

Planificación y Administración de Redes

T.4 La capa de enlace de datos

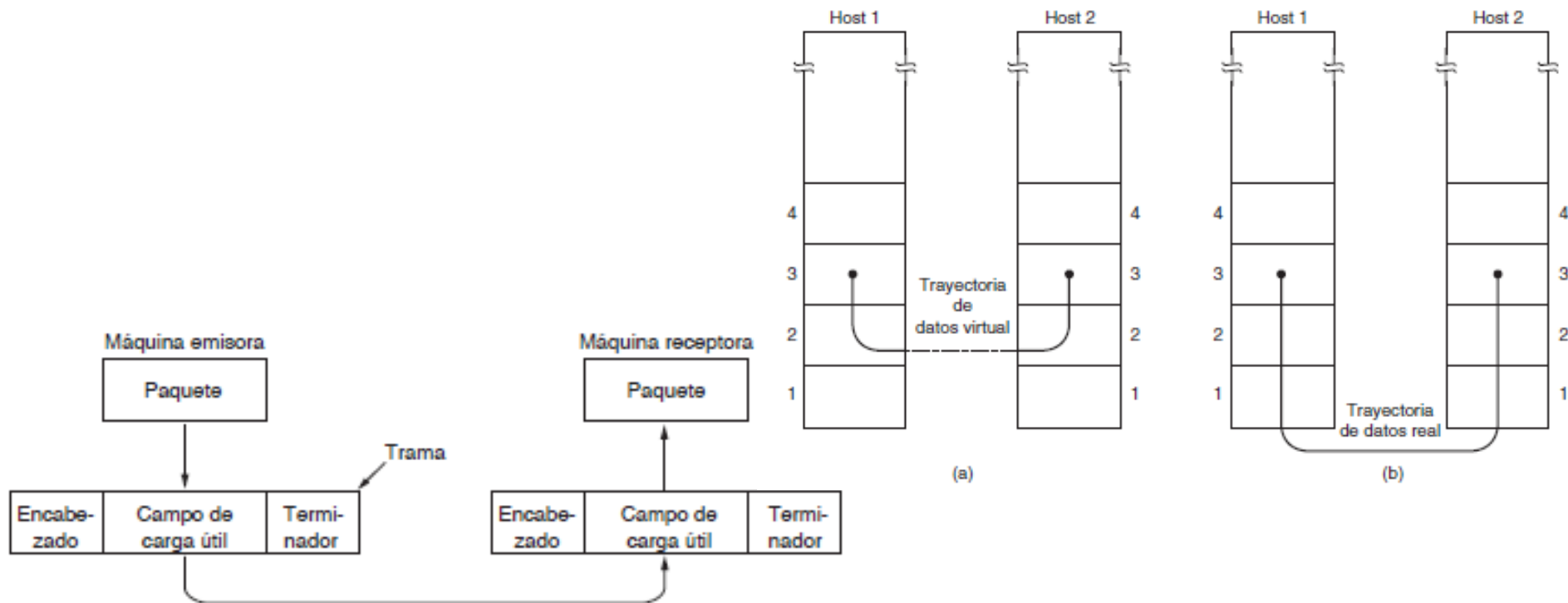
Índice

1. Introducción (6.1)
2. Subcapas de enlace de datos (6.1)
3. Medios de control de acceso (6.2)
4. Trama de enlace de datos (6.3)
5. Ethernet (7.1, 7.2)
6. Funcionamiento Switch (7.3, 7.4)
7. Tipos de Ethernet
8. Point-to-Point Protocol (PPP)

1 Introducción

Introducción

La capa de enlace de datos del modelo OSI (Capa 2) prepara los datos de red para la red física y es responsable de las comunicaciones de tarjeta de interfaz de red (NIC) a NIC.

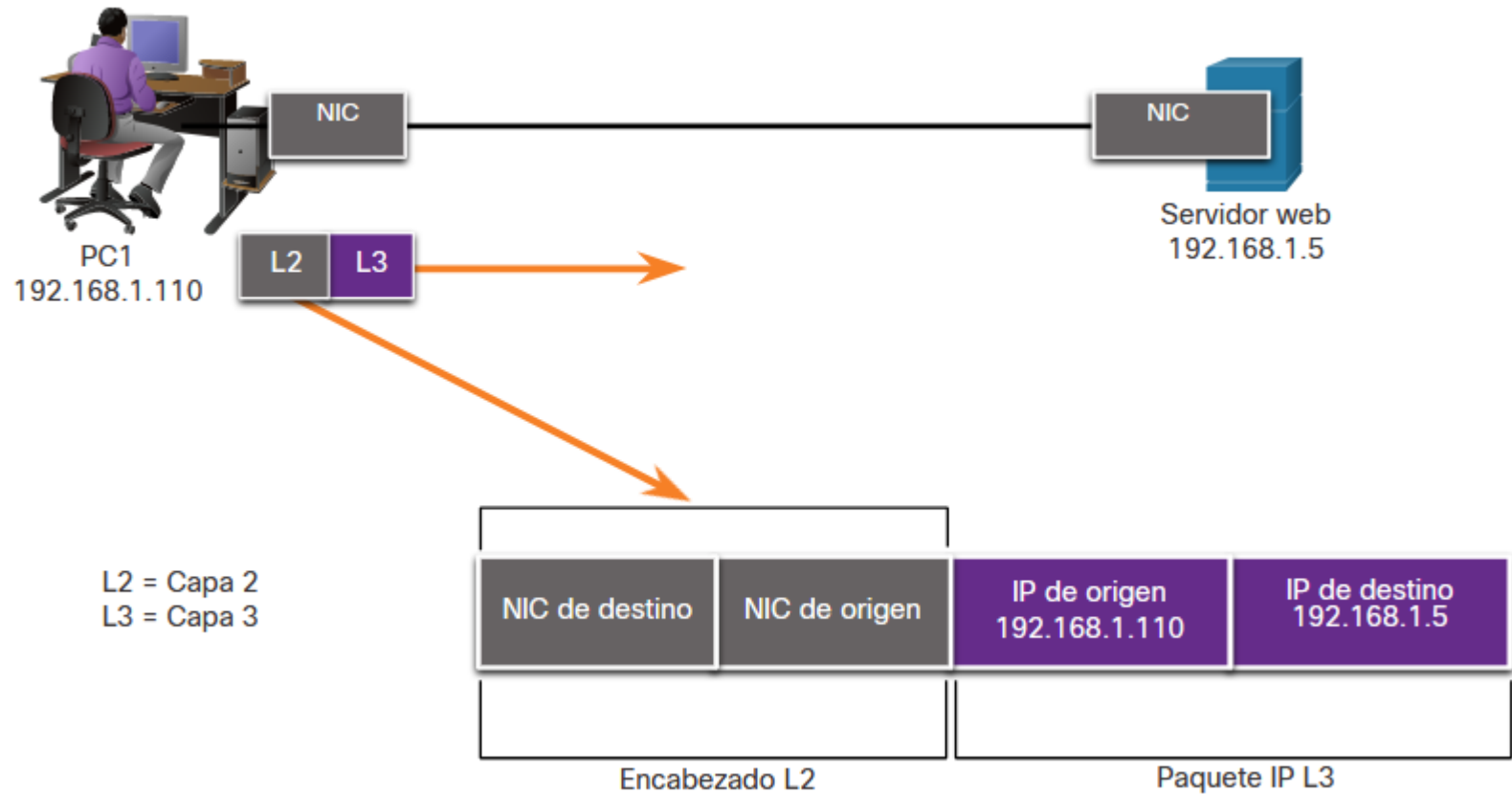


Introducción

La capa de enlace 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.**

Introducción

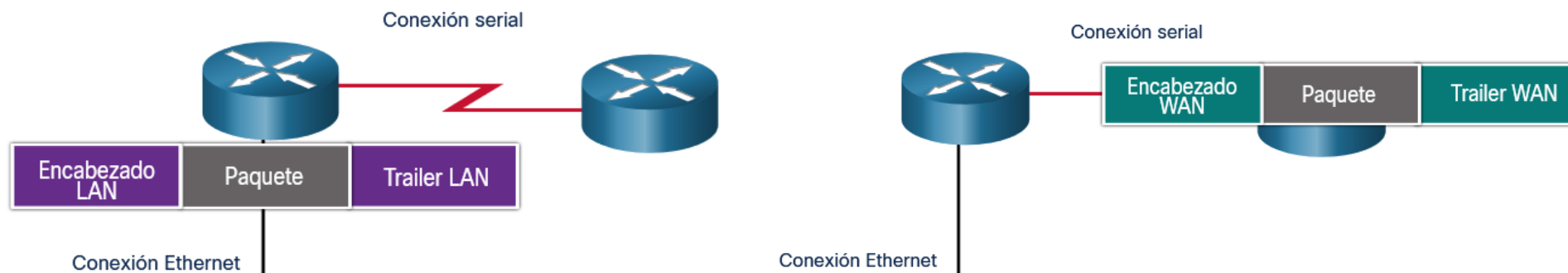


Introducción

Cada entorno de red que los paquetes encuentran cuando viajan desde un host local hasta un host remoto puede tener características diferentes.

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

- 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.



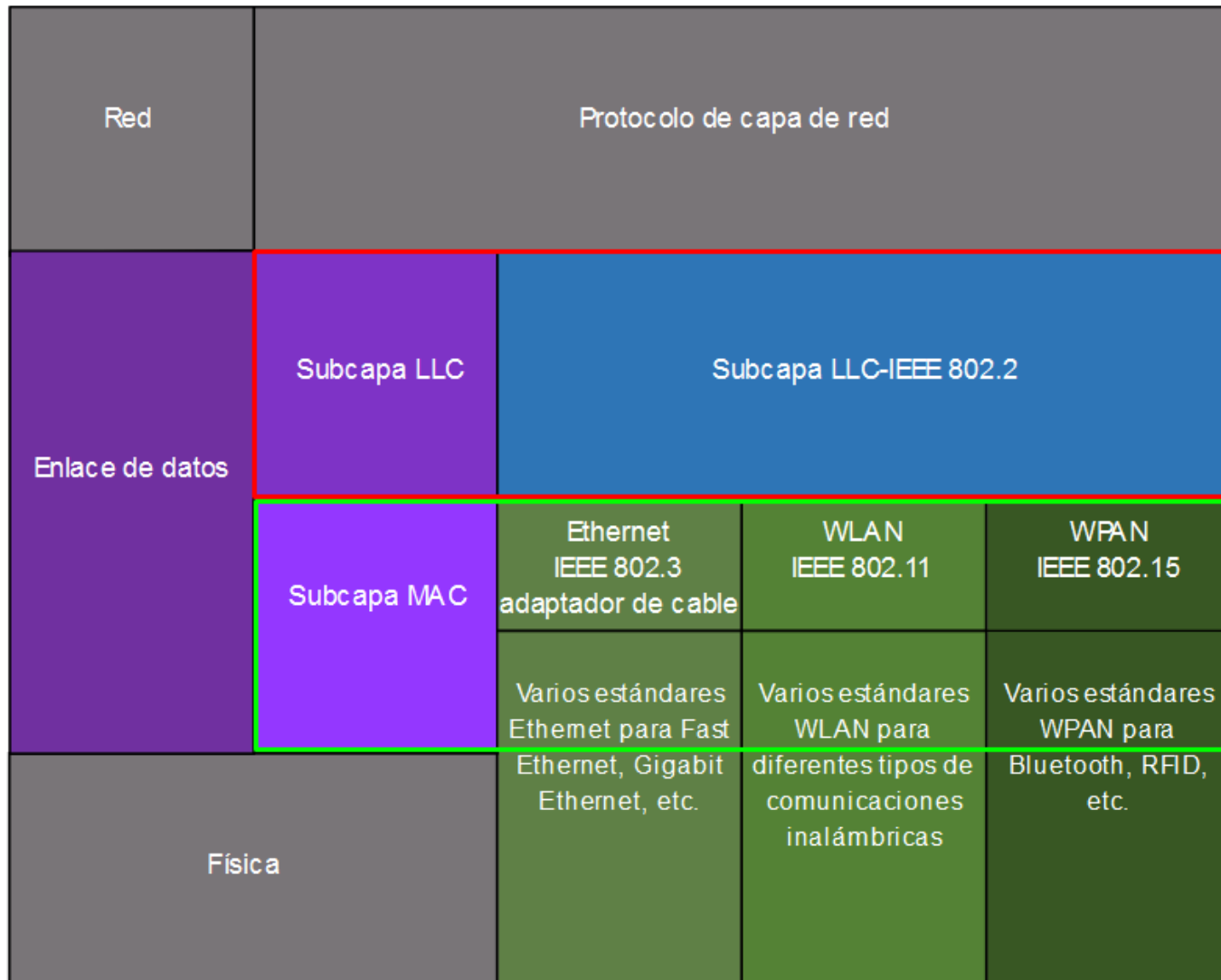
2 Subcapas de enlace de datos IEEE 802 LAN/MAN

Subcapas de enlace de datos IEEE 802

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.

Subcapas de enlace de datos IEEE 802



Subcapas de enlace de datos IEEE 802

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.

Subcapas de enlace de datos IEEE 802

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.

Subcapas de enlace de datos IEEE 802

La **subcapa MAC** también proporciona **control de acceso a medios**, lo que permite que varios dispositivos se comuniquen a través de un medio compartido (half-dúplex).

Las comunicaciones **full-dúplex no requieren control de acceso**.

3 Métodos de control de acceso

Métodos de control de acceso

Las LAN Ethernet y WLAN son un ejemplo de una red de accesos múltiples. Una **red multiacceso** es una red que puede tener dos o más dispositivos finales que intentan acceder a la red simultáneamente.

Algunas redes de acceso múltiple requieren reglas que rijan la forma de compartir los medios físicos. Hay dos métodos básicos de control de acceso al medio para medios compartidos:

- Acceso por contención
- Acceso controlado o control de acceso

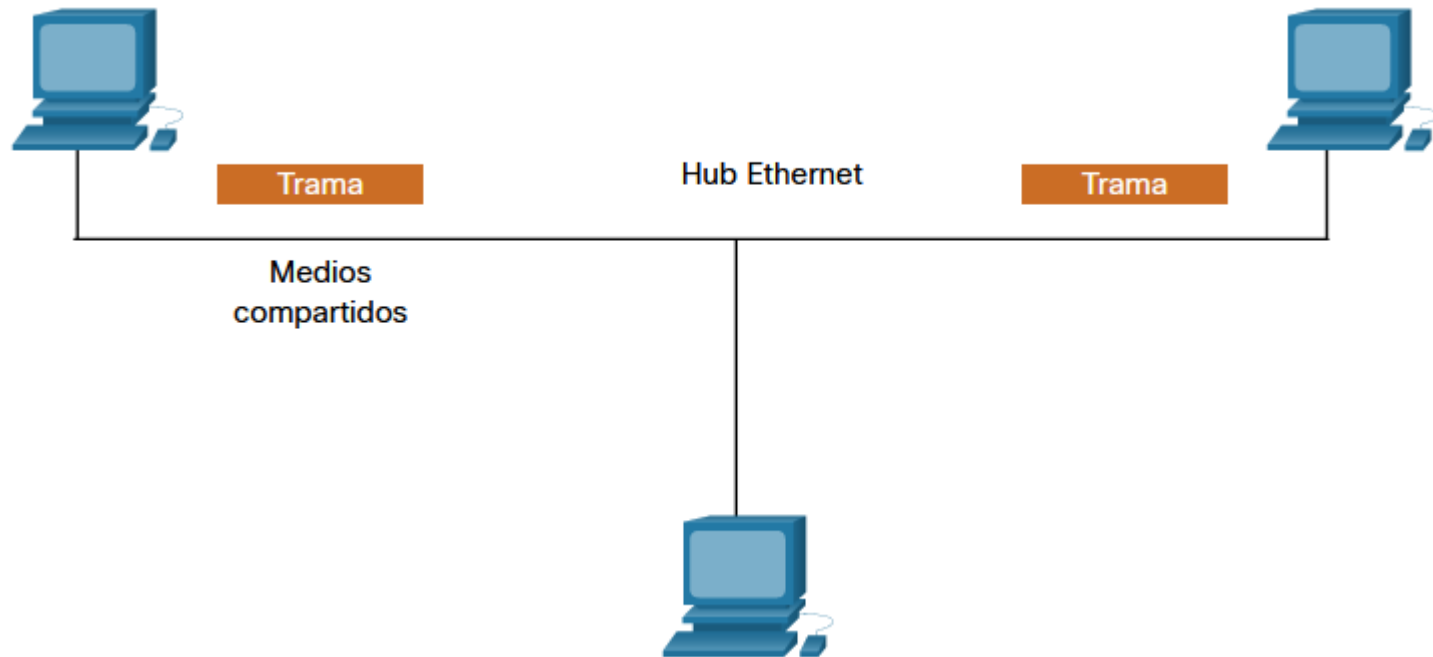
Métodos de control de acceso

Acceso basado en la contención

En las **redes multiacceso basadas en contención**, todos los **nodos** operan en **half-dúplex**, **compitiendo por el uso del medio**. Sin embargo, **solo un dispositivo puede enviar a la vez**. Por lo tanto, hay un proceso si más de un dispositivo transmite al mismo tiempo. Algunos ejemplos de métodos de acceso basados en contención son los siguientes:

- Acceso múltiple con **detección de colisiones (CSMA/CD)** utilizado en LAN Ethernet de topología de bus (**legacy**)
- El operador detecta el acceso múltiple con **prevención de colisiones (CSMA / CA)** utilizado en LAN inalámbricas

Métodos de control de acceso



Métodos de control de acceso

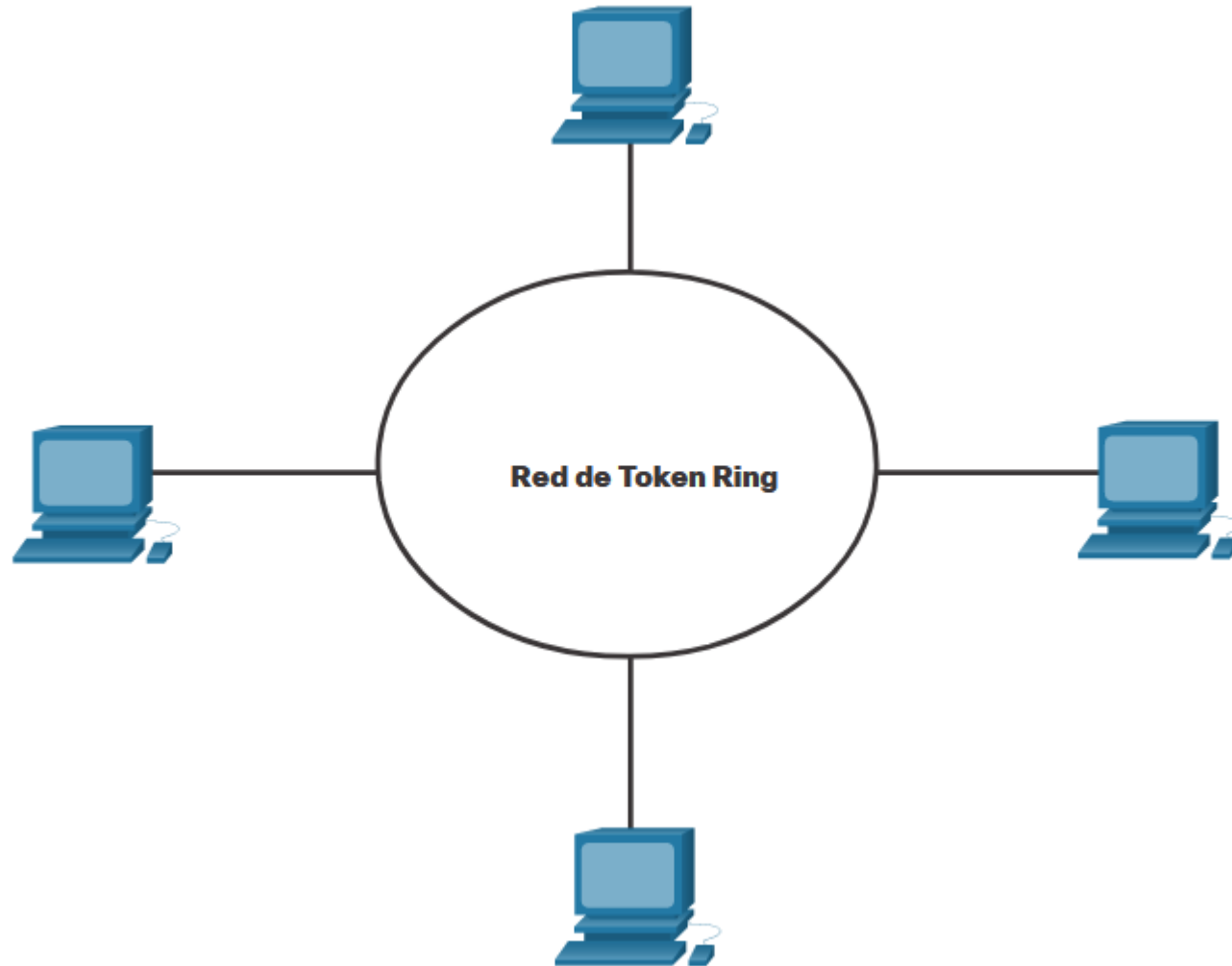
Control de acceso

En una red de acceso múltiple basada en control, **cada nodo tiene su propio tiempo para usar el medio**. Estos tipos deterministas de redes no son eficientes porque un dispositivo debe aguardar su turno para acceder al medio.

Algunos ejemplos de redes multiacceso que utilizan acceso controlado son los siguientes:

- Anillo de Token (Legacy)
- ARCNET (Legacy)

Métodos de control de acceso



CSMA/CD

Estas redes funcionan en modo **half-duplex**, lo que significa que solo un dispositivo puede enviar o recibir a la vez. Esto **requiere un proceso para gestionar cuándo puede enviar un dispositivo y qué sucede cuando múltiples dispositivos envían al mismo tiempo.**

Si dos dispositivos transmiten al mismo tiempo, se produce una colisión.

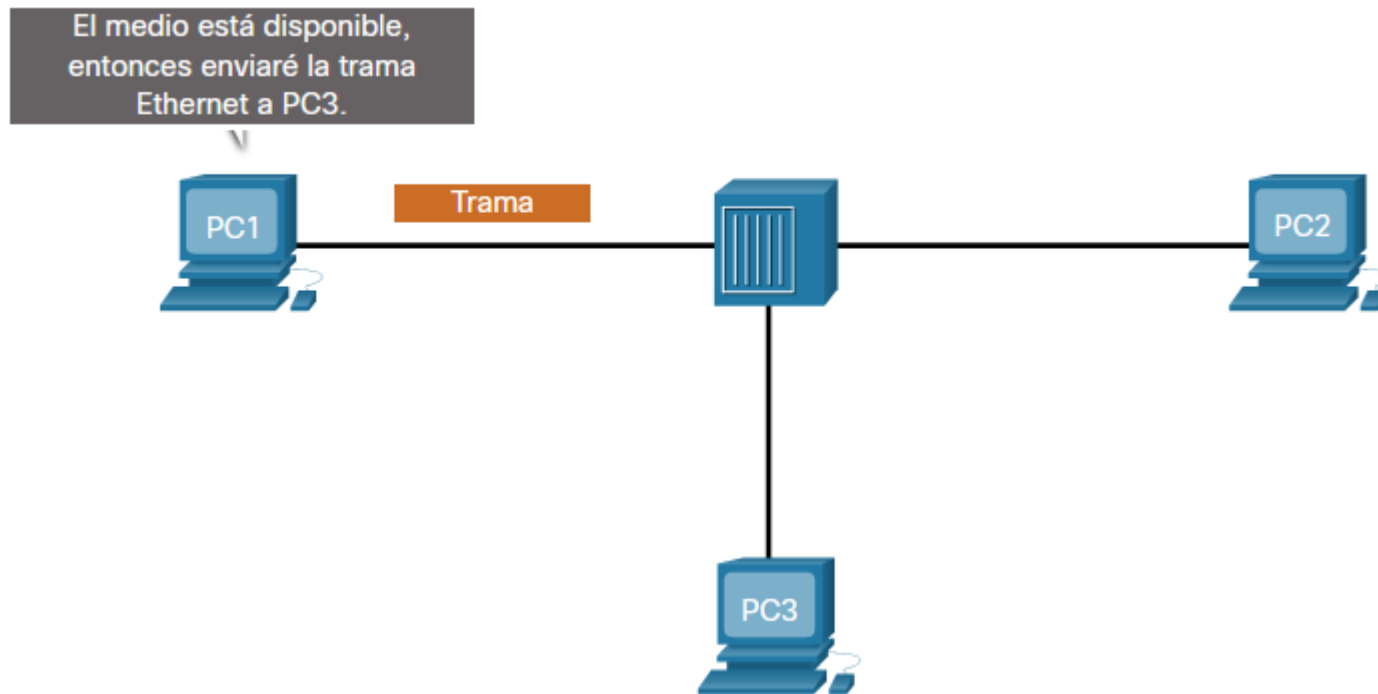
CSMA/CD

Para las LAN Ethernet legacy, **ambos dispositivos detectarán la colisión en la red**. Esta es la parte de detección de colisiones (**CD**) de CSMA/CD. La NIC compara los datos transmitidos con los datos recibidos, o al reconocer que la amplitud de la señal es más alta de lo normal en los medios.

Los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.

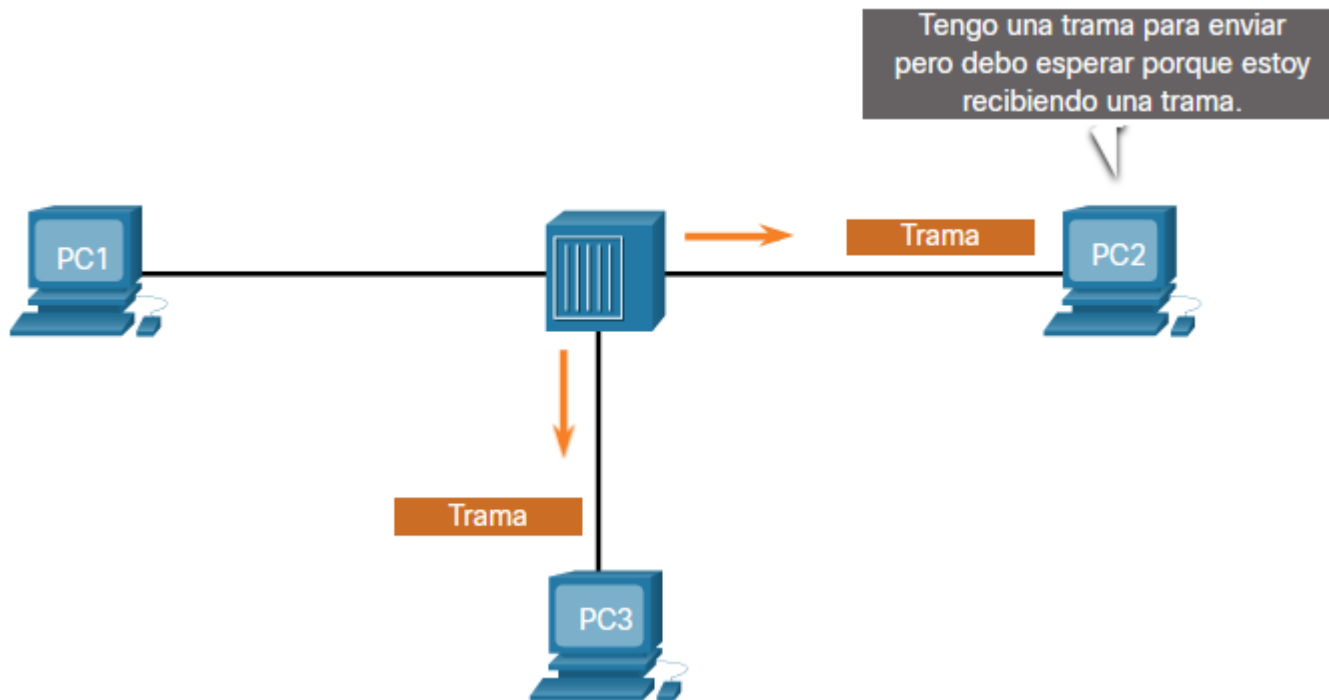
CSMA/CD

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.



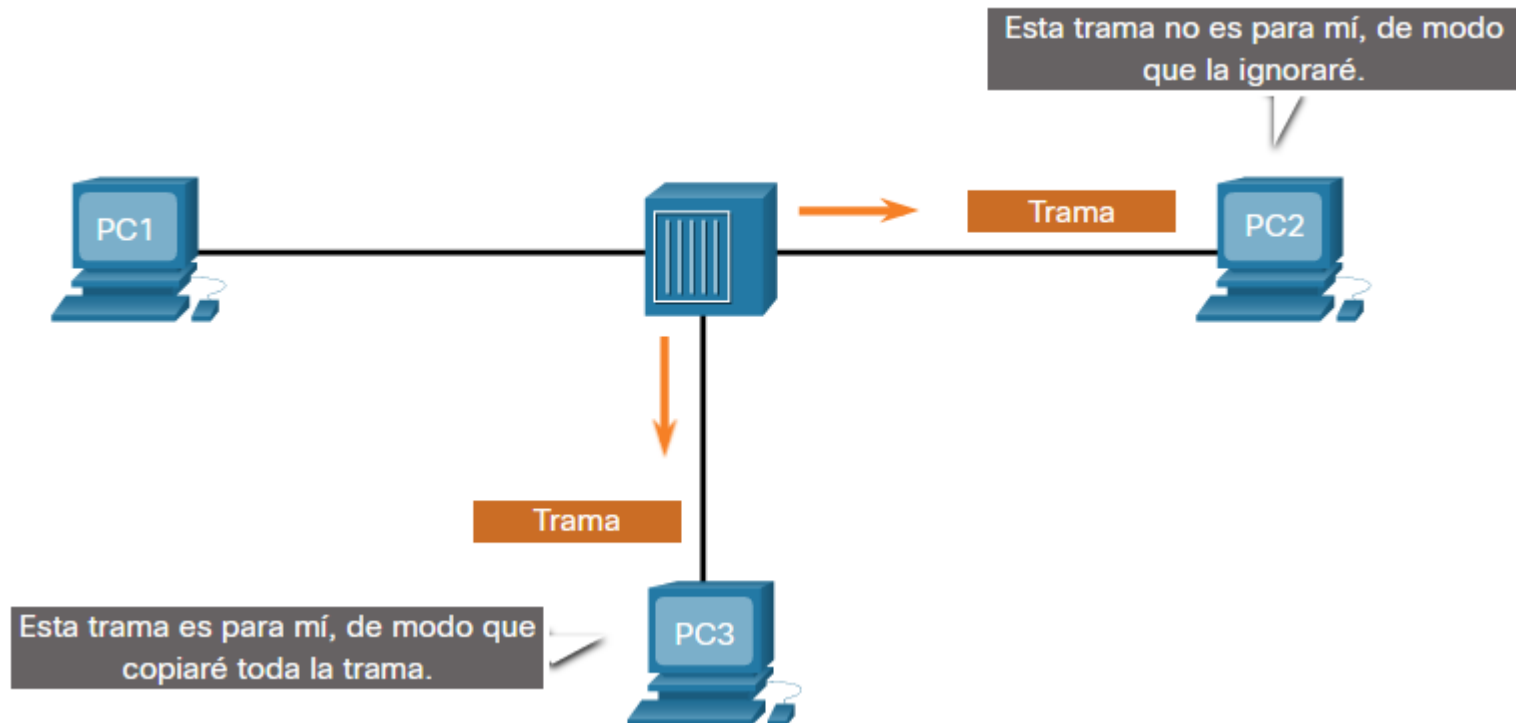
CMSA/CD

Si otro dispositivo quiere transmitir, pero está recibiendo una trama, **deberá esperar hasta que el canal esté libre**.



CSMA/CD

Dado que la trama tiene una dirección destino de enlace de datos, solo ese dispositivo aceptará y copiará toda la trama. Todas las demás NIC del dispositivo ignorarán la trama



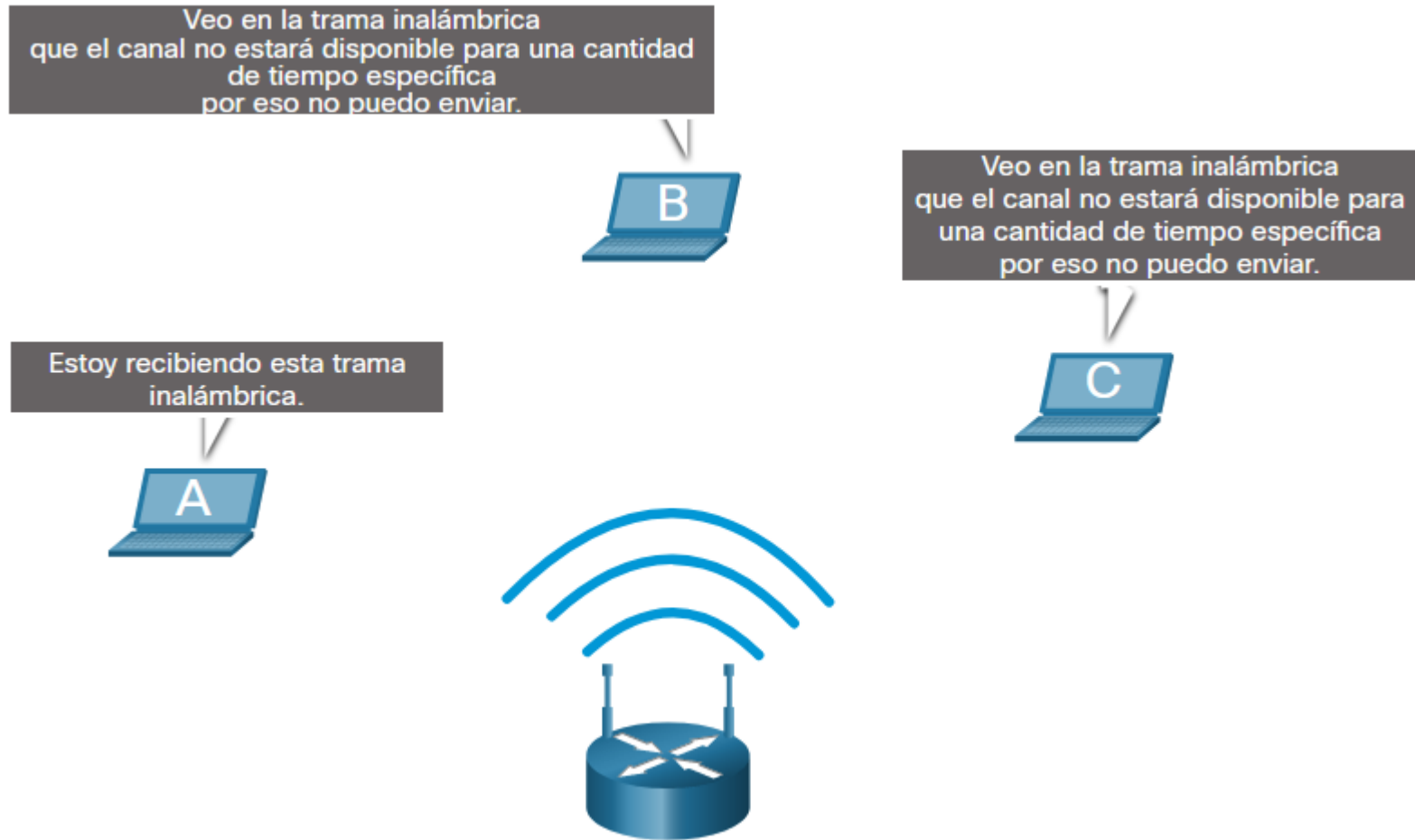
CSMA/CA

Otra forma de CSMA utilizada por las WLAN IEEE 802.11 es el CSMA/CA (prevención de colisión).

CSMA/CA utiliza un método similar a CSMA/CD para detectar si el medio está libre. CSMA/CA usa técnicas adicionales. **En entornos inalámbricos, no es posible que un dispositivo detecte una colisión.**

CSMA/CA no detecta colisiones pero intenta evitarlas ya que aguarda antes de transmitir. Cada dispositivo que transmite incluye la duración que necesita para la transmisión. Todos los demás dispositivos inalámbricos reciben esta información y saben durante cuánto tiempo el medio no estará disponible.

CSMA/CA



4 Trama de enlace de datos

Trama de enlace de datos

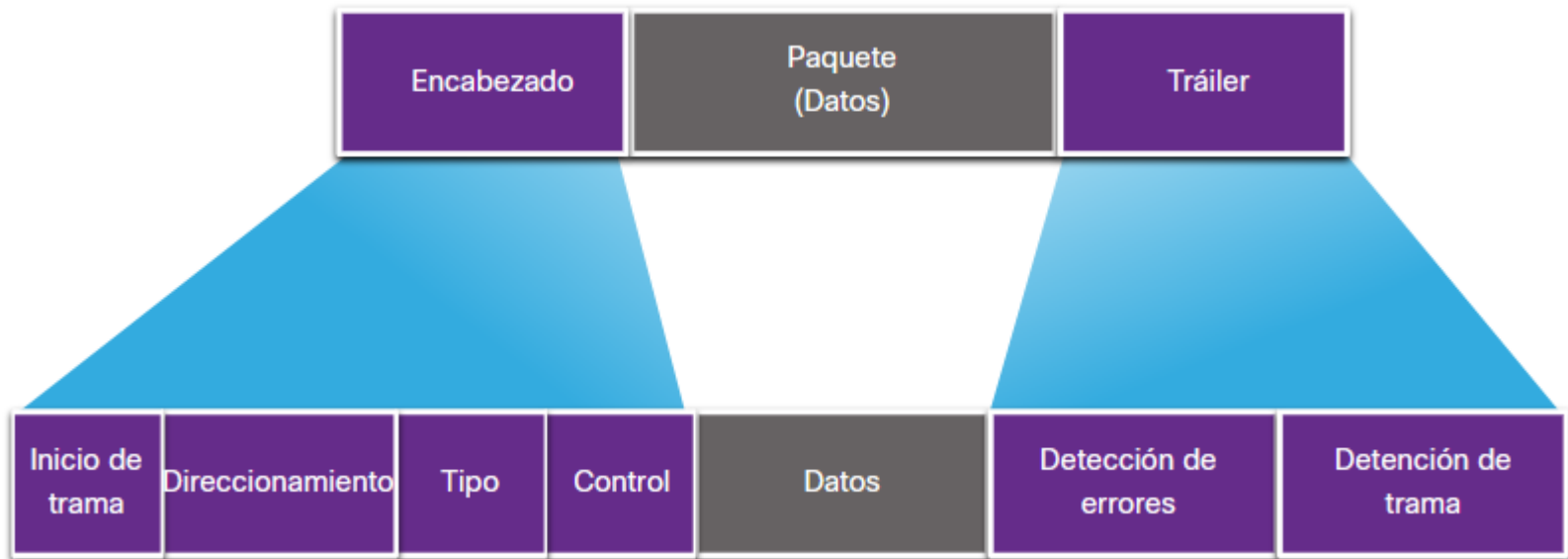
La capa de enlace de datos prepara los datos encapsulados (generalmente un paquete IPv4 o IPv6) para el transporte a través de los medios locales encapsulándolos con un encabezado y un tráiler para crear una trama.

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

Campos de una 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.**



Campos de una 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) (prioridad de servicios).
- **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.

Direcciones de Capa 2

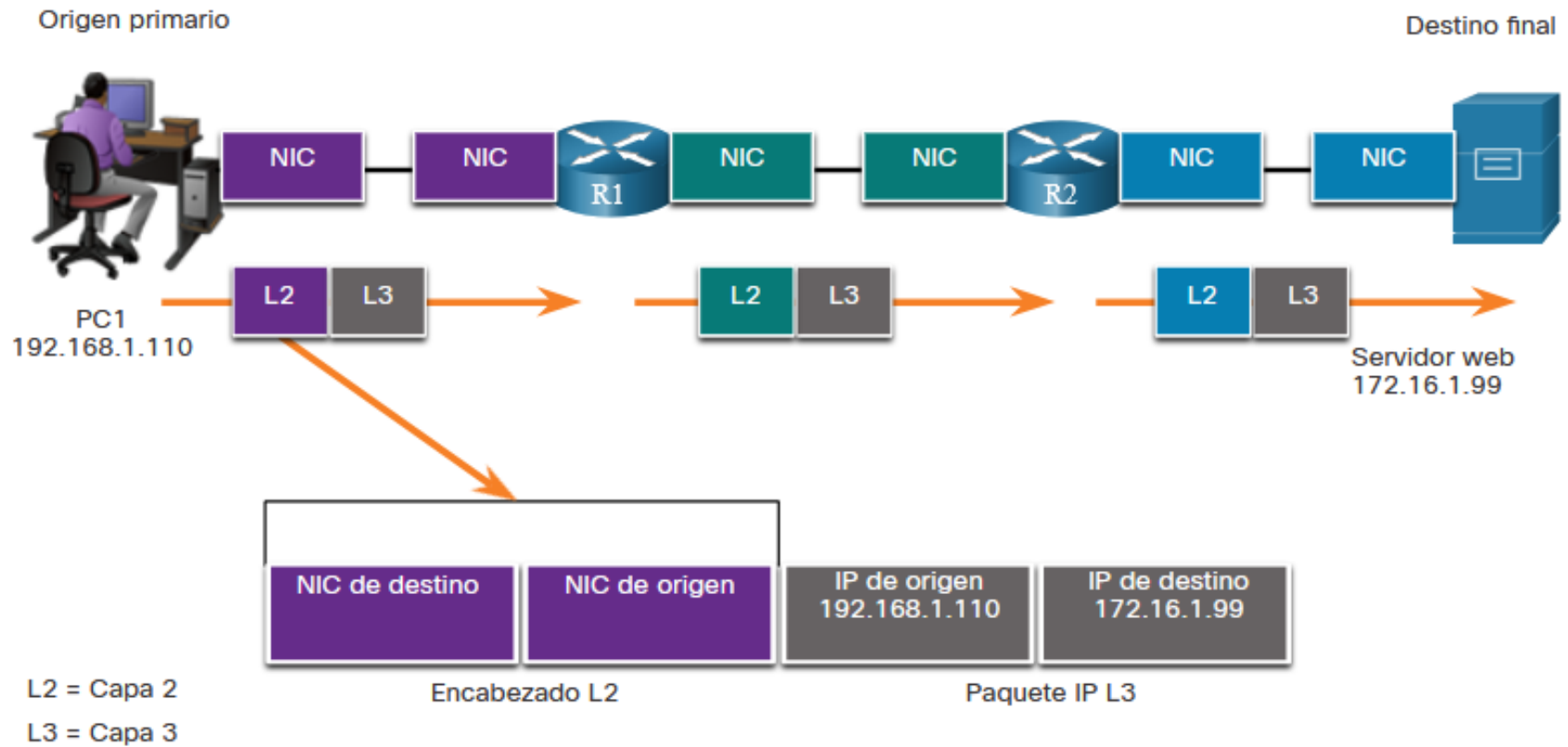
La **capa de enlace de datos proporciona** el direccionamiento utilizado en el transporte de una trama a través de un medio local compartido mediante las **direcciones físicas**.

Las direcciones físicas **no** indican en qué red está ubicado el dispositivo. En cambio, la dirección física es **única** para un dispositivo en particular.

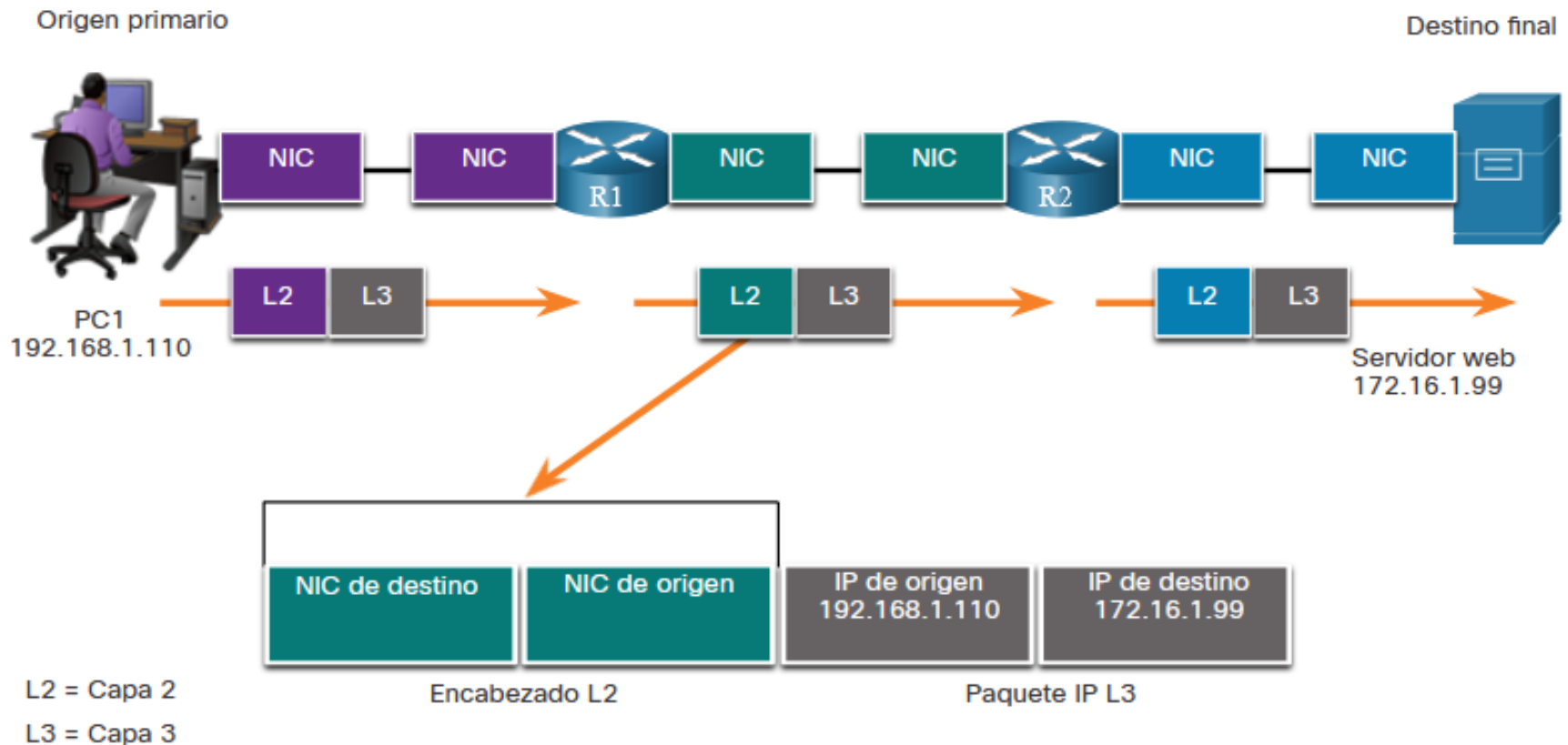
Las direcciones de capa 2 sólo se utilizan para conectar dispositivos **dentro del mismo medio compartido**, en la misma red IP.

La dirección de la capa de enlace de datos **solo se usa para la entrega local**.

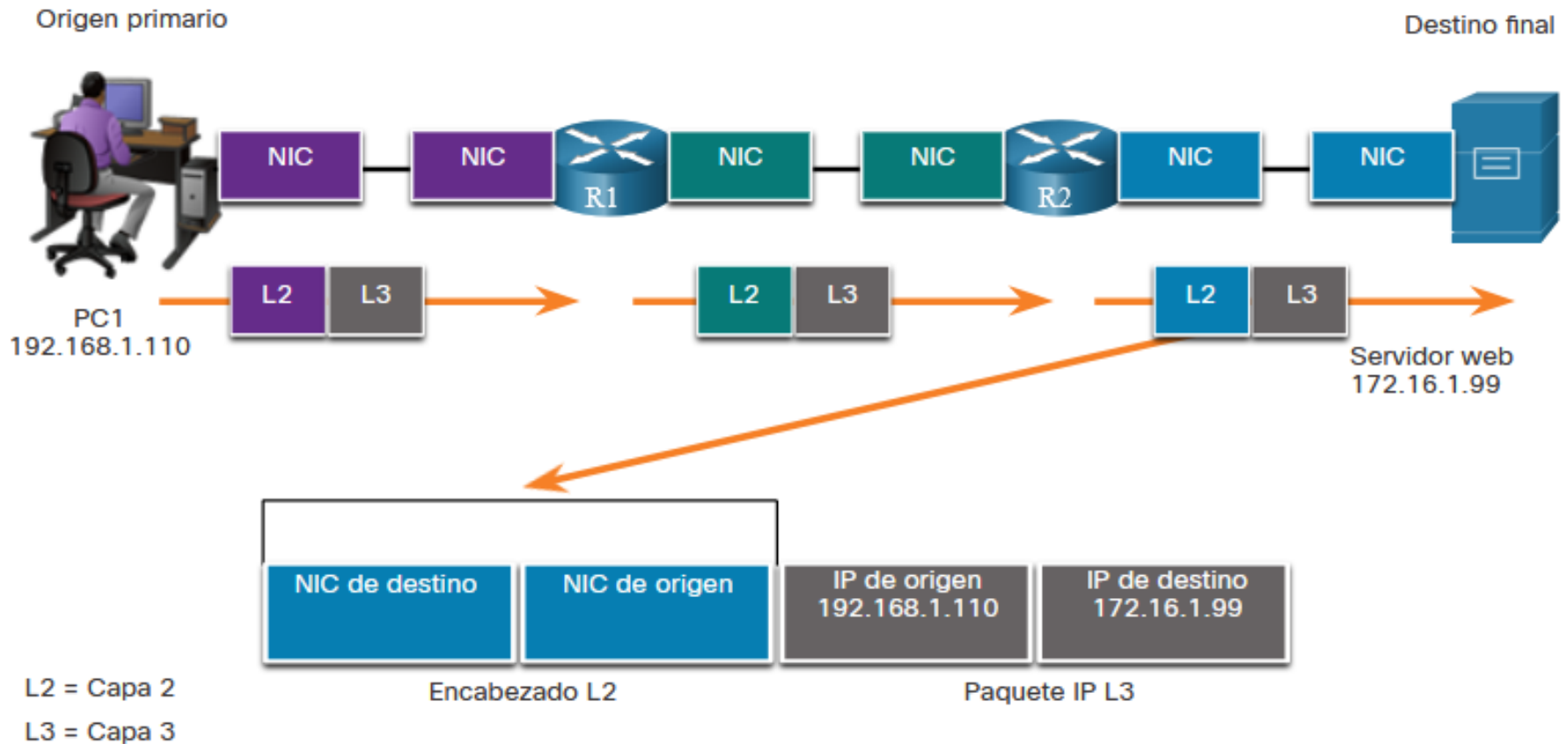
Direcciones de Capa 2



Direcciones de Capa 2



Direcciones de Capa 2



Protocolos de enlace de datos

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

5 Ethernet

Ethernet

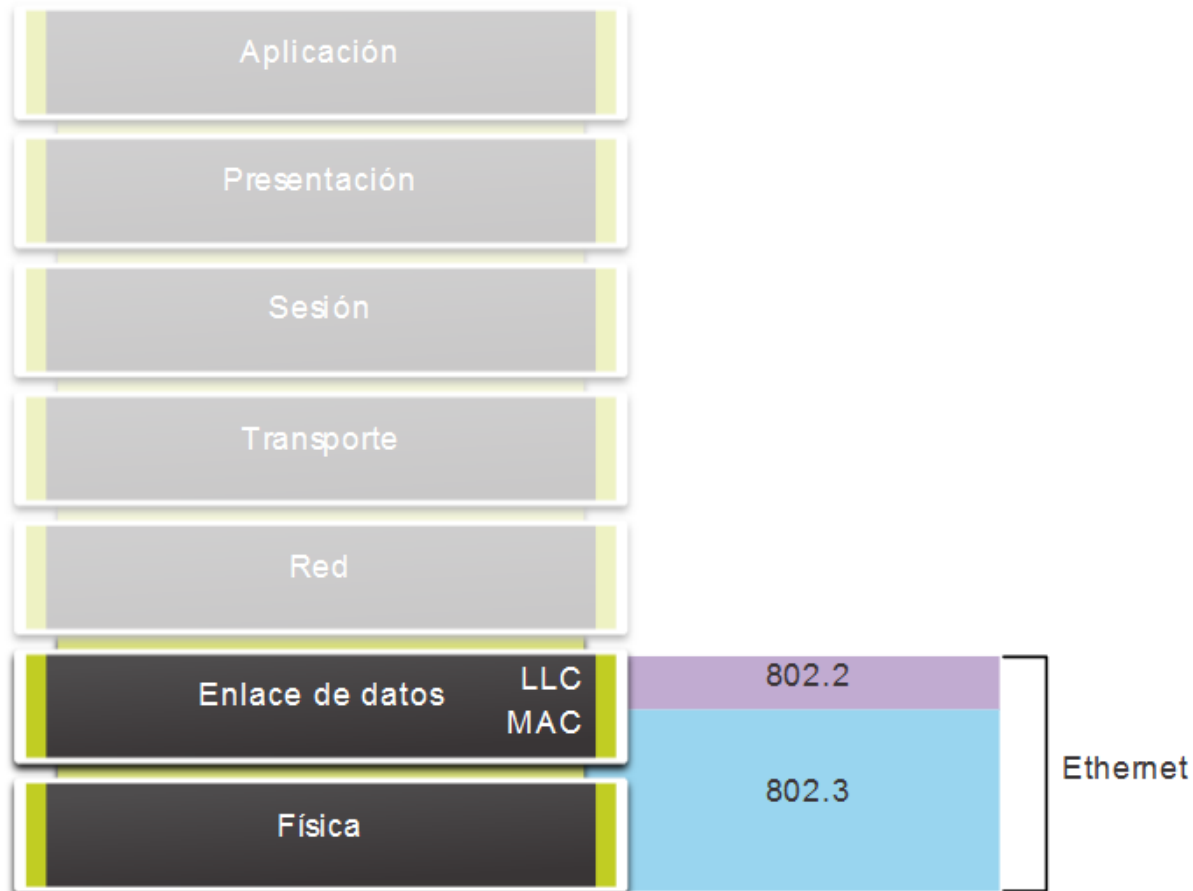
Ethernet es una de las dos tecnologías LAN utilizadas hoy en día, siendo la otra LAN inalámbricas (WLAN). **Ethernet utiliza comunicaciones por cable**, incluyendo pares trenzados, enlaces de fibra óptica y cables coaxiales.

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

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

Ethernet

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

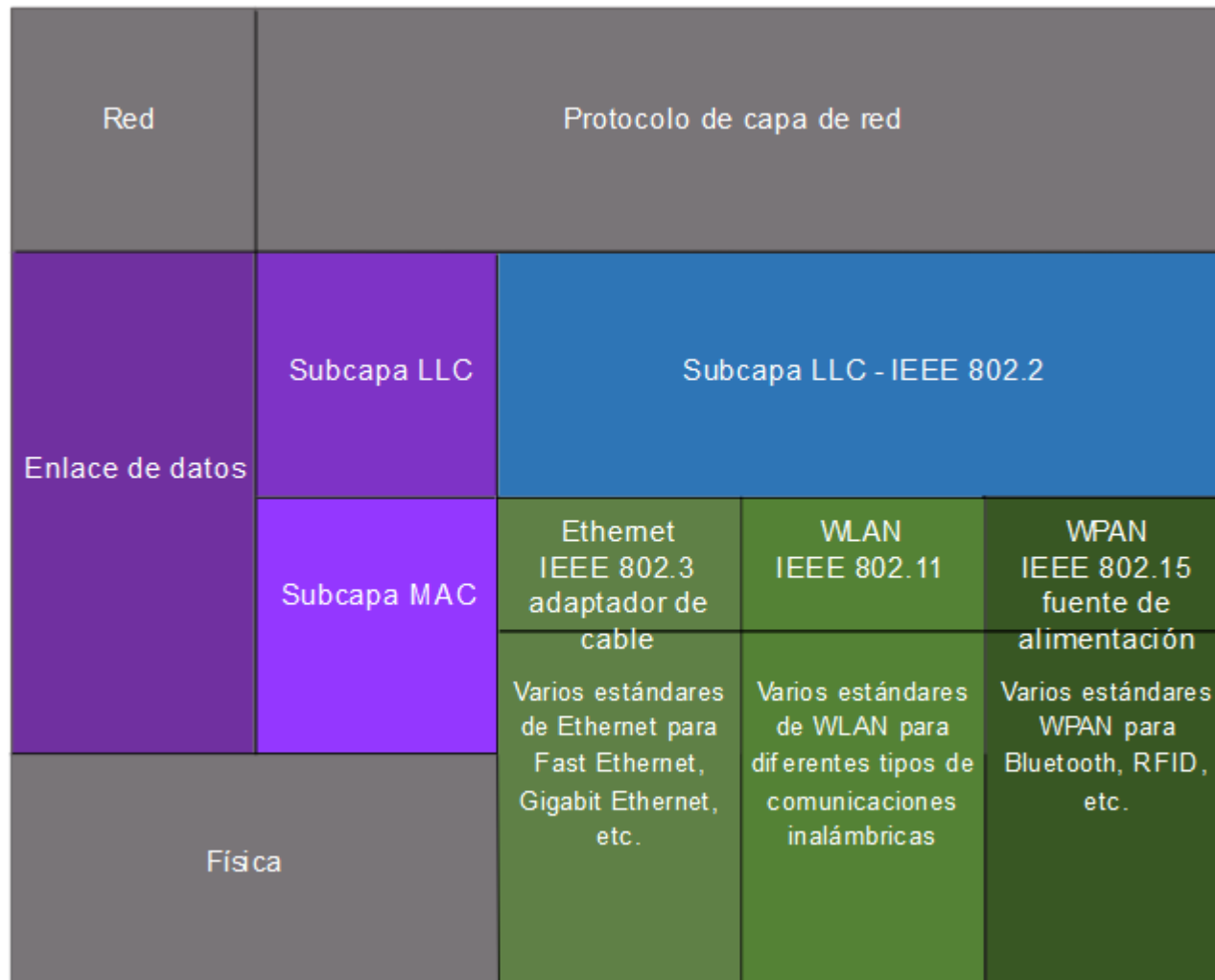


Subcapas de enlace de datos

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.

Subcapas de enlace de datos



Subcapa MAC

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

Encapsulación de datos

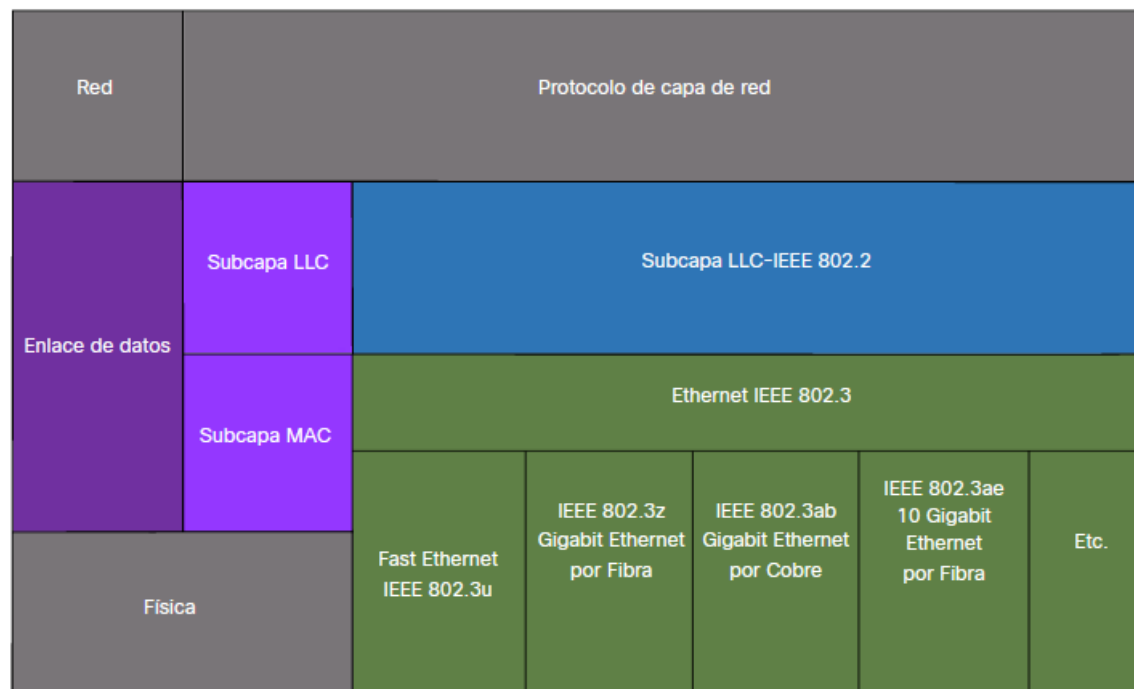
La encapsulación de datos IEEE 802.3 incluye lo siguiente:

- **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.

Subcapa MAC

Accediendo a los medios

La subcapa MAC IEEE 802.3 incluye las especificaciones para diferentes estándares de comunicaciones Ethernet sobre varios tipos de medios, incluyendo cobre y fibra.



Subcapa MAC

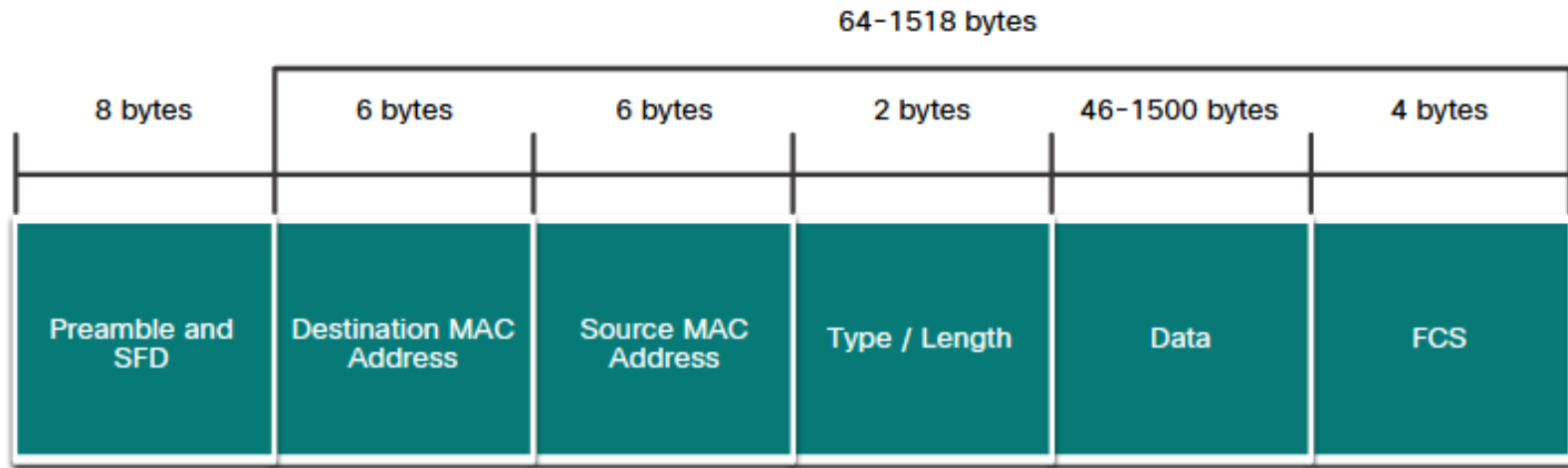
Las LAN Ethernet de hoy utilizan switches que funcionan en full-dúplex. Las comunicaciones **full-dúplex** con switches Ethernet **no** requieren **control de acceso** a través de CSMA/CD.

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.**

Si el tamaño de una trama transmitida es **menor que el mínimo o mayor que el máximo**, el dispositivo receptor descarta la trama.

Campos de trama Ethernet

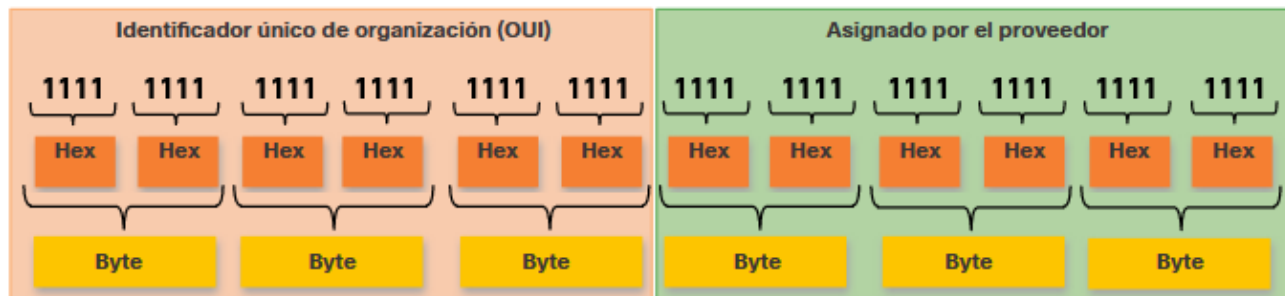


Drección MAC Ethernet

Una dirección MAC Ethernet consta de un valor binario de 48 bits y se puede expresar utilizando 12 valores hexadecimales.

Todas las direcciones MAC deben ser **únicas para el dispositivo Ethernet** o la interfaz Ethernet. Cuando un proveedor asigna una dirección MAC a un dispositivo o interfaz Ethernet, el proveedor debe hacer lo siguiente:

- Utiliza su **OUI** (identificador único de organización) asignado como los primeros 6 dígitos hexadecimales.
- **Asigne un valor único** en los últimos 6 dígitos hexadecimales.



Drección MAC Ethernet

Se puede discriminar entre las direcciones mirando el primer bit, si éste es **0** significa que es de unidestinación o **unicast**, si es **1**, será multidestino (**multicast**) o de difusión (**broadcast**). Si la dirección tiene todos sus bits a 1 entonces será de difusión (0xFFFFFFFFFFFF) y si es de multidestino el resto de bits especificará a cuál grupo corresponde el envío. Por tanto hay tres tipos de direcciones:

- **unicast** (dirección de unidifusión): identifica un solo ordenador, se utiliza para realizar un envío a un ordenador concreto.
- **multicast** (dirección de multidifusión): para referenciar un grupo de ordenadores, usado para enviar sólo un grupo de los ordenadores de la red.
- **broadcast** (dirección de difusión): para referenciar todos los ordenadores, usado por realizar un envío a todos los ordenadores.

Procesamiento de tramas

La dirección MAC 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.

Cuando el PC 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:

- Dirección MAC origen
- Dirección MAC destino

Procesamiento de tramas

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

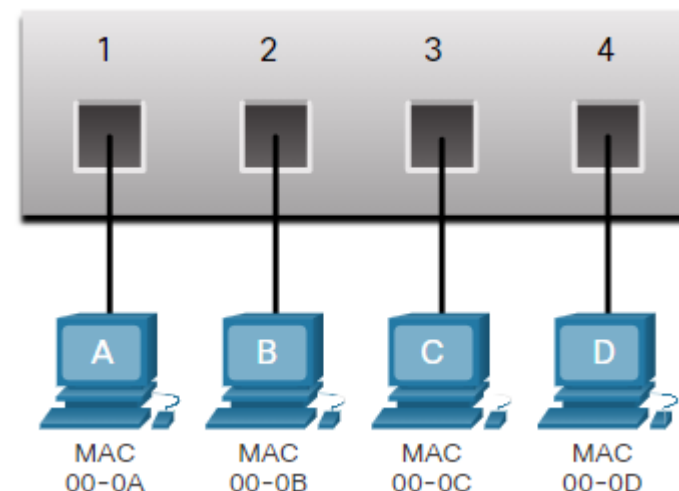
Cualquier dispositivo que sea la origen o destino de una trama Ethernet, tendrá una NIC Ethernet y, por lo tanto, una dirección MAC. Esto incluye estaciones de trabajo, servidores, impresoras, dispositivos móviles y routers

6 Funcionamiento de un Switch

Funcionamiento de un Switch

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.

Tabla de direcciones MAC	
Puerto	Dirección MAC



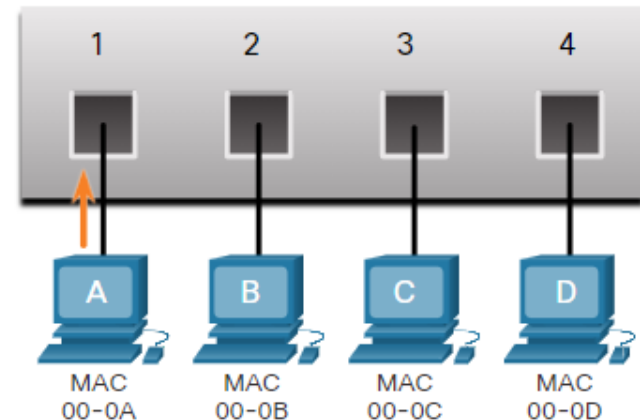
Funcionamiento de un Switch

El switch construye 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.

Funcionamiento de un Switch

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

Tabla de direcciones MAC	
Puerto	Dirección MAC
1	00-0A

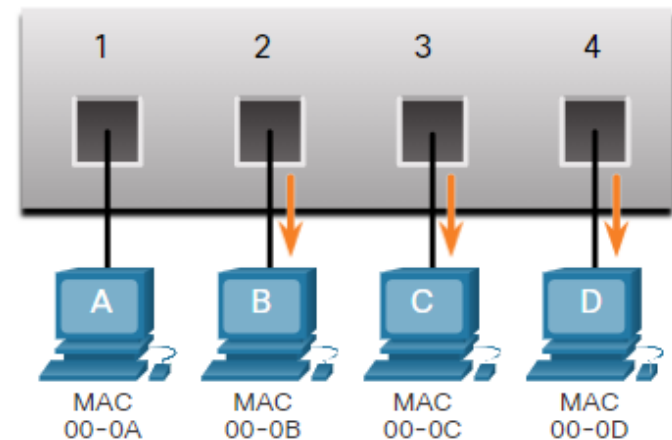


MAC de destino 00-0D	MAC de origen 00-0A	Tipo	Datos	FCS
-------------------------	------------------------	------	-------	-----

Funcionamiento de un Switch

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 desconocida.

Tabla de direcciones MAC	
Puerto	Dirección MAC
1	00-0A



MAC de destino 00-0D	MAC de origen 00-0A	Tipo	Datos	FCS
-------------------------	------------------------	------	-------	-----

Métodos de envío de un Switch

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

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

Métodos de envío de un Switch

Una gran ventaja de store-and-forward switching, es que **determina si una trama tiene errores antes de propagarla.**

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

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.

Cut-through switching

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

Fast-forward switching - Este método ofrece el nivel de latencia más bajo. Fast-forward switching reenvía el paquete inmediatamente después de leer la dirección de destino. Como el fast-forward switching comienza a reenviar el paquete antes de recibirlo por completo, es posible que, a veces, los paquetes se distribuyan con errores. Esto ocurre con poca frecuencia y la NIC de destino descarta el paquete defectuoso al recibirlo. En el modo de fast-forward, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. El fast-forward switching es el método de cut-through típico.

Cut-through switching

Fragment-free switching - 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.

Almacenamiento en memoria

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.

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

Configuración dúplex y velocidad

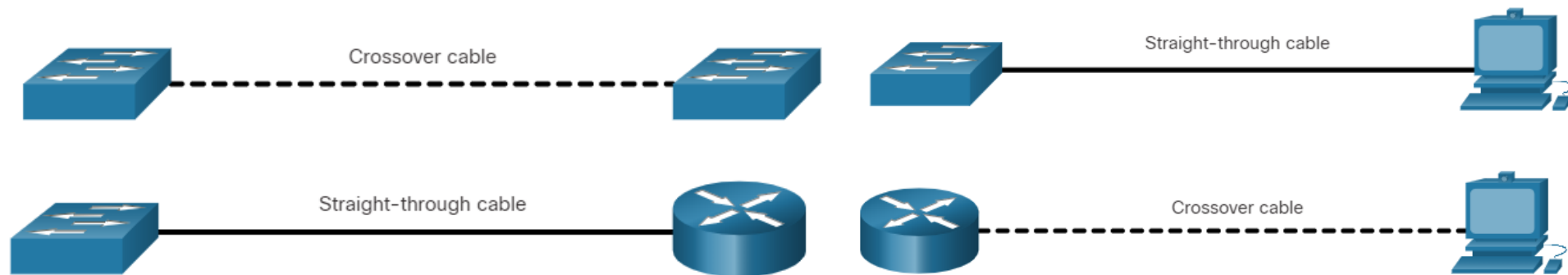
Se utilizan dos tipos de parámetros dúplex para las comunicaciones en una red Ethernet:

- **Full-duplex** - Ambos extremos de la conexión pueden enviar y recibir datos simultáneamente.
- **Half-duplex** - Solo uno de los extremos de la conexión puede enviar datos por vez.

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

Auto-MDIX

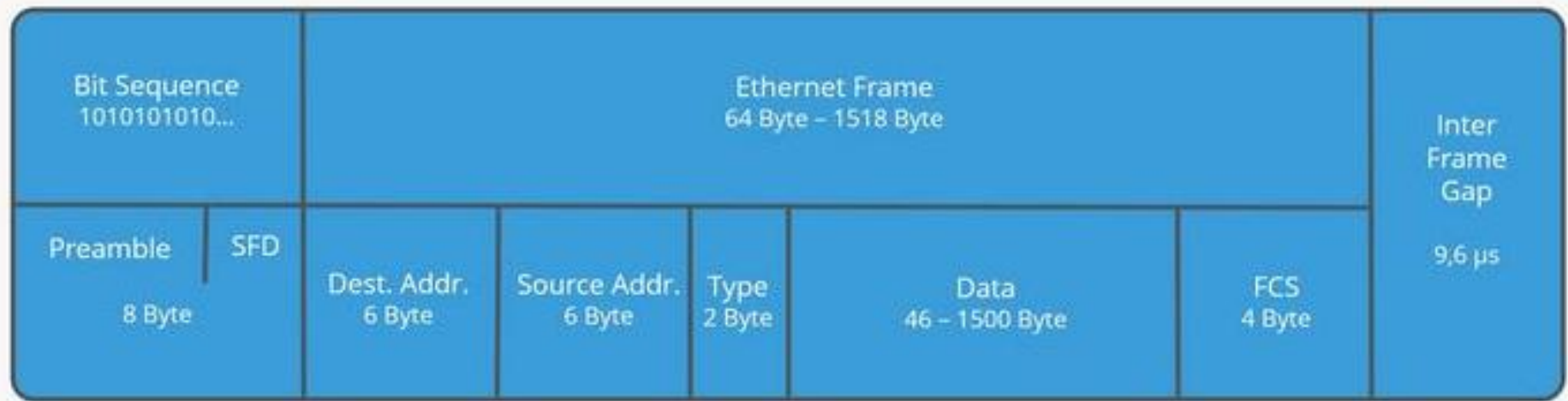
Actualmente, la mayor parte de los dispositivos admiten la característica interfaz cruzada automática dependiente del medio (**auto-MDIX**). Cuando está habilitado, el **switch detecta automáticamente el tipo de cable conectado al puerto y configura las interfaces en consecuencia**. Por lo tanto, se 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.



7 Tipos de Ethernet

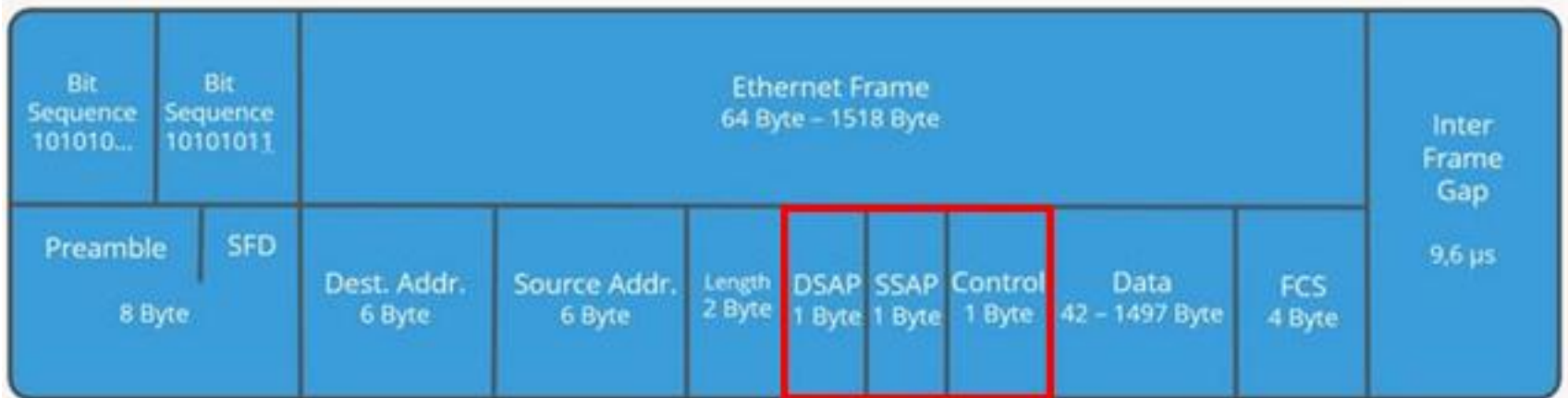
Tipos de Ethernet

Frame structure: Ethernet II



Tipos de Ethernet

Frame structure: Ethernet IEEE 802.3

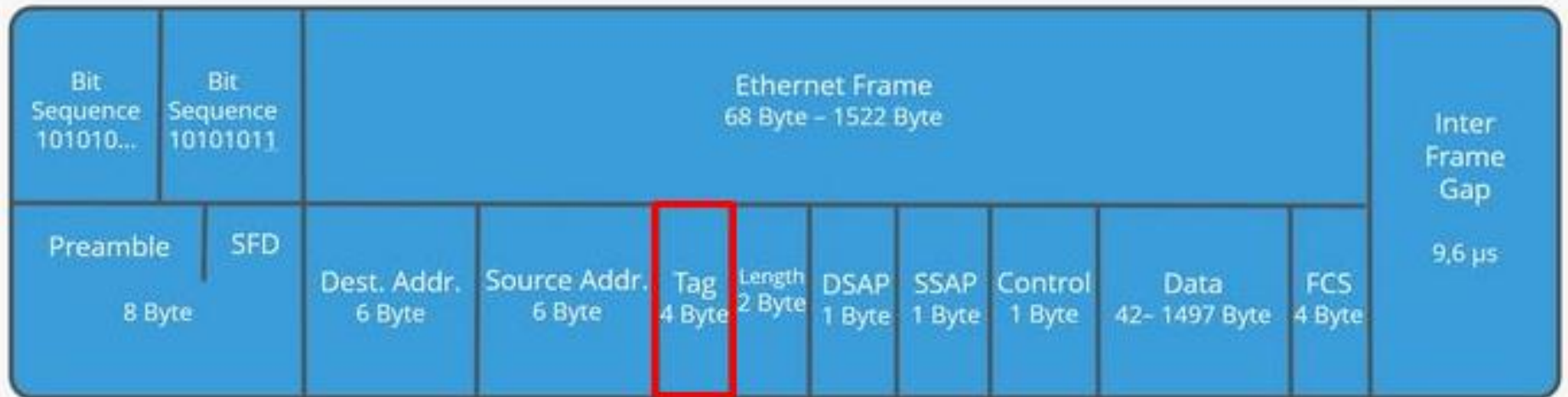


Bits introducidos por la subcapa LLC

Tipos de Ethernet

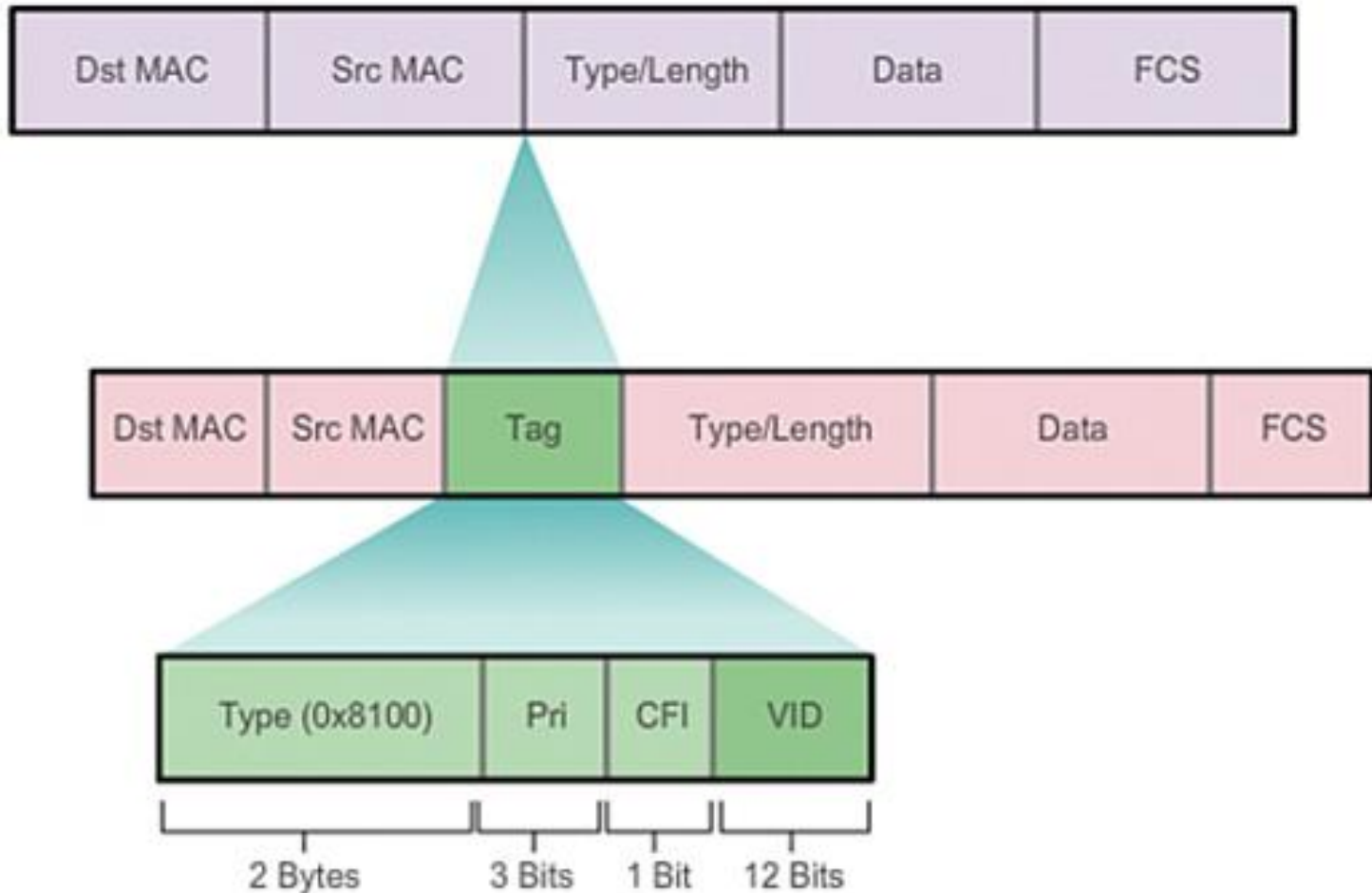
Para VLAN: 802.1Q

Frame structure: Ethernet 802.3 Tagged



Tipos de Ethernet

Para VLAN: 802.1Q



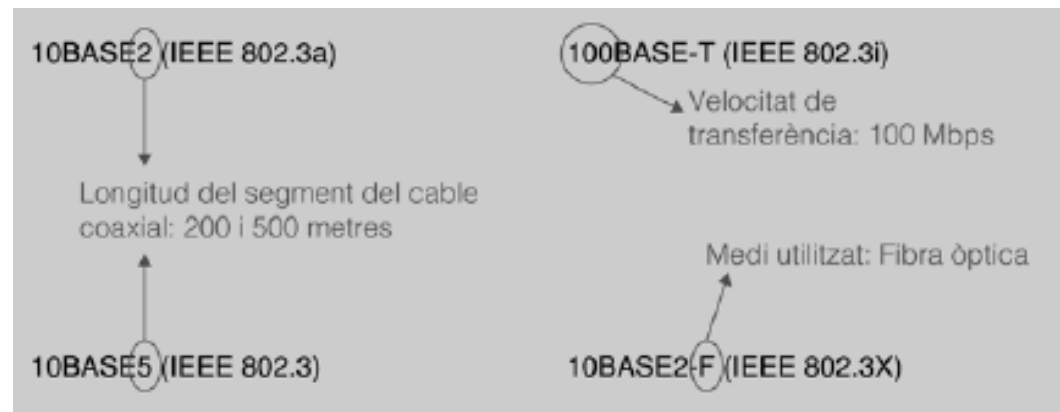
Tipos de Ethernet

Base-T

La 10Base-T fue la primera en utilizar cables trenzados como medio de transmisión. El cable utilizado es UTP de categoría mínima 3.

Base-TX

Éste es el tipo de LAN más usado en la actualidad. Utiliza topología en estrella con cables de par trenzados de clase D (categoría 5) UTP y STP.



Tipos de Ethernet

	Implementación	Estandar IEEE	Año	Velocidad	Tipo de cable	Full duplex
Ethernet	10base-T	802.3i	1990	10 Mbps	UTP CAT 3	Si
	10base-5	802.3	1983	10 Mbps	RG8 o RG11	No
	10base-3	802.3a	1985	10 Mbps	RG-58	No
Fast Ethernet	100base-TX	802.3u	1995	100 Mbps	UTP CAT5	Si
	100base-FX	802.3	1995	100 Mbps	Fibra óptica	Si
	100base-T4	802.3u	1995	100 Mbps	UTP CAT 5	No
Gigabit Ethernet	1000base-T	802.3ab	1999	1000 Mbps	UTP cat 5e	Si
	1000base-X	802.3z y ab	1998	1000 Mbps	Fibra óptica	Si
	1000base-SX	802.3z	1998	1000 Mbps	Fibra óptica	Si
	1000base-LX	802.3ab y z	1998	1000 Mbps	Fibra óptica	Si
10 Gigabit Ethernet	10Gbase-SR	802.3ae	2002	10 Gbps	Fibra óptica	No
	10Gbase-LR	802.3ae	2002	10.3 Gbps	Fibra óptica	No
	10Gbase-LX4	802.3ae	2002	10.3 Gbps	Fibra óptica	No
	10Gbase-ER	802.3	2002	10.312 Gbps	Fibra óptica	No
	10Gbase-LRM	802.3aq	2002	10.312 Gbps	Fibra óptica	No
	10Gbase-CX4	802.3ak	2002	10.312 Gbps	Cable de cobre	Si
	10Gbase-T	802.3ae	2002	10.00 Gbps	Fibra óptica	Si

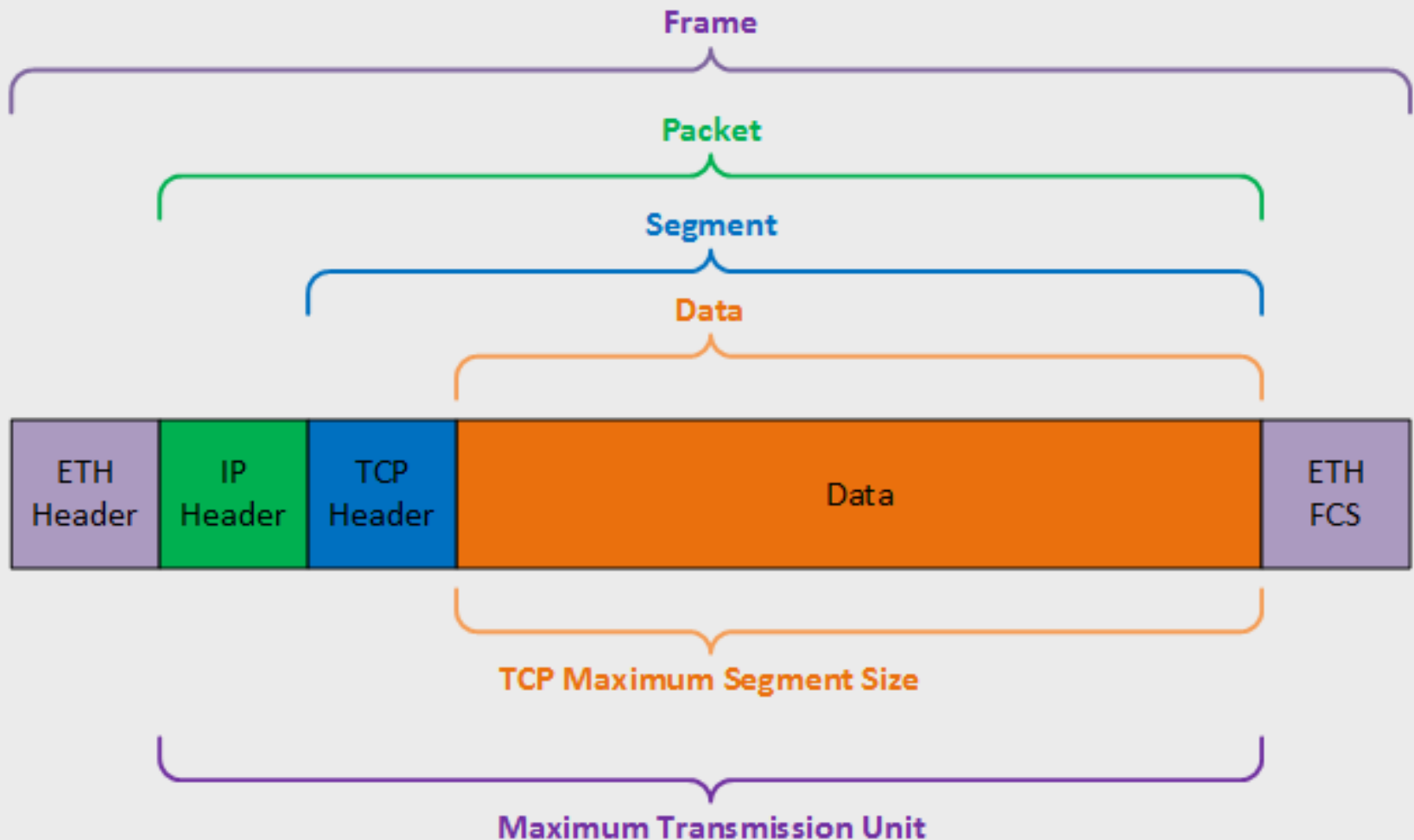
Tipos de Ethernet

Tipos de Ethernet

Tipos de Ethernet	Ancho de banda	Tipo de cable	Duplex	Distancia máxima
10Base-5	10mbps	Coaxial thicknet	Half	500m
10Base-2	10mbps	Coaxial thinnet	Half	185m
10Base-T	10mbps	UTP Cat3/Cat5	Half	100m
100Base-T	100mbps	UTP Cat5	Half	100m
100Base-TX	200mbps	UTP Cat5	Full	100m
100Base-FX	100Mbps	Fibra multimodo	Half	400m
100Base-FX	200mbps	Fibra multimodo	Full	2km
1000Base-T	1Gbps	UTP Cat 5e	Full	100m
1000Base-TX	1Gbps	UTP Cat 6	Full	100m
1000Base-SX	1Gbps	Fibra multimodo	Full	550m
1000Base-LX	1Gbps	Fibra monomodo	Full	5km
10GBase-CX4	10Gbps	Twinaxial	Full	15m
10GBase-T	10Gbps	UTP Cat6a/Cat7	Full	100m
10GBase-LX4	10Gbps	Fibra multimodo	Full	300m
10GBase-LX4	10Gbps	Fibra monomodo	Full	10km

Tipos de Ethernet

The PDUs of the TCP/IP protocol suite



8 Point-to-Point Protocol (PPP)

PPP

Protocolo punto a punto (PPP) es un protocolo del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una red. Conecta dos enrutadores directamente sin ningún equipo u otro dispositivo de red entremedias de ambos.

PPP es usado en varios tipos de redes físicas, incluyendo: cable serial, línea telefónica, línea troncal, telefonía celular, especializado en enlace de radio y enlace de fibra óptica como SONET (Synchronous Optical Network). También es utilizado en las conexiones de acceso a Internet (publicitado como banda ancha o *broadband*). Los proveedores de servicios de Internet (ISP) han usado PPP para que accedan a Internet los usuarios de una línea de conmutación, ya que los paquetes de IP no pueden ser transmitidos vía módem, sin tener un protocolo de enlace de datos.

Usado comúnmente por los ISP para establecer una línea de abonado digital (*digital subscriber line*, DSL) de servicios de internet para clientes.

PPP

Protocolo punto a punto

Un protocolo de enlace de datos común para las redes WAN

Trama						
Nombre de campo	Señaliza- dor	Dirección	Control	Protocolo	Datos	FCS
Tamaño	1 byte	1 byte	1 byte	2 bytes	variable	2 o 4 bytes

Indicador: un único byte que indica el inicio y el final de una trama. El campo Indicador está formado por la secuencia binaria 01111110.

Dirección: un único byte que contiene la dirección de broadcast PPP estándar. El protocolo PPP no asigna direcciones de estaciones individuales.

Control: un único byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos de usuario en una trama no secuencial.

Protocolo: dos bytes que identifican el protocolo encapsulado en el campo de datos de la trama. Los valores más actualizados del campo Protocolo se especifican en la Solicitud de comentarios (RFC) de números asignados más reciente.

Datos: cero o más bytes que contienen el datagrama para el protocolo especificado en el campo Protocolo.

Secuencia de verificación de trama (FCS): normalmente, tiene 16 bits (2 bytes). Mediante un acuerdo previo, con la aceptación de las implementaciones PPP se puede utilizar una FCS de 32 bits (4 bytes) para una mayor detección de errores.