UD6. Nivel de Enlace de datos

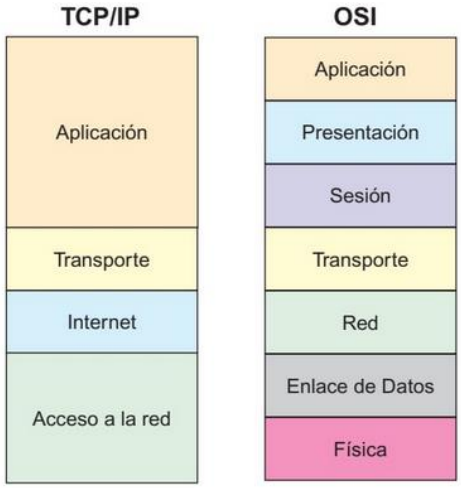
1. Estructura de la Arquitectura TCP/IP Vs OSI

TCP/IP no es un protocolo, sino un conjunto de protocolos, también llamado pila de protocolos.

Recuerda que la arquitectura TCP/IP **no es un estándar oficial**, al contrario que el **modelo OSI.**

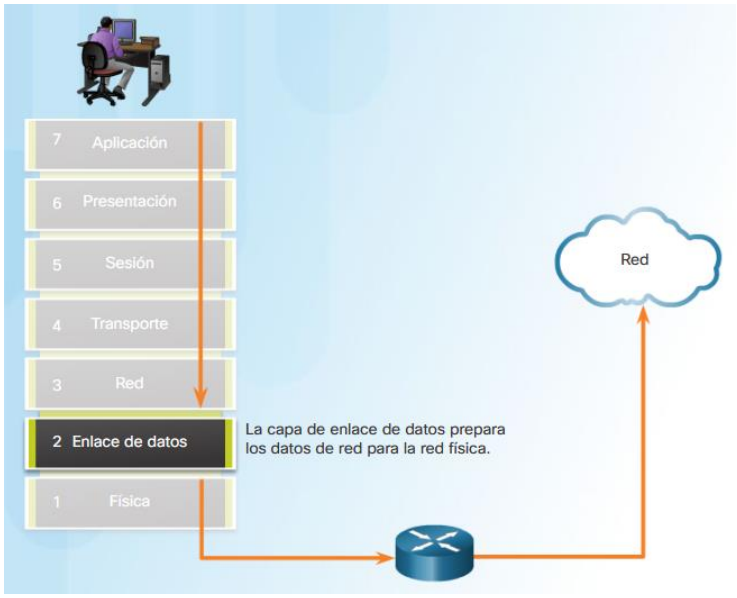
Esta arquitectura empezó a desarrollarse como base de **ARPANET**, red de comunicaciones militar del gobierno de los EEUU, origen de lo que hoy conocemos como Internet.

La **comparación** entre la arquitectura TCP/IP y el modelo OSI es la siguiente:



La pila de protocolos TCP/IP está formada por 4 niveles:

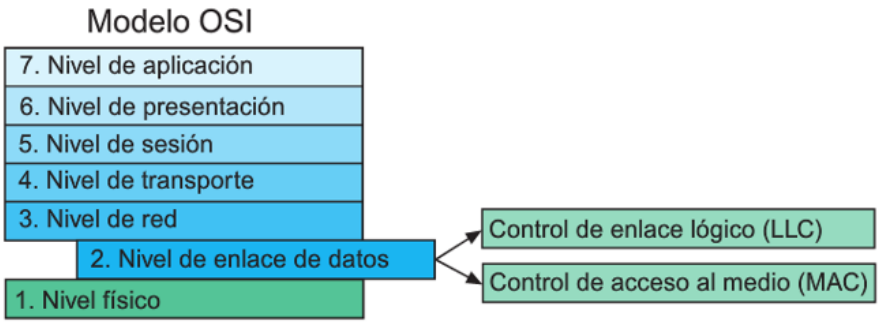
- Las aplicaciones de los usuarios (los programas) se comunican con el **Nivel de Aplicación**. En dicha capa encontramos protocolos como **DHCP**, **DNS**, **HTTP**, **FTP**, **SMTP**, **POP3**,…. Cada tipo de programa interacciona con un protocolo de aplicación distinto, en función de su propósito.
- Para procesar las peticiones de los programas de usuario, los protocolos de nivel de aplicación se comunican con un protocolo del **Nivel de Transporte**, que puede ser **TCP** o **UDP**. Esta capa toma los datos que recibe del nivel de aplicación, los divide en paquetes y los envía al nivel de Red (también conocido como Internet). Durante la recepción, esta capa pasa al nivel de aplicación los paquetes que recibe del nivel de Red. El nivel de transporte no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza.
- En el **Nivel de Red** opera el protocolo **IP** (IPv4 y/o IPv6) que añade información de direccionamiento a los paquetes que le llegan del nivel de transporte y los pasa al nivel de acceso a la red. Dicha información de direccionamiento consiste en la dirección IP de las máquinas de origen y destino del paquete.
- El **Nivel de Acceso a la Red** toma los paquetes que recibe del nivel de Red (que pasan a llamarse **datagramas**) y los envía a la red. Durante la recepción, esta capa recibe los datagramas que le llegan de la red y los pasa al nivel de red. Los protocolos que operan en este nivel dependen del tipo de red en el que se esté trabajando. Hoy en día casi todas las máquinas utilizan redes tipo **Ethernet**, de manera que en este nivel se encuentran las capas Ethernet, es decir, LLC, MAC y Física. Los datagramas que viajan por la red se llaman **tramas.**



2. Nivel de Enlace de datos

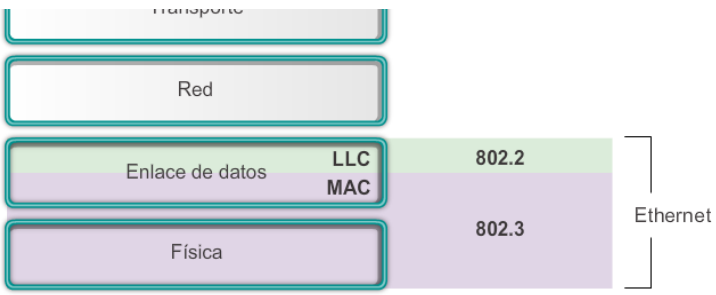
2.1. Subniveles

La norma **IEEE 802 divide el Nivel de Enlace de datos en dos subniveles** denominados **MAC** (Control de Acceso al Medio) y **LLC** (Control de Enlace Lógico)



El **Subnivel MAC** es el más cercano al Nivel Físico, su misión es la de independizar a los niveles superiores del medio de transmisión utilizado (norma IEEEE 802.3).

El **Subnivel LLC** se relaciona con el nivel supeior, es decir, proporciona servicios al Nivel de Red. Está implementado en software, en lo que se conoce como driver o controlador de la tarjeta de red (norma IEEEE 802.2).



2.2. Funciones

El Subnivel MAC tiene como funciones:

- **Empaquetar Tramas:**
  La información recibida del nivel superior (LLC) se empaqueta en tramas, junto con otra información de direccionamiento y el código para detectar errores.
- **Desempaquetar Tramas:**
  La información recibida del nivel inferior (Nivel Físico) se desempaqueta, reconociendo la información de direccionamiento y el código para detectar errores.
- **Control de acceso al medio:**
  Se encarga de establecer los turnos de transmisión de los equipos de la red local cuando hay un medio compartido (redes de difusión).

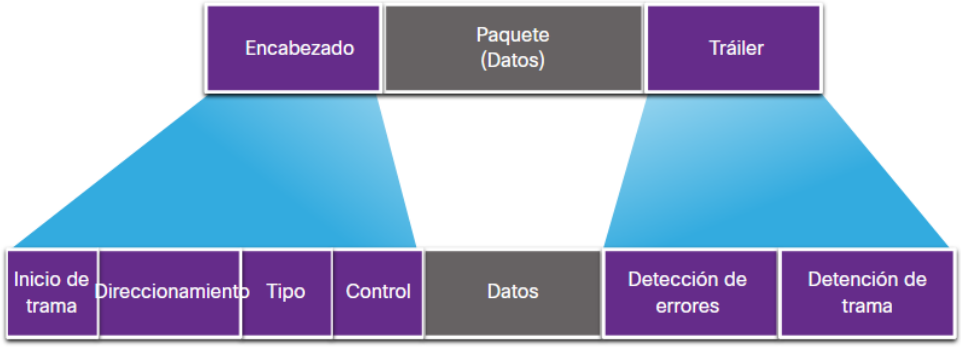
> Para que se entienda mejor, se podría comparar la red local con una habitación llena de personas que desean hablar. Cuando dos o más personas hablan a la vez se produce lo que llamamos *colisión*, es decir, no se entiende lo que dice ninguna de ellas. Por este motivo sería necesario distribuir el tiempo para que todos los que desean hablar puedan hacerlo y todo pueda entenderse con claridad. Pues de la misma manera hay que distribuir el medio de transmisión entre todas las estaciones de la red que desean transmitir.

El Subnivel LLC tiene como funciones:

- **Control de flujo:**
  Mecanismo por el que el receptor puede controlar la velocidad a la que el emisor le envía los datos. Sirve para que un emisor rápido no sature a un receptor lento.
- **Control de errores:**
  Realiza la corrección de los errores detectados en el subnivel MAC. Esta corrección se realiza solicitando al emisor que vuelva a transmitir las Tramas que no se han recibido correctamente.
- **Direccionamiento físico:**
  Son las direcciones MAC asociadas a las tarjetas de red. Permite la identificación de los equipos en una red de área local (LAN).

3. Empaquetar / Desempaquetar Tramas

Una trama en este nivel está formada por:



- **Inicio de trama:** Bits que se utilizan para identificar el inicio de una trama. También se le denomina preámbulo
- **Direccionamiento:** Indica la dirección física de origen y la dirección fisica de destino
- **Tipo:** Identifica el protocolo de la capa 3 (nivel de red) utilizado (Ipv4, Ipv6, ICMP, ARP,…)
- **Control:** Determina los servicios especiales de control de fluo que lleva esa trama, por ejemplo la calidad del servicio (QoS).
- **Datos:** Son los datos recibidos del nivel superior o del nivel inferior, dependiendo de si está actuando como emisor o receptor.
- **Detección de errores:** Son los bits que se utilizan para determinar el control de errores. Se denomina FCS (Frame Check Secuence)
- **Fin de trama:** Bits que se utilizan para identificar el fin de una trama

4. Control de acceso al medio

Los protocolos de la Capa 2 especifican el encapsulamiento de un paquete en una **trama** y **las técnicas para colocar y sacar el paquete encapsulado de cada medio**.

La técnica utilizada para colocar y sacar la trama de los medios se llama método de **control de acceso al medio**.

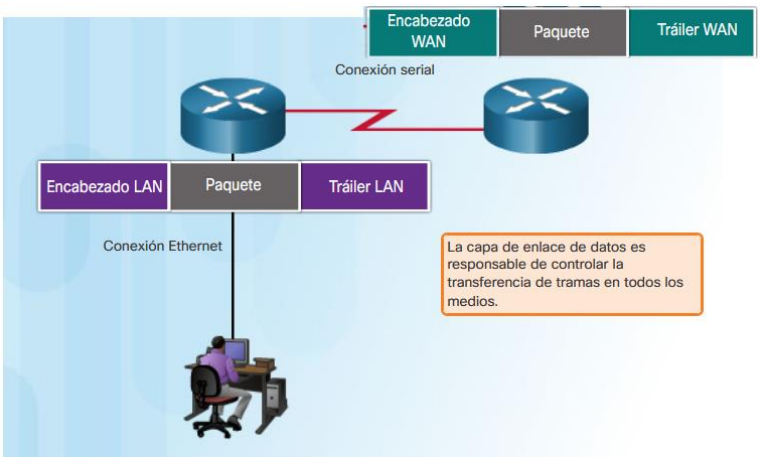
A medida que los paquetes se transfieren del host de origen al host de destino, generalmente deben atravesar diferentes redes físicas. Estas redes físicas pueden constar de **diferentes tipos de medios físicos**, como cables de cobre, fibra óptica y tecnología inalámbrica compuesta por señales electromagnéticas, frecuencias de radio y microondas, y enlaces satelitales.

En la figura, se proporciona un ejemplo de un PC en París que se conecta a un PC portátil en Japón. Si bien los dos hosts se comunican exclusivamente mediante el protocolo IP, se utilizan numerosos protocolos de capa de enlace de datos para transportar los paquetes IP a través de diferentes tipos de redes LAN y WAN. Cada transición a un router puede requerir un protocolo de capa de enlace de datos diferente para el transporte a un medio nuevo.

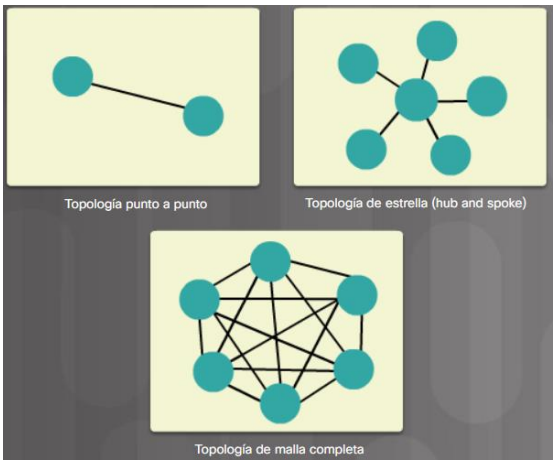
Sin la capa de enlace de datos, un protocolo de capa de red, tal como IP, tendría que tomar medidas para conectarse con todos los tipos de medios que pudieran existir a lo largo de la ruta de envío. Más aún, IP debería adaptarse cada vez que se desarrolle una nueva tecnología de red o medio. Este proceso dificultaría la innovación y desarrollo de protocolos y medios de red. Este es un motivo clave para usar un método en capas en interconexión de redes.

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

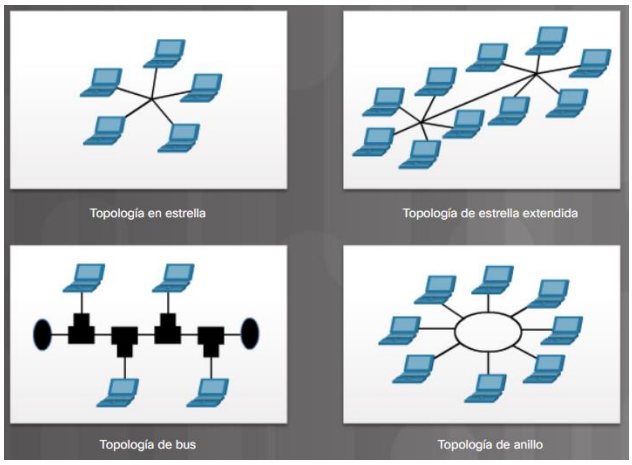
- Aceptan una trama proveniente de un medio.
- Desencapsulan la trama.
- Vuelven a encapsular el paquete en una trama nueva.
- Reenvían la nueva trama adecuada al medio de ese segmento de la red física.



Topologías físicas de WAN

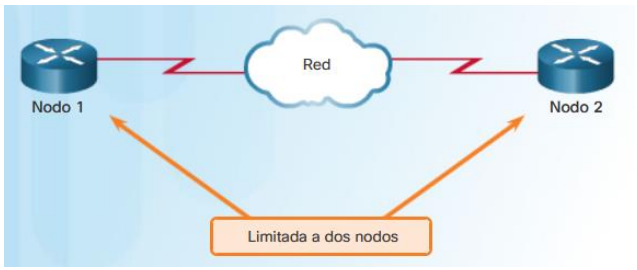


Topologías físicas de LAN



Topologías físicas de las WAN:

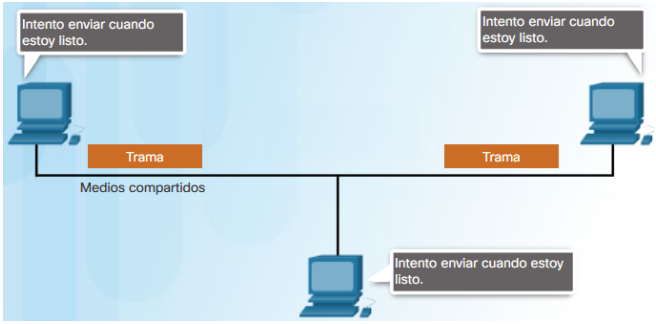
- **Punto a punto:** esta es la topología más simple, que consta de un enlace permanente entre dos terminales. Por este motivo, es una topología de WAN muy popular.



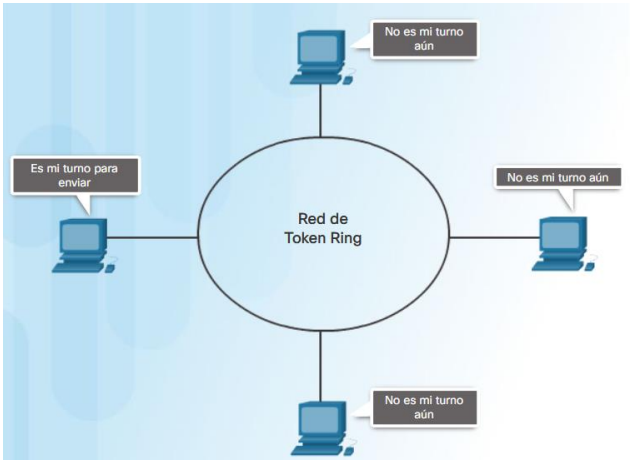
- **Hub-and-spoke:** es una versión WAN de la topología en estrella, en la que un sitio central interconecta sitios de sucursal mediante enlaces punto a punto.
- **Malla:** esta topología proporciona alta disponibilidad, pero requiere que cada sistema final esté interconectado con todos los demás sistemas. Por lo tanto, los costos administrativos y físicos pueden ser importantes. Básicamente, cada enlace es un enlace punto a punto al otro nodo.

Métodos de control de acceso al medio:

- **Acceso por contención:** Todos los nodos compiten por el uso del medio, pero solo un dispositivo puede enviar a la vez. **CSMA/CD** (acceso múltiple al medio con detección de portadora y detección de colisiones)



- **Acceso controlado:** Cada nodo tiene su propio tiempo para utilizar el medio. Estos tipos de redes no son eficientes porque un dispositivo debe aguardar su turno para acceder al medio. **CSMA/CA** (Acceso múltiple al medio con detección de portadora y prevención de colisiones)



5. Control de flujo

El control de flujo es el **procedimiento que le indica al emisor cuantos datos puede transmitir hasta recibir un reconocimiento del receptor**.

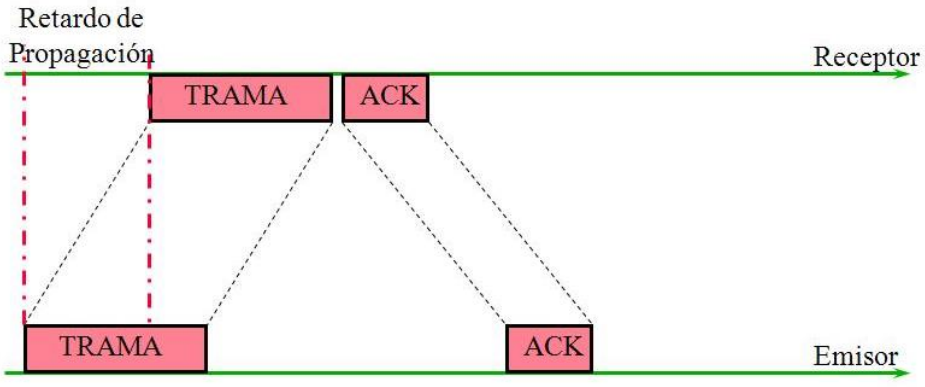
El receptor debe procesar los datos recibidos para detectar errores, por eso la recepción es un proceso más lento que la transmisión.

El dispositivo receptor contiene un bloque de memoria llamado **buffer**, para almacenar los datos recibidos hasta procesarlos.

Cuando el buffer se llena el emisor debe esperar para emitir hasta la confirmación del receptor.

Tipos de control de flujo:

- **Parada y espera:** el emisor espera un reconocimiento (ACK) después de cada trama que envía, y solamente envía si recibe el reconocimiento. Este proceso se repite hasta la trama EOT. El proceso es simple pero muy lento.



Retardo de Transmisión = Tamaño de la trama / Flujo de datos
Retardo de Propagación = Distancia / Velocidad de propagación

- **Ventana deslizante:** El emisor puede enviar varias tramas antes de necesitar un reconocimiento. Utiliza unas cajas imaginarias en el emisor y receptor, puede mantener tramas en cualquiera de los dos extremos emisor o receptor y determina el nº de tramas transmitidas sin ACK.

6. Control de errores

6.1. Concepto

La transmisión de datos a través de una red debe realizarse libre de errores, sin embargo, muchos factores pueden alterar o eliminar uno o más bits de cada unidad de datos enviada.

Tipos de errores:

- **Error de bit:** Significa que únicamente un bit de la secuencia de datos ha cambiado su valor. Por ejemplo, se envía la secuencia de datos 11001100 y se recibe 10001100. Se ha alterado el segundo bit.
- **Error de ráfaga:** Significa que varios bits, consecutivos o no, de la secuencia de datos ha cambiado su valor. Por ejemplo, se envía la secuencia de datos 11001100 y se recibe 10001110. Se han alterado el segundo y el séptimo bits.

Existen una serie de **métodos de detección y corrección de bits** que se detallan a continuación:

- Redundancia Vertical (VCR)
- Redundancia Longitudinal (LCR)
- Redundancia Cíclica (CRC)
- Código Hamming

Esta capa se encarga, entre otras cosas, de comprobar si se han producido errores en el mensaje recibido, pero ¿cómo se comunican el emisor y el receptor para indicar si se va recibiendo tramas correctas o erróneas?

Existen dos métodos principales.

- **Método de envío y espera:** Este método se basa en el envío una a una de las tramas. Cuando el receptor recibe una trama la valida, si resulta que no contiene errores le devuelve al emisor una trama de confirmación (**ACK** - Acknowledge); cuando se detectan errores le devuelve al emisor una trama de confirmación negativa (**NACK** – Negative Acknowledge)

  Mientras el emisor espera la recepción de las señales ACK o NACK mantiene el mensaje enviado en un buffer de memoria. Cuando recibe la señal NACK vuelve a enviar el contenido del buffer y si recibe la señal ACK copia en el buffer una nueva trama y la envía hacia el receptor.

  Se utilizan temporizadores tanto en el emisor como en el receptor.

- **Método de envío continuo:** En este método se envía la información de manera continua, sin esperar confirmación por parte del receptor. Cuando el canal queda libre el receptor informa el emisor de las tramas que han sido erróneas y el emisor las reenvía.

6.2. Comprobación de Redundancia Vertical (VCR)

También conocida como Comprobación de Paridad, es el mecanismo más simple para **detectar errores**.

Consiste en añadir un bit al final de cada bloque de datos, de modo que el **número total de unos sea par o impar**, según se indique.

Ejemplo: Supongamos que queremos transmitir el carácter “a” (código ASCII 97) con el método VCR con paridad par.

> El Dato a enviar es: 110 0001 (7 bits), pero en realidad enviamos el dato más un bit adicional que en este caso será 1 para conseguir que la suma de 1´s sea par, Luego el dato enviado será: 110 0001 **1** (8 bits)

Este método es **capaz de detectar Errores de bits** y también **Errores de ráfaga**, siempre y cuando el número cambiado de bits sea impar.

Este método **no es capaz de Corregir Errores**.

6.3. Comprobación de Redundancia Longitudinal (LCR)

Los bloques de bits se deben organizar en forma de **Tabla**.

Consiste en añadir un bit al final de cada columna, de modo que el número total de unos sea par o impar, según se indique.

Ejemplo: Supongamos que queremos transmitir el carácter “a” (código ASCII 97), “b” (código ASCII 98) y “c” (código ASCII 99) con el método LCR con paridad par.

El Dato a enviar en forma de tabla es:

110 0001		110 0001
110 0010	Pero se envía:	110 0010
110 0011		110 0011
		110 0000 (Se genera esta nueva fila)

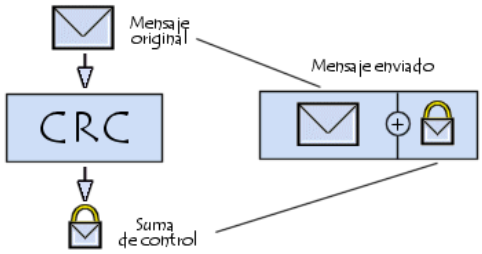
Este método es **capaz de detectar Errores de bits** y también **Errores de ráfaga**, siempre y cuando el número cambiado de bits sea impar.

Este método **es capaz de Corregir Errores**, aunque puede fallar.

6.4. Comprobación de Redundancia Cíclica (CRC)

Es un sistema muy potente de **detección y corrección de errores**.

Se basa en la división binaria y consiste en añadir a la Trama que se envía un código denominado de control (FCS). El receptor utiliza la misma clave que el emisor. Es una clave conocida.



Ejemplo: Supongamos que queremos enviar el número 17 (mensaje), lo que hacemos es dividir ese número por la clave, en este caso 7, obteniendo como cociente 2 y como resto 3.

El Dato a enviar es: 173, es decir, Mensaje + Resto.

El receptor separará el Mensaje (17) del Resto (3) y realizará la división con la clave conocida (7). Como le dará el mismo resto, el mensaje ha llegado correcto.

Si el receptor recibiera 193, separaría el Mensaje (19) del Resto (3) y realizará la división con la clave conocida (7). Como le dará distinto resto (5), el mensaje ha llegado incorrecto.

Este método se basa en las **propiedades matemáticas de los polinomios**, donde la clave es un polinomio generador.

Su fiabilidad es del 99% ya que existe un único tipo de error que no puede ser detectado y se produce cuando la diferencia entre lo enviado y lo recibido es múltiplo de la clave.

Ejemplo: Si enviamos el número 173 (Mensaje + Resto) y recibimos 383, no se podría detectar el error ya que la diferencia entre 38 y 17 es 21, que es múltiplo de 7 (clave).

6.5. Código Hamming

Es un sistema muy potente de **detección y corrección de errores**.

Está formado por los **bits de información más los bits de control**, con la particularidad de que estos bits nos informan, en caso de producirse un error, de cuál es el bit o el conjunto de bits erróneos.

Los códigos Hamming están diseñados para detectar y corregir un número predeterminado de bits erróneos, así se diseñan para 1 bit erróneo, 2 bits erróneos,…

La estructura de una palabra Hamming para la detección y corrección de 1 bit erróneo es:

1	2	3	4	5	6	7	8	9	10	11	12
C1	C2	D1	C3	D2	D3	D4	C4	D5	D6	D7	D8

Donde tenemos:

- 8 bits de datos (2^3). D1…..D8
- 4 bits de control. C1…C3
- C1, C2, C3 y C4 corresponden con las posiciones 1, 2, 4 y 8, es decir, de las potencias de 2 (2^0, 2^1, 2^2 y 2^3)
- D1, D2, D3,…. D8 corresponden con las otras posiciones, 3, 5, 6, 7,…. y 12

Cada uno de los bits de control se emplea para controlar la paridad par de un grupo determinado de bits de datos.

La siguiente tabla muestra la información de los bits de control y los bits de datos a los que afecta:

1	2	3	4	5	6	7	8	9	10	11	12
C1	C2	D1	C3	D2	D3	D4	C4	D5	D6	D7	D8
?		X		X		X		X		X	
	?	X			X	X			X	X	
			?	X	X	X					X
							?	X	X	X	X

Cuando se envían los datos, se debe calcular previamente el valor de los bits de control (C1, C2, C3 y C4), con el método de paridad par del conjunto de bits de datos a los que afecta.

Cuando el receptor reciba los datos realizará los mismos cálculos y si los resultados son iguales, la transmisión será correcta.

Ejemplo: Si queremos enviar la trama 11110100, deberíamos escribirla en la tabla Hamming y calcular después el valor de los bits de control, con los datos (D1, D2, D3, D4, D5, D6, D7 y D8) en sus posiciones, quedaría:

1	2	3	4	5	6	7	8	9	10	11	12
C1	C2	D1	C3	D2	D3	D4	C4	D5	D6	D7	D8
?	?	1	?	1	1	1	?	0	1	0	0

Y después de calcular los bits de control (C1, C2, C3 y C4), la tabla quedaría:

1	2	3	4	5	6	7	8	9	10	11	12
C1	C2	D1	C3	D2	D3	D4	C4	D5	D6	D7	D8
1	0	1	1	1	1	1	1	0	1	0	0

Luego deberíamos enviar la trama: 1011 1111 0100

El **problema del Código Hamming** es que se necesitan enviar muchos bits de control, con lo que la utilización efectiva del canal se ve reducida considerablemente, en el caso del ejemplo 4 bits de control por cada 8 bits de datos, luego un tercio del canal se desaprovecha.

7. Direccionamiento físico

Una dirección MAC (Media Access Control) **es un identificador único** que cada fabricante le asigna a la tarjeta de red de sus dispositivos, desde un ordenador o móvil hasta routers, impresoras u otros dispositivos como tu Chromecast.

Como hay dispositivos con diferentes tarjetas de red, como una para WiFi y otra para Ethernet, algunos pueden tener diferentes direcciones MAC dependiendo de por dónde se conecten.

Las direcciones MAC están formadas por 48 bits representados por dígitos hexadecimales. Como cada hexadecimal equivale a cuatro binarios (48 / 4 = 12), la dirección acaba siendo formada por 12 dígitos agrupados en seis parejas separadas generalmente por dos puntos, aunque también puede haber un guion. De esta manera, un ejemplo de dirección MAC podría ser 00:1e:c2:9e:28:6b.

La mitad de los bits de una dirección MAC, **identifican al fabricante**, y la otra mitad al **modelo**.

Por ejemplo, la MAC 00:1e:c2:9e:28:6b pertenecen al fabricante Apple Inc. Hay buscadores especializados para saber el fabricante de un dispositivo dependiendo de los primeros seis dígitos de su MAC.

Como son identificadores únicos, las MAC **pueden ser utilizadas por un administrador de red para permitir o denegar el acceso de determinados dispositivos a una red**. En teoría son fijas para cada dispositivo, aunque existen maneras de cambiarlas en el caso de que quieras hacerlas más reconocibles en tu red o evitar bloqueos.

Esta exclusividad de cada MAC hacia un único dispositivo también exige que tengas especial cuidado. Por ejemplo, cuando te conectas o intentas conectarte a un router, tu móvil u ordenador le enviará automáticamente su MAC. Es una de las razones por las que tienes que saber siempre dónde te conectas a Internet y a quién le pertenece esta red.

La capa de enlace de datos proporciona direccionamiento que es utilizado para transportar una trama a través de los medios locales compartidos.

Las direcciones de dispositivo en esta capa se llaman **direcciones físicas (MAC)**.

El direccionamiento de la capa de enlace de datos está contenido en el encabezado de la **trama** y especifica la **dirección del nodo de destino** y **la dirección del nodo origen**.

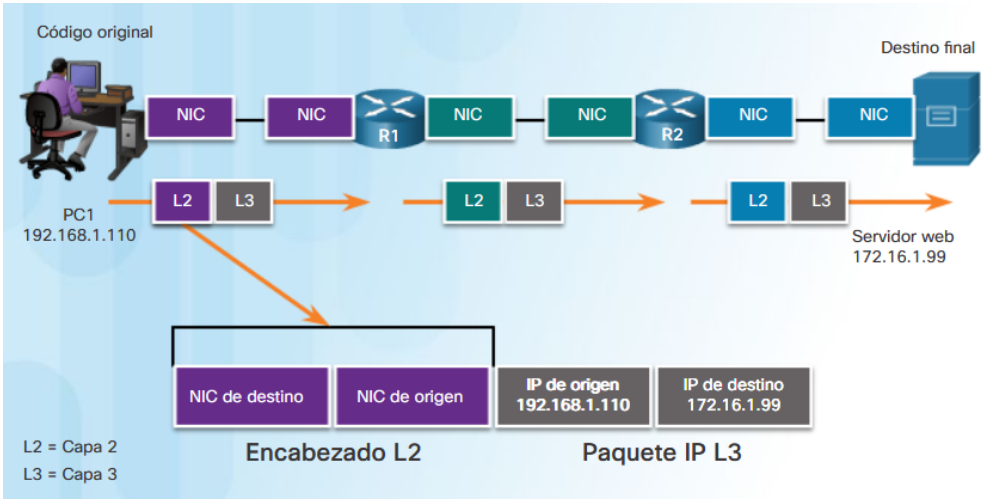
A diferencia de las **direcciones lógicas de la Capa 3, que son jerárquicas**, las direcciones físicas no indican en qué red está ubicado el dispositivo. En cambio, la dirección física es única para un dispositivo en particular. Si el dispositivo se traslada a otra red o subred, sigue funcionando con la misma dirección física de la Capa 2

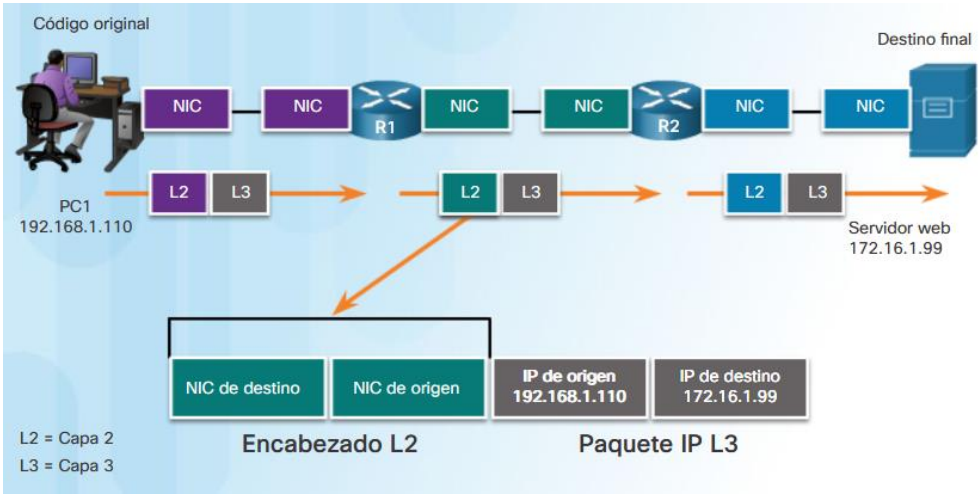
No se puede utilizar una dirección específica de un dispositivo y no jerárquica para localizar un dispositivo en grandes redes o Internet.

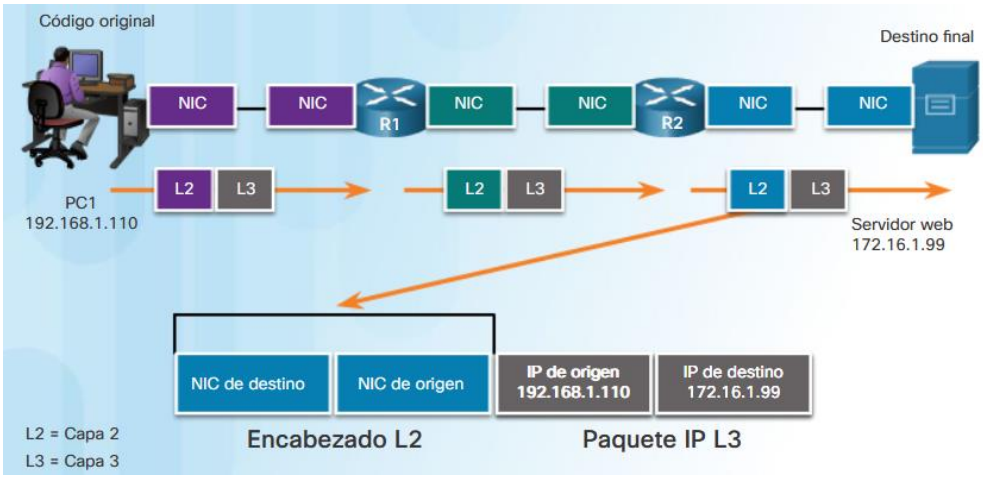
Eso sería como intentar localizar una casa específica en todo el mundo, sin más datos que el nombre de la calle y el número de la casa. Sin embargo, la dirección física se puede usar para localizar un dispositivo dentro de un área limitada.

Por este motivo, **la dirección de la capa de enlace de datos solo se utiliza para entregas locales**. Las direcciones en esta capa no tienen significado más allá de la red local.

Direcciones de la capa 2 y 3 a medida que un paquete IP se mueve del PC1 al Servidor WEB.







Tramas LAN y WAN

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.

En general, las redes LAN utilizan una tecnología de ancho de banda elevado que es capaz de admitir una gran cantidad de hosts. El área geográfica relativamente pequeña de una LANy 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 (802.3)
- Inalámbrico (802.11)
- Protocolo punto a punto (PPP)
- HDLC
- Frame Relay