

# Redes



## Manual

Vol. 1 (Capa 1 y 2 Modelo OSI)



**ALHUBO**

Alejandro Huerta Bolaños

**Primera Edición**

2023

# Índice

<b>Índice</b>	<b>1</b>
<b>Redes</b>	<b>3</b>
<b>Fundamentos de la comunicación</b>	<b>3</b>
<b>Protocolos</b>	<b>3</b>
Codificación de los mensajes	3
Formato y encapsulamiento del mensaje	4
Tamaño del mensaje	4
Sincronización del mensaje	4
Opciones de entrega del mensaje	5
<b>Descripción general del protocolo de red</b>	<b>5</b>
<b>Funciones de protocolo de red</b>	<b>6</b>
<b>Interacción de protocolos</b>	<b>7</b>
<b>Evolución de los conjuntos de protocolos</b>	<b>8</b>
<b>Ejemplo de protocolo TCP/IP</b>	<b>9</b>
<b>Conjunto de TCP/IP</b>	<b>10</b>
<b>Proceso de comunicación TCP/IP</b>	<b>10</b>
<b>Modelos en capas</b>	<b>11</b>
El modelo de referencia OSI	12
Modelo de protocolo TCP/IP	12
Comparación del modelo OSI y el modelo TCP/IP	13
<b>Encapsulamiento de datos</b>	<b>13</b>
Segmentación del mensaje	13
Secuenciación	14
Unidades de datos de protocolo	14
<b>Acceso a los datos</b>	<b>16</b>
Direcciones	16
Dirección lógica de capa 3	16
Dispositivos en la misma red	17
La misma red IP	18
Dispositivos en una red remota	19
Función de las direcciones de la capa de red	19
Diferentes redes IP	20
Direcciones de enlace de datos	21
<b>La conexión física</b>	<b>22</b>
<b>La capa física</b>	<b>23</b>
Componentes físicos	23
Codificación	23
Señalización	24
<b>La capa de enlace de datos</b>	<b>26</b>
Subcapas de enlace de datos IEEE 802 LAN/MAN	27
Frame de enlace de datos	30

Campos del frame	30
Direcciones de Capa 2	32
Tramas LAN y WAN	32
<b>Frames de Ethernet</b>	<b>34</b>
Subcapa MAC	35
Estándares Ethernet en la subcapa MAC	36
Campos de trama de Ethernet	37
Campos de trama en internet	37
Detalle de los campos del Ethernet Frame	37
<b>Procesamiento de tramas</b>	<b>38</b>
Dirección MAC de unicast	39
Dirección MAC broadcast	39
Dirección MAC de multicast	40
<b>Fundamentos de switches</b>	<b>41</b>
Switch, Aprendiendo y Reenviando	42
Examinar la dirección MAC de Origen	42
Buscar dirección MAC de destino	43
Se conoce la dirección MAC destino	44
No se conoce la dirección MAC destino	44
Métodos de reenvío de tramas de los switches Cisco	45
Switching de almacenamiento y envío (Store-and-forward switching)	45
Switching por método de corte (Cut-through switching)	45
Almacenamiento en búfer de memoria en los switches (Memory Buffering on Switches)	46
Memory Buffering Methods	46
Configuración de dúplex y velocidad	47
Auto-MDIX (MDIX automático)	48

# Redes

Esencialmente Redes es la interconexión y comunicación de dispositivos electrónicos a través de un medio. Pueden ser PAN, LAN, Campus, MAN y WAN.

**Nota** [Este volumen solo abarca el funcionamiento de la capa 1 y 2 del modelo OSI.]

## Fundamentos de la comunicación

### **Los orígenes de los mensajes**

Son los dispositivos que envían un mensaje.

### **Destino del mensaje(recibidor)**

Dispositivo al cual se destina el mensaje.

### **Canal**

Medio por el cual viaja el mensaje, puede ser utp, fibra o wifi.

Para que una comunicación pueda ocurrir se requieren reglas precisas que conoceremos como **protocolos**:

- Un emisor y un receptor identificados
- Idioma y gramática común
- Velocidad y momento de entrega
- Requisitos de confirmación o acuse de recibo

## Protocolos

Los protocolos de red tienen los siguientes requisitos:

- Codificación de los mensajes
- Formato y encapsulamiento del mensaje
- Tamaño del mensaje
- Sincronización del mensaje
- Opciones de entrega del mensaje

## Codificación de los mensajes

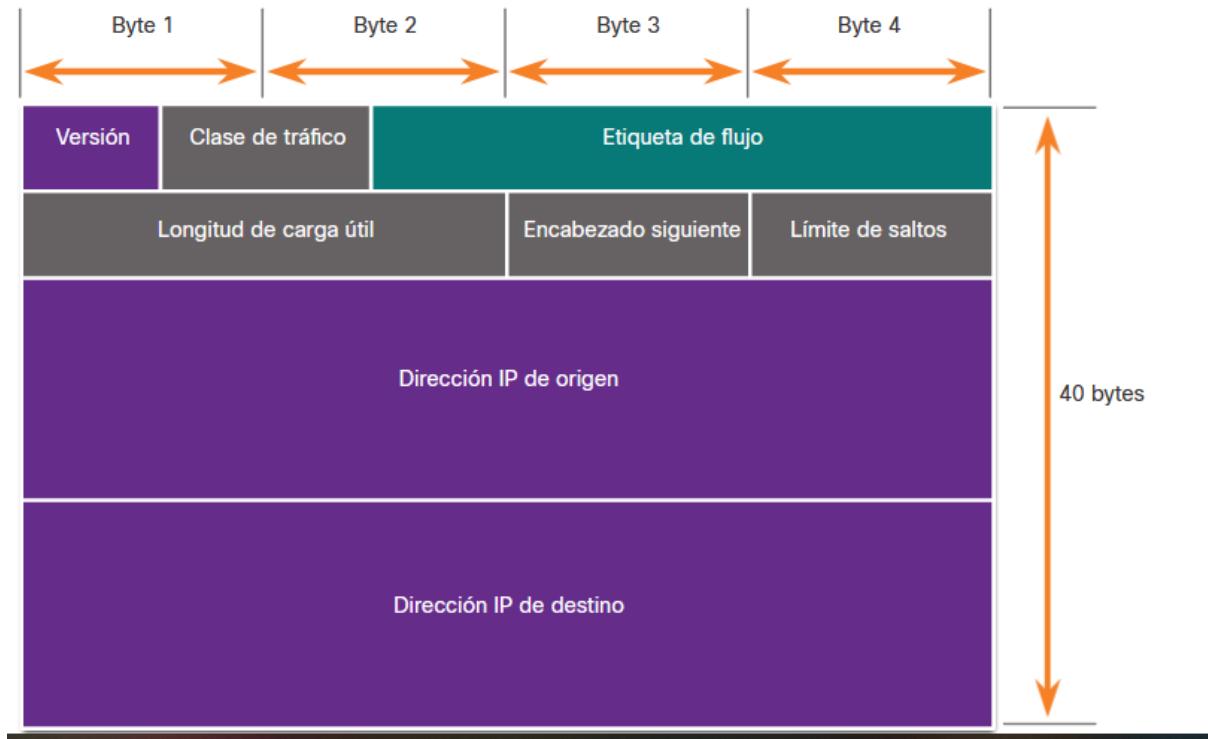
El primer paso es codificar el mensaje para poder enviarlo a través del medio, en caso de la transmisión de red el mensaje se tiene que codificar en binario.

**Nota** [Esto no encripta el mensaje, solo permite que la información pueda pasar por el medio.]

## Formato y encapsulamiento del mensaje

Para que el mensaje pueda llegar al destino se debe utilizar un formato o estructura específicos. Los formatos de los mensajes dependen del tipo de mensaje y el canal que se utilice para entregar el mensaje.

A continuación se ve un ejemplo general de cómo sería la estructura o encapsulado de un mensaje.



## Tamaño del mensaje

Para evitar congestión o interrupción en el tráfico de red por un solo host que acapara todo el canal para transmitir un mensaje muy grande, estos se dividen en partes estándar para poder permitir que otros mensajes utilicen el canal para transmitir o recibir.

## Sincronización del mensaje

El tiempo de los mensajes también es muy importante en las comunicaciones de red. El tiempo de los mensajes incluye lo siguiente:

- **Control de flujo**
  - Este es el proceso de gestión de la velocidad de transmisión de datos. La sincronización también afecta la cantidad de información que se puede enviar y la velocidad con la que puede entregarse. En la

comunicación de red, existen protocolos de red utilizados por los dispositivos de origen y destino para negociar y administrar el flujo de información.

- **Tiempo de espera de respuesta (Response Timeout)**
  - Los hosts de las redes tienen reglas que especifican cuánto tiempo deben esperar una respuesta y qué deben hacer si se agota el tiempo de espera para la respuesta.
- **El método de acceso**
  - Determina en qué momento alguien puede enviar un mensaje.

## Opciones de entrega del mensaje

Un mensaje se puede entregar de diferentes maneras.

- **Unicast**
  - La información se transmite a un único dispositivo final.
- **Multicast**
  - La información se transmite a uno o varios dispositivos finales.
- **Broadcast**
  - La información se transmite a todos los dispositivos finales.

## Descripción general del protocolo de red

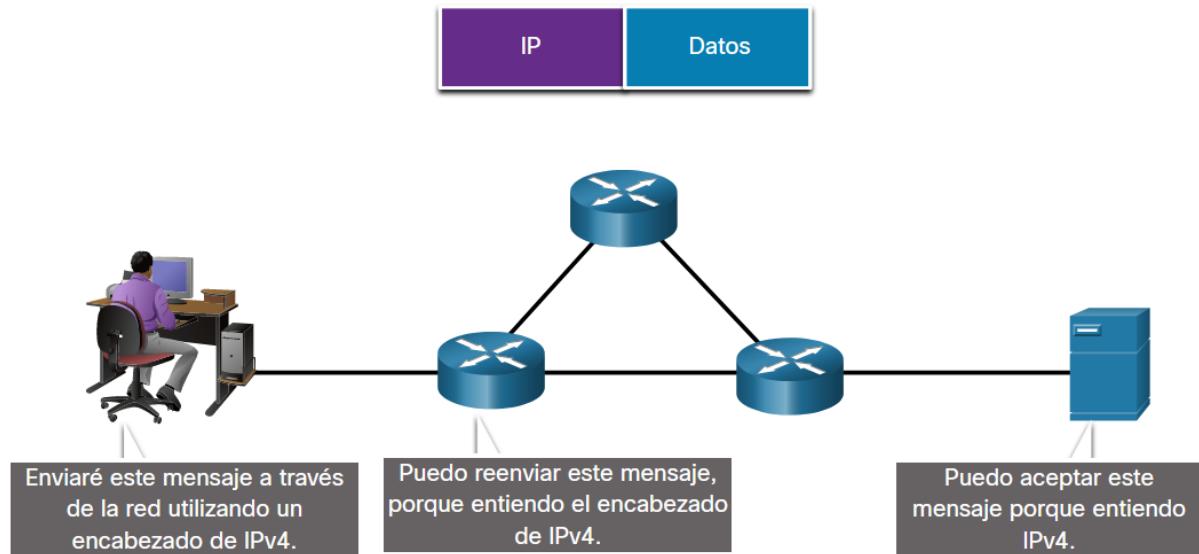
Para que los dispositivos finales puedan comunicarse a través de una red, cada dispositivo debe cumplir el mismo conjunto de reglas. Estas reglas se denominan protocolos y tienen muchas funciones en una red.

Tipo de protocolo	Descripción
<b>Protocolos de comunicaciones de red</b>	Permiten que dos o más dispositivos se comuniquen a través de uno o más compatibles. La familia de tecnologías Ethernet implica una variedad de protocolos como IP, Protocolo de control de transmisión (TCP), HyperText Protocolo de transferencia (HTTP) y muchos más.
<b>Protocolos de seguridad de red</b>	Protegen los datos para proporcionar autenticación, integridad de los datos y cifrado de datos. Ejemplos de protocolos seguros incluyen Secure Shell (SSH),

	Secure Sockets Layer (SSL) y Capa de transporte Security (TLS).
<b>Protocolos de routing</b>	Permiten a los routers intercambiar información de ruta, comparar ruta y, a continuación, seleccionar la mejor ruta al destino. Ejemplos de protocolos de enrutamiento incluyen Abrir ruta más corta primero OSPF y Protocolo de puerta de enlace de borde (BGP)
<b>Protocolos de Detección de servicios</b>	Se utilizan para la detección automática de dispositivos o servicios. Entre los ejemplos de protocolos de descubrimiento de servicios se incluyen Dynamic Host Protocol de configuración (DHCP) que descubre servicios para la dirección IP y Sistema de nombres de dominio (DNS) que se utiliza para realizar traducción de nombre a dirección IP

## Funciones de protocolo de red

Para comprender mejor el funcionamiento de los protocolos, a continuación se ejemplifica cómo para enviar un mensaje todos los dispositivos de la red acuerdan utilizar el mismo protocolo IPv4.

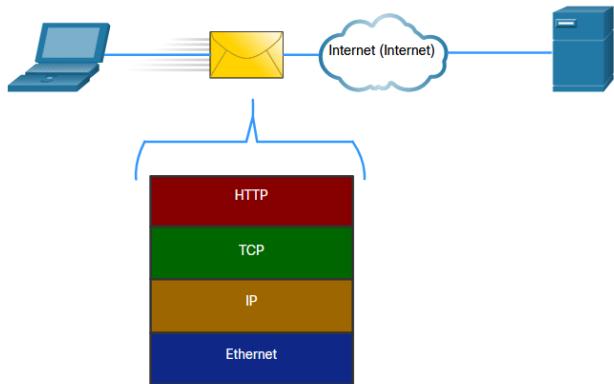


La siguiente tabla enumera las funciones de estos protocolos.

Función	Descripción
<b>Direccionamiento</b>	Esto identifica al remitente y al destinatario del mensaje utilizando un esquema de direccionamiento definido. Ejemplos de protocolos que proporcionan incluyen Ethernet, IPv4 e IPv6.
<b>Confiabilidad</b>	Esta función proporciona mecanismos de entrega garantizados en caso de mensajes se pierden o se corrompen en tránsito. TCP proporciona entrega garantizada.
<b>Control de flujo</b>	Esta función asegura que los datos fluyan a una velocidad eficiente entre dos dispositivos de comunicación. TCP proporciona servicios de control de flujo.
<b>Secuenciación</b>	Esta función etiqueta de forma única cada segmento de datos transmitido. Utiliza la información de secuenciación para volver a ensamblar la información correctamente. Esto es útil si se pierden los segmentos de dato, retrasado o recibido fuera de pedido. TCP proporciona servicios de secuenciación.
<b>Detección de errores</b>	Esta función se utiliza para determinar si los datos se dañaron durante la transmisión. Varios protocolos que proporcionan detección de errores incluyen Ethernet, IPv4, IPv6 y TCP.
<b>Interfaz de la aplicación</b>	Esta función contiene información utilizada para paso a paso comunicaciones entre aplicaciones de red. Por ejemplo, al acceder a una página web, los protocolos HTTP o HTTPS se utilizan para comunicarse entre el cliente y el servidor web.

## Interacción de protocolos

Normalmente la transmisión de un mensaje a través de una red requiere varios protocolos, cada uno con sus propias funciones y formatos. A continuación se ve un ejemplo general de los protocolos que se ocupan para resolver un mensaje de petición de una página web.



Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos.

Una de las mejores formas para visualizar el modo en que los protocolos interactúan dentro de una suite es ver la interacción como una pila. Los protocolos se muestran en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Las capas inferiores de la pila se encargan del movimiento de datos por la red y proporcionan servicios a las capas superiores, las cuales se enfocan en el contenido del mensaje que se va a enviar.

## Evolución de los conjuntos de protocolos

Desde la década de 1970 ha habido varios conjuntos de protocolos diferentes, algunos desarrollados por una organización de estándares y otros desarrollados por varios proveedores.

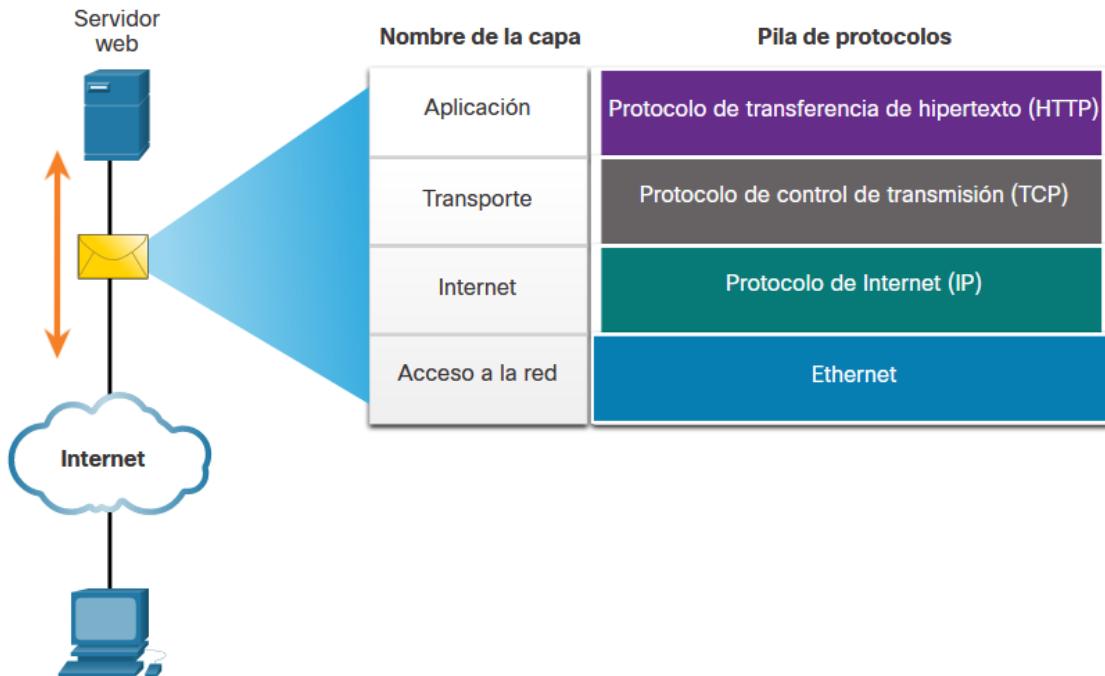
Durante la evolución de las comunicaciones de red e Internet hubo varios conjuntos de protocolos competidores, como se muestra en la figura.

Nombre de capa TCP / IP	TCP/IP	ISO	AppleTalk	Novell Netware
Aplicación	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transporte	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Acceso a la red	Ethernet ARP WLAN			

## Ejemplo de protocolo TCP/IP

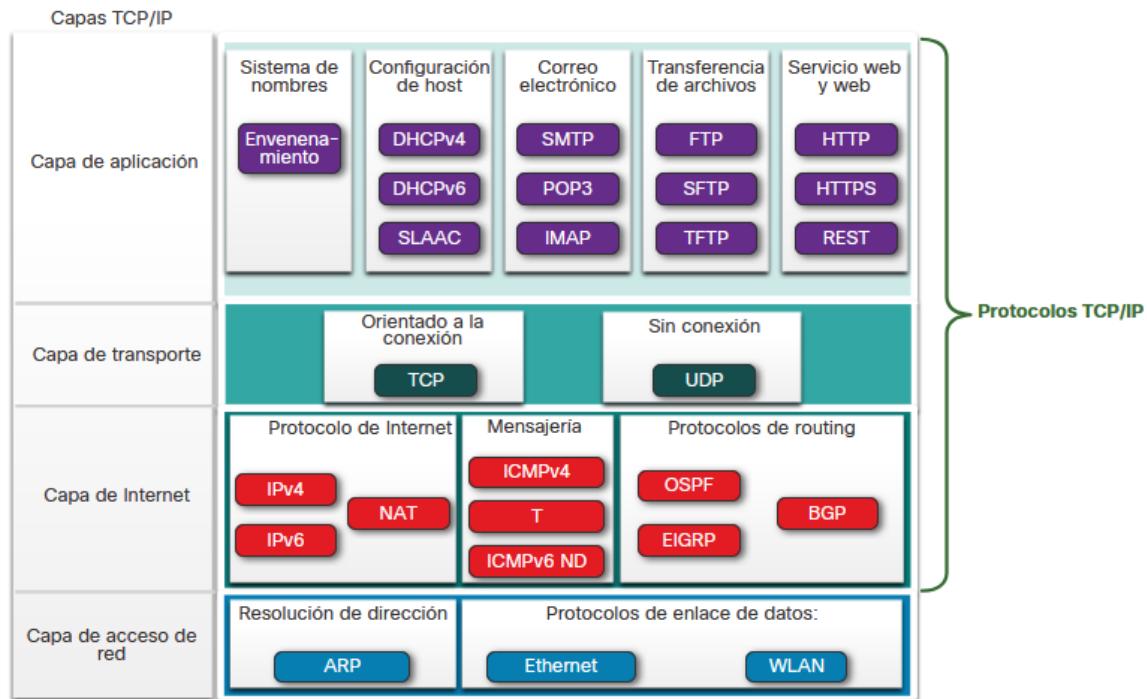
**Nota** [ Los protocolos TCP/IP son específicos de las capas Aplicación, Transporte e Internet. No hay protocolos TCP/IP en la capa de acceso a la red.]

La figura muestra un ejemplo de los tres protocolos TCP/IP utilizados para enviar paquetes entre el navegador web de un host y el servidor web.

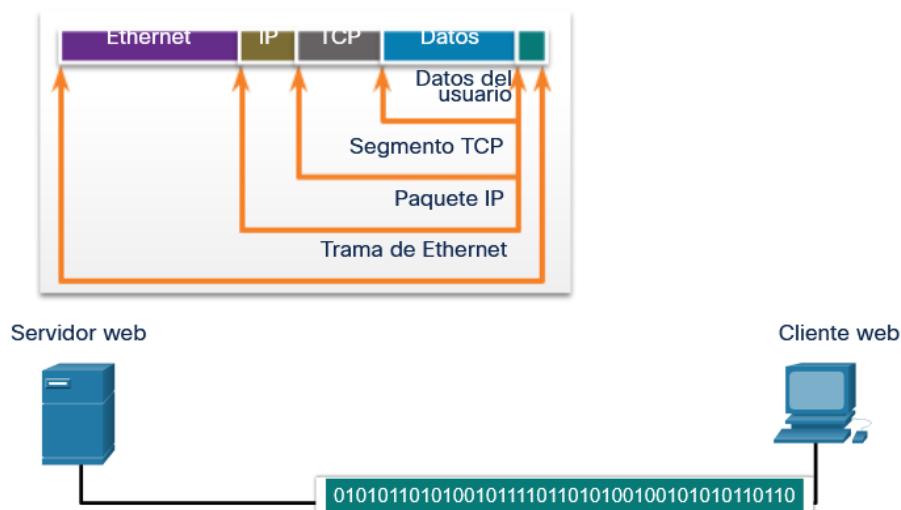


# Conjunto de TCP/IP

Hoy en día, el conjunto de protocolos TCP/IP incluye muchos protocolos y continúa evolucionando para admitir nuevos servicios. Algunos de los más populares se muestran en la figura.



## Proceso de comunicación TCP/IP

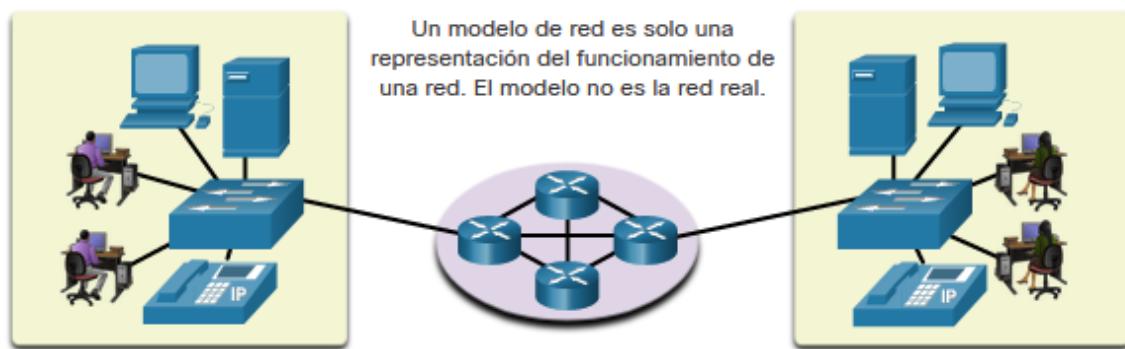


En la imagen se puede observar que para enviar un paquete este primero encapsula los datos con el protocolo **TCP** (Para verificar que los datos lleguen), después se

encapsula con **IP** (Para direccionar en capa 3) y por último **Ethernet** (Para direccionar en capa 2).

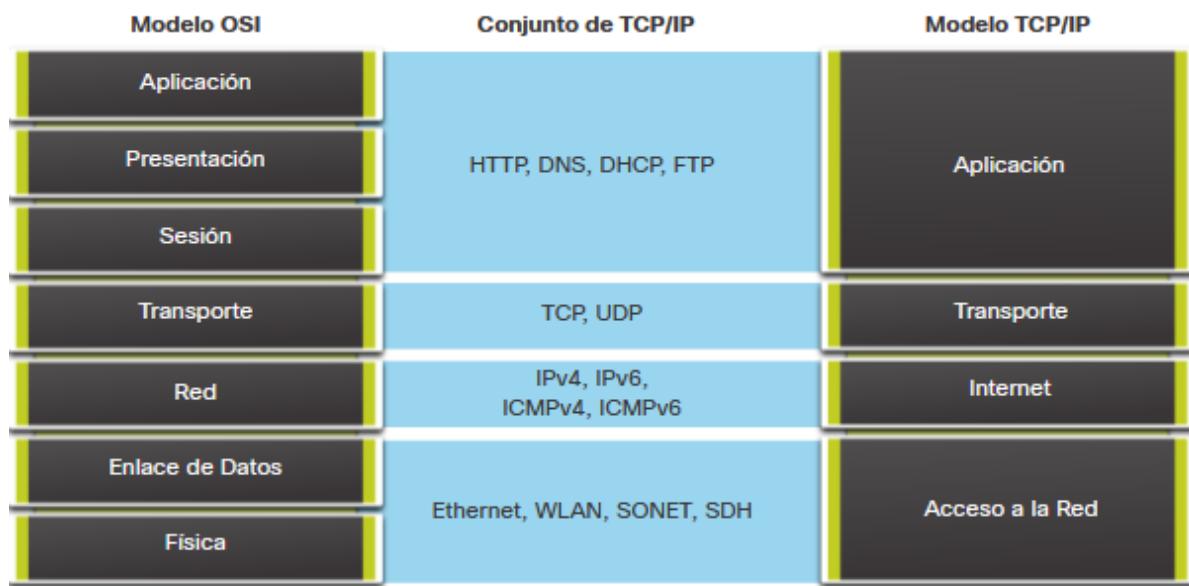
## Modelos en capas

El modelo en capas ayuda a entender cómo funciona el transporte de un mensaje a través de la red, capa por capa como se encapsula para poder viajar a través de los dispositivos.



Para ello existen 2 modelos que son equiparables

- TCP/IP
- OSI



Cuando un mensaje necesita enviarse empieza en la sima del modelo y baja capa por capa hasta llegar a la capa física. Pero cuando un mensaje necesita ser recibido empieza por la parte inferior del modelo hasta llegar a la capa de aplicación.

## El modelo de referencia OSI

Este modelo presenta varias capas que ayudan a comprender mejor todos los pasos por los que pasa un mensaje.

<b>capa del modelo OSI</b>	<b>Descripción</b>
<b>7 - Aplicación</b>	La capa de aplicación contiene protocolos utilizados para comunicaciones paso a paso.
<b>6 - Presentación</b>	La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de capa de aplicación.
<b>5 - Sesión</b>	La capa de sesión proporciona servicios a la capa de presentación para organizar el diálogo y administrar el intercambio de datos.
<b>4 - Transporte</b>	La capa de transporte define servicios para segmentar, transferir y volver a montar los datos para las comunicaciones individuales.
<b>3 - Red</b>	La capa de red proporciona servicios para intercambiar las piezas individuales a través de la red entre los dispositivos finales identificados.
<b>2 - Enlace de datos</b>	Los protocolos de la capa de enlace de datos describen métodos para intercambiar datos. Frames entre dispositivos a través de un medio común.
<b>1 - Física</b>	Los protocolos de capa física describen los componentes mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para una transmisión de bits hacia y desde una red dispositivo.

**Nota** [ Mientras las capas del modelo TCP/IP se mencionan solo por el nombre, las siete capas del modelo OSI se mencionan con frecuencia por número y no por nombre. Por ejemplo, la capa física se conoce como Capa 1 del modelo OSI, la capa de enlace de datos es Capa 2, y así sucesivamente.]

## Modelo de protocolo TCP/IP

El modelo TCP/IP muestra una representación más fiel de cómo funciona la transportación de un mensaje a través de la red.

<b>Capa del modelo TCP/IP</b>	<b>Descripción</b>
<b>4 - Aplicación</b>	Representa datos para el usuario más el control de codificación y de diálogo.
<b>3 - Transporte</b>	Admite la comunicación entre distintos dispositivos a través de diversas redes.
<b>2 - Internet</b>	Determina el mejor camino a través de una red.
<b>1 - Acceso a la red</b>	Controla los dispositivos del hardware y los medios que forman la red.

## Comparación del modelo OSI y el modelo TCP/IP

En su mayoría las capas del modelo TCP/IP pueden describir las capas del modelo OSI, exceptuando la capa de acceso a la red ya que TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; sólo describe la transferencia desde la capa de Internet a los protocolos de red física. Las capas OSI 1 y 2 tratan los procedimientos necesarios para acceder a los medios y las maneras físicas de enviar datos por la red.

## Encapsulamiento de datos

### Segmentación del mensaje

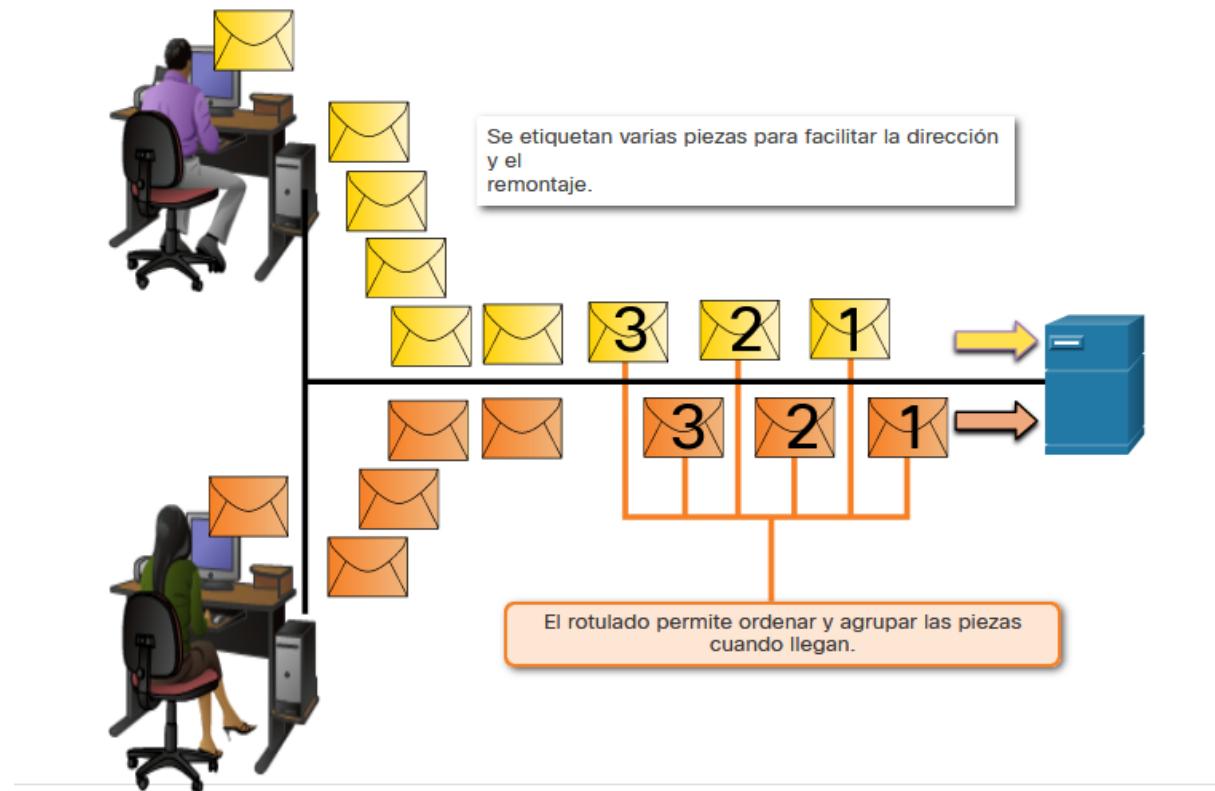
Cuando un mensaje tiene una gran cantidad de tamaño este se divide en partes para poder enviarlo a través de la red. Esto permite utilizar la **multiplexación** para enviar más de un mensaje a la vez.

La segmentación de mensajes tiene dos beneficios principales.

- **Aumenta la velocidad**
  - Al enviar un mensaje en partes permite que otros mensajes puedan utilizar el canal y llegar rápidamente en lugar de tener que esperar a que otro termine.
- **Aumenta la eficiencia**
  - Si la transmisión de datos llega a fallar, permite enviar sólo las partes dañadas en lugar de todo el mensaje.

## Secuenciación

Al segmentar un mensaje se aumenta la dificultad por el hecho de que pueden llegar en desorden, para ello cada parte es enumerada para poder ser ensamblada en el destino.



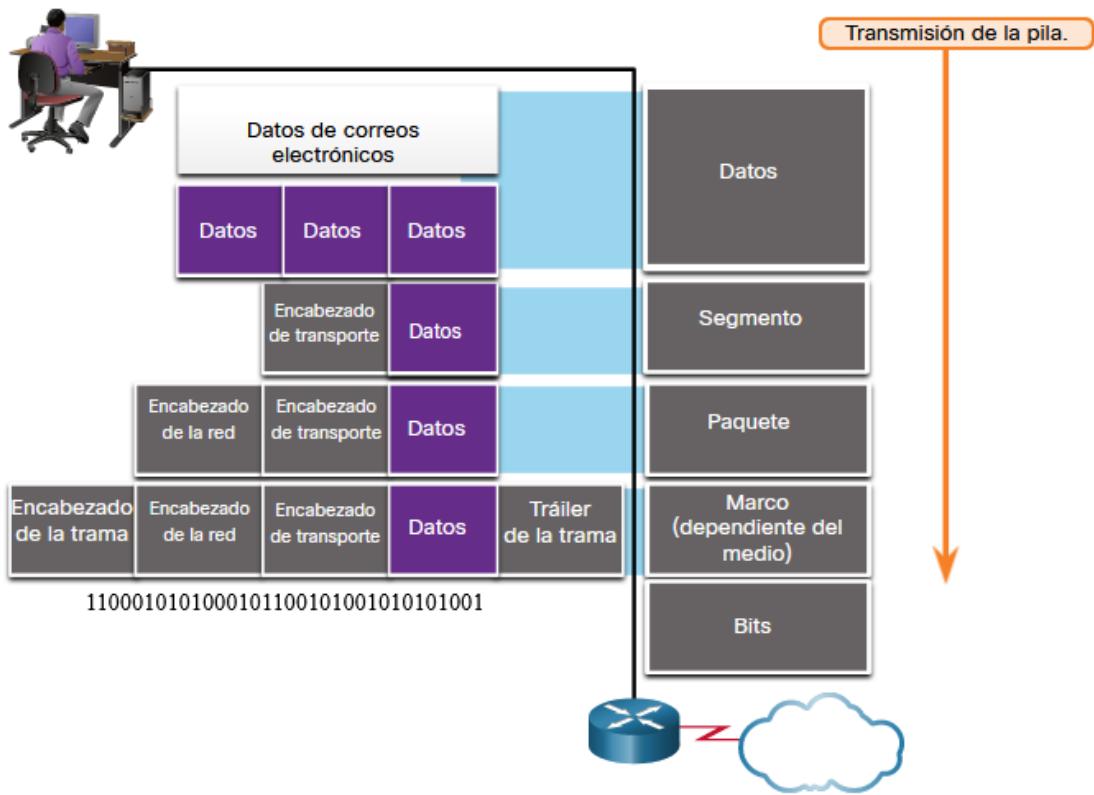
## Unidades de datos de protocolo

Mientras los datos de la aplicación bajan a la pila del protocolo y se transmiten por los medios de la red, se agrega diversa información de protocolos en cada nivel. Esto comúnmente se conoce como proceso de encapsulamiento.

**Nota** [Aunque la PDU(Protocol Data Unit) UDP (Unidades de datos de protocolo) se denomina datagrama, los paquetes IP a veces también se conocen como datagramas IP. ]

Durante el encapsulamiento, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar sus funciones nuevas.

Aunque no existe una convención universal de nombres para las PDU, se denominará de acuerdo con los protocolos de la suite TCP/IP. Las PDU de cada tipo de datos se muestran en la figura.



- **Datos**
  - Término general que se utiliza en la capa de aplicación para la PDU.
- **Segmento**
  - PDU de la capa de transporte
- **Paquete**
  - PDU de la capa de red
- **Trama o Frame**
  - PDU de la capa de enlace de datos
- **Bits**
  - PDU de capa física que se utiliza cuando se transmiten datos físicamente por el medio.

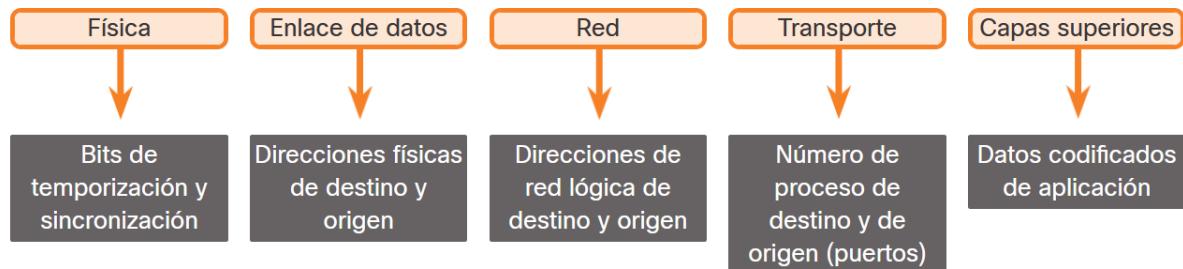
**Nota** [Si el encabezado de transporte es **TCP**, entonces es un segmento. Si el encabezado de transporte es **UDP**, entonces es un datagrama]

# Acceso a los datos

## Direcciones

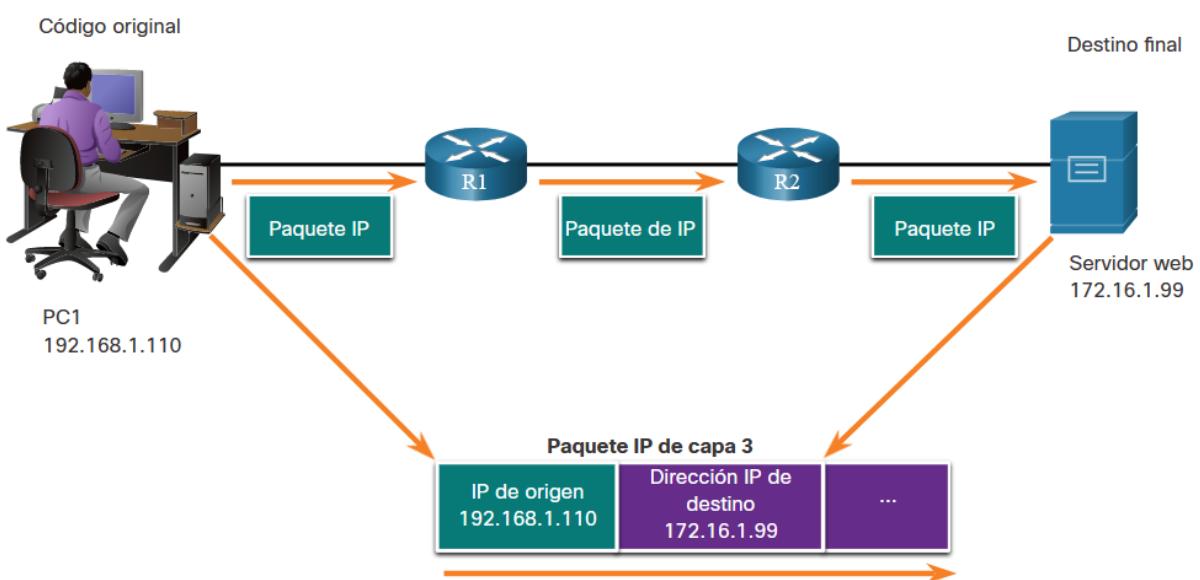
La capa de red y la capa de enlace de datos son responsables de enviar los datos desde el dispositivo de origen o emisor hasta el dispositivo de destino o receptor.

- **Direcciones de origen y de destino de la capa de red**
  - Son responsables de enviar el frame en la red o de una red a otra.
- **Direcciones de origen y de destino de la capa de enlace de datos**
  - Son responsables de enviar el frame de enlace de datos desde una tarjeta de interfaz de red (NIC) a otra en la misma red.



## Dirección lógica de capa 3

Una dirección lógica de la capa de red, o capa 3, se utiliza para enviar el paquete IP desde el dispositivo de origen hasta el dispositivo de destino, como se muestra en la figura.



Los paquetes IP contienen dos direcciones IP:

- **Dirección IP de origen**
  - La dirección IP del dispositivo emisor, la fuente de origen del paquete.
- **Dirección IP de destino**
  - La dirección IP del dispositivo receptor, es decir, el destino final del paquete.

**Nota** [Las direcciones IP pueden o no estar en la misma red.]

Un paquete IP contiene dos partes:

- **Porción de red (IPv4) o Prefijo (IPv6)**
  - La sección más a la izquierda de la dirección que indica la red de la que es miembro la dirección IP. Todos los dispositivos de la misma red tienen la misma porción de red de la dirección.
- **Porción de host (IPv4) o ID de interfaz (IPv6)**
  - La parte restante de la dirección que identifica un dispositivo específico de la red. La sección de host es única para cada dispositivo o interfaz en la red.

**Nota** [La máscara de subred (IPv4) o la longitud del prefijo (IPv6) se utiliza para identificar la porción de red de una dirección IP de la porción del host.]

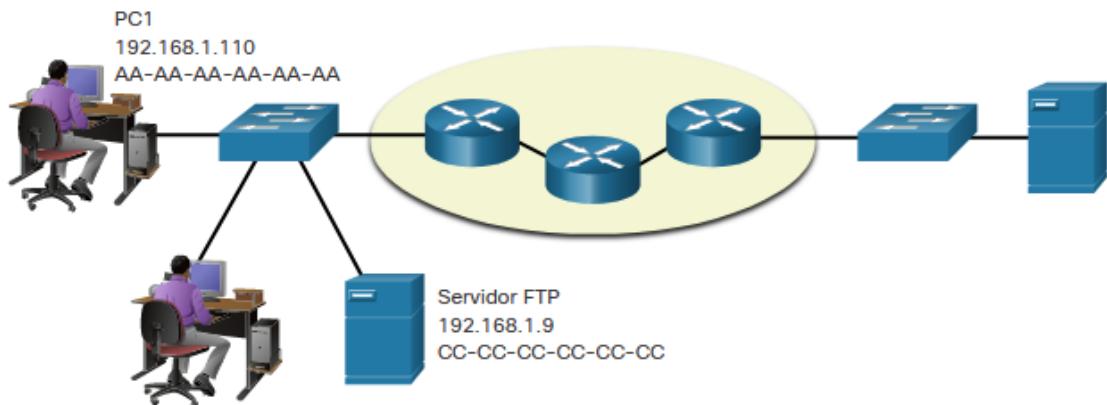
## Dispositivos en la misma red

En este ejemplo, tenemos un equipo cliente, PC1, que se comunica con un servidor FTP, en la misma red IP.

- **Dirección IPv4 de origen:** - la dirección IPv4 del dispositivo emisor, es decir, el equipo cliente PC1: 192.168.1.110.
- **Dirección IPv4 de destino:** - la dirección IPv4 del dispositivo receptor, el servidor FTP: 192.168.1.9.

En la figura, observe que la porción de red de las direcciones IP de origen y de destino se encuentran en la misma red. Observe en la figura que la parte de red de la dirección IPv4 de origen y la parte de red de la dirección IPv4 de destino son iguales y, por tanto, el origen y el destino están en la misma red.

Encabezado de la trama de Ethernet de enlace de datos		Encabezado de paquete IP de la capa de red		Datos
Destino	Origen	Origen	Destino	
CC-CC-CC-CC-CC-CC	AA-AA-AA-AA-AA-AA	Red 192.168.1. Host 110	Red 192.168.1. Host 9	

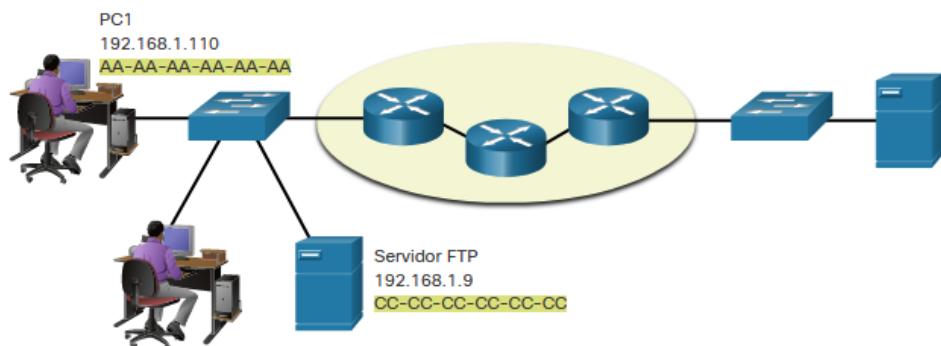


## La misma red IP

La función de las direcciones de la capa de enlace de datos.

Cuando el emisor y el receptor del paquete IP están en la misma red, la trama de enlace de datos se envía directamente al dispositivo receptor. En una red Ethernet, las direcciones de enlace de datos se conocen como direcciones de Control de acceso a medios de Ethernet (MAC), como se resalta en la figura.

Encabezado de la trama de Ethernet de enlace de datos		Encabezado de paquete IP de la capa de red		Datos
Destino	Origen	Origen	Destino	
CC-CC-CC-CC-CC-CC	AA-AA-AA-AA-AA-AA	Red 192.168.1. Host 110	Red 192.168.1. Host 9	



## Dispositivos en una red remota

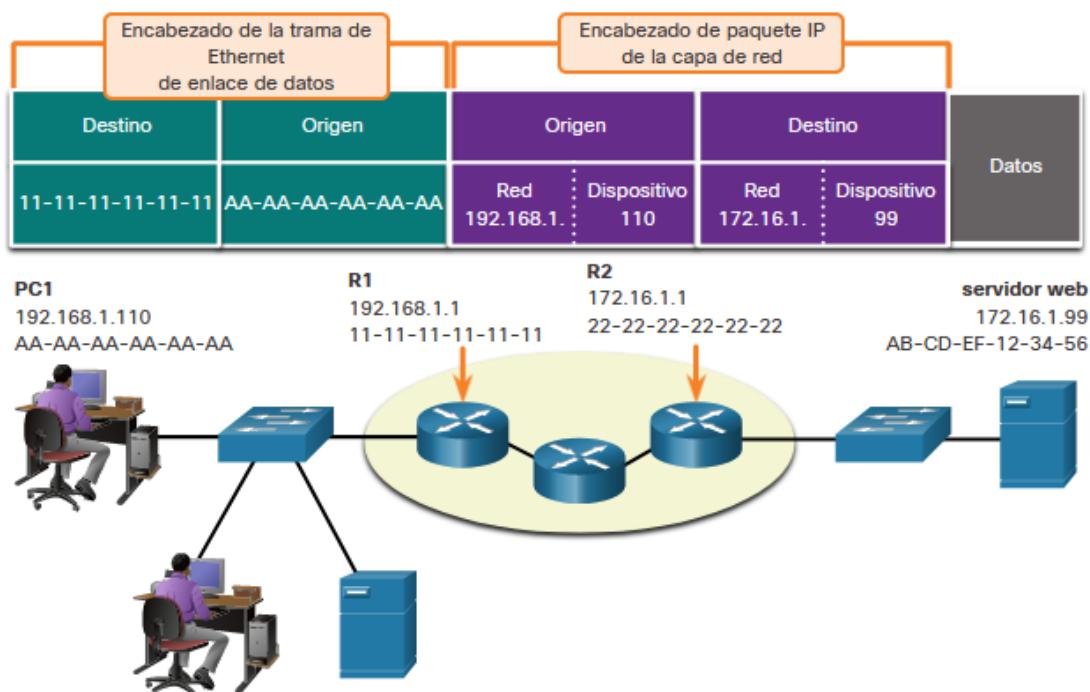
Ahora cuando el mensaje se envía a otra red el funcionamiento de la capa de red cambia.

Función de las direcciones de la capa de red

Se sabe que el mensaje va dirigido a otra red cuando las direcciones IP de origen y de destino representan la porción de red de dirección IP en redes diferentes.

- **Dirección IPv4 de origen:** - la dirección IPv4 del dispositivo emisor, es decir, el equipo cliente PC1: 192.168.1.110.
- **Dirección IPv4 de destino:** - la dirección IPv4 del dispositivo receptor, es decir, el servidor web: 172.16.1.99.

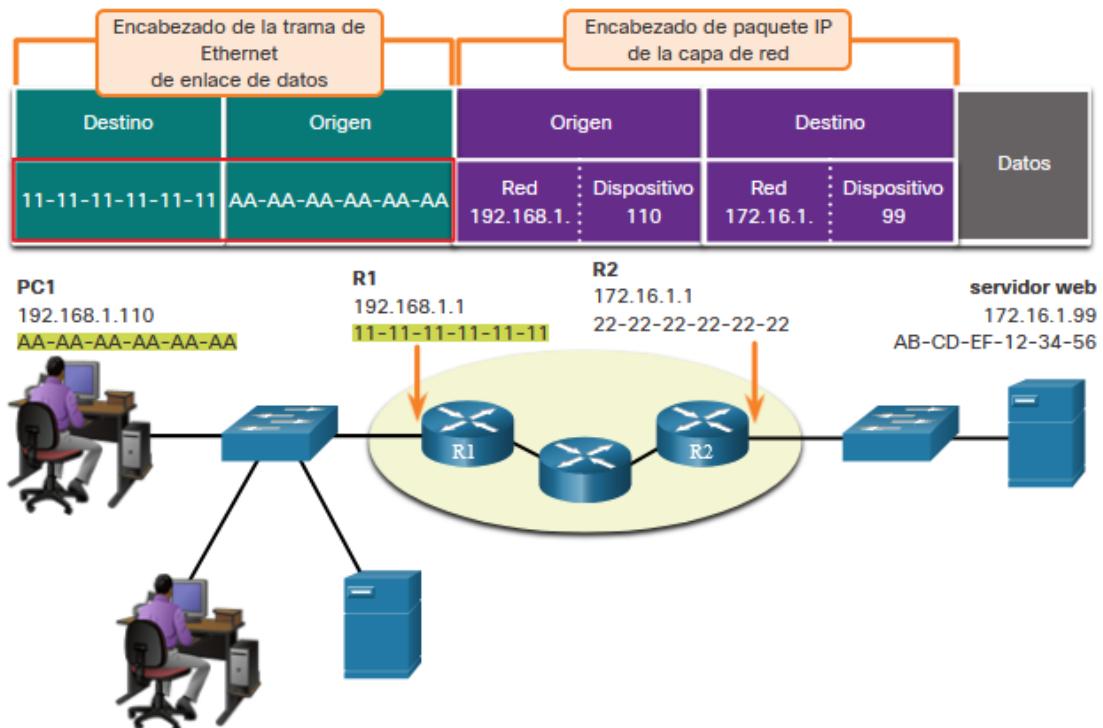
En la figura, observe que la porción de red de las direcciones IP de origen y de destino se encuentran en redes diferentes.



## Diferentes redes IP

Cuando el emisor y el receptor del paquete IP se encuentran en redes diferentes, el frame de enlace de datos de Ethernet no se puede enviar directamente al host de destino, debido a que en la red del emisor no se puede tener acceso directamente al host. El frame de Ethernet se debe enviar al router o gateway predeterminado. En nuestro ejemplo, el gateway predeterminado es R1. R1 tiene una dirección de enlace de datos de Ethernet que se encuentra en la misma red que PC1. Esto permite que PC1 alcance el router directamente.

- **Dirección MAC de origen:** la dirección MAC de Ethernet del dispositivo emisor, PC1. La dirección MAC de la interfaz Ethernet de PC1 es AA-AA-AA-AA-AA-AA.
- **Dirección MAC de destino:** cuando el dispositivo receptor, la dirección IP de destino, está en una red distinta de la del dispositivo emisor, este utiliza la dirección MAC de Ethernet del gateway predeterminado o el router. En este ejemplo, la dirección MAC de destino es la dirección MAC de la interfaz Ethernet de R1, 11-11-11-11-11-11. Esta es la interfaz que está conectada a la misma red que PC1, como se muestra en la figura.



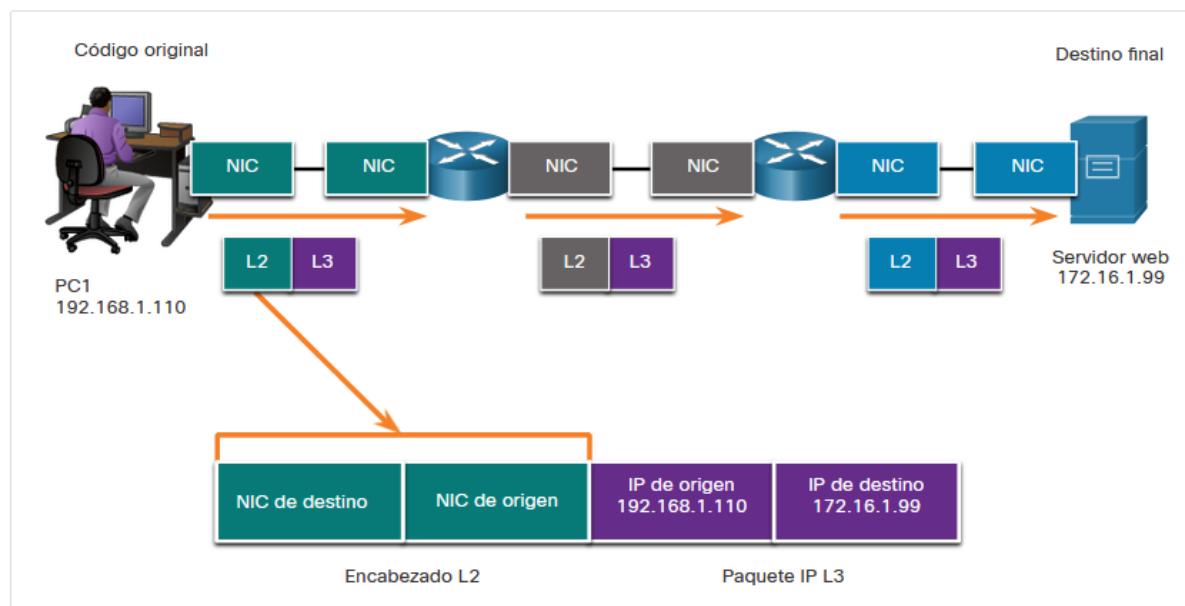
Ahora R1 es capaz de reenviar el frame modificando el encabezado de Ethernet.

## Direcciones de enlace de datos

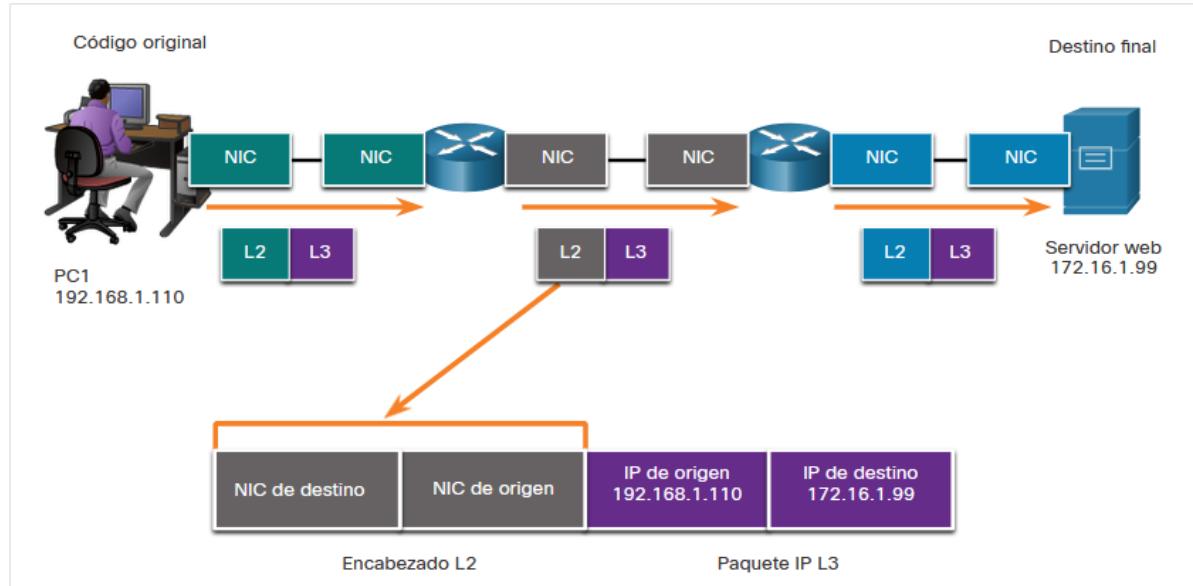
La dirección física de la capa de enlace de datos, o capa 2, tiene una función distinta. Su propósito es enviar el frame de enlace de datos desde una interfaz de red hasta otra interfaz de red en la misma red.

Antes de que un paquete IP pueda enviarse a través de una red conectada por cable o inalámbrica, se debe encapsular en un frame de enlace de datos de modo que pueda transmitirse a través del medio físico.

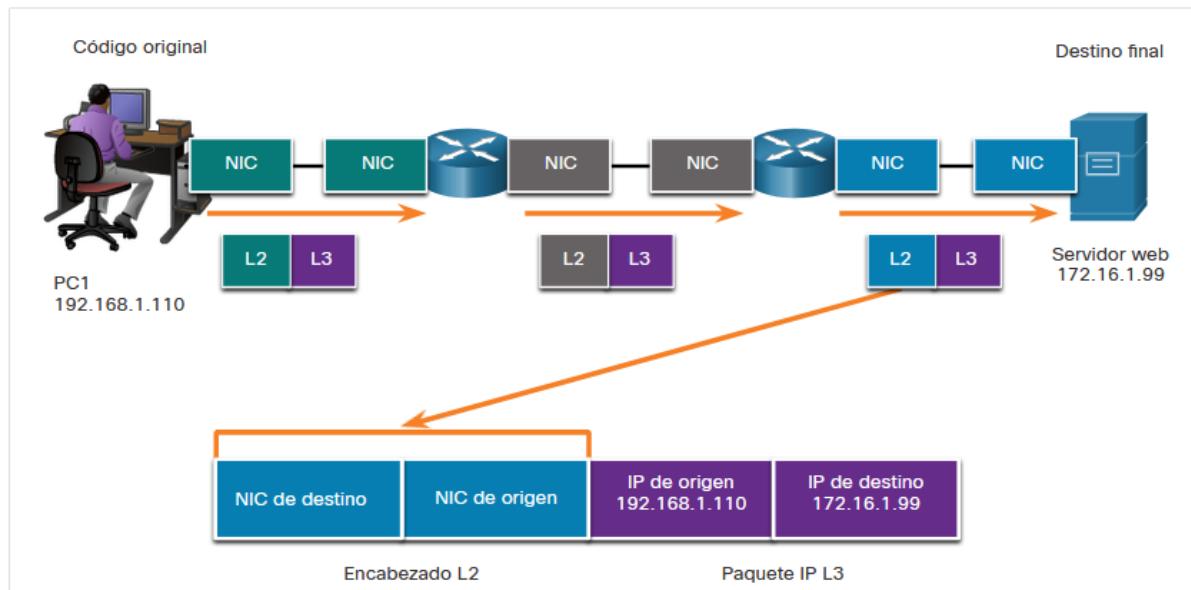
Host a enrutador



Enrutador a enrutador



### Enrutador a servidor



A medida que el paquete IP se mueve de host a router, de router a router y, finalmente, de router a host, es encapsulado en una nueva trama de enlace de datos, en cada punto del recorrido. Cada trama de enlace de datos contiene la dirección de origen de enlace de datos de la tarjeta NIC que envía la trama y la dirección de destino de enlace de datos de la tarjeta NIC que recibe la trama.

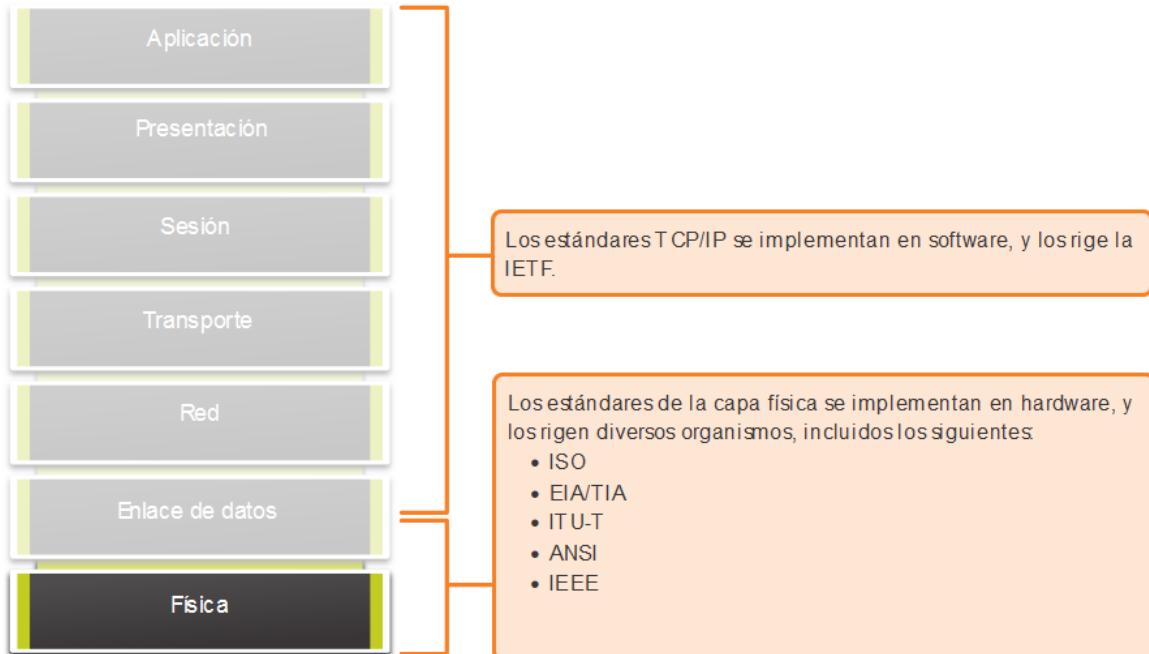
El protocolo de enlace de datos de capa 2 sólo se utiliza para enviar el paquete de NIC a NIC en la misma red. El router elimina la información de la capa 2 a medida que una NIC la recibe y agrega nueva información de enlace de datos antes de reenviarla a la NIC de salida en su recorrido hacia el dispositivo de destino final.

El paquete IP se encapsula en una trama de enlace de datos que contiene información de enlace de datos, como la siguiente:

- **Dirección de enlace de datos de origen:** la dirección física de la NIC del dispositivo que envía la trama de enlace de datos.
- **Dirección de enlace de datos de destino:** la dirección física de la NIC que recibe la trama de enlace de datos. Esta dirección es el router del salto siguiente o el dispositivo de destino final.

## La conexión física

Para que pueda existir una comunicación de red necesita haber una conexión física, esta puede ser por cable o inalámbrica. Todo dependerá de los recursos con los que se cuente. La capa 1.



## La capa física

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. Esta capa acepta una trama completa desde la capa de enlace de datos y la codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermedio recibe los bits codificados que componen una trama.

Los estándares de la capa física abarcan tres áreas funcionales:

- Componentes físicos
- Codificación
- Señalización

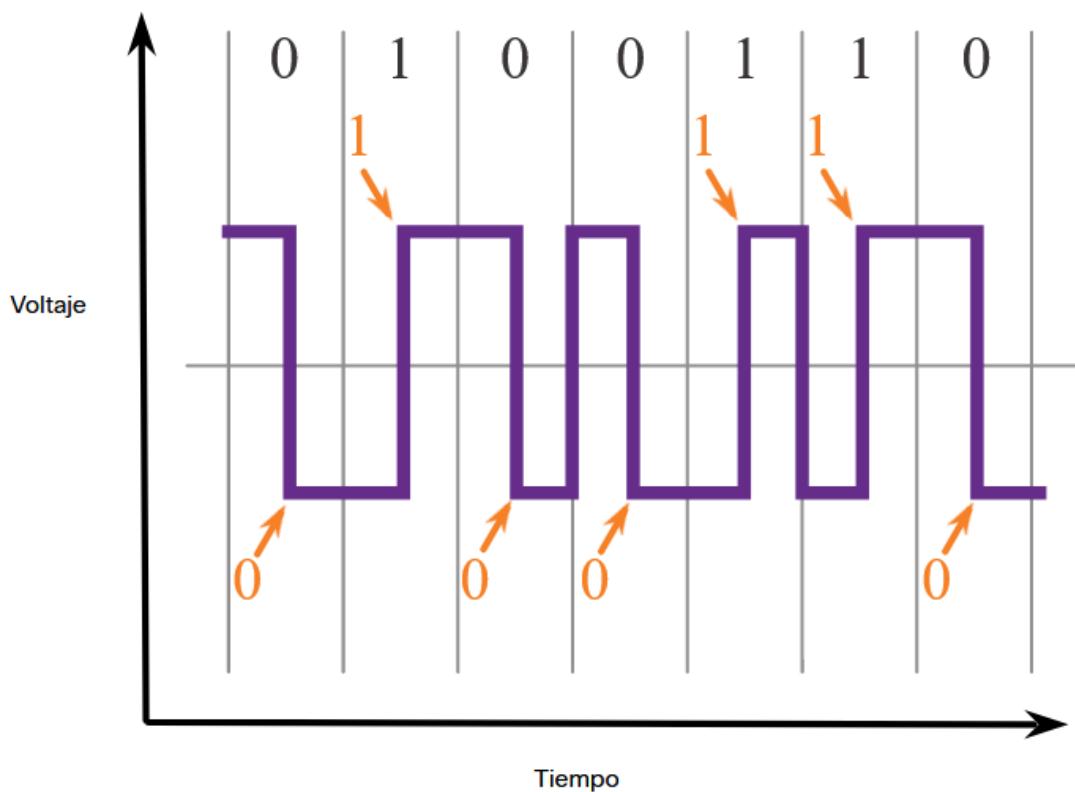
## Componentes físicos

Los componentes físicos son los dispositivos de hardware electrónico, medios y otros conectores que transmiten las señales que representan los bits. Todos los componentes de hardware, como NIC, interfaces y conectores, materiales y diseño de los cables, se especifican en los estándares asociados con la capa física.

## Codificación

La codificación, o codificación de línea, es un método que se utiliza para convertir una transmisión de bits de datos en un “código” predefinido. Los códigos son grupos de bits utilizados para ofrecer un patrón predecible que pueda reconocer tanto el emisor como el receptor.

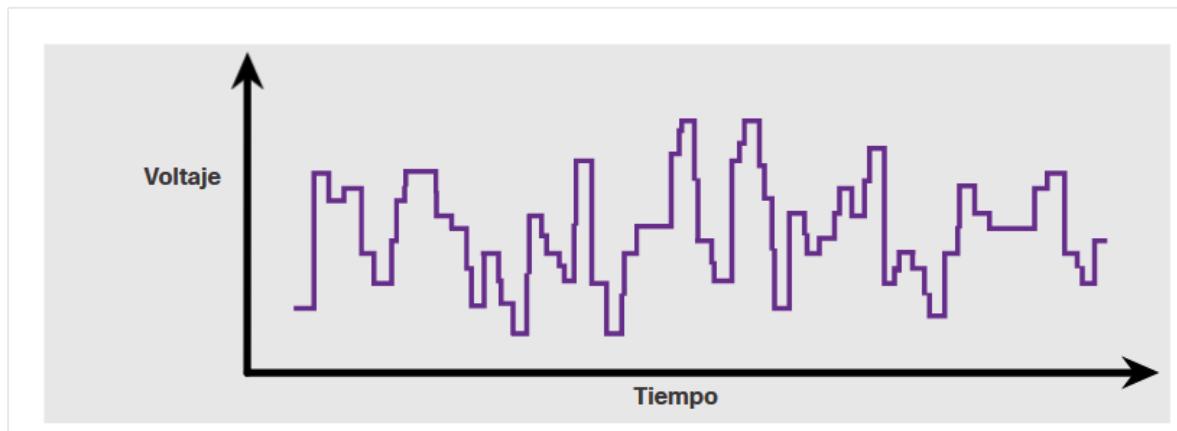
Por ejemplo, en la codificación Manchester los 0 se representan mediante una transición de voltaje de alto a bajo y los 1 se representan como una transición de voltaje de bajo a alto. Este tipo de codificación se usa en Ethernet de 10 Mbps. Las velocidades de datos más rápidas requieren codificación más compleja. La codificación Manchester se utiliza en estándares Ethernet más antiguos, como 10BASE-T. Ethernet 100BASE-TX usa codificación 4B / 5B y 1000BASE-T usa codificación 8B / 10B.



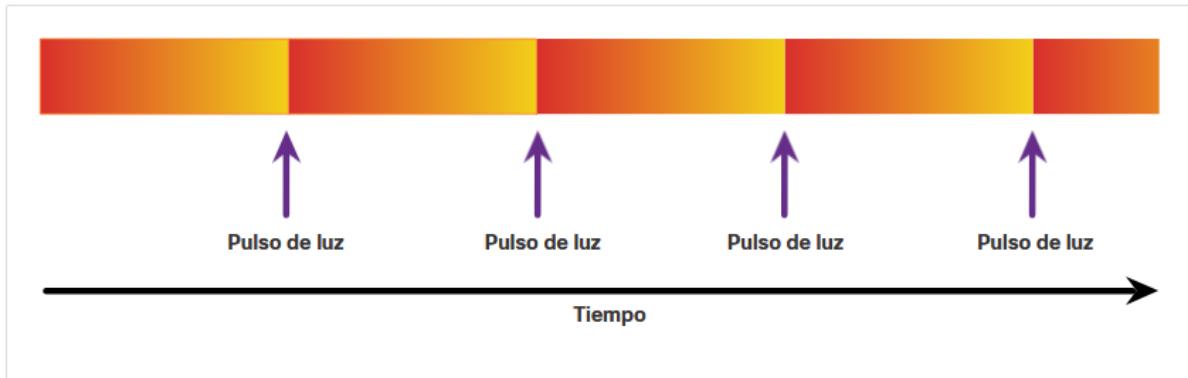
## Señalización

La capa física debe generar las señales inalámbricas, ópticas o eléctricas que representan los “1” y los “0” en los medios. La forma en que se representan los bits se denomina método de señalización. Los estándares de la capa física deben definir qué tipo de señal representa un “1” y qué tipo de señal representa un “0”. Esto puede ser tan simple como un cambio en el nivel de una señal eléctrica o de un pulso óptico. Por ejemplo, un pulso largo podría representar un 1 mientras que un pulso corto podría representar un 0.

**Señales eléctricas sobre cable**

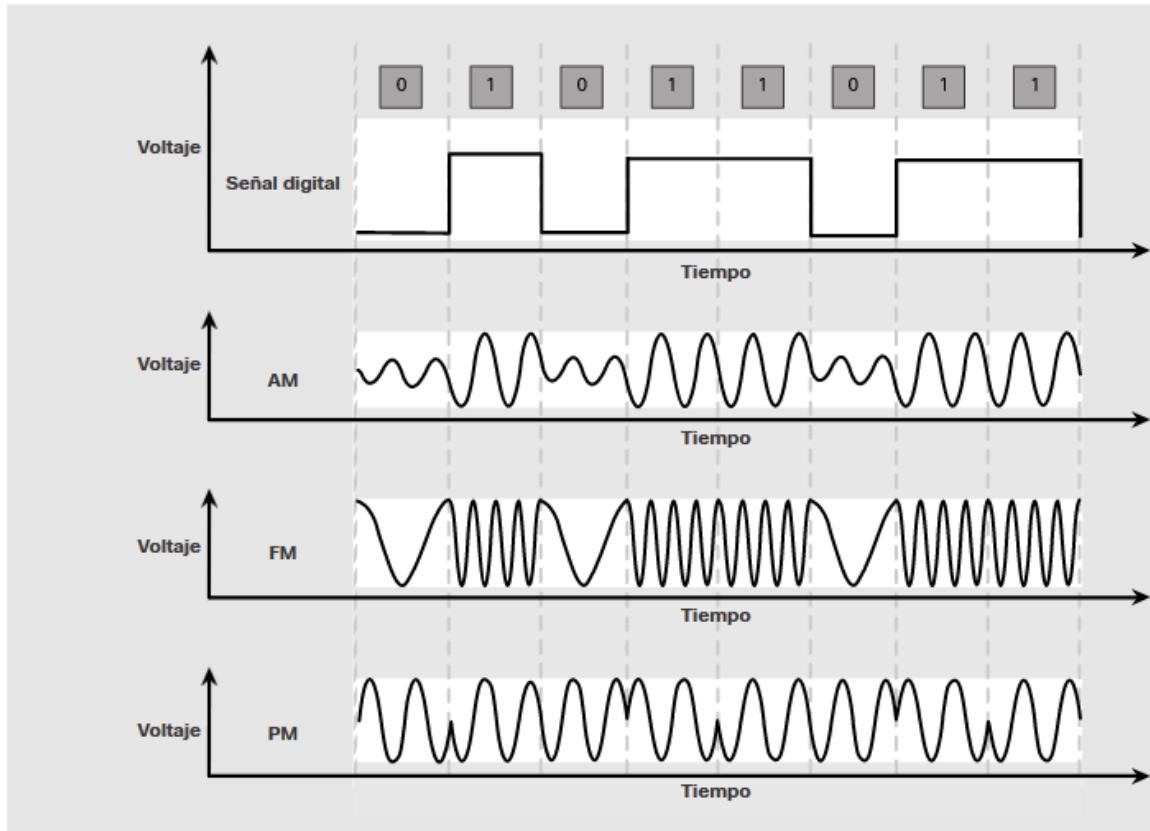


**Pulsos de luz sobre cable de fibra óptica**



**Señales de microondas sobre medios inalámbricos**

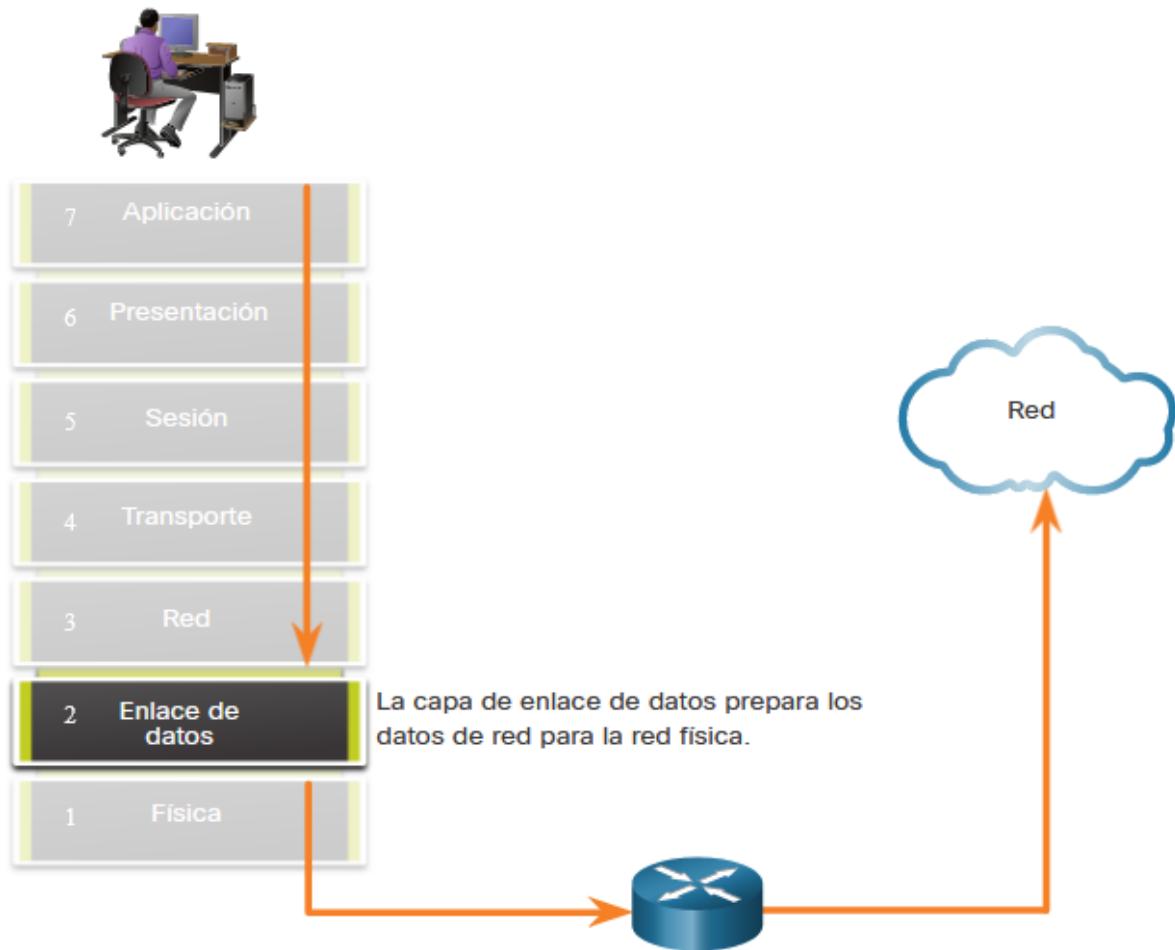




## La capa de enlace de datos

La capa de enlace de datos del modelo OSI (Capa 2), como se muestra en la figura, prepara los datos de red para la red física. La capa de enlace de datos es responsable de las comunicaciones de tarjeta de interfaz de red (NIC) a tarjeta de interfaz de red. La capa de vínculo de datos realiza lo siguiente:

- Permite que las capas superiores accedan a los medios. El protocolo de capa superior no conoce completamente el tipo de medio que se utiliza para reenviar los datos.
- Acepta datos, generalmente paquetes de Capa 3 (es decir, IPv4 o IPv6) y los encapsula en tramas de Capa 2.
- Controla cómo los datos se colocan y reciben en los medios.
- Intercambia tramas entre puntos finales a través de los medios de red.
- Recibe datos encapsulados, generalmente paquetes de Capa 3, y los dirige al protocolo de capa superior adecuado.
- Realiza la detección de errores y rechaza cualquier trama dañada.



## Subcapas de enlace de datos IEEE 802 LAN/MAN

Los estándares IEEE 802 LAN/MAN son específicos para LAN Ethernet, LAN inalámbricas (WLAN), redes de área personal inalámbrica (WPAN) y otros tipos de redes locales y metropolitanas. La capa de enlace de datos IEEE 802 LAN/MAN consta de las dos subcapas siguientes:

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

La figura muestra las dos subcapas (LLC y MAC) de la capa de enlace de datos.

Red	Protocolo de capa de red			
Enlace de datos	Subcapa LLC	Subcapa LLC-IEEE 802.2		
	Subcapa MAC	Ethernet IEEE 802.3 adaptador de cable	WLAN IEEE 802.11	WPAN IEEE 802.15
Física		Varios estándares Ethernet para Fast Ethernet, Gigabit Ethernet, etc.	Varios estándares WLAN para diferentes tipos de comunicaciones inalámbricas	Varios estándares WPAN para Bluetooth, RFID, etc.

La subcapa LLC toma los datos del protocolo de red, que generalmente es un paquete IPv4 o IPv6, y agrega información de control de Capa 2 para ayudar a entregar el paquete al nodo de destino.

La subcapa MAC controla la NIC y otro hardware que es responsable de enviar y recibir datos en el medio LAN/MAN con cable o inalámbrico.

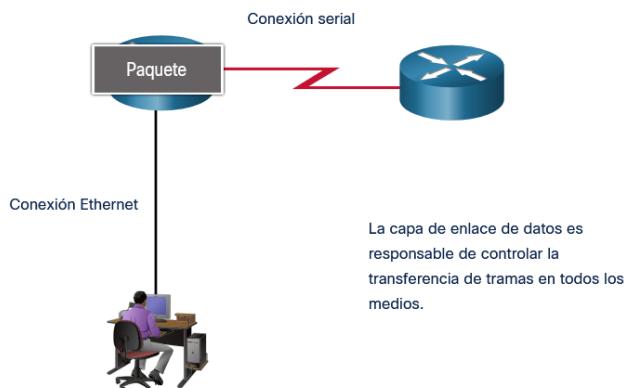
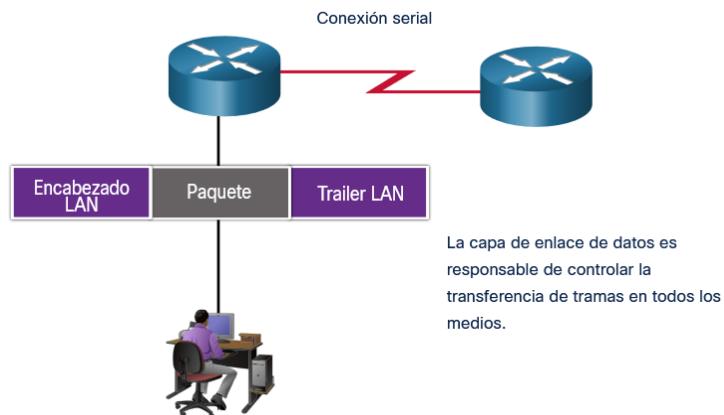
La subcapa MAC proporciona encapsulación de datos:

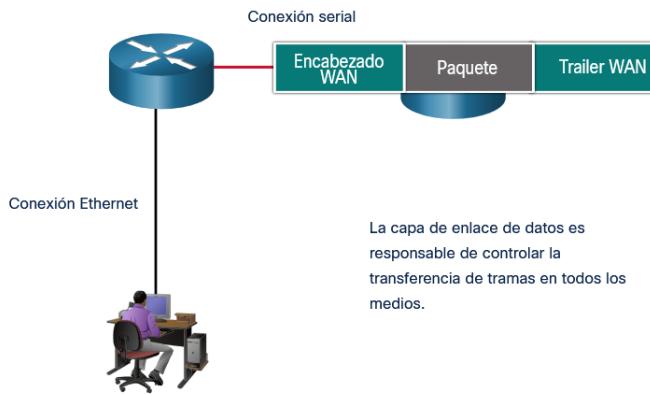
- **Delimitación de tramas** - El proceso de entramado proporciona delimitadores importantes que se utilizan para identificar un grupo de bits que componen una trama. Estos bits delimitadores proporcionan sincronización entre los nodos de transmisión y de recepción.
- **Direccionamiento** - proporciona direccionamiento de origen y destino para transportar la trama de capa 2 entre dispositivos en el mismo medio compartido.
- **Detección de errores** - Cada trama contiene un tráiler utilizado para detectar errores de transmisión.

La subcapa MAC también proporciona control de acceso a medios, lo que permite que varios dispositivos se comuniquen a través de un medio compartido (semidúplex). Las comunicaciones dúplex completo no requieren control de acceso.

En cada salto a lo largo de la ruta, un router realiza las siguientes funciones de Capa 2:

1. Aceptan una trama proveniente de un medio.
2. Desencapsulan la trama.
3. Vuelven a encapsular el paquete en una trama nueva.
4. Reenvían la nueva trama adecuada al medio de ese segmento de la red física.





## Frame de enlace de datos

La capa de enlace de datos prepara los datos encapsulados (generalmente un paquete IPv4 o IPv6) para el transporte a través de los medios locales encapsulándolos con un encabezado y un trailer para crear una trama.

El protocolo de enlace de datos es responsable de las comunicaciones de NIC a NIC dentro de la misma red. Si bien existen muchos protocolos de capa de enlace de datos diferentes que describen las tramas de la capa de enlace de datos, cada tipo de trama tiene tres partes básicas:

- Encabezado
- Datos
- Tráiler

A diferencia de otros protocolos de encapsulación, la capa de enlace de datos agrega información en forma de trailer al final de la trama.

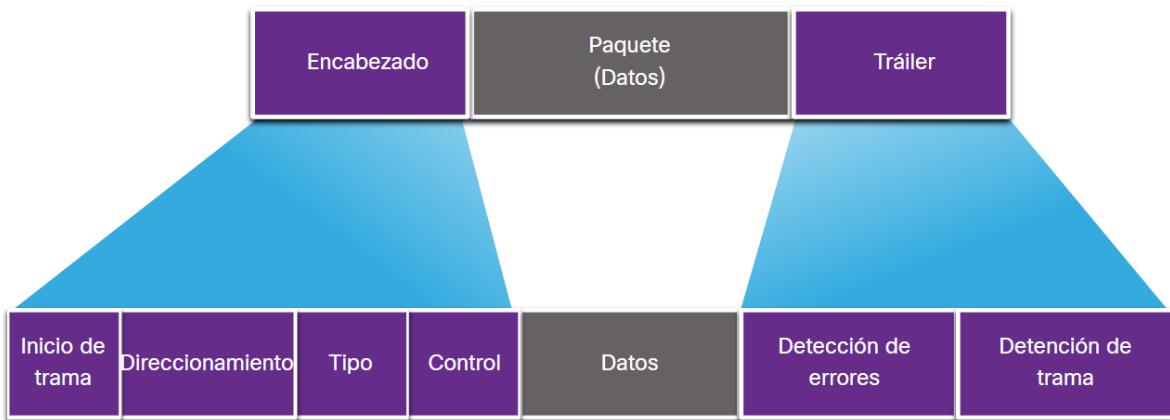
Todos los protocolos de capa de enlace de datos encapsulan los datos dentro del campo de datos de la trama. Sin embargo, la estructura de la trama y los campos contenidos en el encabezado y tráiler varían de acuerdo con el protocolo.

No hay una estructura de trama que cumpla con las necesidades de todos los transportes de datos a través de todos los tipos de medios. Según el entorno, la cantidad de información de control que se necesita en la trama varía para cumplir con los requisitos de control de acceso al medio de la topología lógica y de los medios. Por ejemplo, una trama WLAN debe incluir procedimientos para evitar colisiones y, por lo tanto, requiere información de control adicional en comparación con una trama Ethernet.

## Campos del frame

El tramo rompe la transmisión en agrupaciones decifrables, con la información de control insertada en el encabezado y tráiler como valores en campos diferentes. Este formato proporciona a las señales físicas una estructura reconocida por los nodos y decodificada en paquetes en el destino.

Los campos de trama genéricos se muestran en la figura. No todos los protocolos incluyen todos estos campos. Los estándares para un protocolo específico de enlace de datos definen el formato real de la trama.



Los campos de trama incluyen los siguientes:

- **Indicadores de arranque y detención de trama** - Se utilizan para identificar 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 calidad de servicio (QoS). QoS otorga prioridad de reenvío a ciertos tipos de mensajes. Por ejemplo, las tramas de voz sobre IP (VoIP) normalmente reciben prioridad porque son sensibles al retraso.
- **Datos** - Incluye el contenido de la trama (es decir, el encabezado del paquete, el encabezado del segmento y los datos).
- **Detección de Errores** - se incluye después de los datos para formar el trailer.

Los protocolos de capa de enlace de datos agregan un tráiler al final de cada trama. En un proceso llamado detección de errores, el avance determina si la trama llegó sin error. Coloca un resumen lógico o matemático de los bits que componen la trama en el avance. La capa de enlace de datos agrega detección de errores porque las señales en los medios podrían estar sujetas a interferencia, distorsión o pérdida que cambiaría sustancialmente los valores de bits que representan esas señales.

Un nodo de transmisión crea un resumen lógico del contenido de la trama, conocido como el valor de comprobación de redundancia cíclica (CRC). Este valor se coloca en el campo Secuencia de Verificación de la Trama (FCS) para representar el contenido de la trama. En

el tráiler Ethernet, el FCS proporciona un método para que el nodo receptor determine si la trama experimentó errores de transmisión.

## Direcciones de Capa 2

La capa de enlace de datos proporciona el direccionamiento utilizado en el transporte de una trama a través de un medio local compartido. Las direcciones de dispositivo en esta capa se llaman direcciones físicas. El direccionamiento de la capa de enlace de datos está contenido en el encabezado de la trama y especifica el nodo de destino de la trama en la red local. Normalmente se encuentra al principio de la trama, por lo que la NIC puede determinar rápidamente si coincide con su propia dirección de Capa 2 antes de aceptar el resto de la trama. El encabezado de la trama también puede contener la dirección de origen de la trama.

A diferencia de las direcciones lógicas de la Capa 3, que son jerárquicas, las direcciones físicas no indican en qué red está ubicado el dispositivo. En cambio, la dirección física es única para un dispositivo en particular. Un dispositivo seguirá funcionando con la misma dirección física de capa 2, incluso si el dispositivo se mueve a otra red o subred. Por lo tanto, las direcciones de capa 2 sólo se utilizan para conectar dispositivos dentro del mismo medio compartido, en la misma red IP.

## Tramas LAN y WAN

Los protocolos Ethernet son utilizados por LAN cableadas. Las comunicaciones inalámbricas caen bajo los protocolos WLAN (IEEE 802.11). Estos protocolos fueron diseñados para redes multiacceso.

Tradicionalmente, los WAN utilizaban otros tipos de protocolos para varios tipos de topologías punto a punto, hub-spoke y de malla completa. Algunos de los protocolos WAN comunes a lo largo de los años han incluido:

- Protocolo punto a punto (PPP)
- Control de enlace de datos de alto nivel (HDLC, High-Level Data Link Control)
- Frame Relay
- Modo de transferencia asíncrona (ATM)
- X.25

Estos protocolos de capa 2 ahora están siendo reemplazados en la WAN por Ethernet.

En una red TCP/IP, todos los protocolos de capa 2 del modelo OSI funcionan con la dirección IP en la capa 3. Sin embargo, el protocolo de capa 2 específico que se utilice depende de la topología lógica y de los medios físicos.

Cada protocolo realiza el control de acceso a los medios para las topologías lógicas de Capa 2 que se especifican. Esto significa que una cantidad de diferentes dispositivos de red puede actuar como nodos que operan en la capa de enlace de datos al implementar estos

protocolos. Estos dispositivos incluyen las tarjetas de interfaz de red en PC, así como las interfaces en routers y en switches de la Capa 2.

El protocolo de la Capa 2 que se utiliza para una topología de red particular está determinado por la tecnología utilizada para implementar esa topología. La tecnología está, a su vez, determinada por el tamaño de la red, en términos de cantidad de hosts y alcance geográfico y los servicios que se proveerán a través de la red.

Una LAN generalmente usa una tecnología de alto ancho de banda capaz de soportar grandes cantidades de hosts. El área geográfica relativamente pequeña de una LAN (un solo edificio o un campus de varios edificios) y su alta densidad de usuarios hacen que esta tecnología sea rentable.

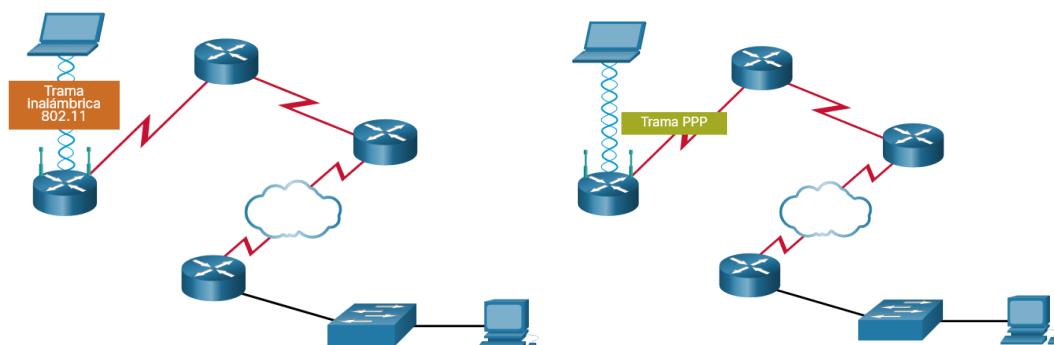
Sin embargo, utilizar una tecnología de ancho de banda alto no es generalmente rentable para redes de área extensa que cubren grandes áreas geográficas (varias ciudades, por ejemplo). El costo de los enlaces físicos de larga distancia y la tecnología utilizada para transportar las señales a través de esas distancias, generalmente, ocasiona una menor capacidad de ancho de banda.

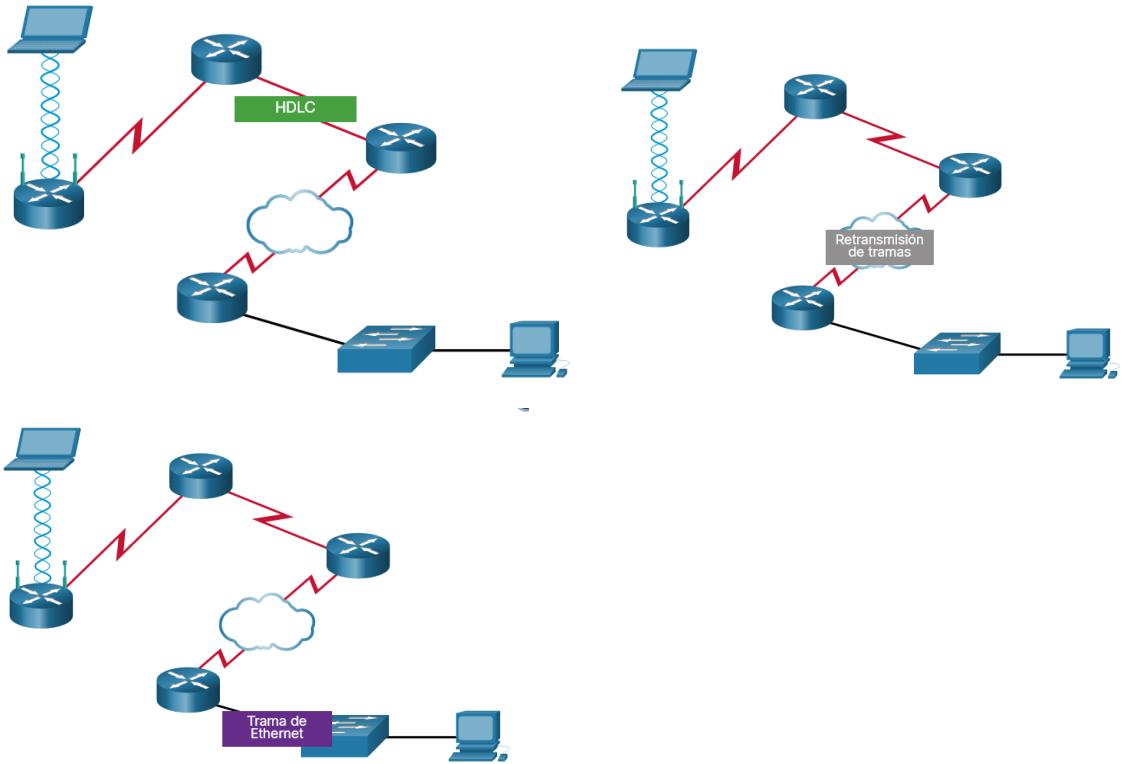
La diferencia de ancho de banda normalmente produce el uso de diferentes protocolos para las LAN y las WAN.

Los protocolos de la capa de enlace de datos incluyen:

- Ethernet
- 802.11 inalámbrico
- Protocolo punto a punto (PPP)
- Control de enlace de datos de alto nivel (HDLC, High-Level Data Link Control)
- Frame Relay

Haga clic en el botón Reproducir para ver ejemplos de protocolos de capa 2.



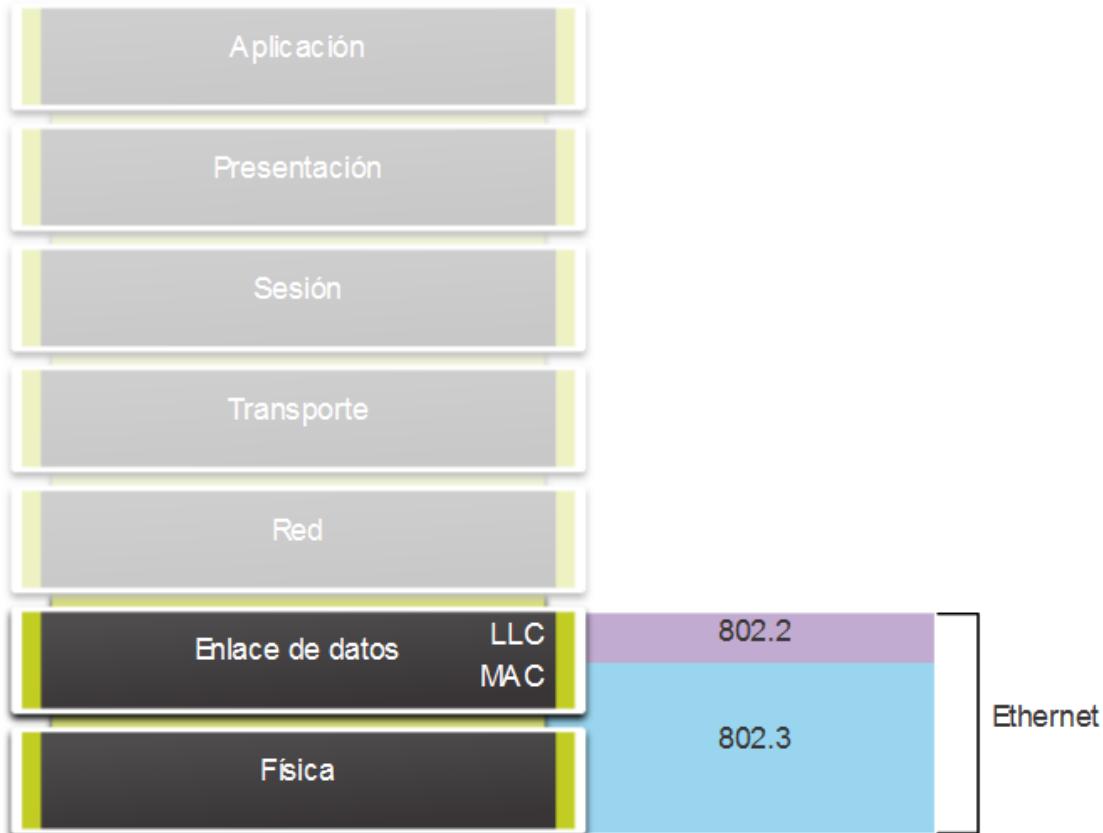


## Frames de Ethernet

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

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

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



## Subcapa MAC

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

### Encapsulación de datos

La encapsulación de datos IEEE 802.3 incluye lo siguiente:

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

### Accediendo a los medios

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

El diagrama muestra varios estándares Ethernet en la subcapa MAC. En la parte superior del diagrama se encuentra la capa de red y el protocolo de capa de red . Debajo de eso

está la capa de enlace de datos y sus subcapas. La subcapa superior es la subcapa IEEE 802.2 LLC. La siguiente es la subcapa MAC Ethernet IEEE 802.3. Debajo hay cinco columnas con varios estándares Ethernet y tipos de medios que abarcan la parte inferior de la subcapa MAC y toda la capa física OSI. De izquierda a derecha, las columnas son: IEEE 802.3u Fast Ethernet; IEEE 802.3z Gigabit Ethernet sobre fibra; IEEE 802.ab Gigabit Ethernet sobre cobre; IEEE 802.3ae 10 Gigabit Ethernet sobre fibra; y Etc.

## Estándares Ethernet en la subcapa MAC

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

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

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

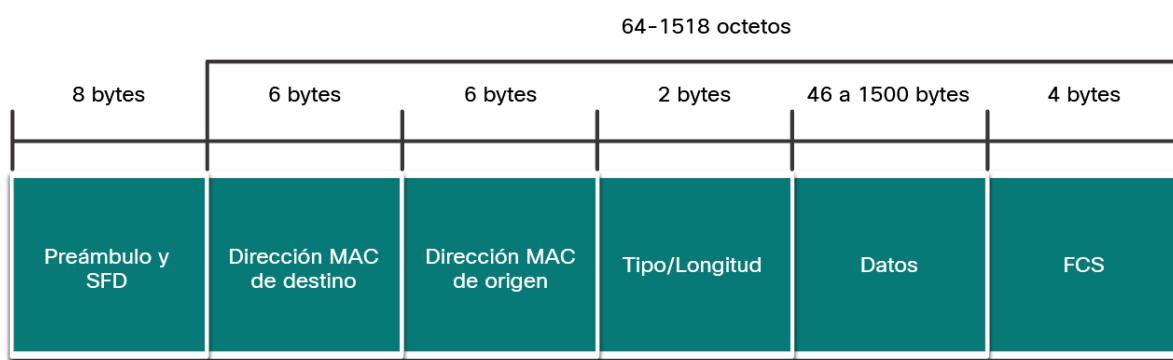
## Campos de trama de Ethernet

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

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

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

## Campos de trama en internet



## Detalle de los campos del Ethernet Frame

Campo	Descripción
Campos Preámbulo y Delimitador de inicio de trama	El Preámbulo (7 bytes) y el Delimitador de tramas de inicio (SFD), también llamado Inicio de Trama (1 byte), los campos se utilizan para la sincronización entre el envío y recepción de dispositivos. Estos primeros ocho bytes de trama son utilizados para llamar la atención de los nodos receptores. Esencialmente, los primeros cuantos bytes le dicen a los receptores que se preparen para recibir una nueva trama.

Campo Dirección MAC de destino	Este campo de 6 bytes es el identificador del destinatario deseado. Como usted recordará, esta dirección es utilizada por la capa 2 para ayudar a los dispositivos en determinar si una trama está dirigido a ellos. La dirección en la trama es comparada con la dirección MAC en el dispositivo. Si hay una coincidencia, el acepta la trama. Puede ser unicast, multicast o broadcast dirección.
Campo Dirección MAC de origen	Este campo de 6 bytes identifica la NIC o la interfaz de origen de la trama
Tipo/Longitud	Este campo de 2 bytes identifica el protocolo de capa superior encapsulado en la trama de Ethernet Los valores comunes son, en hexadecimal, 0x800 para IPv4, 0x86DD para IPv6 y 0x806 para ARP. <b>Nota:</b> También puede ver este campo denominado como EtherType, Type o Length.
Campo de datos	Este campo (46 - 1500 bytes) contiene los datos encapsulados de una capa superior, que es una PDU genérica de Capa 3, o más comúnmente, un IPv4 paquete. Todas las tramas deben tener, al menos, 64 bytes de longitud. Si un paquete pequeño es encapsulado, bits adicionales llamados pad se utilizan para aumentar el tamaño de la trama a este tamaño mínimo.
Campo Secuencia de verificación de trama	El campo Secuencia de verificación de trama (FCS Frame Check Sequence) (4 bytes) se usa para detectar errores en una trama. Utiliza una comprobación cíclica de redundancia (CRC cyclic redundancy check). El dispositivo de envío incluye los resultados de un CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar por errores. Si los cálculos coinciden, significa que no se produjo ningún error. Cálculos que no coinciden son una indicación de que los datos han cambiado; por lo tanto, la trama se descarta. Un cambio en los datos podría ser el resultado de una interrupción de las señales eléctricas que representan los bits.

## Procesamiento de tramas

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

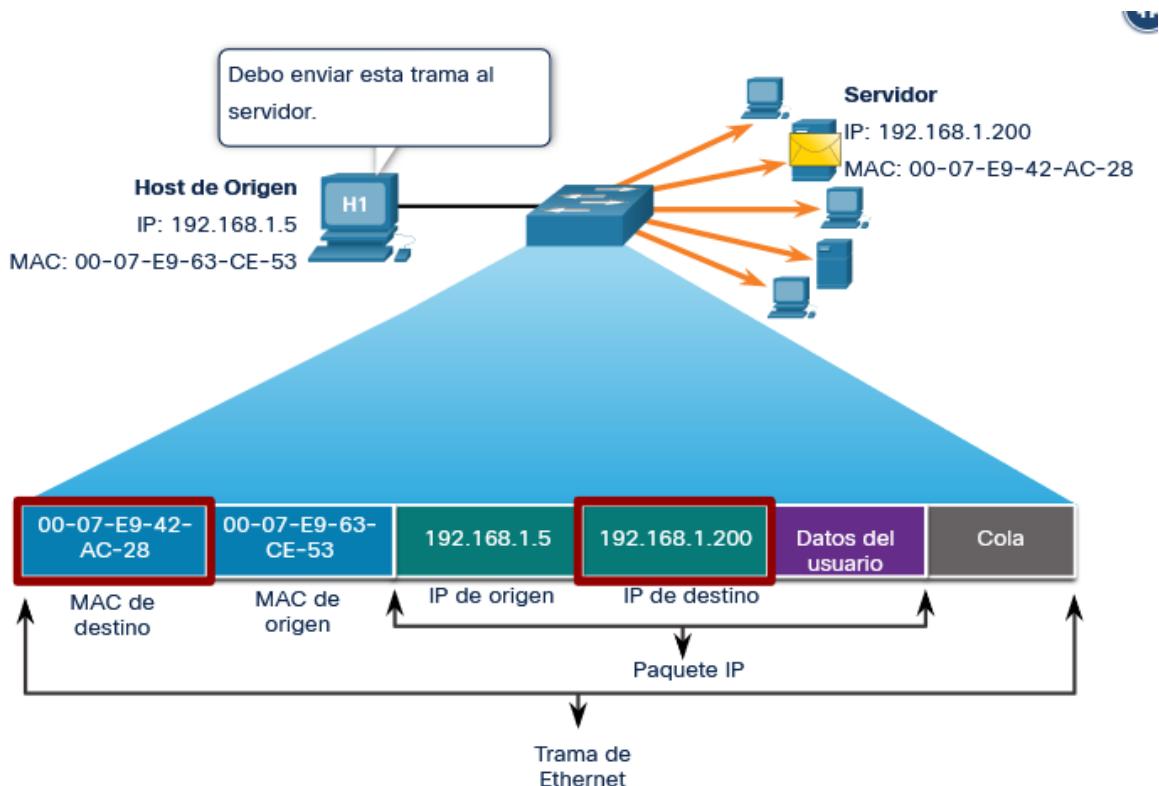
**Nota** [En los sistemas operativos de PC y NIC modernos, es posible cambiar la dirección MAC en el software. Esto es útil cuando se intenta acceder a una red filtrada por BIA. En consecuencia, el filtrado o el control de tráfico basado en la dirección MAC ya no son tan seguros.]

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

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

## Dirección MAC de unicast

La dirección de MAC unicast es cuando el dispositivo que envía sabe la dirección MAC del dispositivo al cual enviará la información.

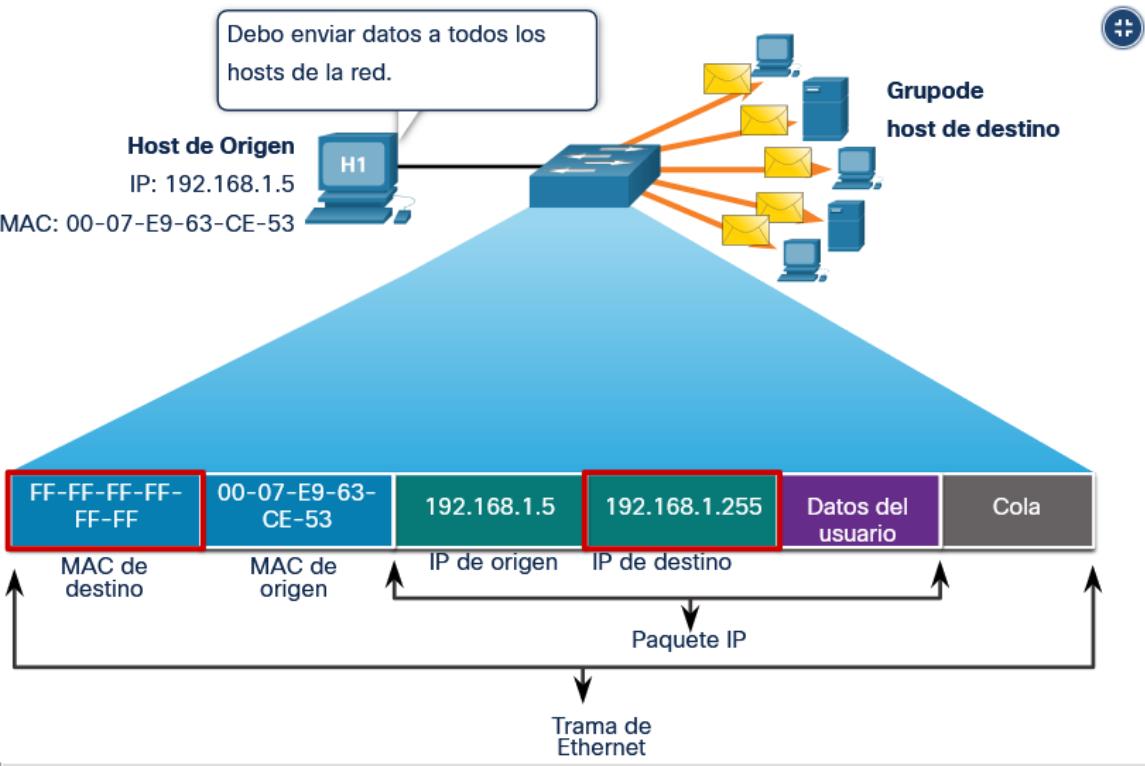


## Dirección MAC broadcast

El frame Ethernet broadcast:

- Tiene una dirección MAC de destino de FF-FF-FF-FF-FF-FF en hexadecimal (48 unidades en binario).
- Está inundado todos los puertos del switch Ethernet excepto el puerto entrante.

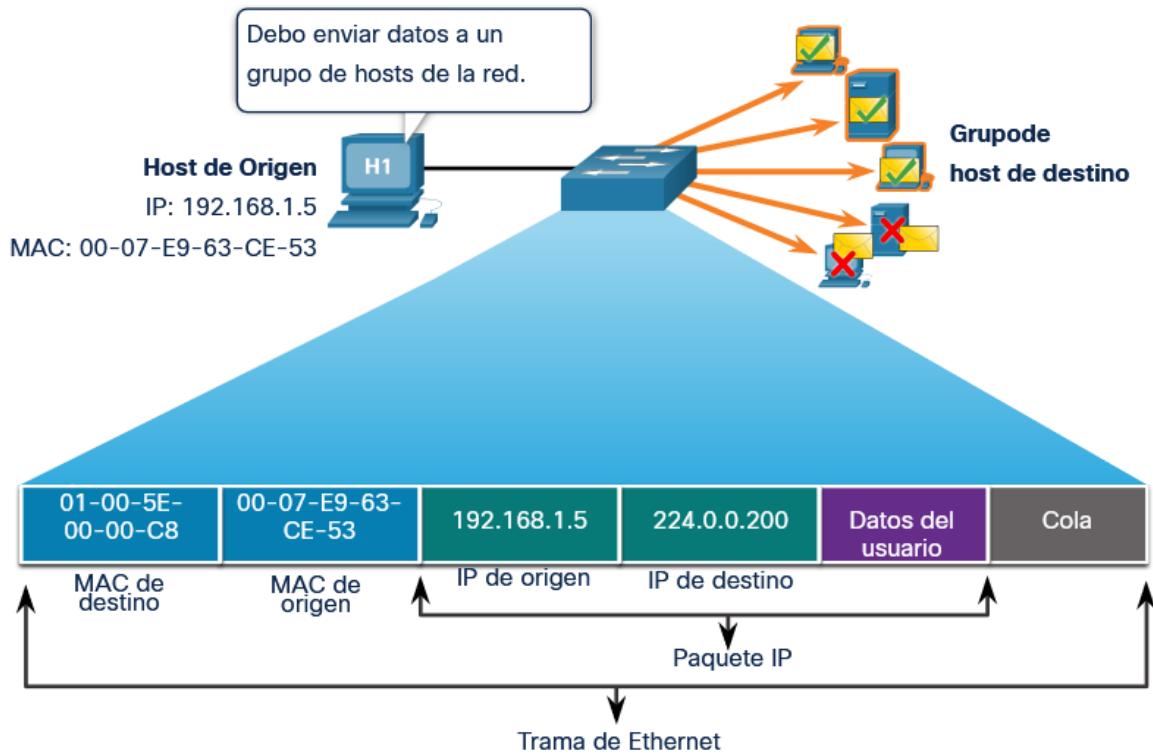
- No es reenviado por un router.



## Dirección MAC de multicast

Las características de una multicast Ethernet son las siguientes:

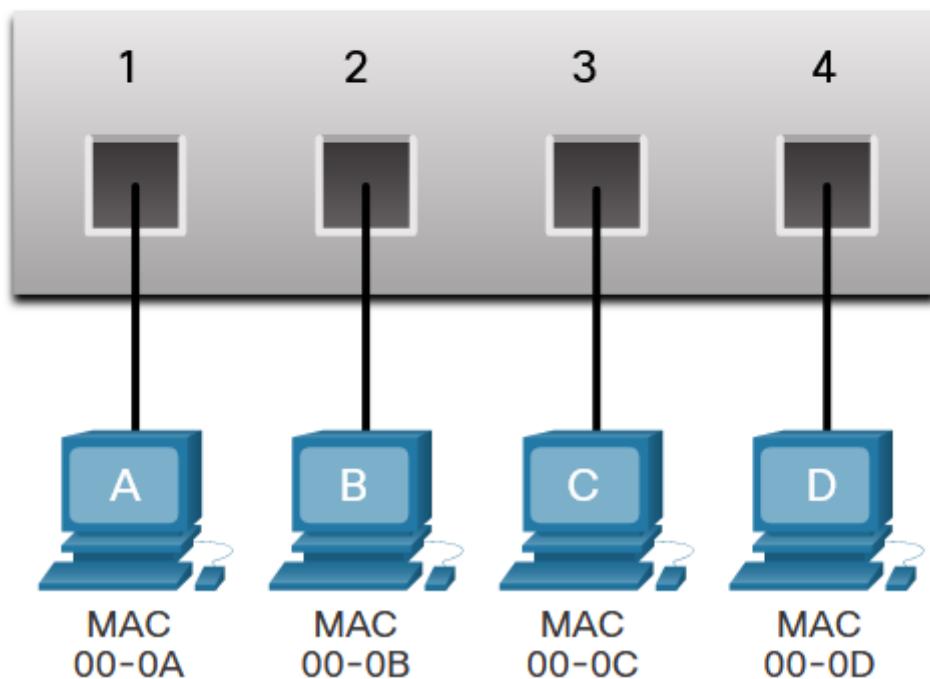
- Hay una dirección MAC de destino 01-00-5E cuando los datos encapsulados son un paquete de multicast IPv4 y una dirección MAC de destino de 33-33 cuando los datos encapsulados son un paquete de multicast IPv6.
- Existen otras direcciones MAC de destino de multicast reservadas para cuando los datos encapsulados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



## Fundamentos de switches

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

<b>Tabla de direcciones MAC</b>	
<b>Puerto</b>	<b>Dirección MAC</b>



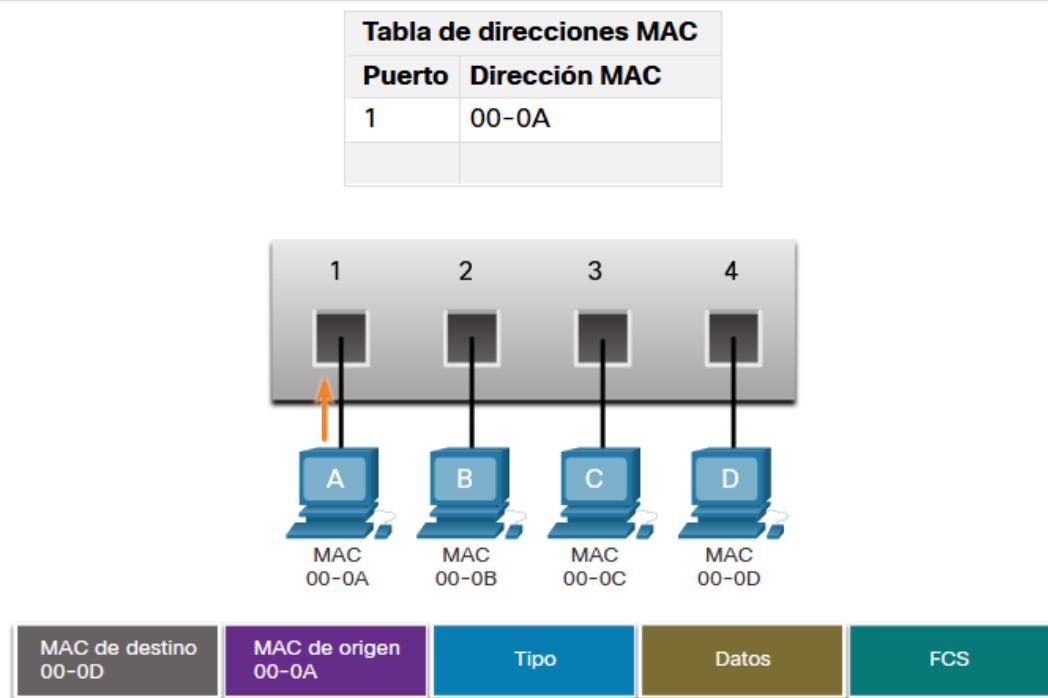
## Switch, Aprendiendo y Reenviando

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

### Examinar la dirección MAC de Origen

Cuando un frame entra a un switch este verifica la MAC de origen y el puerto por donde llegó, si no existe en la tabla mac lo agrega. Puede haber más de una dirección MAC por puerto si se conecta un Switch. Si la dirección ya existe en la tabla solo actualiza el temporizador de existencia de esa MAC. Normalmente los switches guardan la dirección en la tabla MAC por cinco minutos.

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



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

### Buscar dirección MAC de destino

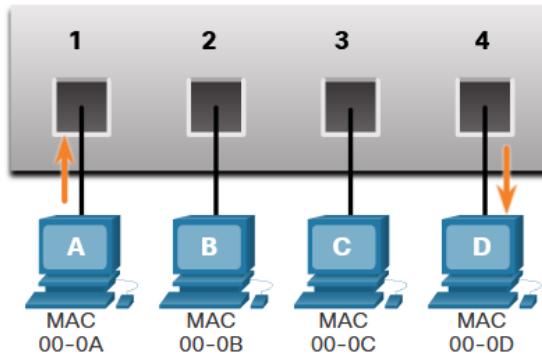
Si la dirección MAC de destino es una dirección de unicast, el switch busca una coincidencia entre la dirección MAC de destino de la trama y una entrada en la tabla de direcciones MAC. Si la dirección MAC de destino está en la tabla, reenvía la trama por el puerto especificado. Si la dirección MAC de destino no está en la tabla, el switch reenvía la trama por todos los puertos, excepto el de entrada. Esto se conoce como unicast desconocido.

**Nota** [Si la dirección MAC de destino es de broadcast o de multicast, la trama también se envía por todos los puertos, excepto el de entrada.]

Se conoce la dirección MAC destino

Tabla de direcciones MAC

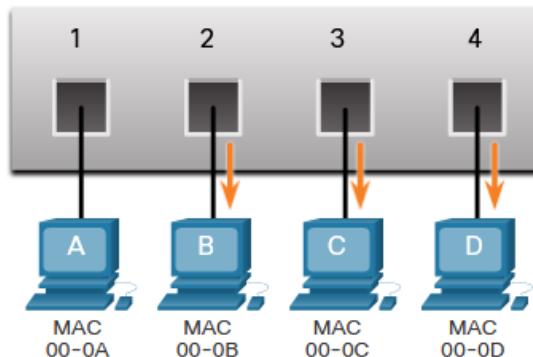
Puerto	Dirección MAC
1	00-0A
4	00-0D



No se conoce la dirección MAC destino

Tabla de direcciones MAC

Puerto	Dirección MAC
1	00-0A



1. La dirección MAC de destino no está en la tabla.
2. El switch reenviará la trama a todos los puertos.

## Métodos de reenvío de tramas de los switches Cisco

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

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

Este método de reenvío de trama recibe la trama completa y calcula el CRC. Si la CRC es válida, el switch busca la dirección de destino, que determina la interfaz de salida. Luego, la trama se reenvía desde el puerto correcto.

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

### **Switching por método de corte (Cut-through switching)**

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

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

- **Switching de reenvío rápido** - Este método ofrece el nivel de latencia más bajo. Fast-forward switching reenvía el paquete inmediatamente después de leer la dirección de destino. Como el fast-forward switching comienza a reenviar el paquete antes de recibirlo por completo, es posible que, a veces, los paquetes se distribuyan con errores. Esto ocurre con poca frecuencia y la NIC de destino descarta el paquete defectuoso al recibirla. En el modo de fast-forward, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. El fast-forward switching es el método de corte típico.
- **Switching libre de fragmentos** - En este método, el switch almacena los primeros 64 bytes de la trama antes de reenviarla. El fragment-free switching se puede ver como un punto medio entre el store-and-forward switching y el fast-forward switching. El motivo por el que el fragment-free switching

almacena solamente los primeros 64 bytes de la trama es que la mayoría de los errores y las colisiones de la red se producen en esos primeros 64 bytes. El fragment-free switching intenta mejorar el fast-forward switching al realizar una pequeña verificación de errores en los 64 bytes de la trama para asegurar que no haya ocurrido una colisión antes de reenviarla. Este método de fragment-free switching es un punto medio entre la alta latencia y la alta integridad del store-and-forward switching, y la baja latencia y la baja integridad del fast-forward switching.

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

## **Almacenamiento en búfer de memoria en los switches (Memory Buffering on Switches)**

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

### **Memory Buffering Methods**

Método	Descripción
<b>Memoria basada en puerto</b>	<ul style="list-style-type: none"><li>Las tramas se almacenan en colas que se enlazan a puertos específicos de entrada y puertos de salida.</li><li>Una trama se transmite al puerto de salida sólo cuando todas las tramas en la cola se han transmitido correctamente.</li><li>Es posible que una sola trama retrase la transmisión de todas las tramas en memoria debido a un puerto de destino ocupado.</li><li>Esta demora se produce aunque las demás tramas se puedan transmitir a puertos de destino abiertos.</li></ul>

## Memoria compartida

- Deposita todas las tramas en un búfer de memoria común compartido por todos los switches y la cantidad de memoria intermedia requerida por un puerto es asignada dinámicamente.
- Las tramas que están en el búfer se enlazan de forma dinámica al puerto de destino. que permite recibir un paquete en un puerto y, a continuación, transmitido en otro puerto, sin moverlo a una cola diferente.

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

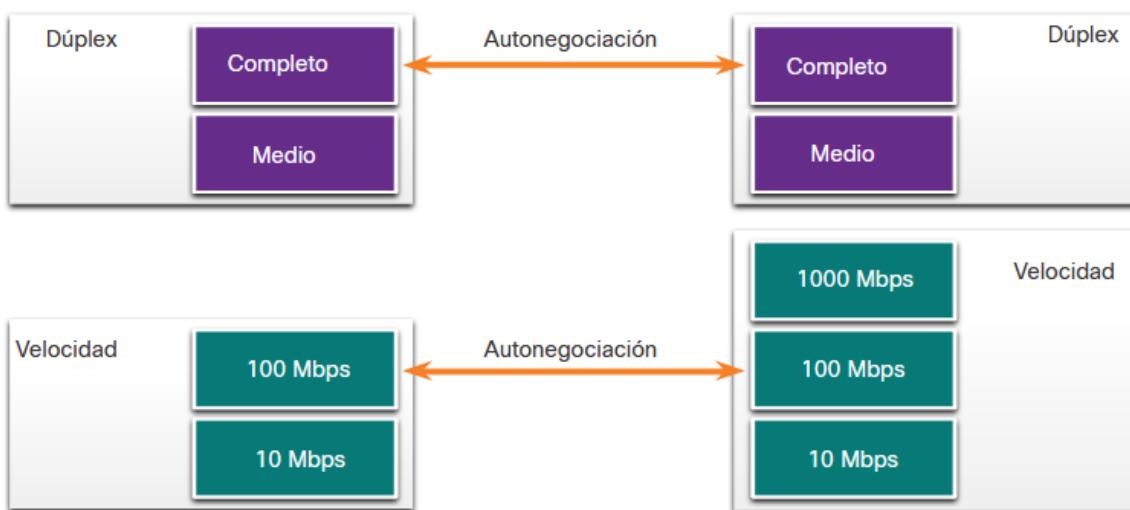
## Configuración de dúplex y velocidad

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

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

- **Dúplex completo (Full-duplex)**- Ambos extremos de la conexión pueden enviar y recibir datos simultáneamente.
- **Semidúplex (Half-duplex)**- Sólo uno de los extremos de la conexión puede enviar datos por vez.

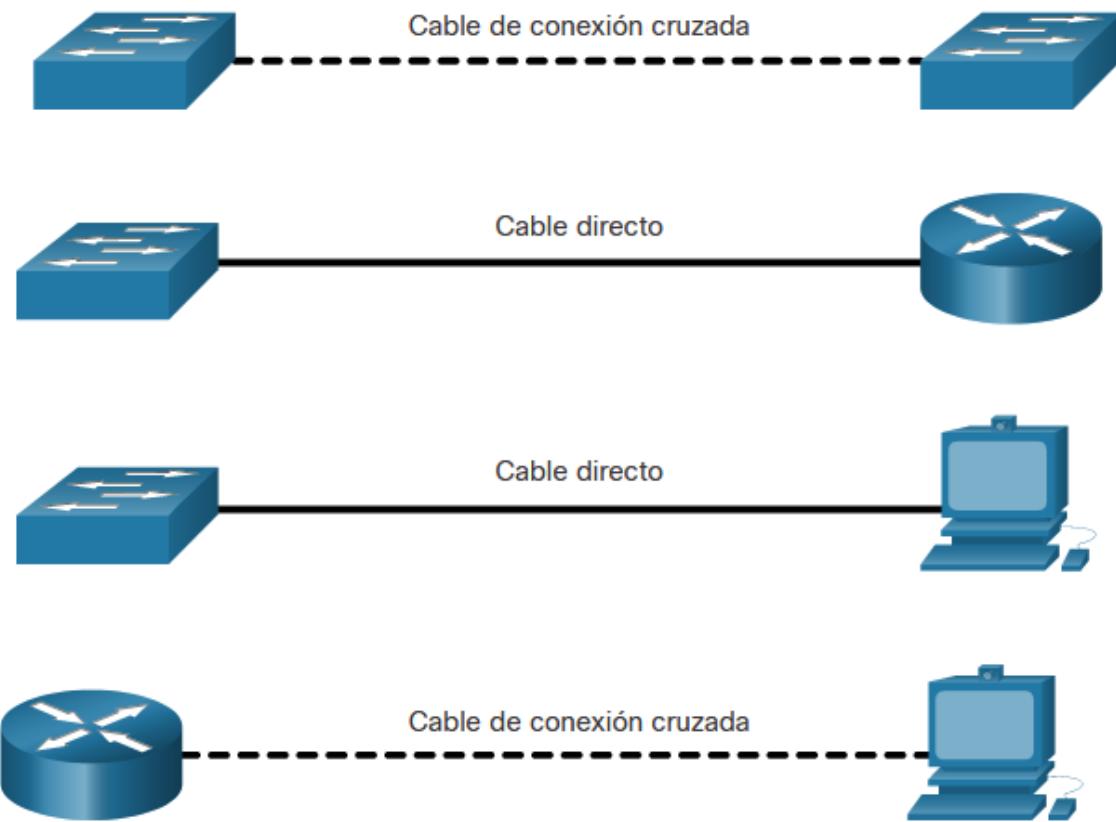
La autonegociación es una función optativa que se encuentra en la mayoría de los switches Ethernet y NICs. Permite que dos dispositivos negocien automáticamente las mejores capacidades de velocidad y dúplex. Si ambos dispositivos tienen la funcionalidad, se selecciona dúplex completo, junto con el ancho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



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

## Auto-MDIX (MDIX automático)

Las conexiones entre dispositivos iguales o entre un router y un host requerían el uso de un cable cruzado. De lo contrario un cable directo. El tipo de cable requerido dependía del tipo de dispositivos de interconexión.



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

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