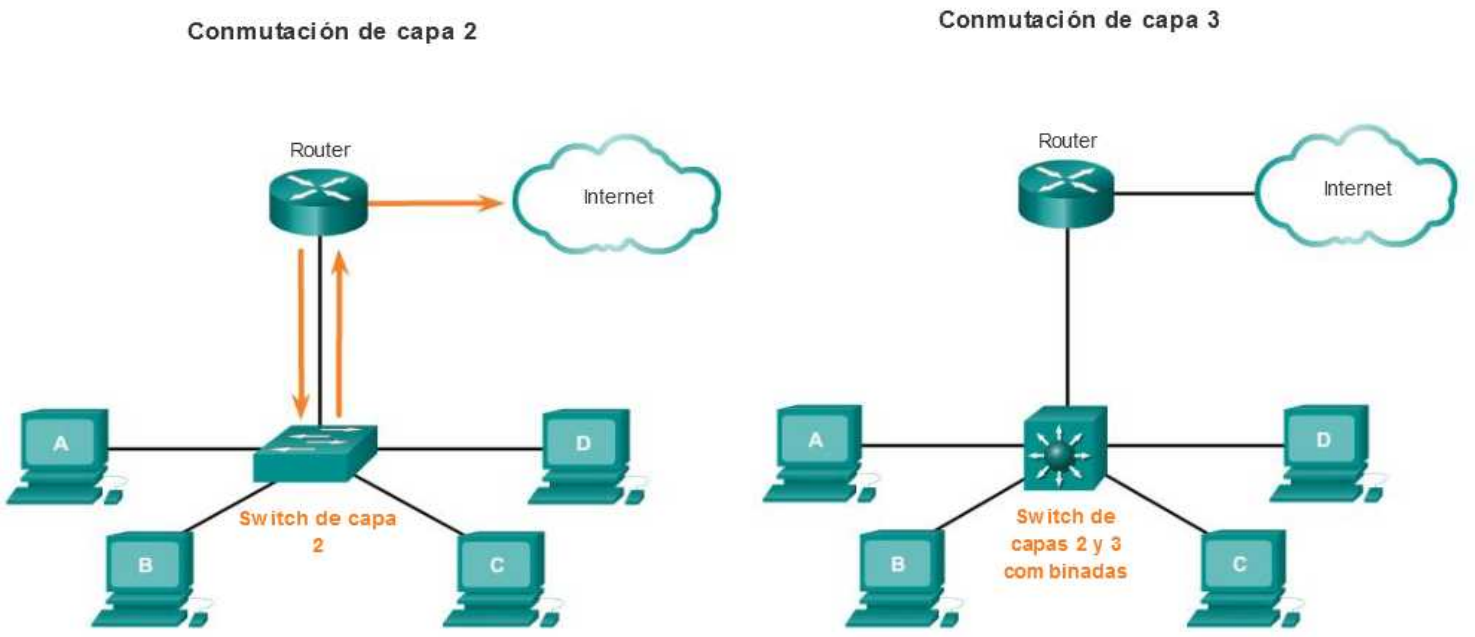
Conmutación de capa 3

Además de determinar los diversos factores de forma de switch, es posible que también sea necesario elegir entre un switch LAN de capa 2 y un switch de capa 3.

Recuerde que los switches LAN de capa 2 llevan a cabo los procesos de conmutación y filtrado solo según la dirección MAC de la capa de enlace de datos (capa 2) del modelo OSI y dependen de los routers para pasar datos entre subredes IP independientes.

Como se muestra en la figura, un switch de capa 3, como el Catalyst 3560, funciona de manera similar a un switch de capa 2, como el Catalyst 2960, pero en lugar de utilizar solo la información de la dirección MAC de la capa 2 para las decisiones de reenvío, los switches de capa 3 también pueden utilizar la información de la dirección IP. En lugar de aprender qué direcciones MAC están vinculadas con cada uno de sus puertos, el switch de Capa 3 puede también conocer qué direcciones IP están relacionadas con sus interfaces. Esto permite que el switch de capa 3 también dirija el tráfico a través de la red sobre la base de la información de la dirección IP.

Los switches de Capa 3 son también capaces de llevar a cabo funciones de enrutamiento de Capa 3, con lo cual se reduce la necesidad de colocar routers dedicados en una LAN. Dado que los switches de Capa 3 cuentan con un hardware de conmutación especializado, pueden normalmente enviar datos con la misma rapidez con la que pueden conmutar.



Los dispositivos Cisco que admiten conmutación de capa 3 utilizan Cisco Express Forwarding (CEF). Este método de reenvío es muy complejo, pero afortunadamente CEF requiere muy poca configuración en los dispositivos Cisco.

Básicamente, CEF desacopla la interdependencia estricta habitual entre la toma de decisiones de capa 2 y de capa 3. Lo que lentifica el reenvío de paquetes IP es la referencia constante en ambos sentidos entre las construcciones de capa 2 y capa 3 dentro de un dispositivo de red. Entonces, en la medida en que se puedan desacoplar las estructuras de datos de capa 2 y la capa 3, se acelera el reenvío.

Los dos componentes principales de la operación de CEF son los siguientes:

- Base de información de reenvío (FIB)
- Tablas de adyacencia

La FIB es conceptualmente similar a una tabla de enrutamiento. Un router utiliza la tabla de enrutamiento para determinar el mejor camino hacia una red de destino sobre la base de la porción de red de la dirección IP de destino. Con CEF, la información que antes se almacenaba en la caché de la ruta se almacena ahora en varias estructuras de datos para la conmutación CEF. Las estructuras de datos proporcionan búsquedas optimizadas para un reenvío de paquetes eficaz. Los dispositivos de red utilizan la tabla de búsqueda de FIB para tomar decisiones de conmutación basadas en el destino sin tener que acceder a la caché de la ruta.

La FIB se actualiza cuando se producen cambios en la red y contiene todas las rutas conocidas hasta ese momento.

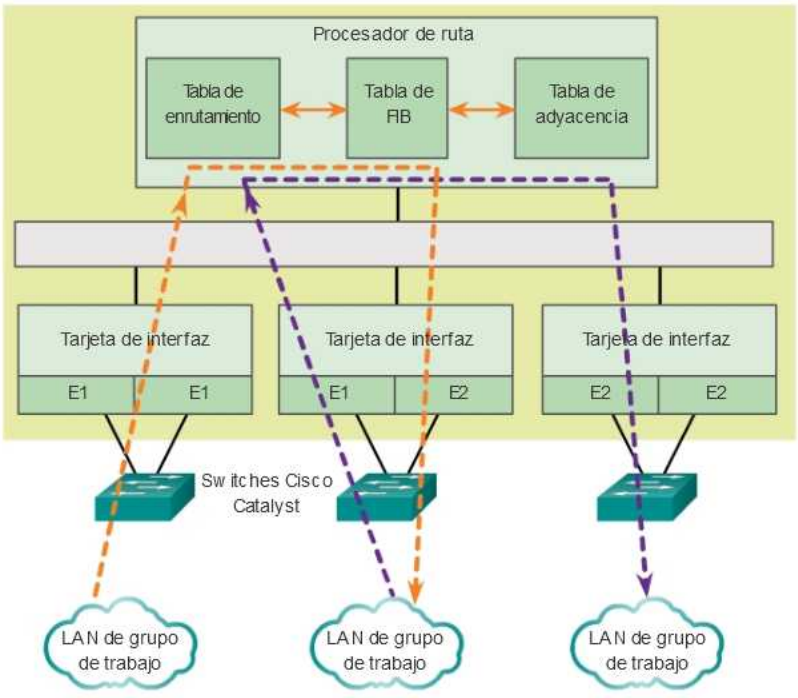
La tabla de adyacencia mantiene las direcciones de siguiente salto de la capa 2 para todas las entradas de FIB.

La separación de la información de posibilidad de conexión (en la tabla FIB) y de la información de reenvío (en la tabla de adyacencia), ofrece varias ventajas:

- La tabla de adyacencia se puede crear independientemente de la tabla FIB, lo que permite que ambas se creen sin que haya paquetes en proceso de conmutación.
- La reescritura del encabezado MAC utilizada para reenviar paquetes no se almacena en las entradas de caché, por lo tanto, los cambios en una cadena de reescritura de encabezado MAC no requiere la invalidación de las entradas de caché.

CEF está habilitado de manera predeterminada en la mayoría de los dispositivos Cisco que realizan conmutación de capa 3.

Los dispositivos de red Cisco admiten varios tipos de interfaces de capa 3 diferentes. Las interfaces de capa 3 son aquellas que admiten el reenvío de paquetes IP a un destino final sobre la base de la dirección IP.

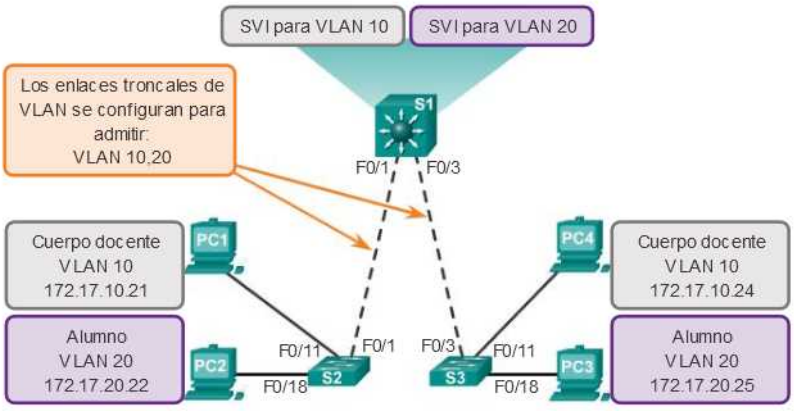


Los principales tipos de interfaces de capa 3 son los siguientes:

- **Interfaz virtual de switch (SVI):** interfaz lógica en un switch asociado a una red de área local virtual (VLAN).
- **Puerto enrutado:** puerto físico en un switch de capa 3 configurado para funcionar como puerto de router.
- **EtherChannel de capa 3:** interfaz lógica en dispositivos Cisco asociada a un conjunto de puertos enrutados.

Como se mostró anteriormente, se debe habilitar una SVI para la VLAN predeterminada (VLAN1) a fin de proporcionar conectividad de host IP al switch y permitir la administración remota del switch. También se deben configurar SVI para permitir el enrutamiento entre redes VLAN. Como ya se mencionó, las SVI son interfaces lógicas configuradas para VLAN específicas; para crear una ruta entre dos o más redes VLAN, cada VLAN debe tener habilitada una SVI independiente.

Interfaces virtuales de switch



Los puertos enrutados permiten que los switches Cisco (de capa 3) funcionen como routers de manera eficaz. Cada puerto de un switch se puede configurar como puerto en una red IP independiente.

Los EtherChannels de capa 3 se utilizan para agrupar enlaces de Ethernet de capa 3 entre dispositivos Cisco para agregar ancho de banda, por lo general en uplinks.

Nota: además de las SVI y los EtherChannels de capa 3, existen otras interfaces lógicas en los dispositivos Cisco, que incluyen interfaces loopback e interfaces de túnel.

Un puerto de switch se puede configurar para que funcione como puerto enrutado de capa 3 y se comporte como una interfaz de router normal. Las características específicas de un puerto enrutado son las siguientes:

- No está relacionado con una VLAN determinada.
- Se puede configurar con un protocolo de enrutamiento de capa 3.
- Es una interfaz de capa 3 únicamente, y no admite el protocolo de capa 2.

Configuración de un puerto enrutado

```
S1(config)#interface f0/6
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.200.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
*Mar  1 00:15:40.115: %SYS-5-CONFIG_I: Configured from console by console
S1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        192.168.200.1   YES manual up                    up
FastEthernet0/7        unassigned      YES unset  up                    up
FastEthernet0/8        unassigned      YES unset  up                    up
<Resultado omitido>
```

Configure los puertos enrutados colocando la interfaz en modo de capa 3 con el comando de configuración de interfaz **no switchport**. A continuación, asigne una dirección IP al puerto. Eso es todo.

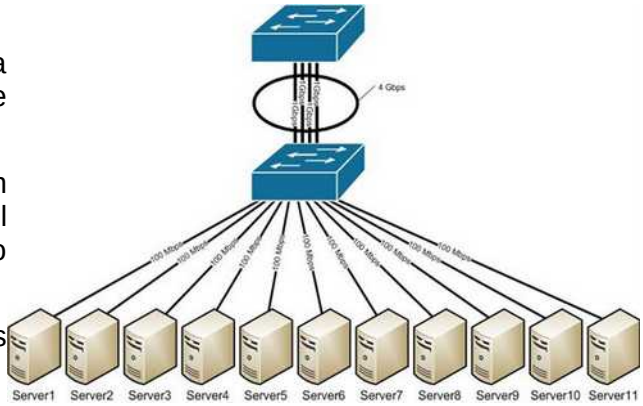
Port trunking (link aggregation)

Permite combinar varios enlaces físicos en un enlace lógico (trunk), que funciona como un único puerto de mayor ancho de banda

Características:

- Aumenta el ancho de banda entre 2 switches, un switch o varios de un stack
- Implica redundancia, lo que mejora la fiabilidad
- Pueden unirse hasta 8 puertos FE, GE y 10GE
- Puede usarse para aumentar el ancho de banda entre un switch y un equipo de la red

Cisco denomina esta técnica como EtherChannel.



EtherChannel nos permite sumar la velocidad de cada puerto físico y así obtener un único enlace troncal de alta velocidad.

Cuando tenemos muchos servidores que salen por un único enlace troncal, puede que el tráfico colapse el enlace. Una de las soluciones más prácticas es el uso de EtherChannel.

De esta manera sumamos la velocidad de los puertos que agregamos al enlace lógico.

Modos de configuración:
Podemos configurar un **EtherChannel** de 3 formas diferentes:

- **Mode ON**: no se realiza ningún tipo de negociación, todos los puertos se ponen activos. No utiliza ningún protocolo.

  S# **config t**
  S(config)# **interface range f0/3-4**
  A1(config-if-range)# **channel-group 1 mode on**
- **PAgP (Port Aggregation Protocol)**: es un protocolo propietario de **Cisco**. El switch negocia con el otro extremo qué puertos usar con los modos desirable/auto como en DTP
  S(config-if-range)# **channel-group 2 mode desirable**
- **LACP (Link Aggregation Control Protocol)**: protocolo abierto con estándar IEEE 802.3ad y 802.3ax. El switch negocia los puertos con los modos active/pasive

  S(config-if-range)# **channel-group 3 mode active**

Recomendaciones

- Asignar todos los puertos del EtherChannel a la **misma VLANm,** configurar todos como troncales o si se trata de switches de capa 3 ponerlos como enrutados con no switchport.
  S(config)#**interface port-channel 3**
  S(config-if)# **switchport trunk native vlan 999**
  S(config-if)# **ip address 192.168.0.1 255.255.255.0** Establece una IP a la interfaz etherch
- Verificar que todos los puertos del grupo están en un **mismo modo de encapsulación**, ISL o 802.1Q

  show etherchannel summary
  show spanning-tree
  show interfaces trunk
  show interface port-channel número el parámetro BW nos dirá la velocidad del enlace