

Capa 2 - Enlace

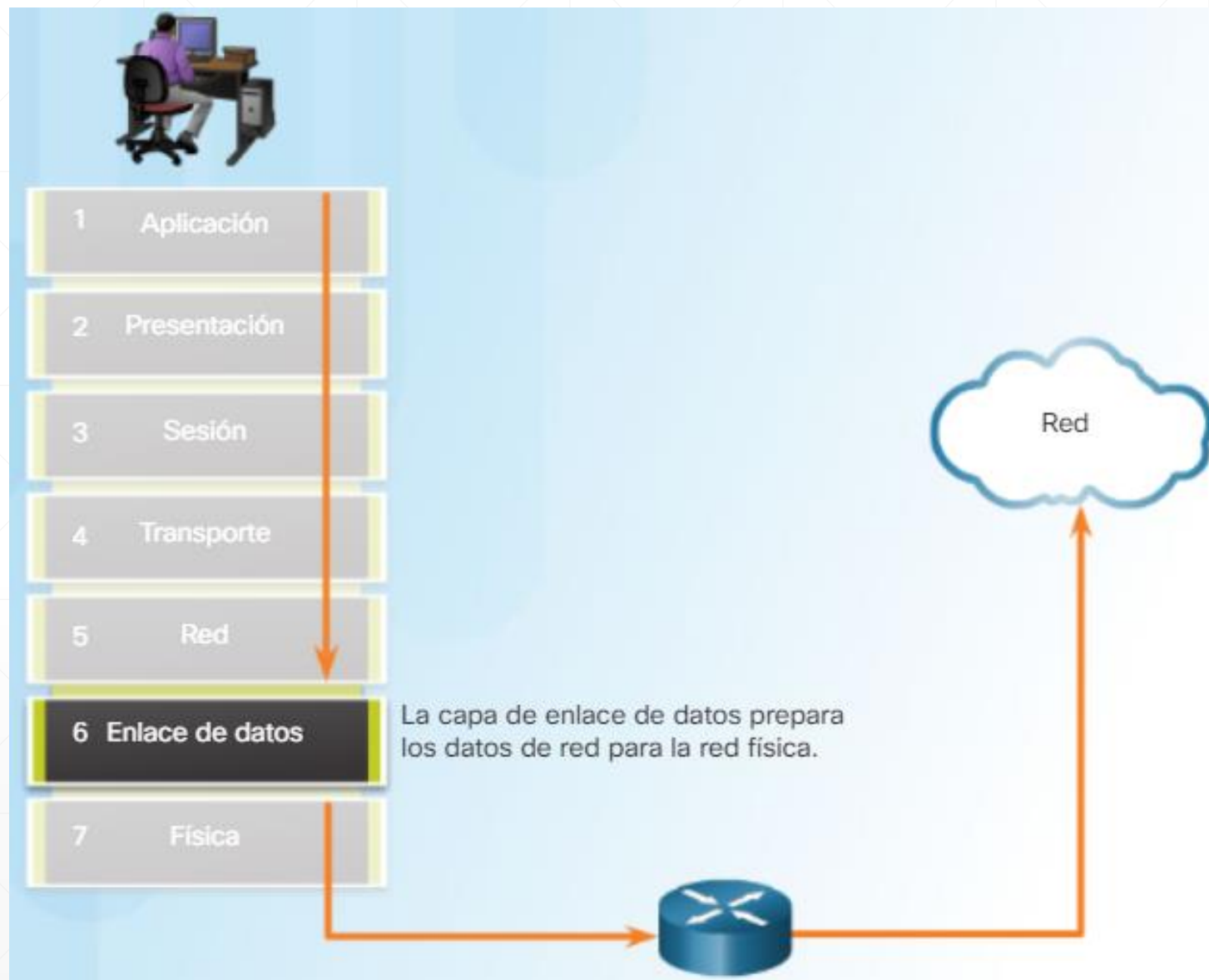
Redes I

La capa de enlace de datos (Modelo OSI)

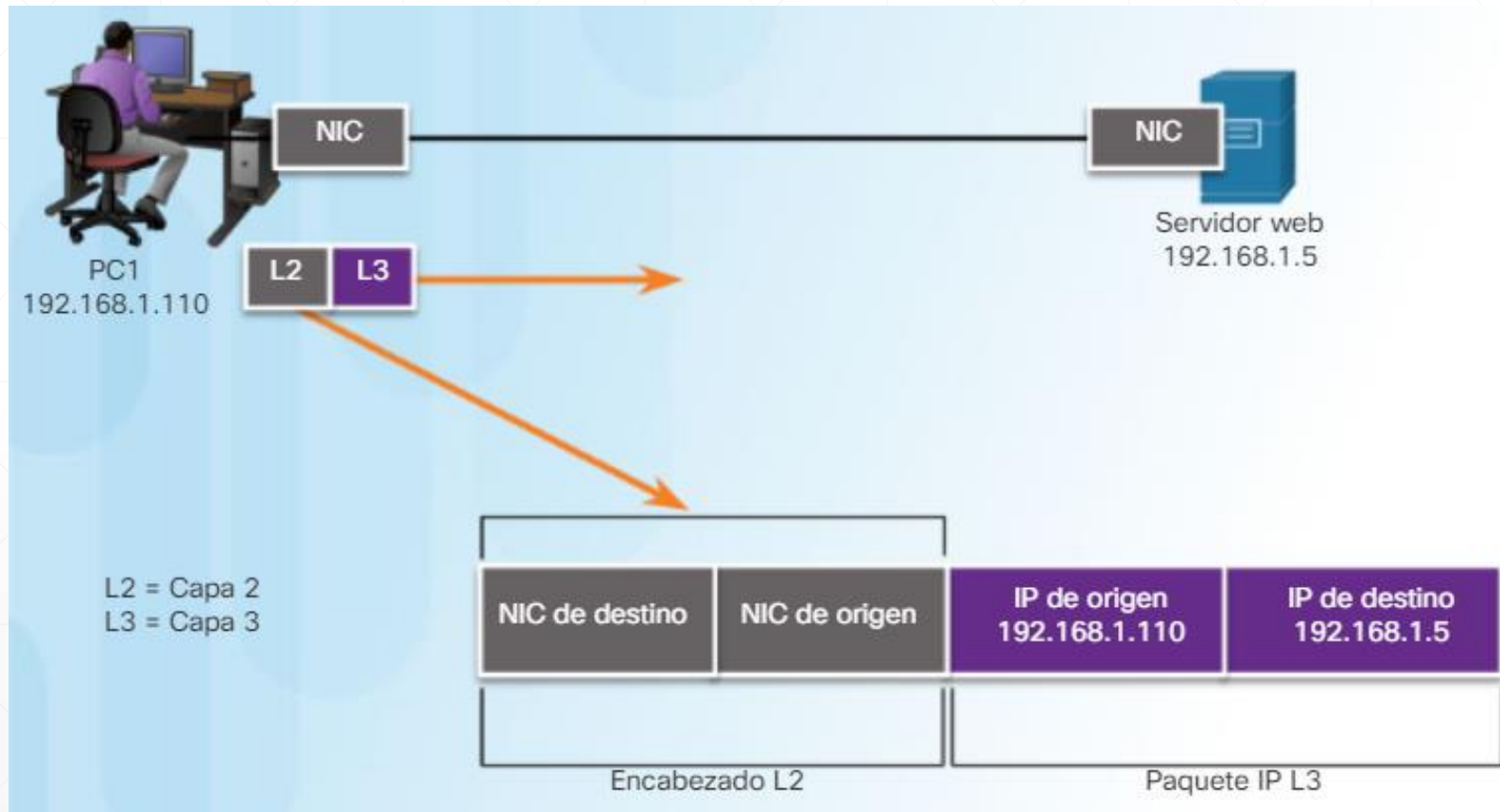
Es responsable de lo siguiente:

- Permite a las capas superiores acceder a los medios
 - Acepta paquetes de la capa 3 y los encapsula en tramas
 - Prepara los datos de red para la red física
 - Controla la forma en que los datos se colocan y reciben en los medios
 - Intercambia tramas entre los nodos en un medio de red físico, como UTP o fibra óptica.
 - Recibe y dirige paquetes a un protocolo de capa superior.
 - Lleva a cabo la detección de errores.
-

Capa de Enlace



Direcciones de enlace de datos de Capa 2 (L2)

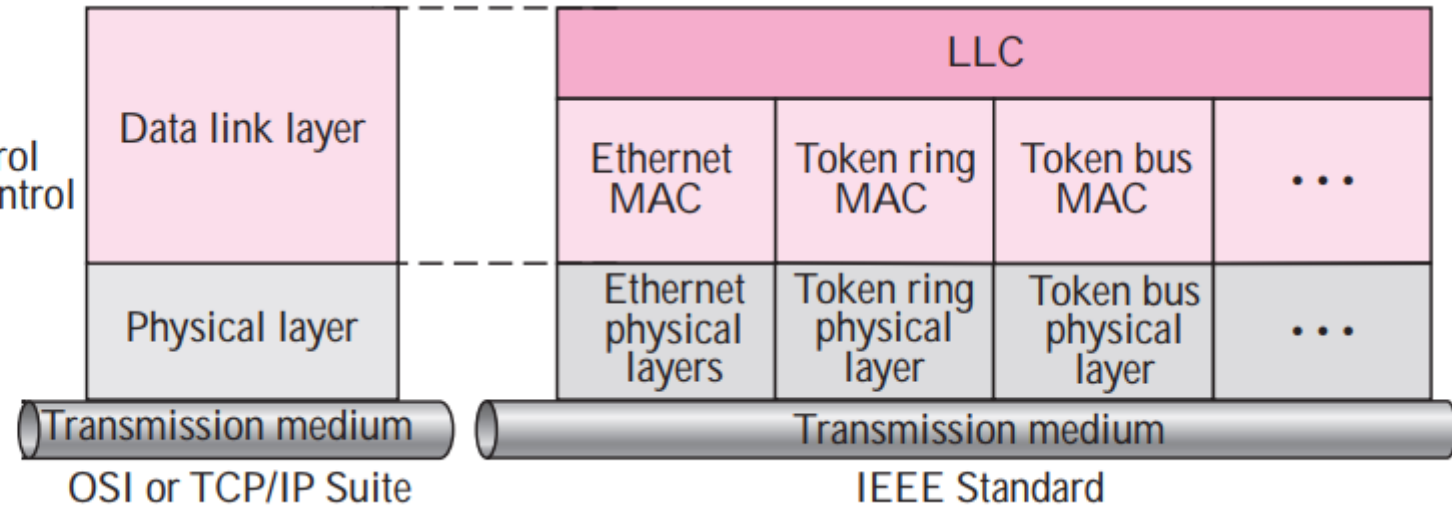


Estándares IEEE

- En 1985 la “Computer Society” de la IEEE inició un proyecto llamado “Project 802” para definir los estándares de intercomunicación entre equipos de varios fabricantes.
 - El “Proyecto 802” especifica el funcionamiento de la Capa Física (L1) y Capa de Enlace (L2) del Modelo OSI.
 - La IEEE subdivide la Capa de Enlace en dos sub-capas: “Logical link control (LLC)” y “Media Access Control (MAC)”.
-

Estándares IEEE para LANs

LLC: Logical link control
MAC: Media access control



Subcapas de enlace de datos

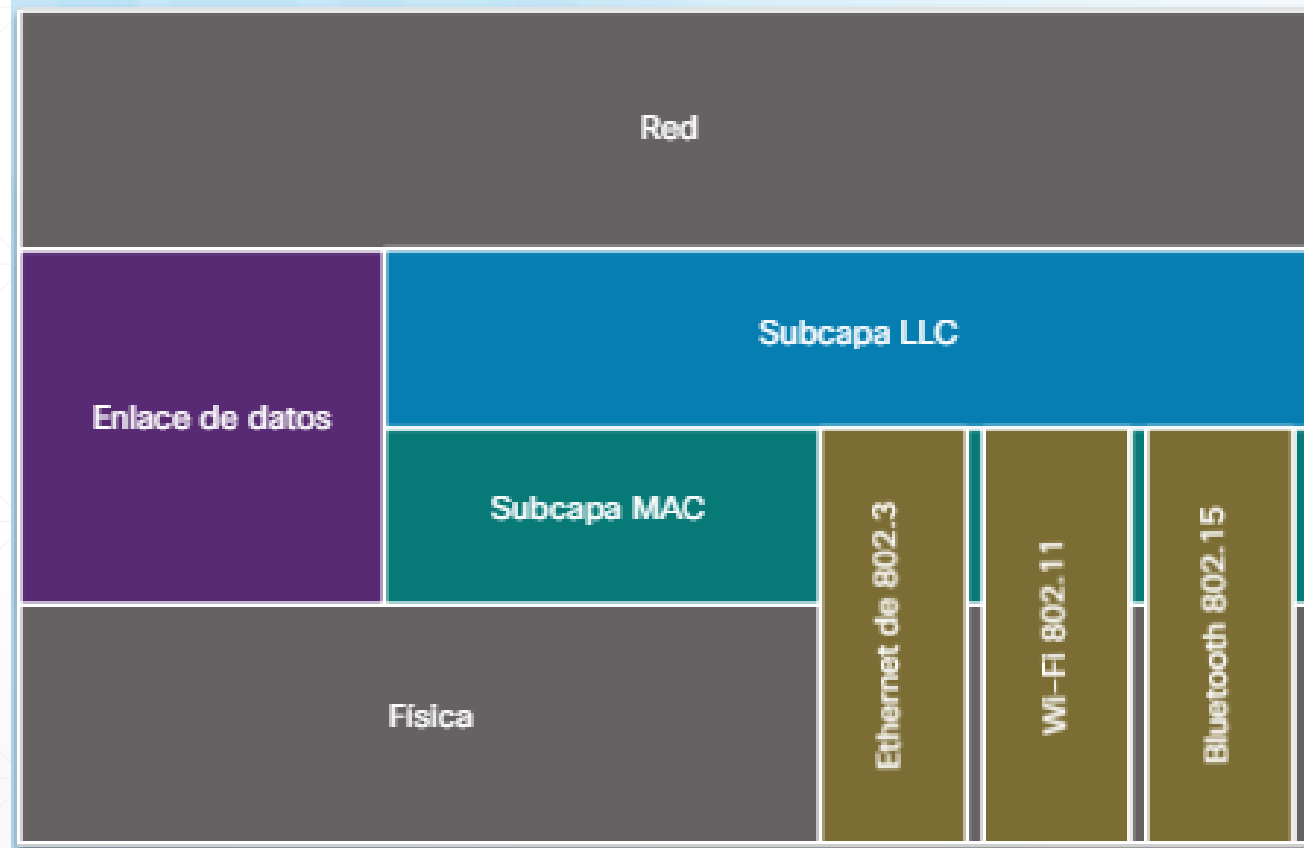
Control de enlace lógico (LLC):

- Esta subcapa superior se comunica con la capa de red.
 - Coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama.
 - Permite que varios protocolos de capa 3 (IPv4 e IPv6) utilicen la misma interfaz de red y los mismos medios.
-

Subcapas de enlace de datos

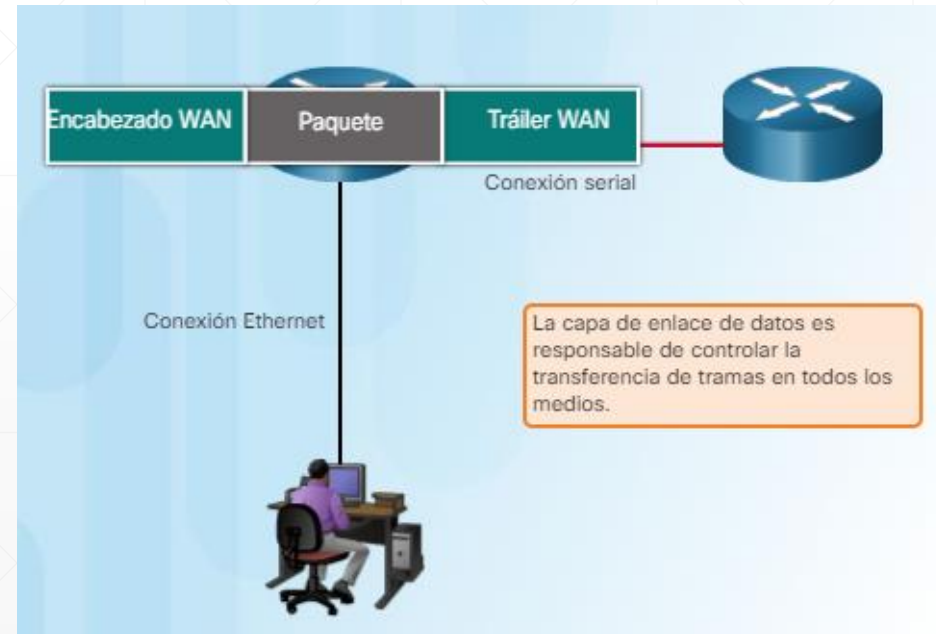
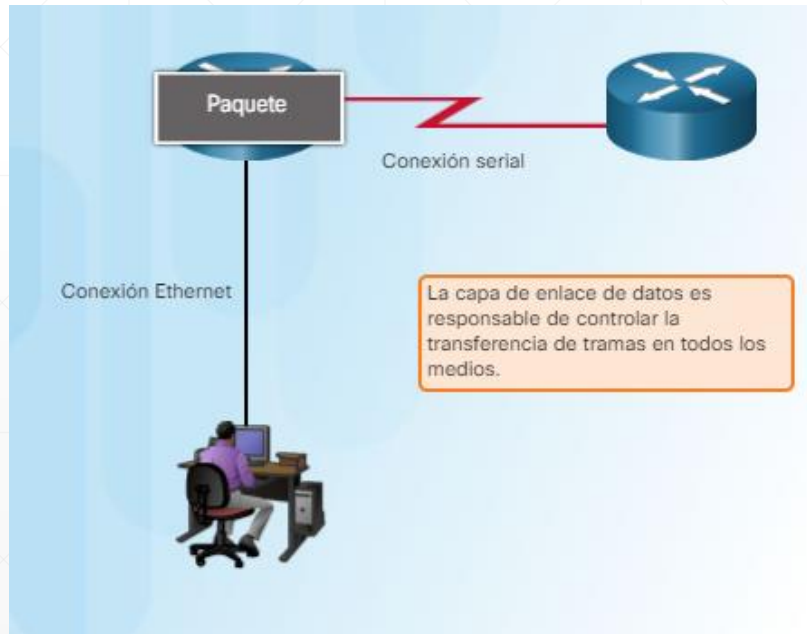
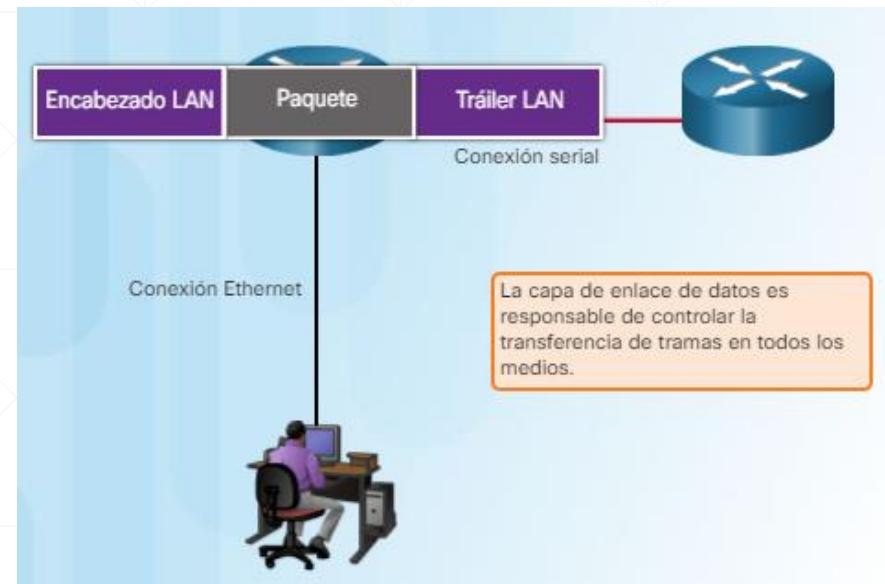
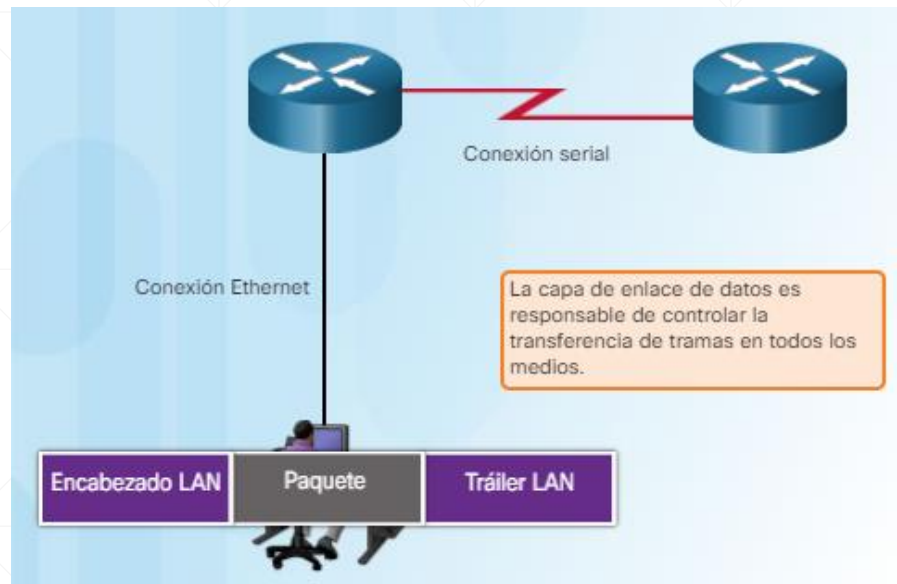
Control de acceso al medio (MAC):

- Subcapa inferior que define los procesos de acceso al medio que realiza el hardware.
 - Proporciona direccionamiento de la capa de enlace de datos y acceso a varias tecnologías de capa física.
 - Por ejemplo, esta subcapa se comunica con la tecnología LAN Ethernet para enviar y recibir tramas a través de cables de cobre, fibra, Wi-Fi o Bluetooth.
-



Control de acceso al medio

- Es la técnica utilizada para colocar y sacar la trama de los medios.
 - Por ejemplo, una LAN Ethernet consta de muchos hosts que compiten por acceder al medio de red.
 - Los enlaces seriales constan de una conexión directa entre dos dispositivos únicamente.
 - Las interfaces del router encapsulan el paquete en la trama correspondiente, y se utiliza un método de control de acceso al medio adecuado para acceder a cada enlace.
-



Control de acceso al medio

En cada salto a lo largo de la ruta, los routers realizan lo siguiente

- Aceptan una trama proveniente de un medio
 - Desencapsulan la trama
 - Vuelven a encapsular el paquete en una trama nueva
 - Reenvían la nueva trama adecuada al medio de ese segmento de la red física
-

Control de acceso al medio

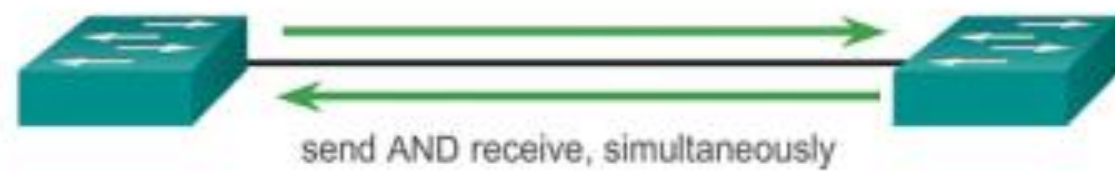
El método real de control de acceso al medio utilizado depende de lo siguiente:

- **Topología:** cómo se muestra la conexión entre los nodos a la capa de enlace de datos.
 - **Uso compartido de medio:** de qué modo los nodos comparten los medios. El uso compartido de los medios puede ser punto a punto, como en las conexiones WAN, o compartido, como en las redes LAN.
-

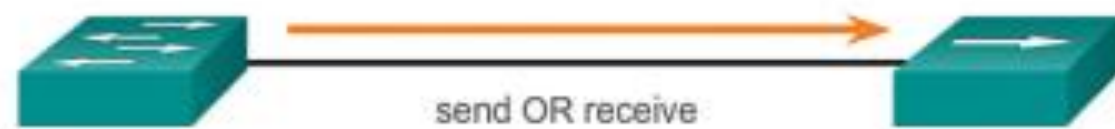
Half duplex y Full duplex

- Las comunicaciones dúplex refieren a la dirección en la que se transmiten los datos entre dos dispositivos.
 - **Half-dúplex:** los dos dispositivos pueden transmitir y recibir en los medios pero no pueden hacerlo simultáneamente. Redes WLAN utilizan half-dúplex.
 - **Full-dúplex:** los dos dispositivos pueden transmitir y recibir en los medios al mismo tiempo.
 - Si las interfaces interconectadas de dos host están configurados con modos dúplex diferentes, existirá ineficiencia y latencia en el enlace.
-

Full-Duplex Communication



Half-Duplex Communication



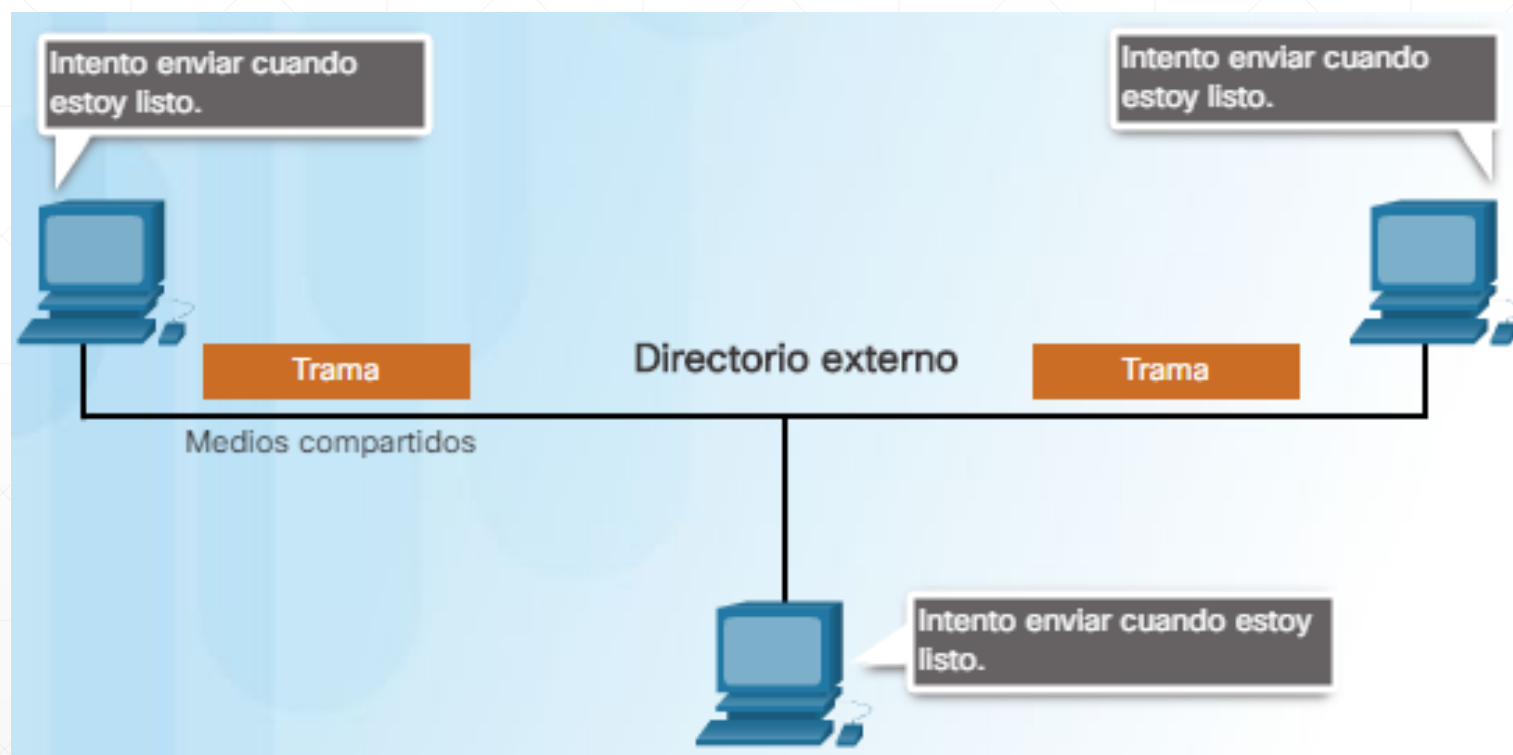
Métodos de control de acceso al medio

- Algunas topologías de red comparten un medio común con varios nodos. Estas se denominan redes de acceso múltiple.
 - En cualquier momento una cantidad de dispositivos intentará enviar y recibir datos utilizando los mismos medios de red.
 - Métodos básicos para controlar el acceso:
 - Acceso por contención
 - Acceso controlado
-

Acceso por contención

- Todos los nodos en half-dúplex compiten por el uso del medio, pero solo un dispositivo puede enviar a la vez.
 - Existe un proceso en caso de que más de un dispositivo transmita al mismo tiempo.
-

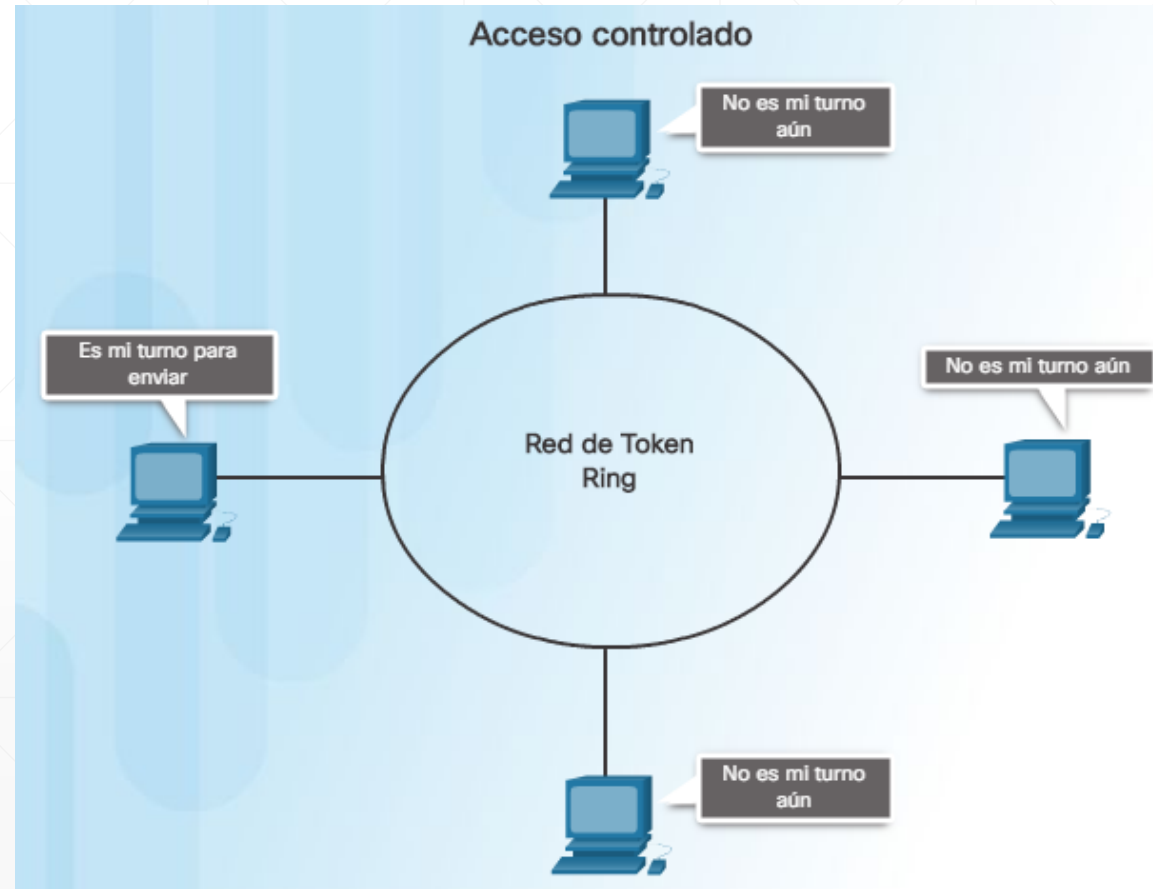
Acceso por contención



Acceso controlado

- Cada nodo tiene su propio tiempo para utilizar el medio.
 - Estas redes deterministas no son eficientes porque un dispositivo debe aguardar su turno para acceder al medio.
 - Las LAN de Token Ring son un ejemplo de este tipo de control de acceso.
-

Acceso controlado

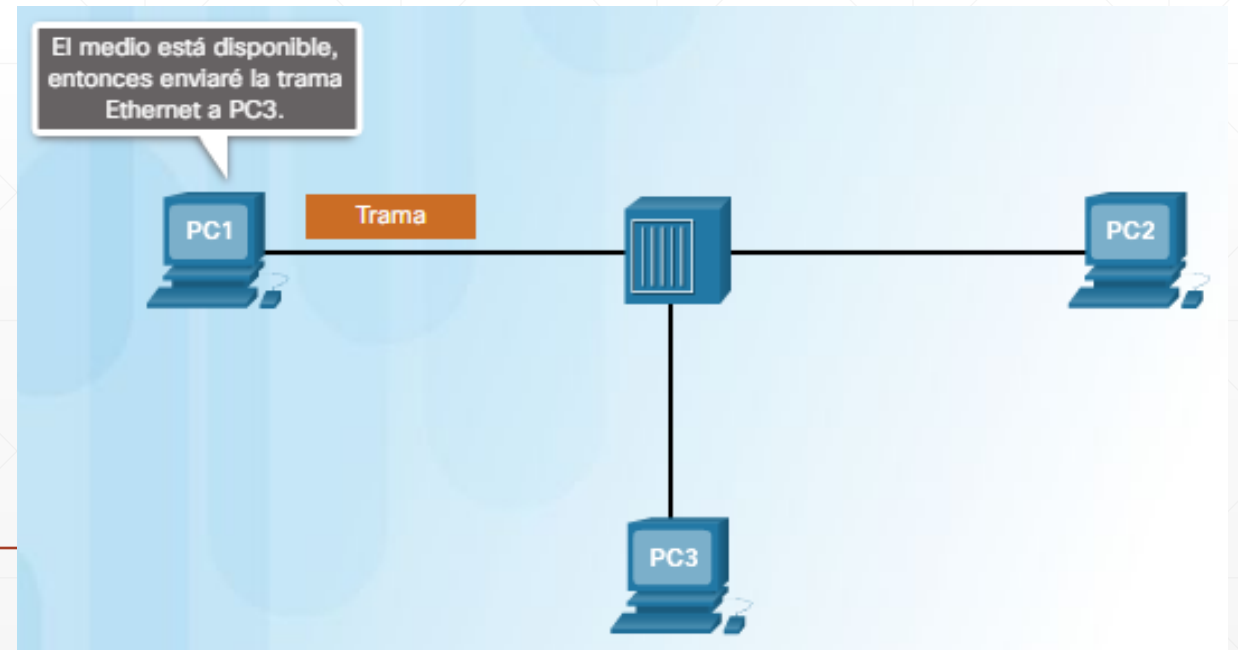


Acceso por contención: CSMA /CD

- El proceso de “Acceso múltiple por detección de portadora y detección de colisiones” (CSMA/CD) es utilizado en las redes LAN Ethernet de half-dúplex.
-

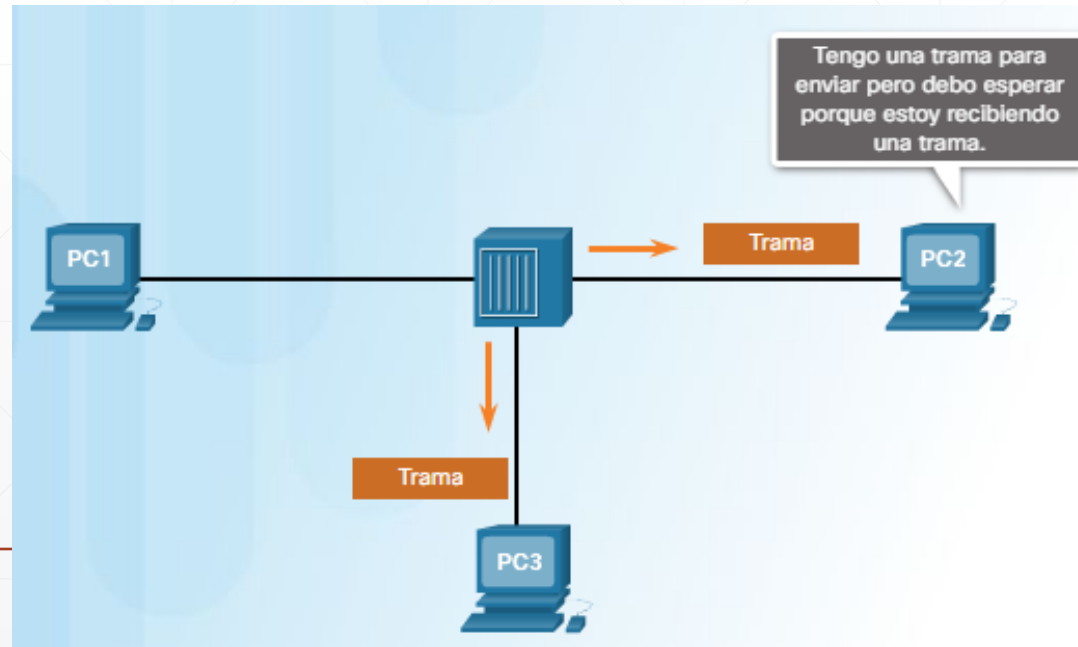
CSMA /CD

1. La PC1 tiene una trama que se debe enviar a la PC3
2. La NIC de la PC1 debe determinar si alguien está transmitiendo en el medio. Si no detecta un proveedor de señal, en otras palabras, si no recibe transmisiones de otro dispositivo, asumirá que la red está disponible para enviar.
3. La NIC envía la trama de Ethernet



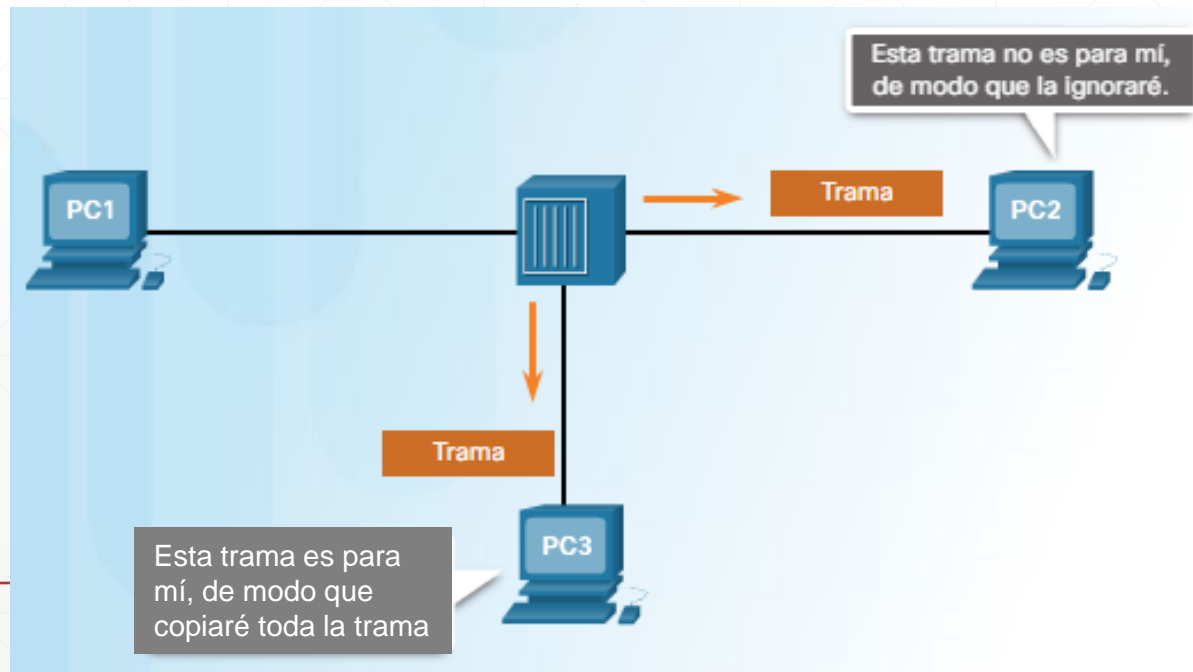
CSMA /CD

4. El repetidor de múltiples puertos (Hub) recibe la trama. La trama completa se regenera y se reenvía a través de todos los puertos del hub.
5. Si otro dispositivo, como la PC2, quiere transmitir, pero está recibiendo una trama, deberá aguardar hasta que el canal esté libre.



CSMA /CD

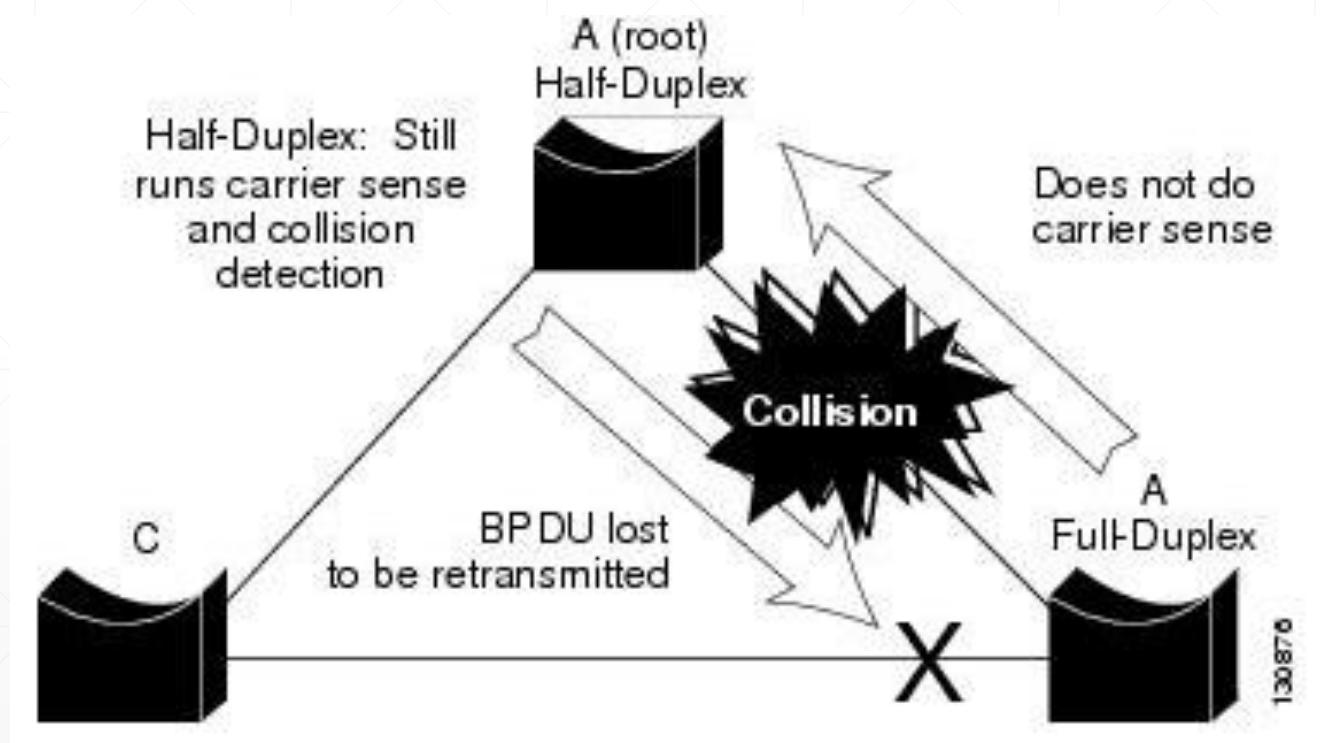
6. Todos los dispositivos que están conectados al Hub reciben la trama. Dado que la trama tiene una dirección destino de enlace de datos para la PC3, solo ese dispositivo aceptará y copiará toda la trama.
7. Las NIC de todos los demás dispositivos ignorarán la trama.



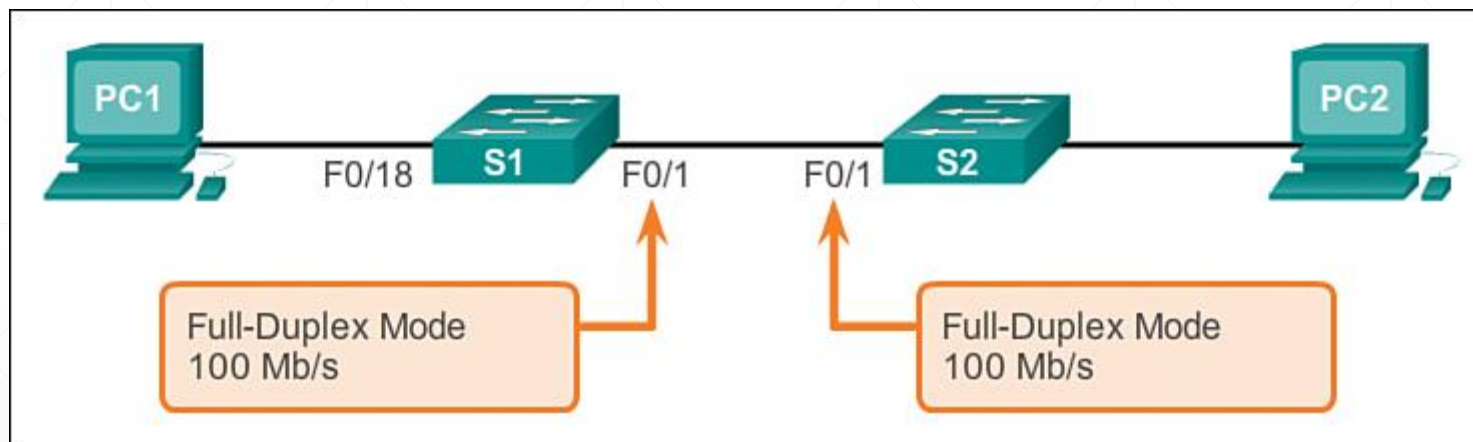
CSMA /CD

- Si dos dispositivos transmiten al mismo tiempo, se produce una colisión. Los dos dispositivos detectarán la colisión en la red, es decir, la detección de colisión (CD). Esto se logra mediante la comparación de los datos transmitidos con los datos recibidos que realiza la NIC o bien mediante el reconocimiento de la amplitud de señal si esta es más alta de lo normal en los medios. Los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.
 - En una red Full Duplex no existen colisiones, debido que la conexión está limitada a dos dispositivos que hacen la negociación de quien transmite y recibe en un momento determinado. Por lo tanto no se utiliza CSMA /CD en Full Duplex.
-

Duplex Mismatch



Cisco Switch Port Duplex Configuration



Cisco Swtich Port Duplex Configuration

Enter global configuration mode.
Enter interface configuration mode.
Configure the interface duplex mode.
Configure the interface speed.
Return to privileged EXEC mode.

```
S1# configure terminal  
S1(config)# interface fastethernet 0/1  
S1(config-if)# duplex full  
S1(config-if)# speed 100  
S1(config-if)# end
```

Acceso por contención: CSMA /CA

- Otra forma de CSMA que utilizan las redes WLAN del IEEE 802.11: “Acceso múltiple por detección de portadora con prevención de colisiones (CSMA /CA).
 - CSMA /CA no detecta colisiones pero intenta evitarlas ya que aguarda antes de transmitir.
 - Cada dispositivo inalámbrico que transmite incluye la duración que necesita para la transmisión.
 - Todos los demás dispositivos inalámbricos reciben esta información y saben por cuanto tiempo el medio no estará disponible.
-

CSMA /CA



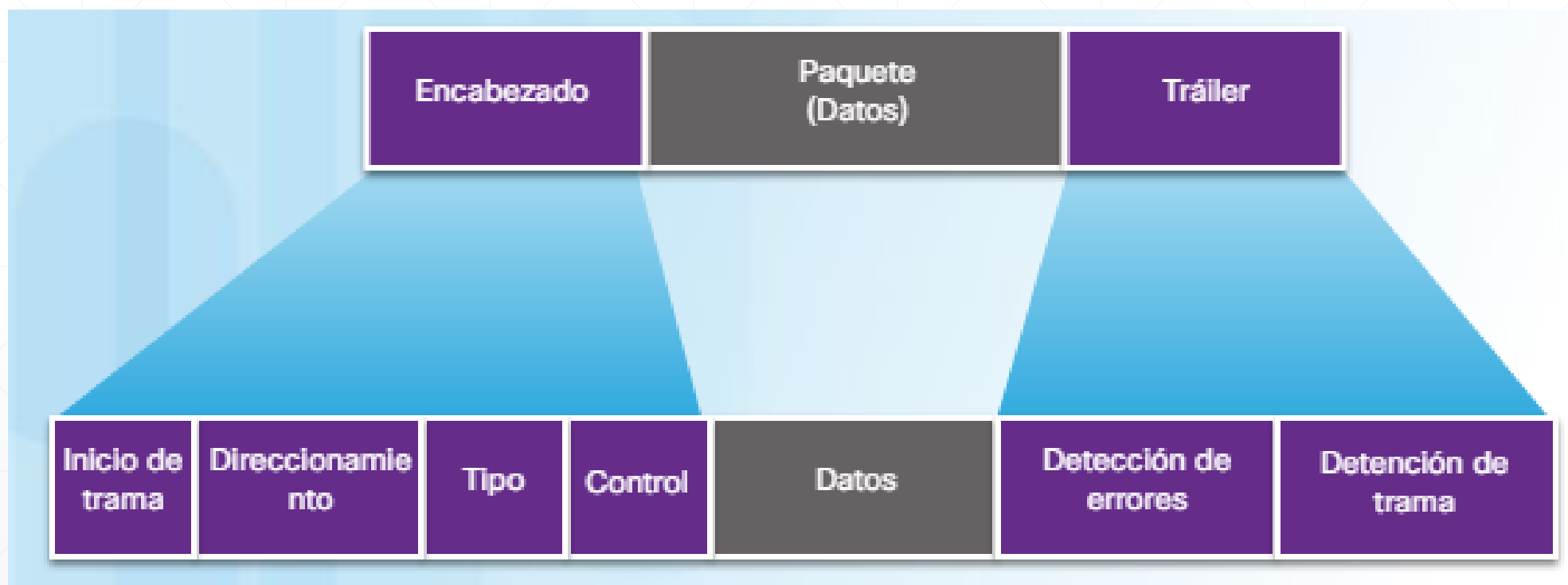
La trama

- La capa de enlace de datos prepara los paquetes para su transporte a través de los medios locales encapsulándolos con un encabezado y un tráiler para crear una trama.
 - Existen diferentes protocolos de capa de enlace de datos que definen la estructura de las tramas. Encabezados y tráiler varían según el protocolo. Los protocolos varían dependiendo de los medios físicos utilizados.
 - Cada tipo de trama tiene 3 partes básicas:
 1. Encabezado
 2. Datos
 3. Tráiler
-

Entornos frágiles



Campos de trama



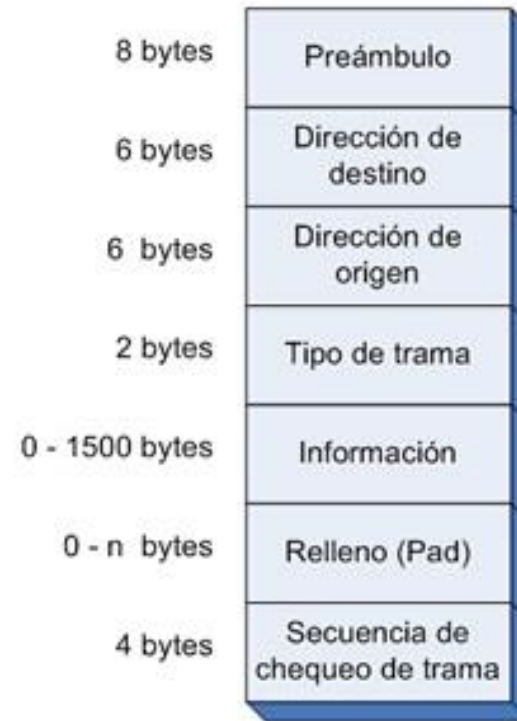
Campos de trama

- **Indicadores de arranque y detención de trama:** identifica los límites de comienzo y finalización de la trama.
 - **Direccionamiento:** indica los nodos de origen y destino en los medios.
 - **Tipo:** identifica el protocolo de capa 3 en el campo de datos.
 - **Control:** identifica los servicios especiales de control de flujo, como QoS.
 - **Datos:** incluye el contenido de la trama (paquete de L3 encapsulado)
 - **Detección de errores:** utilizado para comprobar errores en la recepción de la trama.
-

Frame: IEEE 802.3 vs Ethernet



Formato de la trama IEEE 802.3

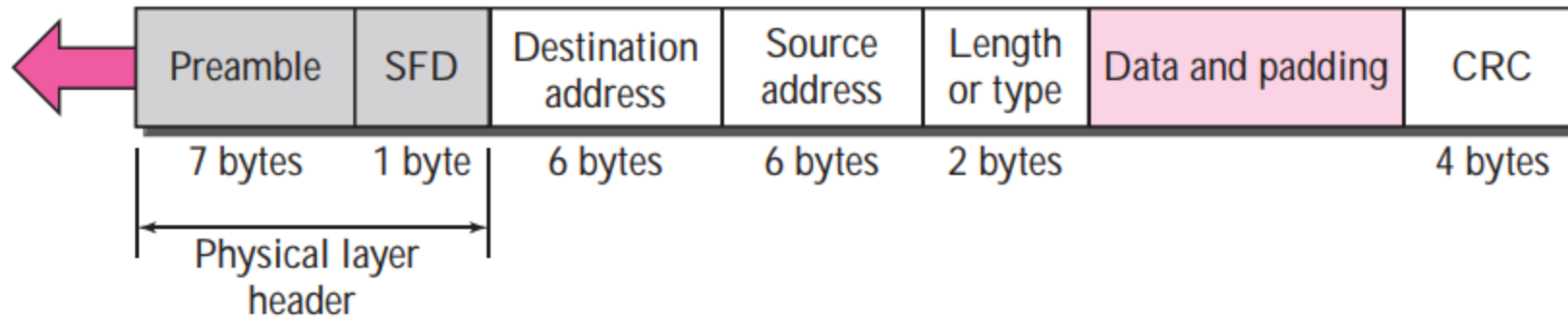


Formato de la trama Ethernet

IEEE 802.3 Frame

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Campos de trama

- La trama definida por el protocolo IEEE 802.3 contiene 7 campos:
 1. Preamble
 2. Start frame delimiter (SFD)
 3. Destination address (DA)
 4. Source address (SA)
 5. Length or type
 6. Data
 7. Frame check sequence (FCS)
-

IEEE Frame Formats

- IEEE 802.3
 - IEEE 802.3 with SNAP (Sub-Network Access Protocol)
 - IEEE 802.3 with 802.2
-

Ethernet II Frame

Ethernet

8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes
Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos	Secuencia de verificación de trama

Preamble

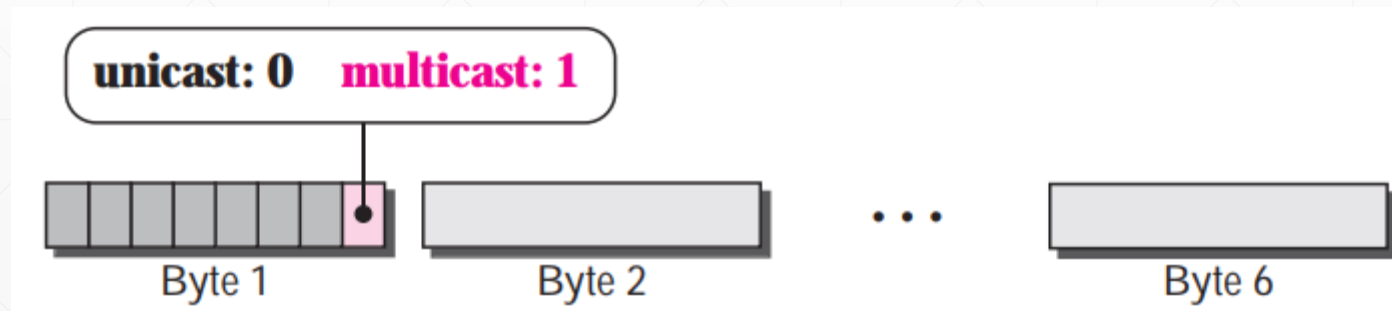
- El propósito del preámbulo es anunciar la trama y permitir a todos los receptores en la red sincronizarse a si mismos a la trama entrante.
 - El preámbulo en Ethernet tiene una longitud de 8 bytes pero en IEEE 802.3 la longitud del mismo es de 7 bytes, el octavo byte se convierte en el comienzo del delimitador de la trama.
 - El patrón de bits del preámbulo provee una alerta y un pulso de tiempo.
 - El preámbulo se inserta en la trama en la capa física.
-

Start frame delimiter (SFD)

- 1 byte (10101011)
 - Indica el inicio del frame
 - SFD advierte al dispositivo receptor (o receptores) que esta es la última oportunidad para sincronizarse.
 - Los dos últimos bits son 11 para indicar que el siguiente “campo” de la trama es el “destination address”
 - El SFD también es agregado en la capa física
-

Destination address (DA)

- 6 bytes
- Contiene la dirección física del dispositivo destinatario (o dispositivos) del paquete
- Puede ser Unicast, Multicast o Broadcast
- El bit menos significativo del primer byte de la MAC Address define el tipo de direccionamiento. Si es 0, la dirección es Unicast; de lo contrario será multicast.



Defina el tipo

- Defina si las siguientes direcciones son Unicast, Multicast o Broadcast.
 - a. 4A:30:10:21:10:1A
 - b. 47:20:1B:2E:08:EE
 - c. FF:FF:FF:FF:FF:FF
-

Source address (SA)

- 6 bytes
 - Contiene la dirección física del emisor del paquete
 - Debe ser Unicast (1:1)
-

Length or type

- Ethernet usa este campo para definir el tipo de protocolo utilizado en el paquete en la capa superior (L3)
 - IEEE 802.3 usa este campo para definir el tamaño del campo de data.
 - Los valores comunes son, en hexadecimal, “0x800” para IPv4, “0x86DD” para IPv6 y “0x806” para ARP.
-

Campo Type de trama en protocolo Ethernet

Ether Type	Protocol
0x0800	Internet Protocol, Version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x8035	Reverse Address Resolution Protocol (RARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q)
0x814C	Simple Network Management Protocol (SNMP)
0x86DD	Internet Protocol, Version 6 (IPv6)
0x8847	MPLS unicast
0x8848	MPLS multicast
0x8870	Jumbo Frames
0x888E	EAP over LAN (IEEE 802.1X)
0x88E5	MAC security (IEEE 802.1AE)
0x88F7	Precision Time Protocol (IEEE 1588)

Data

- Este campo lleva encapsulados los bits del paquete de la capa 3.
 - Tamaño mínimo 46 bytes, máximo 1500 bytes (sin tomar en cuenta 18 bytes de header y tráiler)
-

FCS

- Contiene la información para la detección de errores en la trama.
 - Tamaño de 4 bytes.
 - Utiliza una comprobación de redundancia cíclica (CRC)
 - El dispositivo receptor analiza el FCS de la trama y valida si coincide con los bits de la trama recibida.
 - Si los cálculos no coinciden indica que los datos cambiaron y se descarta la trama.
 - Un cambio en los datos podría ser consecuencia de una interrupción de señales eléctricas que representan los bits.
-

Dirección de Capa 2

- Las direcciones de dispositivo en esta capa se llaman direcciones físicas.
 - A diferencia de las direcciones de Capa 3, que son jerárquicas, las direcciones físicas no indican en qué red está ubicado el dispositivo.
 - La dirección física es única para un dispositivo en particular.
 - Esta dirección solo se utiliza para entregas locales.
-

Protocolos de capa de enlace

- Ethernet
 - 802.11 inalámbrico
 - Protocolo punto a punto (PPP)
 - HDLC
 - Frame Relay
-

Ethernet

- La capa física (OSI) proporciona el medio para transportar los bits que componen una trama de capa de enlace de datos a través de los medios de red.
 - 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 el formato, tamaño, temporización y codificación de las tramas, entre otros aspectos de comunicación.
-

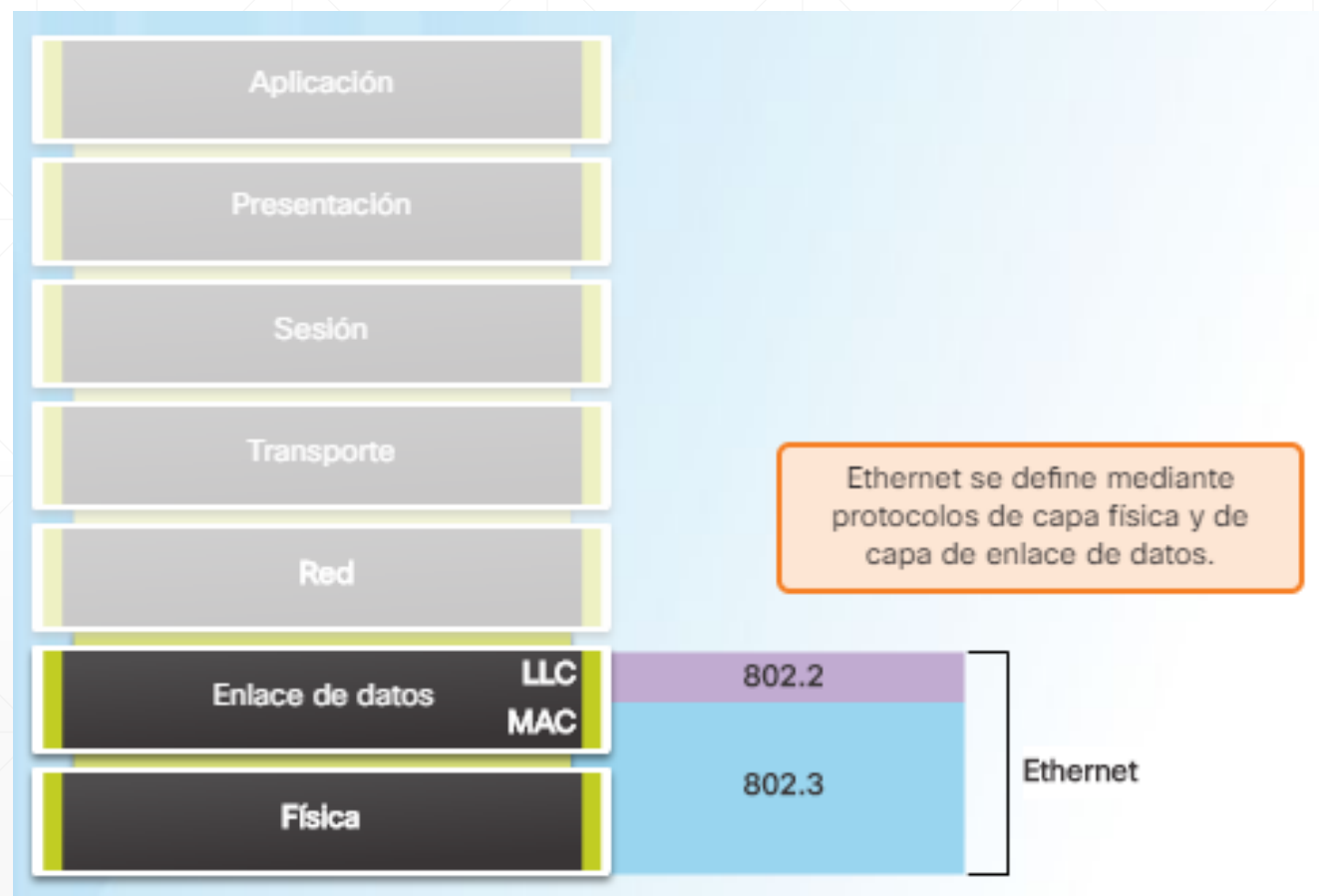
Ethernet

- Los estándares de Ethernet definen:
 - Protocolos de Capa 2
 - Tecnologías de Capa 1.
 - Ethernet admite diferentes medios, anchos de banda y otras variaciones de capa 1 y 2, sin embargo el formato de trama básico y el esquema de direccionamiento son los mismos para todas las variedades de Ethernet.
-

Ethernet

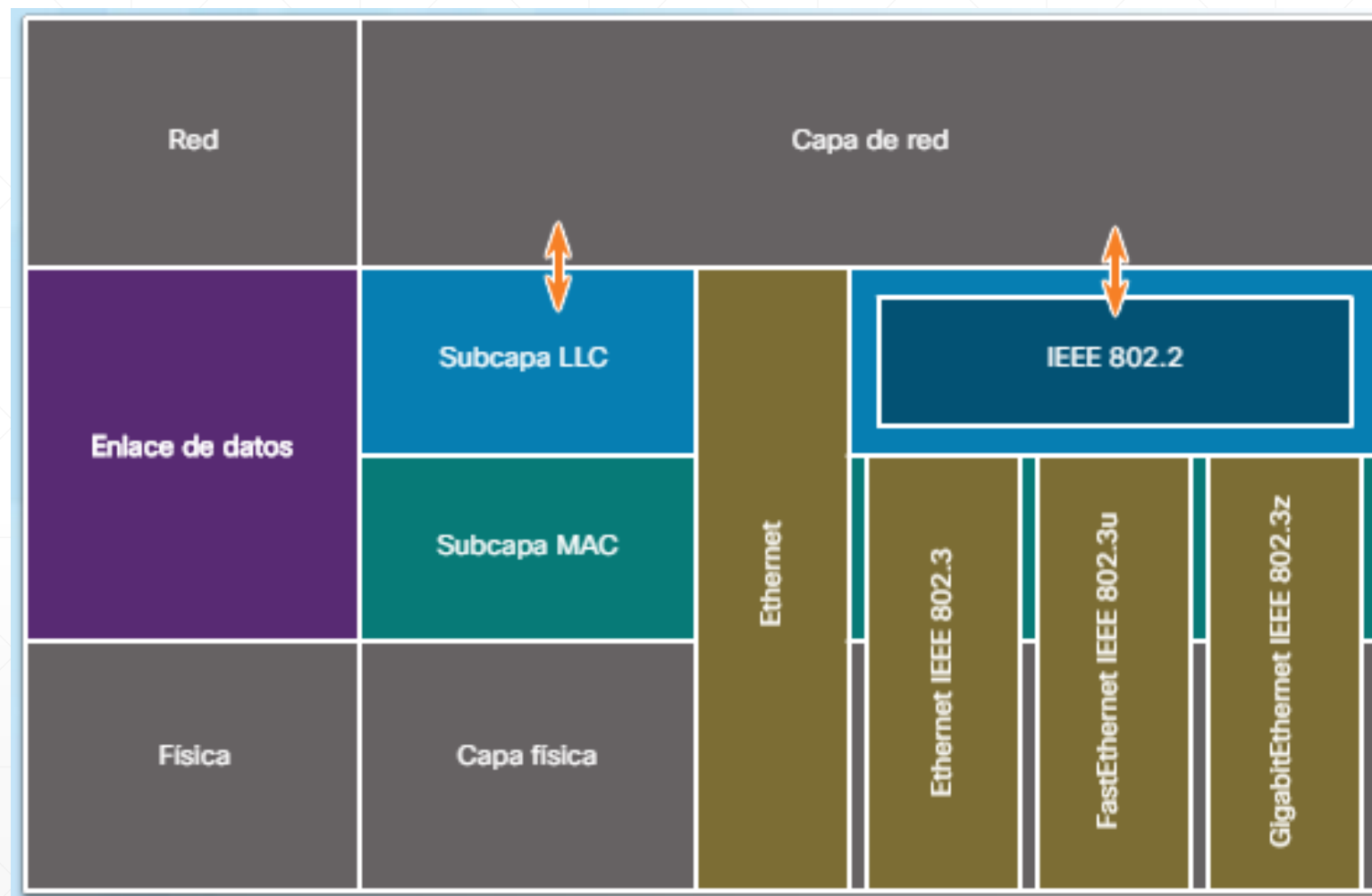
- Ethernet es una familia de tecnologías de red que se definen en los estándares IEEE 802.2 y 802.3.
 - Admite los siguientes anchos de banda
 - 10 Mb/s
 - 100 Mb/s
 - 1,000 Mb/s (1 Gb/s)
 - 10,000 Mb/s (10 Gb/s)
 - 40,000 Mb/s (40 Gb/s)
 - 100,000 Mb/s (100 Gb/s)
-

Ethernet



Subcapa LLC (Logical Link Control)

- La subcapa de Control de enlace lógico (LLC) maneja la comunicación entre las capas superiores e inferiores.
 - Generalmente esto sucede entre el software de red y el hardware del dispositivo
 - LLC toma los datos del protocolo de la red, por lo general IPv4, y agrega información de control para ayudar a distribuir el paquete al nodo de destino.
 - LLC se implementa en el software, y su implementación es independiente al Hardware.
 - En las computadoras el LLC por lo general se encuentra en el driver de la NIC.
-



Subcapa MAC (Media Access Control)

- Se implementa mediante Hardware
 - Generalmente las NIC de las computadoras o equipo de red
 - Sus datos específicos se detallan en el estándar IEEE 802.3
-

Capa física		Capa de enlace de datos
Medio físico	Subcapa de señalización física	
		802.3: Control de acceso al medio
10BASE-5 (500 m) 50 Ohm Coaxial tipo N		
10BASE-2 (185 m) 50 Ohm Coaxial BNC		
10BASE-T (100 m) 100 Ohm UTP RJ-45		
100BASE-TX (100 m) 100 Ohm UTP RJ-45		
1000BASE-CX (25 m) 150 Ohm STP mini-DB-9		
1000BASE-T (100 m) 100 Ohm UTP RJ-45		
1000BASE-ST (220 a 550 m) SC de fibra MM		
1000BASE-LX (550 a 5000 m) SC de fibra MM o SM		Subcapa de control de enlace lógico

Estándares de cableado LAN Ethernet

Ethernet Type	Bandwidth	Cable Type	Maximum Distance
10BASE-T	10Mbps	Cat3/Cat5 UTP	100 m
100BASE-TX	100Mbps	Cat5 UTP	100 m
100BASE-TX	200Mbps	Cat5 UTP	100 m
100BASE-FX	100Mbps	Multimode fiber	400 m
100BASE-FX	200Mbps	Multimode fiber	2 km
1000BASE-T	1Gbps	Cat5e UTP	100 m
1000BASE-TX	1Gbps	Cat6 UTP	100 m
1000BASE-SX	1Gbps	Multimode fiber	550 m
1000BASE-LX	1Gbps	Single-mode fiber	2 km
10GBASE-T	10Gbps	Cat6a/Cat7 UTP	100 m
10GBASE-SX4	10Gbps	Multimode fiber	550 m
10GBASE-LX4	10Gbps	Single-mode fiber	2 km

Subcapa MAC

- La subcapa MAC de Ethernet tiene dos tareas principales:
 1. Encapsulamiento de datos
 2. Control de acceso al medio
-

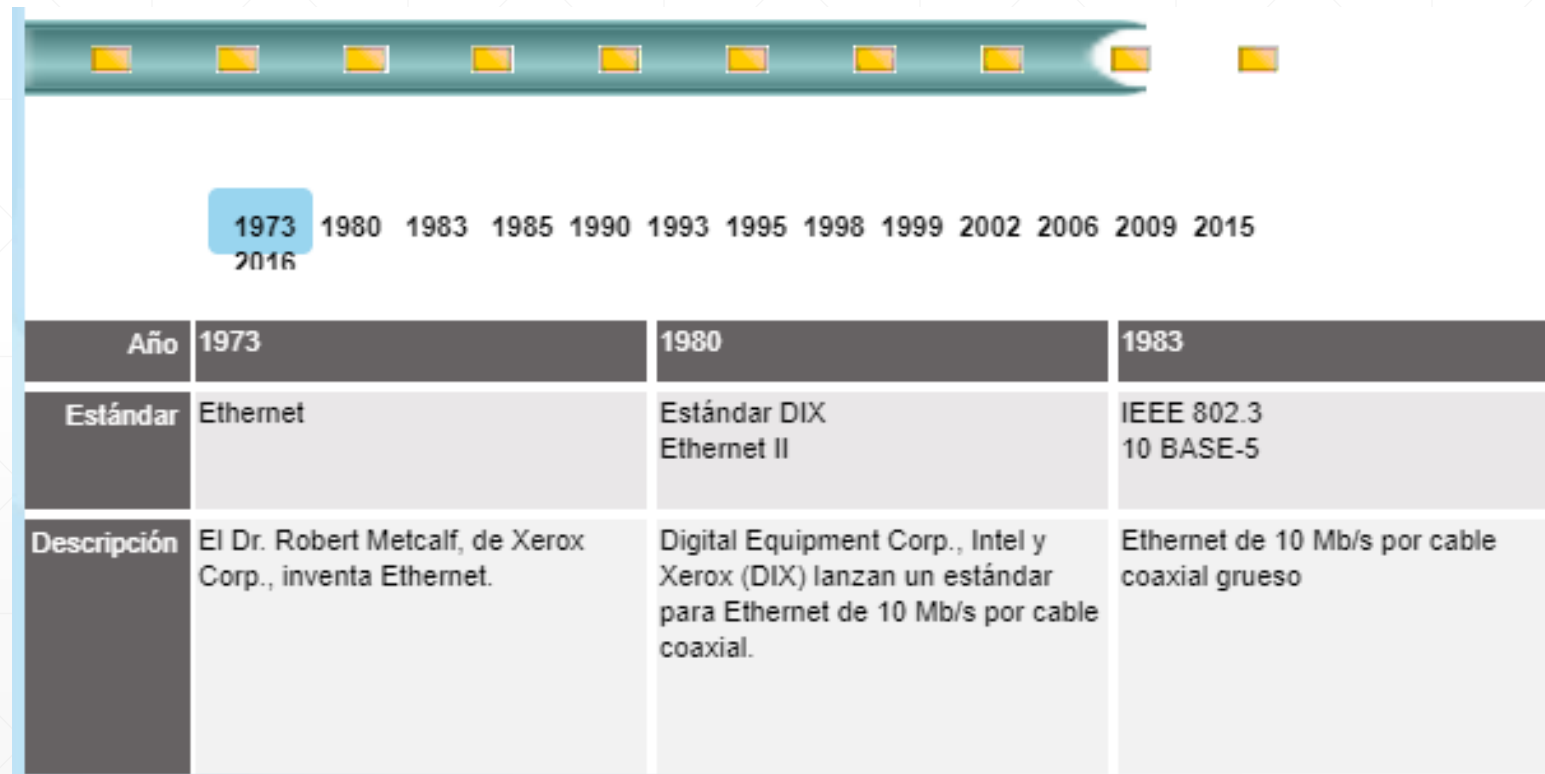
Encapsulamiento de datos – Subcapa MAC

- Se refiere al armado de tramas antes de la transmisión y el desarmado de tramas en el momento de recepción.
 - El encapsulamiento de datos proporciona tres funciones principales:
 1. Delimitación de tramas
 2. Direccionamiento
 3. Detección de errores
-

Control de acceso al medio

- Responsable de colocar las tramas en los medio y de quitarlas de ellos.
 - La topología lógica subyacente de Ethernet es un bus de acceso múltiple, por lo que todos los nodos (dispositivos) de un único segmento de red comparten medio.
-

Evolución de Ethernet



Campos de trama de Ethernet

- El tamaño mínimo de trama Ethernet es de 64 bytes
 - Tamaño máximo es de 1518 bytes
 - Este tamaño se mide desde la Dirección MAC destino hasta el FCS (Frame Check Sequence)
 - Cualquier trama de menos de 64 bytes se considera un fragmento de colisión o una trama corta y se descarta automáticamente en los receptores.
 - Cualquier trama mayor a 1500 se considera un Jumbo Frame.
-

Procesamiento de tramas

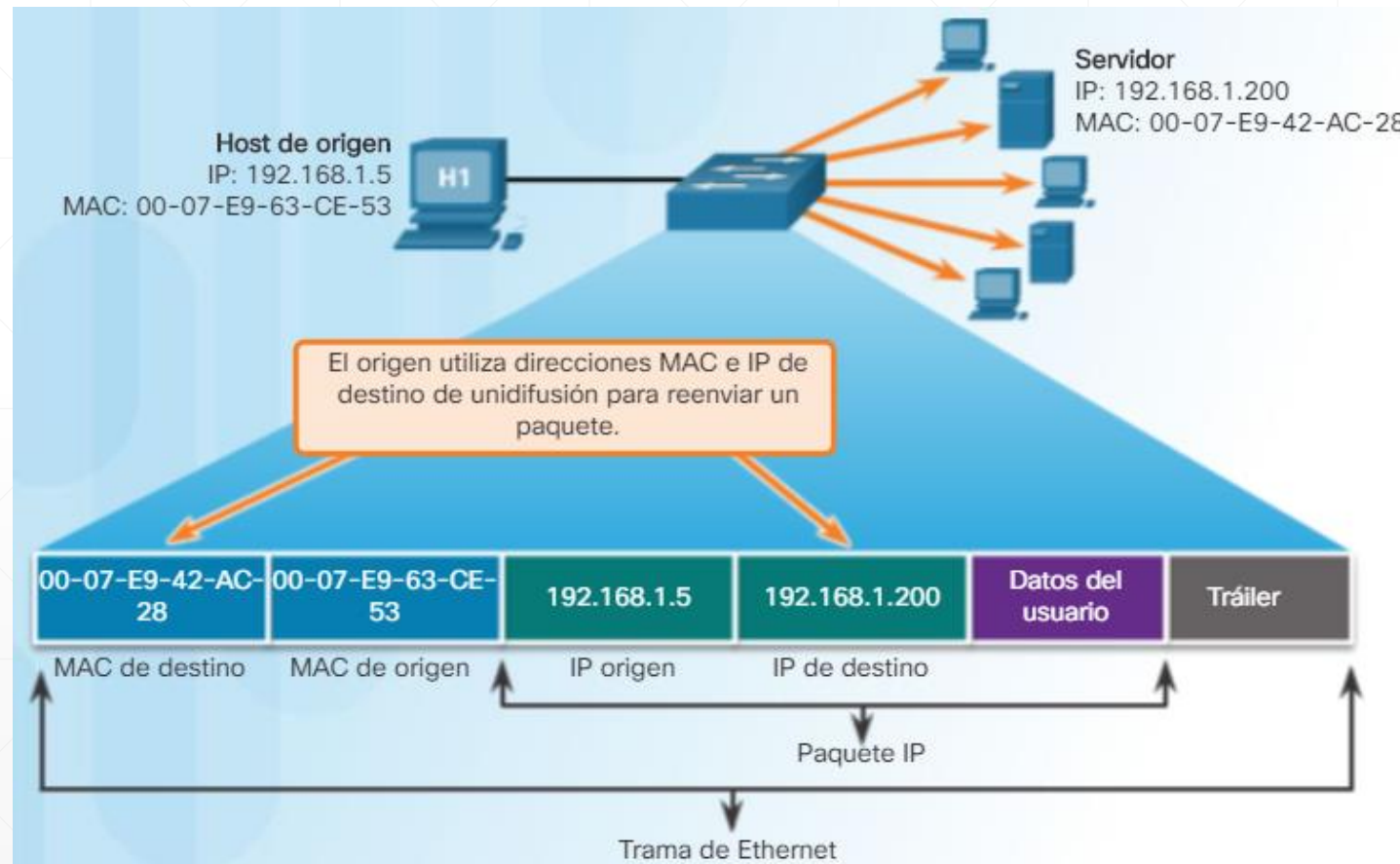
- En las NIC y los sistemas operativos de PC modernos, es posible cambiar la dirección MAC en el software.
 - El filtrado o el control de tráfico basado en la dirección MAC ya no son tan seguros.
 - Cuando la computadora arranca, lo primero que hace la NIC es copiar la dirección MAC de la ROM a la RAM.
 - Las NIC Ethernet también aceptan tramas si la dirección MAC de destino es un grupo de difusión o de multidifusión del cual es miembro el host.
-

Estructura de la dirección MAC de Ethernet

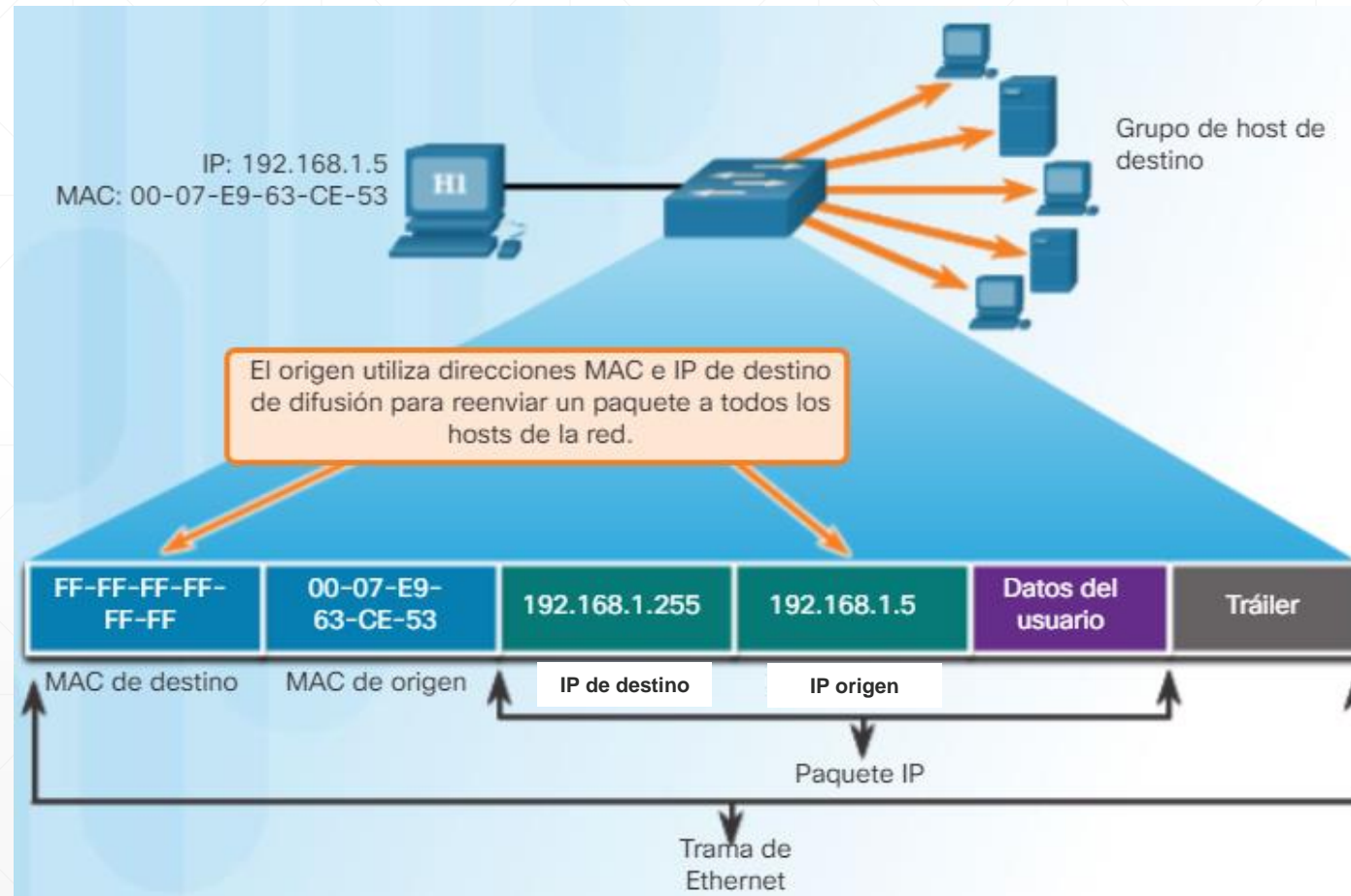
OUI (Identificador único de la organización)	Asignado por el proveedor (NIC, interfaces)
24 bits	24 bits

80:86:F2	3A:F4:E6
Intel	Específico

Dirección MAC de Unidifusión

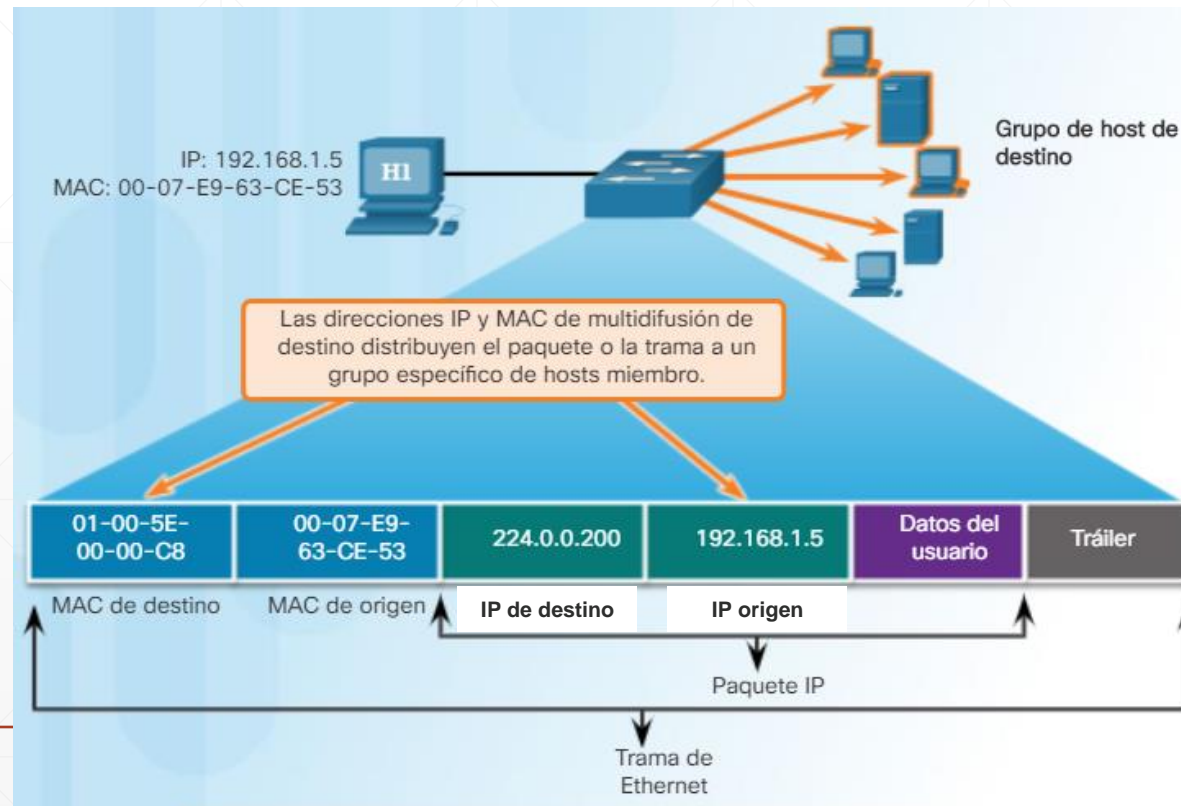


Dirección MAC de Difusión



Dirección MAC de Multidifusión

- El intervalo de direcciones IPv4 de multidifusión va de 224.0.0.0 a 239.255.255.255.



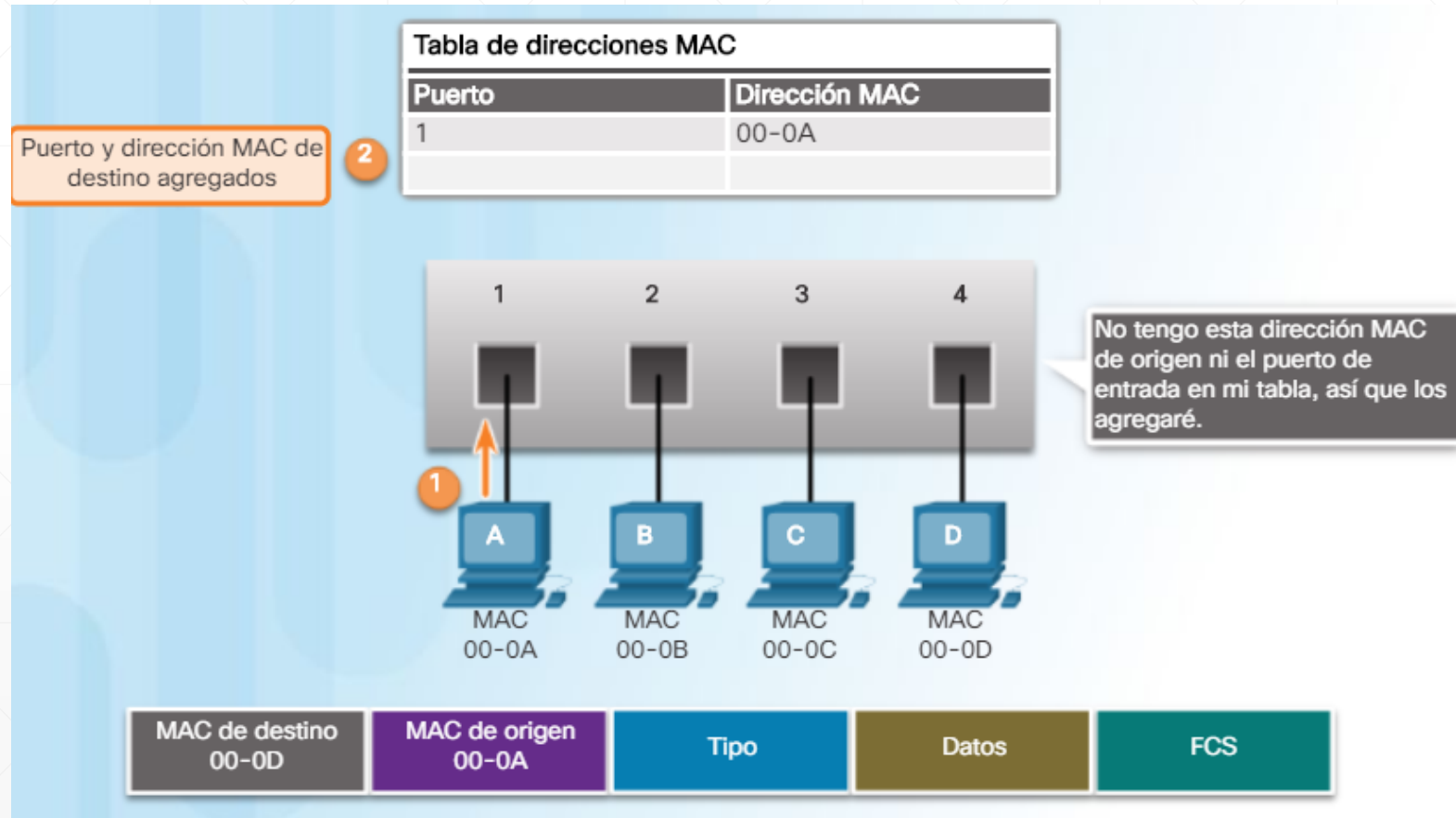
Nociones básicas de switches

- El switch L2 toma decisiones de reenvío solamente según las direcciones MAC Ethernet de capa 2.
 - Un switch Ethernet consulta una tabla de direcciones MAC para tomar una decisión de reenvío para cada trama.
 - A veces, la tabla de direcciones MAC se conoce como “tabla de memoria de contenido direccionable (CAM)”
-

Cuando un switch recibe una trama, elige una de las siguientes acciones a tomar:

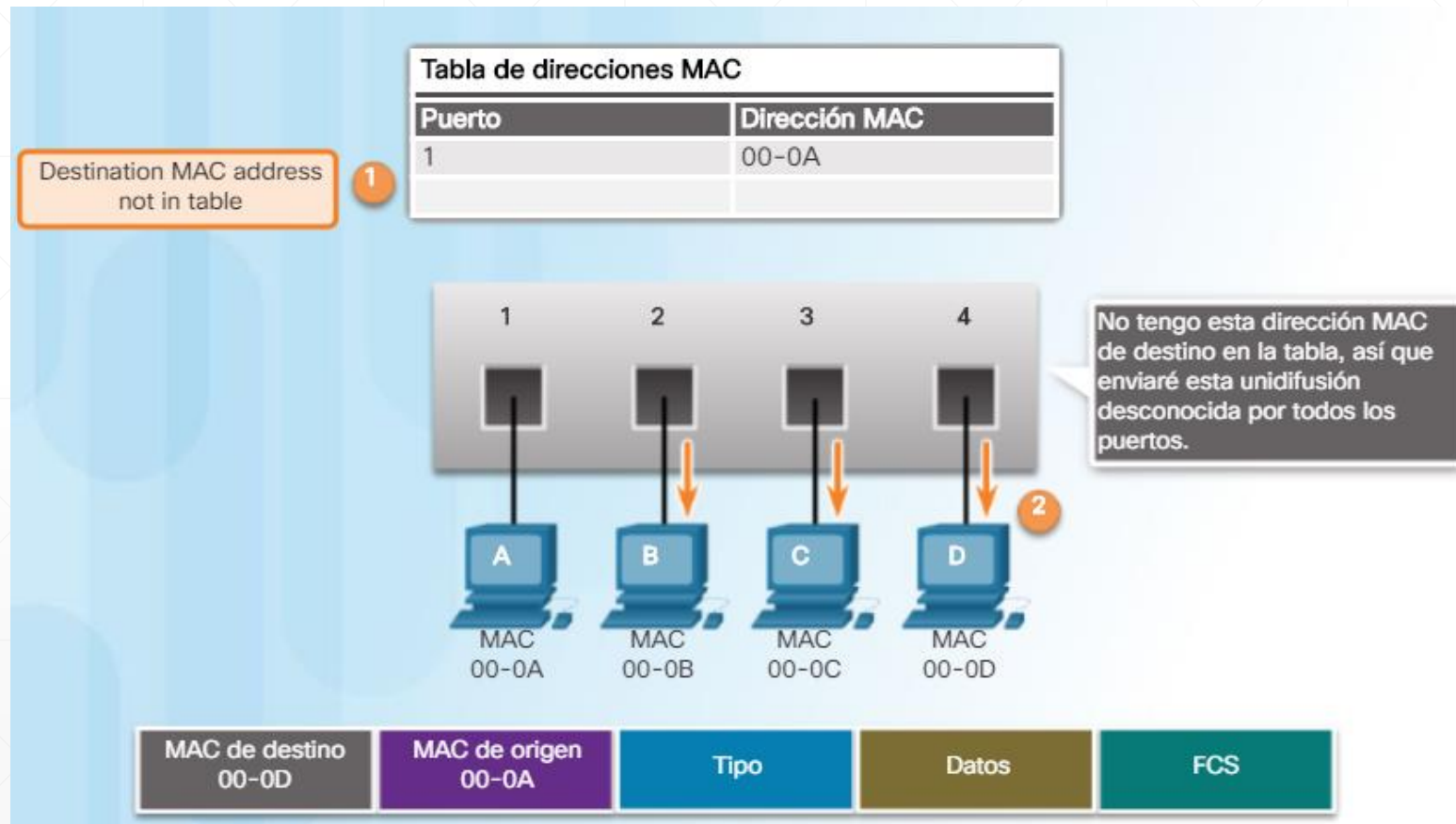
- Forward it:
 - Existe una entrada en la MAC Address Table (CAM) para la MAC Address de destino de la trama. El switch únicamente renvía la trama al puerto asociado a la MAC destino.
 - Flood it:
 - No existe una entrada en la MAC Address Table (CAM) asociada a la MAC Address de destino. El switch debe enviar la trama a todos los puertos habilitados, diferentes al puerto de origen.
 - Filter it:
 - El switch detecta que la MAC Address destino de la trama está asociada al puerto origen por el cual ingresó la trama. El switch descarta la trama.
-

Aprendizaje: Examinar la dirección MAC de Origen

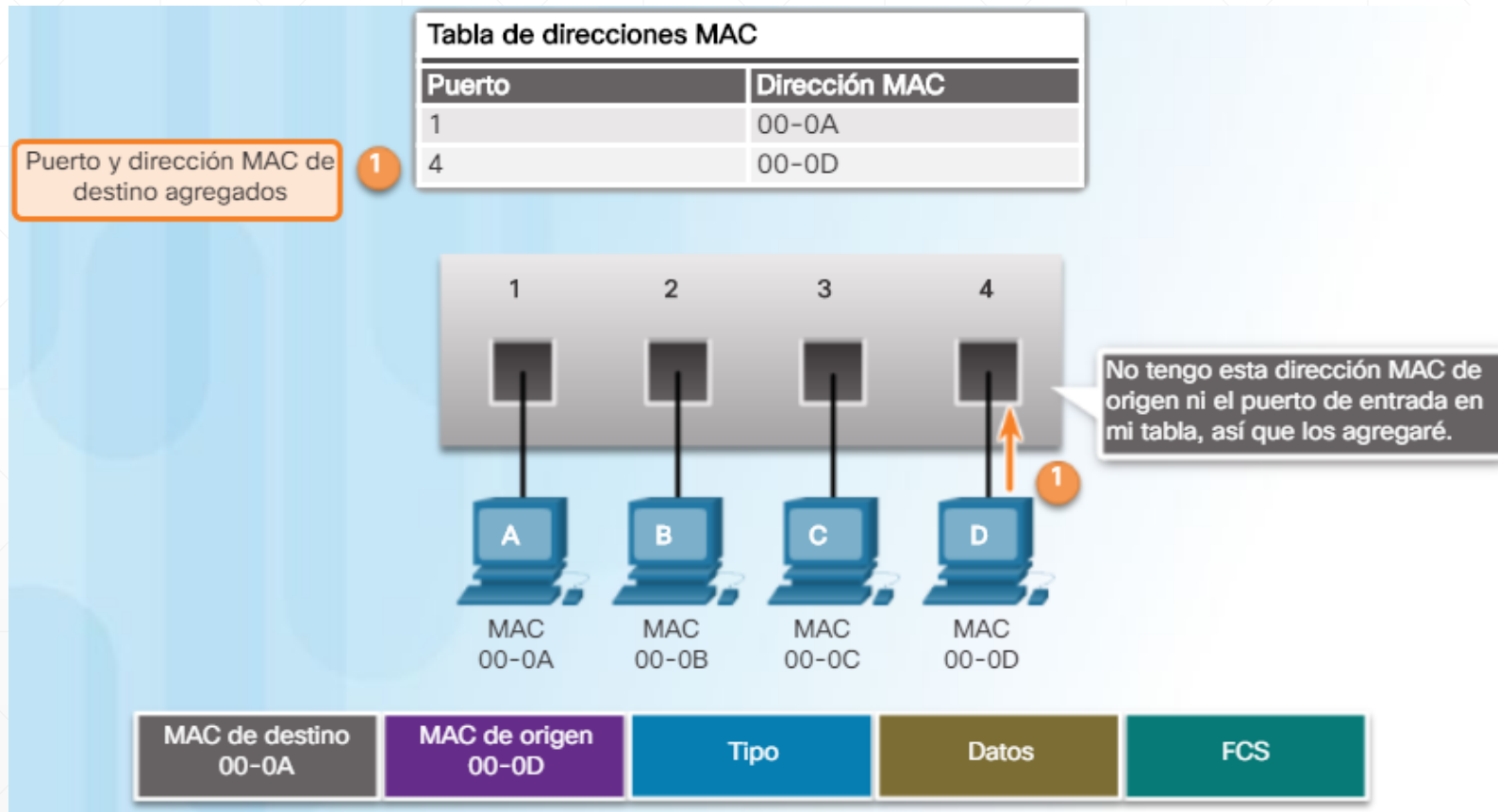


De manera predeterminada, la mayoría de los switches Ethernet guardan una entrada en la tabla durante cinco minutos.

Aprendizaje: Examinar la dirección MAC de origen



Aprendizaje: Examinar la dirección MAC de origen



Métodos de envío de paquetes del switch

- **Switching de almacenamiento y envío (Store-and-forward):**

- Cuando el switch recibe la trama, la almacena en los búferes de datos hasta recibir la trama en su totalidad.
- 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.

- **Switching por método de corte (Cut-through):**

- El switch envía la trama antes de recibirla en su totalidad. Como mínimo, debe leer la dirección de destino para que la trama se pueda enviar.
 - El switch no lleva a cabo ninguna verificación de errores en la trama.
 - Por defecto los switches utilizan este método en sus puertos hasta cierto umbral de errores definido por el administrador. Al alcanzar el umbral automáticamente pasan al método de Store-and-forward.
-

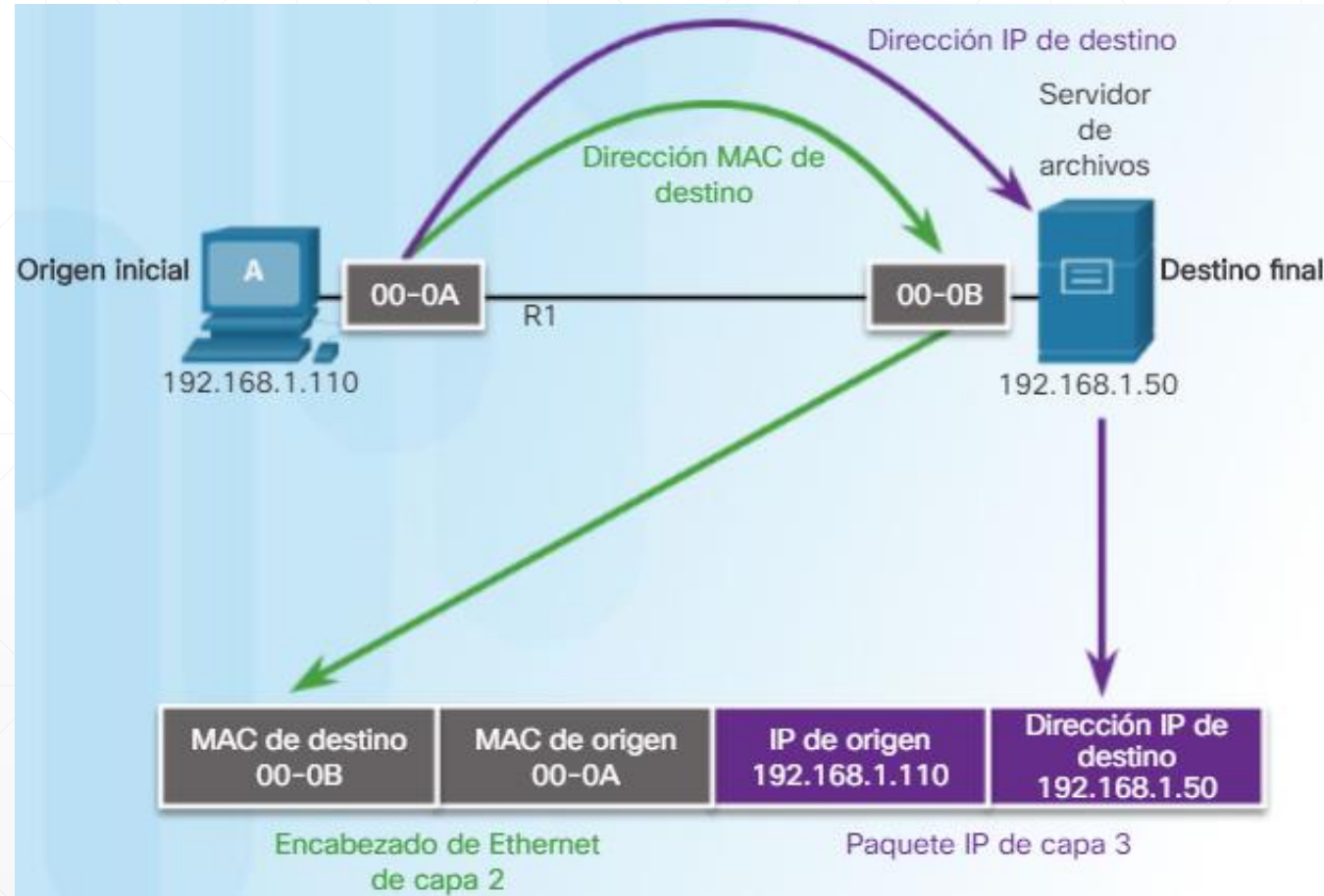
Métodos de envío de paquetes del switch

- **Switching por método de corte libre de fragmentos (Fragment-free)**
 - En este método, el switch almacena los primeros 64 bytes de la trama antes de reenviarla.
 - La mayoría de los errores y las colisiones de la red se producen en esos primeros 64 bytes.
-

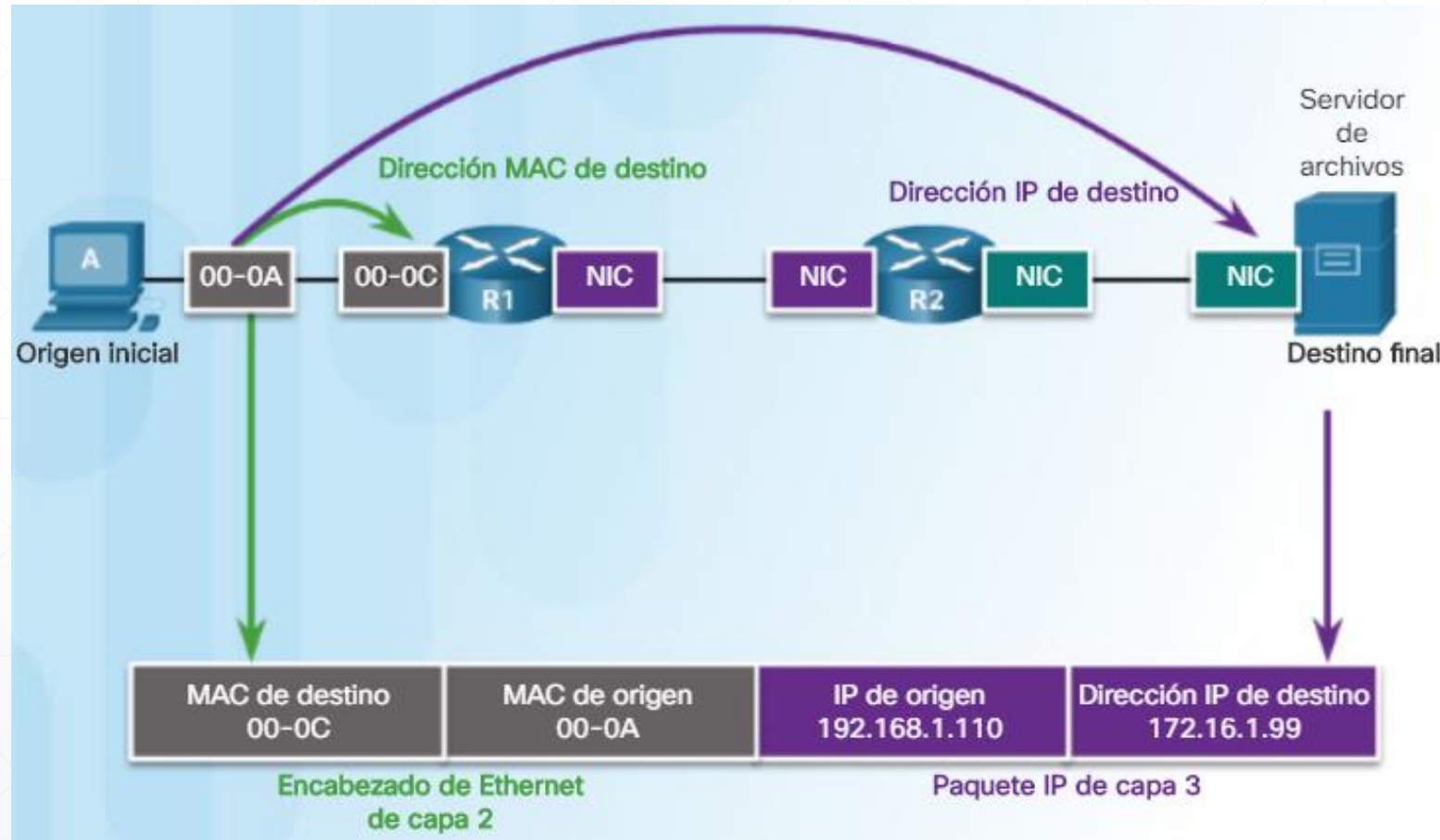
Almacenamiento en búfer de memoria en los switches

- Búfer de memoria basada en puerto
 - Las tramas se almacenan en colas conectadas a puertos de entrada y de salida específicos.
 - Búfer de memoria compartida
 - Deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch.
-

Comunicación en una red local: destino en la misma red



Comunicación con una red remota



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

ARP

ARP proporciona dos funciones básicas:

1. Resolución de direcciones IPv4 a direcciones MAC
 2. Mantenimiento de una tabla de asignaciones
-

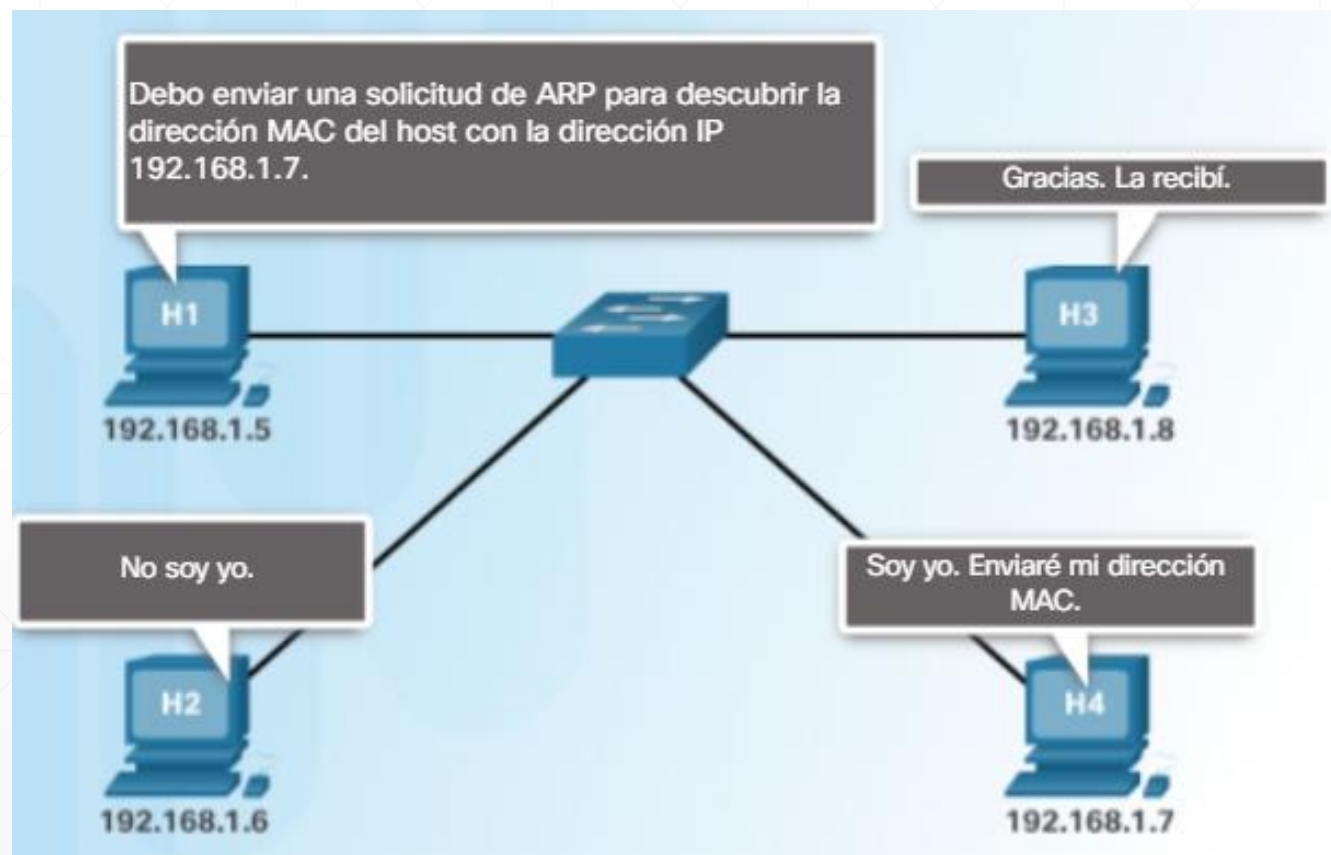
Funciones del ARP

- Cuando se envía un paquete a la capa de enlace de datos para encapsularlo en una trama de Ethernet, el dispositivo consulta una tabla en su memoria para encontrar la dirección MAC que está asignada a la dirección IPv4.
 - Esta tabla se denomina “tabla ARP” o “caché ARP”.
 - El dispositivo emisor busca en su tabla ARP la dirección IPv4 de destino y la dirección MAC correspondiente.
-

Funciones del ARP

- Si la dirección IPv4 de destino del paquete está en la misma red que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 de destino en la tabla ARP.
 - Si la dirección IPv4 de destino está en una red diferente que la dirección IPv4 de origen, el dispositivo busca la dirección IPv4 del gateway predeterminado.
 - Si el dispositivo localiza la dirección IPv4, se utiliza la dirección MAC correspondiente como la dirección MAC de destino de la trama. Si no se encuentra ninguna entrada, el dispositivo envía una solicitud de ARP.
-

El proceso ARP



Eliminación de entradas en una tabla ARP

- Depende del sistema operativo
 - Algunos sistemas operativos Windows eliminan entradas de ARP que no hayan sido usadas en el transcurso de 2 minutos.
-

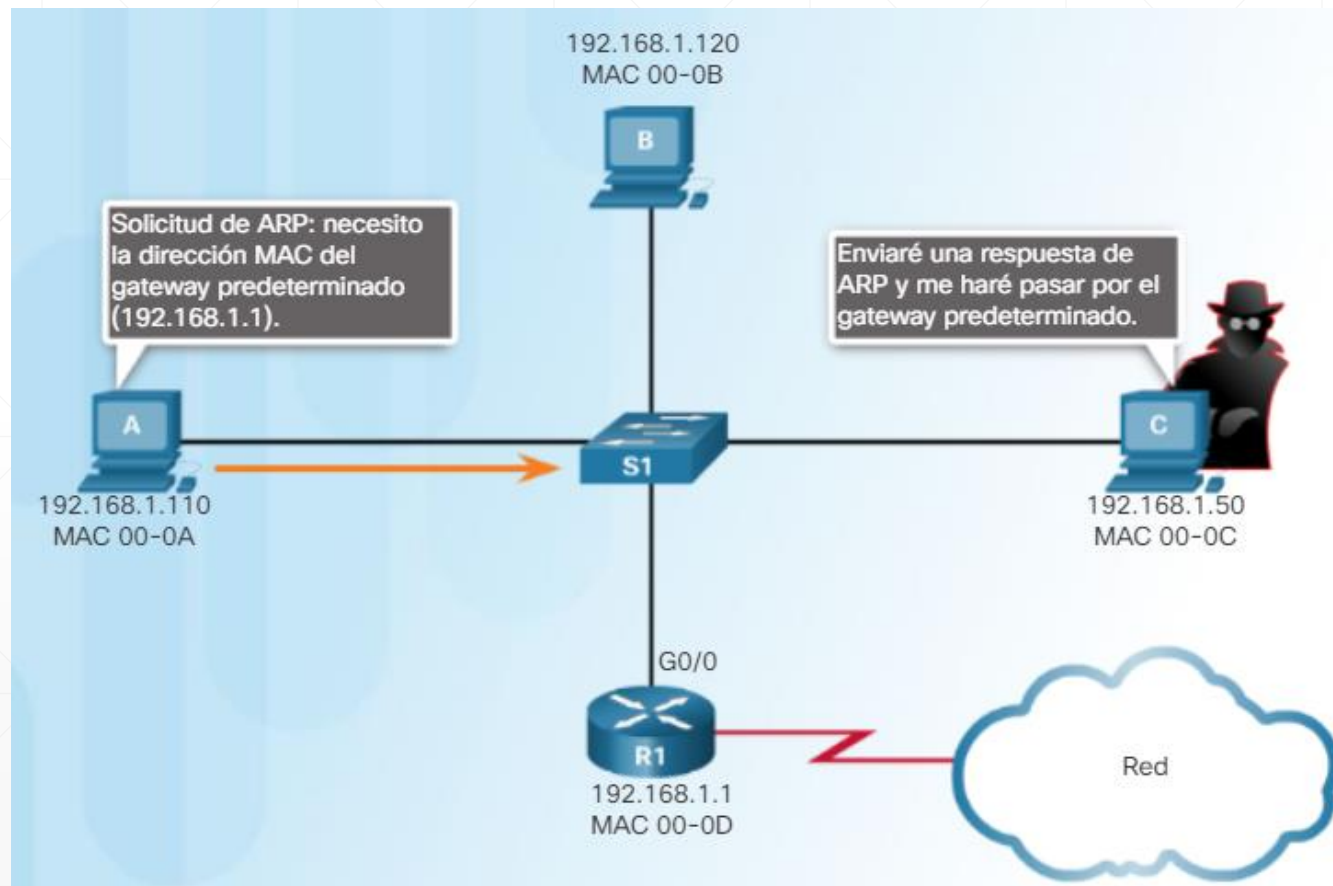
Comando para visualizar Tablas ARP

- Para un router Cisco
 - `show ip arp`
 - Para Windows
 - `arp -a`
-

Difusiones de ARP

- Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de difusión.
 - Si se encendiera una gran cantidad de dispositivos que comenzaran a acceder a los servicios de red al mismo tiempo, el rendimiento podría disminuir durante un breve período.
-

Suplantación de ARP



Actividad

Características de un hacker	MAC	LLC
Controla la tarjeta de interfaz de red mediante controladores.		
Trabaja con las capas superiores a fin de agregar información de la aplicación para la distribución de datos a los protocolos de nivel más alto.		
Trabaja con el hardware para admitir requisitos de ancho de banda; revisa si hay errores en los bits enviados y recibidos.		
Controla el acceso al medio utilizando requisitos de estándares de señalización y medios físicos.		
Admite la tecnología Ethernet mediante el uso de CSMA/CD o CSMA/CA.		
Mantiene una independencia relativa del equipo físico.		

Tarea

1. Para el próximo miércoles: Investigar, en no más de una página, qué es un Jumbo Frame, campos que tiene y diferencia con un frame ethernet normal.

