UD4. Capa de enlace

Módulo: Planificación y administración de redes

Unión Europea
Fondo Social Europeo
El FSE invierte en tu futuro

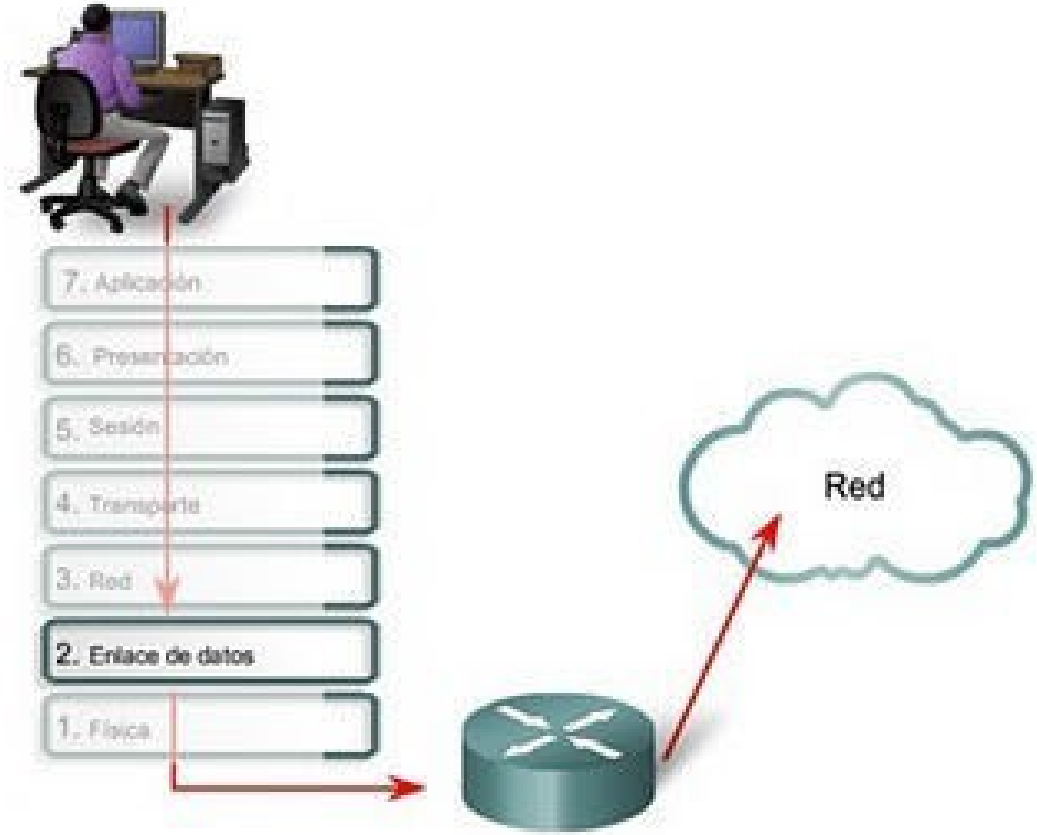
Germán Gascón Grau
g.gascongrau@edu.gva.es

Objetivos

- Comprender la función principal de la capa de enlace
- Conocer los conceptos de trama, enlace, nodo y dispositivos de acceso al medio.
- Identificar las funciones esenciales de la capa de enlace
- Entender las técnicas de delimitación de tramas
- Comprender el direccionamiento MAC
- Analizar los métodos de acceso al medio
- Entender el control de flujo y los métodos asociados
- Comprender el funcionamiento de switches
- Comprender el protocolo Ethernet y su formato de trama

Introducción

La capa de Enlace de datos es la segunda capa del modelo de referencia OSI.



La capa de enlace de datos prepara datos de red para la red física.

Elementos de la capa de enlace

Como en cada una de las capas OSI, existen términos específicos para esta capa

- **Trama**: El PDU de la capa de enlace de datos se llama trama. Aunque odos los protocolos de enlace de datos encapsulan la PDU de la capa 3 dentro del campo de datos de la trama, la estructura de esta y los campos contenidos en el encabezado y tráiler varían según el protocolo usado.

- **Dispositivos de red**: se agrupan en dos categorías:

  - **Nodos**: son dispositivos direccionables a nivel de la capa de red, es decir, que tienen asociada una dirección de red.

  - Dispositivos de acceso al medio: aquellos dispositivos que operan únicamente a nivel de las capas de enlace y/o física y cuya finalidad principal es ofrecer un punto de acceso a un medio de transmisión.

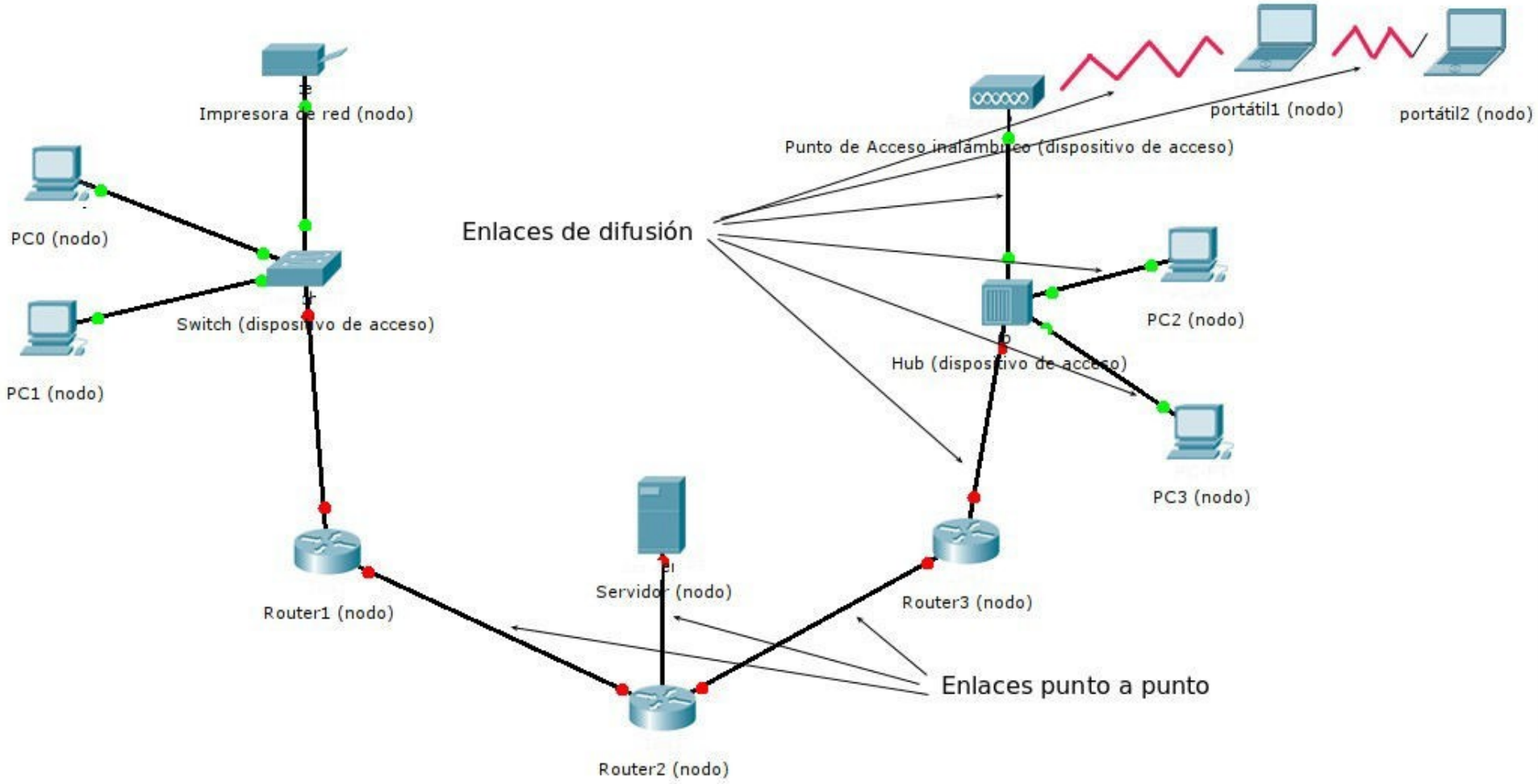
- **Enlace**: es el canal de transmisión que une varios dispositivos de red adyacentes entre sí. Un enlace puede contener, además del propio medio de transmisión, los dispositivos de acceso al medio. Se distinguen dos tipos:

  - Enlaces **punto a punto**: aquellos en los que el canal es exclusivo para dos únicos nodos.

  - **Enlaces de difusión**: aquellos en los que el canal es o puede ser compartido por más de dos nodos, como en las redes inalámbricas.

- **Red** (física): dos o más nodos conectados a un medio común.

Enlaces de punto a punto VS Enlaces de difusión



Objetivo de la capa de enlace

Asegurar una línea de comunicación libre de errores entre dos ordenadores conectados al mismo enlace local. Es decir, debe solventar las deficiencias de la capa física para proporcionar a la capa de red un mensaje continuo y sin errores.

Para ello debe **preparar** los paquetes de la capa de red para ser transmitidos por el nivel físico adecuado y **controlar** el acceso a los medios físicos específicos en caso de ser necesario (en enlaces de difusión).

Objetivo de la capa de enlace

Capa de enlace de datos

Los protocolos de la capa de enlace de datos regulan cómo se da formato a una trama para utilizarla en diferentes medios.

Es posible que distintos protocolos se encuentren en uso para diferentes medios.

En cada salto a lo largo de la ruta, un dispositivo intermediario acepta tramas de un medio, la desencapsula y luego envía los paquetes en una nueva trama. Los encabezados de cada trama se formatean para el medio específico que cruzará.

Funciones / Servicios de la capa de enlace

- Entramado o framing
- Métodos de acceso al medio
- Sincronismo
- Direccionamiento físico
- Control de flujo
- Detección y correción de errores
- Multiplexación de protocolos a través del enlace

Entramado o framing

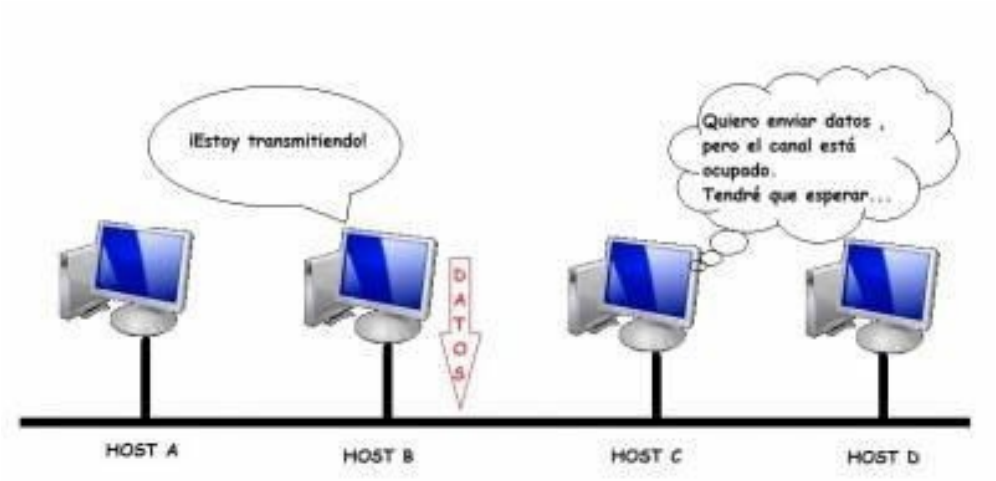
Como el nivel físico sólo transmite bits sin detenerse en su significado, es el nivel de enlace el que debe marcar (encapsular) el principio y final de un bloque de datos (formando tramas) para que el receptor pueda tratarlos.

La trama consta de una cabecera de los datos encapsulados y, en algunos protocolos de una cola o trailer que contiene información de control agregada al final del PDU. La cabecera y la cola contienen una serie de campos que permiten regular los distintos servicios de la capa de enlace.

Entramado o framing

Métodos de acceso al medio

En las redes de área local se necesita algún método que **controle** y **regule** todos los aspectos relacionados con el acceso al enlace. Este servicio puede ser relativamente simple para los enlaces **punto a punto** o relativamente complejo, en el caso de los **enlaces de difusión**.



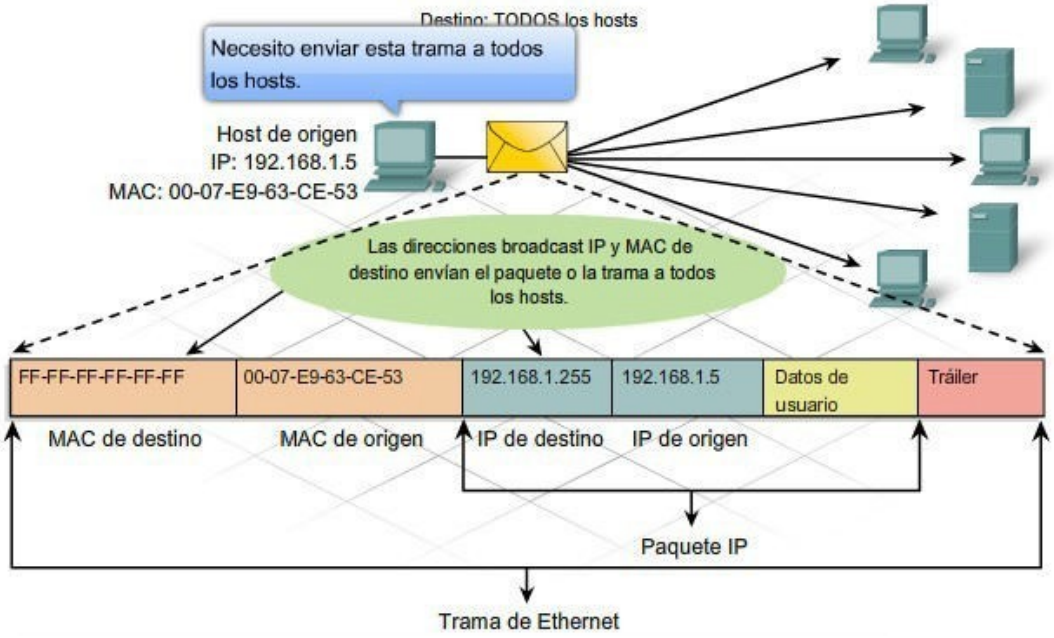
Sincronismo

Se trata de un procedimiento que permite **sincronizar el reloj** del **receptor** con el del **emisor** para poder reconocer los bits transmitidos.

A veces la sincronización es tan sencilla como enviar una cadena preestablecida de bits al inicio de cada trama.

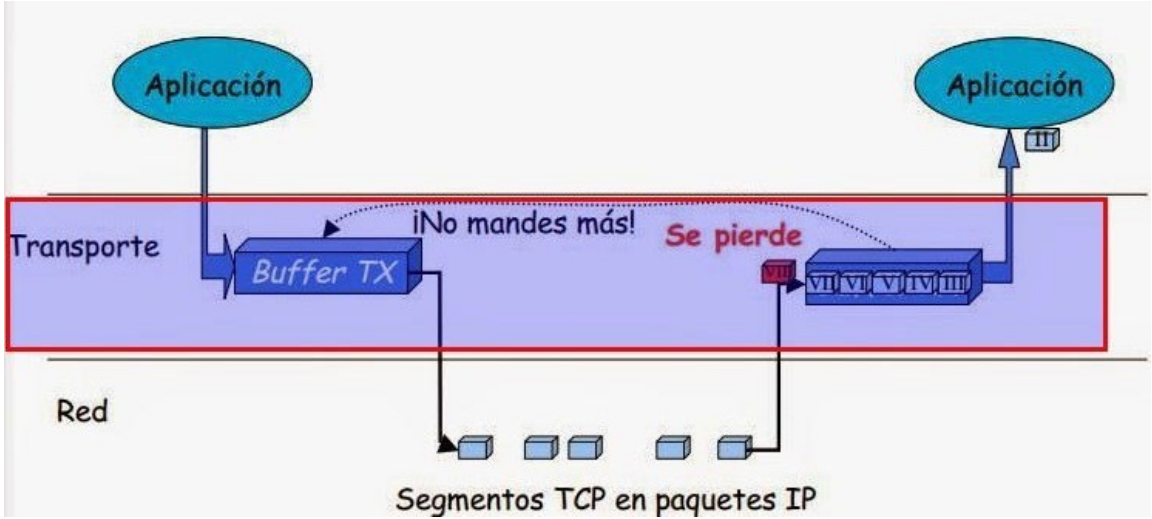
Direccionamiento físico

En el caso de los medios compartidos será muy importante **identificar** de forma unívoca cada uno de los **nodos** presentes. Ello se consigue mediante un identificador, la dirección física, conocida como **dirección MAC**.



Control de flujo

Algunos protocolos del nivel de enlace llevan a cabo un **control de flujo**, que se encarga de **ajustar la velocidad de envío** de las tramas **a la velocidad de procesamiento** del nodo **receptor**, de tal forma que no se pierdan tramas por **desbordamiento** de su memoria intermedia (buffer).



Detección y corrección de errores

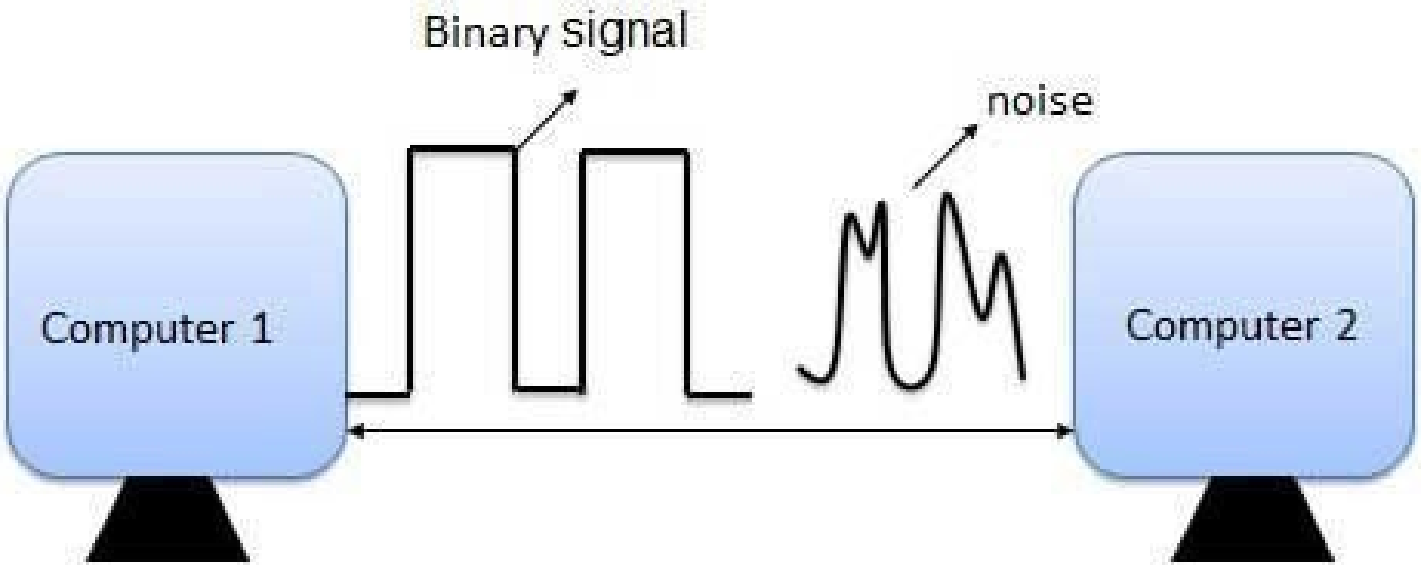
Los protocolos del nivel de enlace suelen ofrecer algún mecanismo para la **detección** de los errores que puedan producirse durante el transporte de la trama a través del enlace.

En ese caso el receptor puede detectar que una trama contiene errores y puede, dependiendo de las características del protocolo, realizar dos acciones:

- Descartar la trama.
- Solicitar la retransmisión de la trama.

Existen además, protocolos de la capa de enlace de datos que no sólo permiten **detectar** errores sino también **corregirlos**.

Detección y corrección de errores

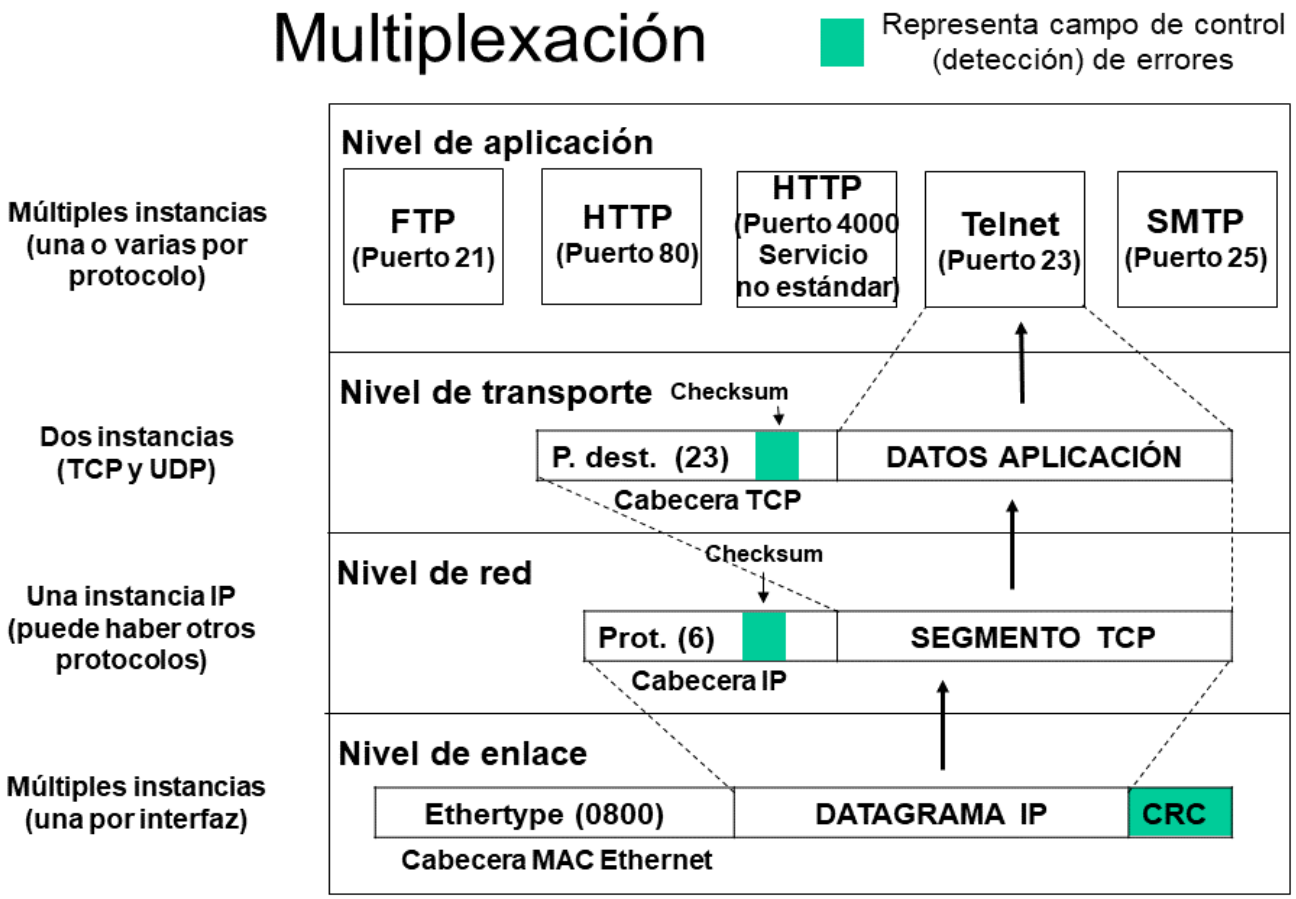


Multiplexación de protocolos

Consiste en la capacidad de enviar PDU de diferentes protocolos de la capa de red a través del mismo enlace. Para ello se **etiquetan** las trama de algún modo **indicando el protocolo** que se está encapsulando.

De esta forma el receptor puede reconocer qué transporta esa trama sin necesidad de analizar los datos encapsulados. Esto le puede permitir dar un trato distinto a cada trama en función del protocolo que transporta.

Multiplexación de protocolos



Uso de funciones / servicios

No todos los **protocolos** implementan todos los servicios descritos, sino que cada protocolo utiliza aquellos que le son más **convenientes**.

Existen protocolos **simples** y **rápidos**, pero poco fiables, que son eficientes en **medios** de transmisión **muy fiables** como la fibra óptica o los pares trenzados de cobre.

También hay protocolos **complejos y lentos**, pero muy fiables, que son útiles en **medios poco fiables** como los inalámbricos.

Implementación las funciones / servicios

La capa de enlace es la primera en la que el hardware se encuentra con el software y se implementa principalmente en la tarjeta de interfaz de red (NIC), su firmware interno y el driver que comunica dicha tarjeta con el sistema operativo.

Desde un punto de vista estructural Donde se implementan las funciones de la capa de enlace

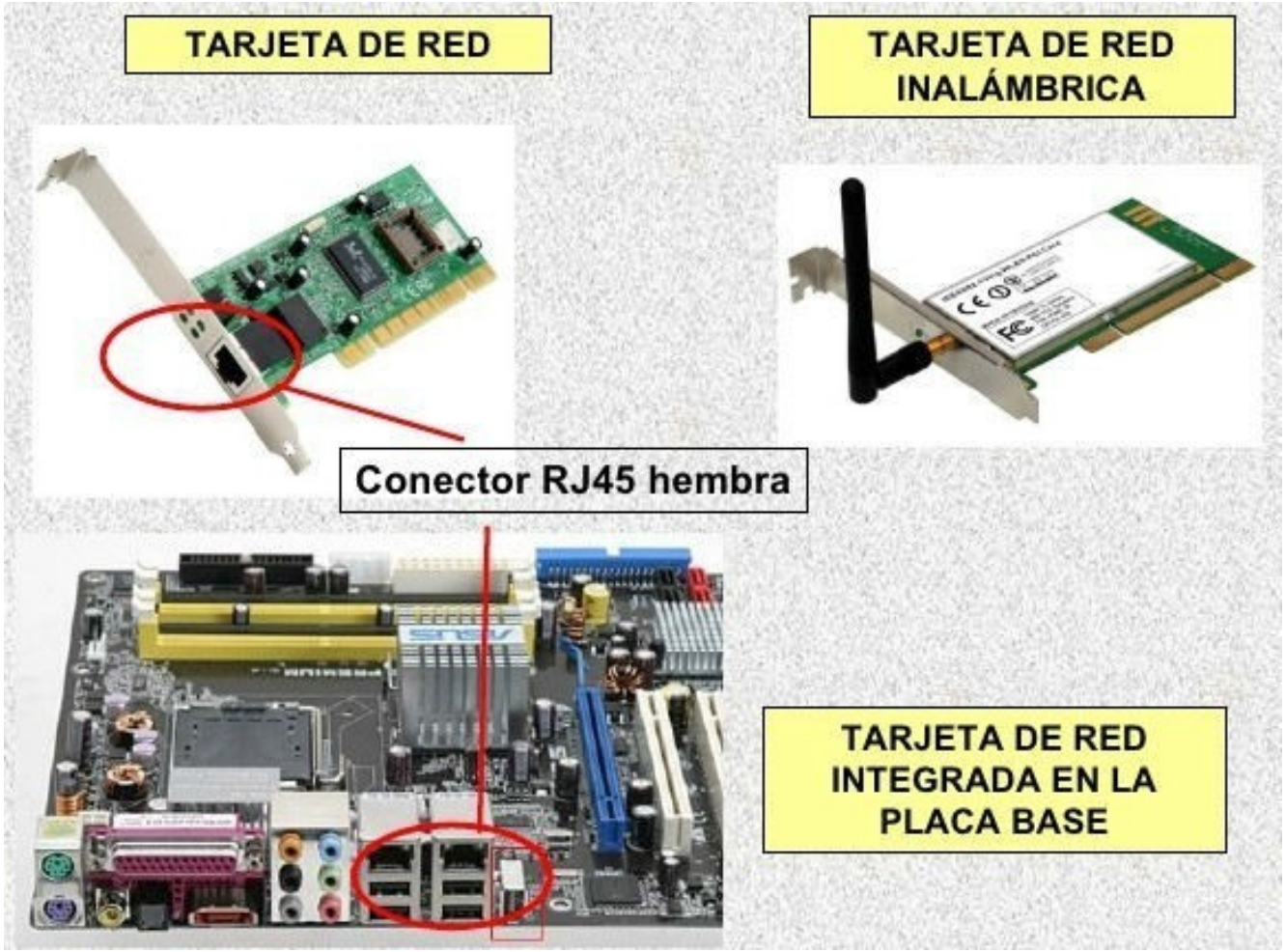
- **Hardware** – Adaptador de red o NIC (Network Interface Card)
  - Gestión de direcciones MAC
  - Reensamblado y envío de tramas
  - Codificación física en el medio (enlace con capa física)Control de acceso al medio (CSMA/CD, CSMA/CA, etc.)
  - Cálculo y verificación de CRC/FCS.
- **Firmware** interno de la NIC
  - Buffering de tramas
  - Gestión de colas de envío y recepción
  - Optimización de tráfico (interrupt moderation, offloading)
- **Driver** de dispositivo en el sistema operativo
  - Interfaz entre el kernel y el hardware
  - Exposición de la interfaz de red al sistema (ej. eth0, wlan0)
  - Gestión de interrupciones de llegada de trama
  - Configuración de parámetros (MTU, promiscuous mode, VLAN tagging)
- **Kernel** del sistema operativo
  - Interacción con otras capas del modelo
  - Conexión entre interfaz de enlace y capa de red (IP)
  - Funciones de filtrado (bridges, bonding, VLANs)
  - En Linux por ejemplo, se apoya en estructuras como net_device y subsistema de red del kernel.

Adaptador de red - NIC

La estructura interna de un adaptador de red suele constar de los siguientes elementos funcionales:

- **Conector de red**: a través de él, el adaptador se conecta al medio físico de transmisión y envía o recibe sus señales.
- **Transceptor**: es el elemento encargado de convertir las señales en bits y los bits en señales.
- **Chip controlador**: es un chip de propósito específico que se encarga de implementar la mayor parte de los servicios de la capa de enlace (entramado, acceso al medio. sincronización, control de flujo, detección de errores...). También se le llama controlador de la capa de enlace. En la integradas estas funciones las suele realizar el Chipset de la placa base.
- **Memoria intermedia o buffer**: pequeña memoria que almacena temporalmente las transmisiones entrantes pendientes de ser tratadas por el chip controlador.
- **Memoria ROM/Flash BIOS** o análoga: almacena la configuración por defecto y la dirección MAC de fábrica del adaptador.
- **Conexión con el bus** de la computadora o dispositivo que alberga el adaptador: a este mismo bus se encuentran conectadas directa o indirectamente la CPU y la memoria principal. Puede tratarse de un conector integrado en la placa base, una conexión PCI, PCIe, PCMCIA, USB, etc.

Adaptador de red - NIC



Tarea

Realizar el boletín 1 de ejercicios del tema 4.

Entramado y sincronismo

La transmisión de datos no se realiza en una única ráfaga, sino en bloques llamados Marcos o Tramas.

Fraccionar un fichero en tramas de un tamaño moderado tiene una gran ventaja. Si el fichero se transmite como un único bloque, la probabilidad de verse afectado algún bit por un error de transmisión es muy alta y una vez producido el error tendríamos que retransmitirlo entero. Si se transmite en tramas, un error sólo afecta a esa trama.

Entramado y sincronismo

Por tanto se hace necesario un mecanismo para **delimitar** claramente **el principio y el fin** de trama.

El receptor recibe un fluir constante de bits y es obvio que necesita saber cual de ellos es el primero y el último de una trama.

Estos mecanismos de delimitación sirven también para realizar el sincronismo del emisor y receptor.

Entramado y sincronismo

Protocolos orientados al bloque. Conteo de caracteres

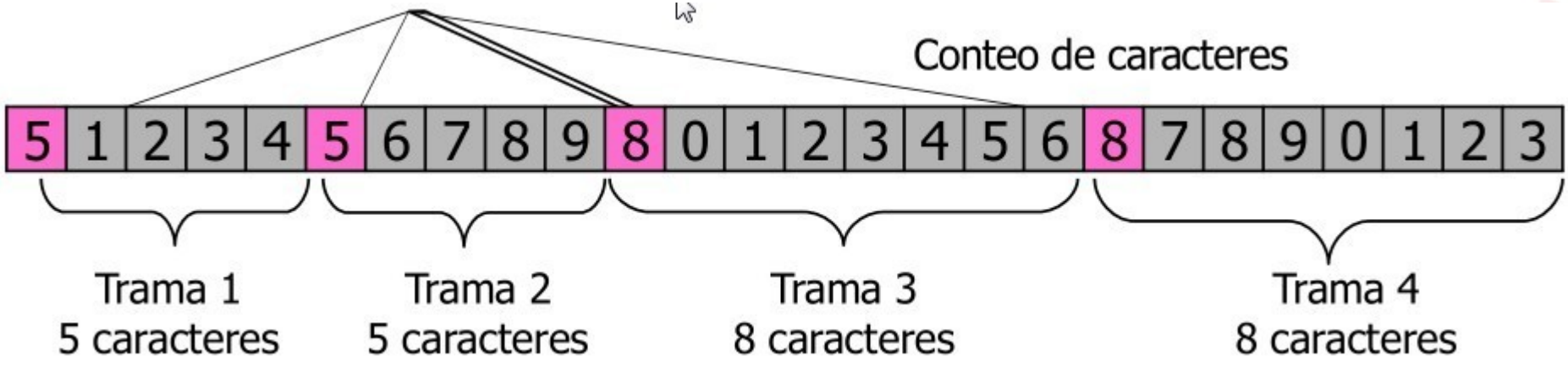
Se pone un campo en el **encabezado** (antes de los datos) indicando **cuantos caracteres ocupa la trama**. Para saber donde termina, contamos los bytes hasta el número indicado en la cabecera.

Es una técnica **débil**, porque si un ruido en la línea modifica justo el carácter contador, fastidiaría todas las tramas que vienen a continuación.

Es una técnica empleada en combinación con otras.

Entramado y sincronismo

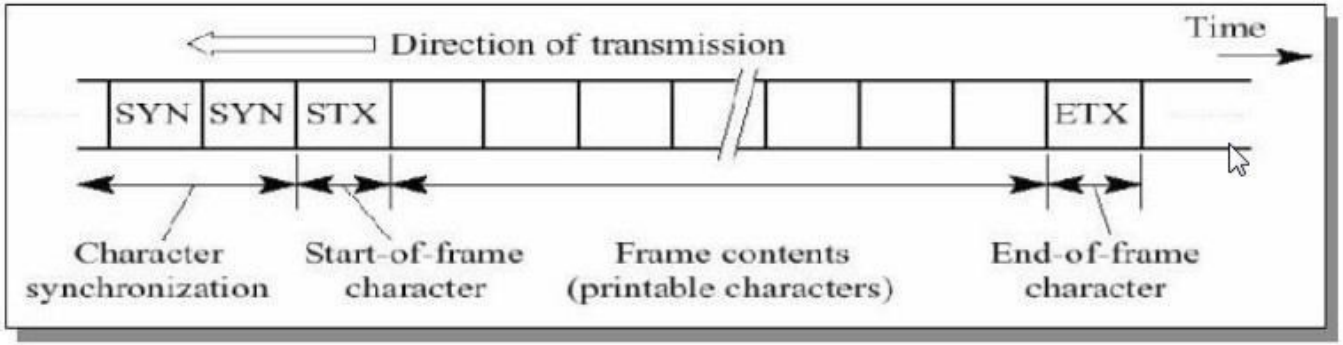
Protocolos orientados al bloque. Conteo de caracteres



Entramado y sincronismo

Protocolos orientados al carácter. Carácter stuffing

Otra opción es **insertar al principio y al final un carácter** o combinación de caracteres bandera reservados como delimitadores.



$STX=00000010_2 \text{--->} 2_{10}$

$ETX=00000011_2 \text{--->} 3_{10}$

Entramado y sincronismo

Protocolos orientados al carácter. Carácter stuffing

En teoría **STX** y **ETX**, son caracteres ASCII reservados y sólo se usarán para delimitar tramas de datos, pero en la práctica:

- No sólo se trasmite texto, la trama de datos podría contener una matriz de números binarios, entre ellos el 2 y 3 que coinciden con los ETX y STX.
- Aunque transmita texto ASCII, NO puedo hacer suposiciones sobre lo que las aplicaciones meten en las tramas que transmito. Puede que alguna utilice los caracteres ETX y STX.

Entramado y sincronismo

Protocolos orientados al carácter. Carácter stuffing

En cualquiera de los dos casos se interpretará prematuramente el final o inicio.

Una solución es la técnica de la inserción de caracteres de relleno (carácter stuffing). Consiste en señalizar con un carácter especial DLE los caracteres de inicio y fin de trama. Así:

- **DLE-STX**: Significa inicio de trama.
- **DLE-ETX**: Significa fin de trama.
- Si **en mitad** de la trama de datos nos encontramos con un STX o ETX "accidental" **se interpreta como un dato**.
- Si en los datos nos encontramos con un DLE accidental, lo señalizamos con otro DLE. Es decir, los DLE accidentales siempre se doblan.

Entramado y sincronismo

Ejemplo Carácter stuffing

Quiero emitir estos datos que me pasa el nivel de red:

A B C 9 X **DLE** T I H **STX** L **ETX** W 7

El nivel de enlace los transforma en:

DLE-STX A B C 9 X **DLE-DLE** T I H **STX** L **ETX** W 7 **DLE-ETX**

Entramado y sincronismo

Protocolos orientados a bit. Bit stuffing

Los protocolos orientados a carácter tienen como desventaja que necesitamos un carácter redundante por cada carácter DLE accidental.

En los orientados a bit, cada trama empieza y termina con la secuencia de bits **01111110**, llamada **bandera de bits**.

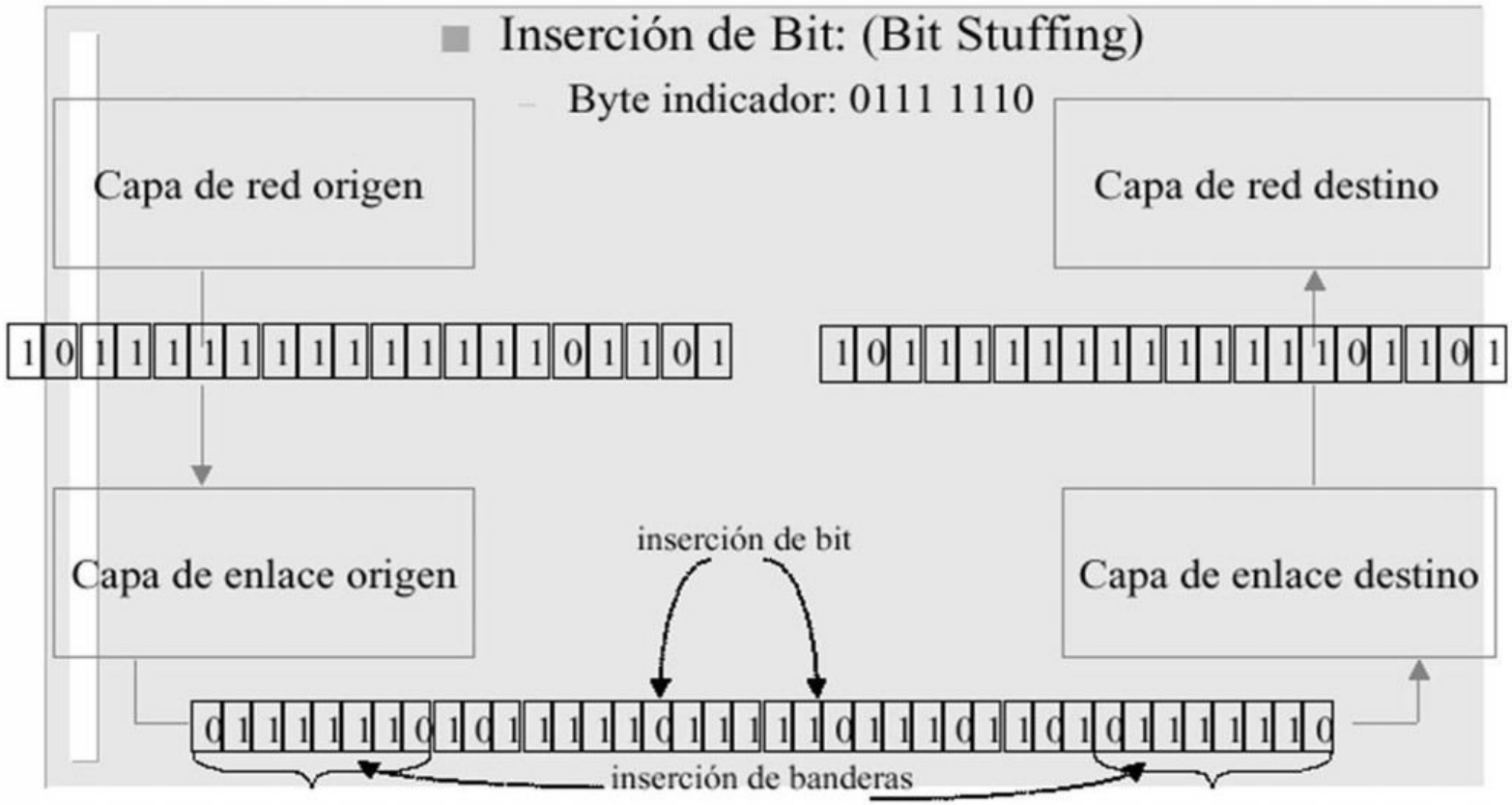
Tendremos el mismo problema de antes. ¿Qué pasa cuando en los datos aparecen 6 unos consecutivos? Tendremos un falso principio o fin de trama. Para evitarlo **introducimos un bit 0 de relleno (bit stuffing)** cada vez que se encuentren **5 unos consecutivos**, y no sea el final de la trama.

El receptor cada vez que encuentra 5 unos seguidos,mira el sexto bit,si es un 1, tenemos un fin de trama, si es un 0 lo descarta porque sólo puede ser un bit de relleno.

Ventaja: Insertamos un bit de relleno cuando antes insertaba un byte

Entramado y sincronismo

Protocolos orientados a bit. Bit stuffing



Direccionamiento físico

Toda comunicación requiere una manera de identificar el **origen** y el **destino**. En el caso de las comunicaciones humanas el origen y el destino se representan con nombres.

En las redes de datos, existe un método similar para identificar los hosts de origen y de destino. Cada host conectado a una red tiene una **dirección física** que sirve para identificar el host en la red.

Esta dirección se establece de fábrica, reside en la tarjeta de red y se conoce como dirección de Control de Acceso al Medio (**MAC**).

Direccionamiento físico

Cuando un host de una red se comunica:

- Envía **tramas** que contienen su propia dirección **MAC** como **origen** y la dirección **MAC** del **destino**.
- Todos los hosts que reciban la trama la decodifican y leerán la dirección MAC de destino.
  - Si la dirección MAC de destino **coincide** con la dirección configurada en la NIC, el host procesa el mensaje y lo almacena para que lo utilice la aplicación del host.
  - Si la dirección MAC de destino **no coincide** con la dirección MAC del host, la NIC simplemente **descarta** el mensaje.

Direccionamiento físico

Modo promiscuo

Cuando un adaptador de red se configura en modo promiscuo **acepta todas las tramas que recibe**, vayan o no destinadas a él.

Este modo de configuración es especialmente útil si queremos **analizar todo el tráfico** que pasa por un determinado punto de la red.

Direccionamiento físico

Ejemplo de comunicación

1. Un equipo de la red desea comunicarse con otro.

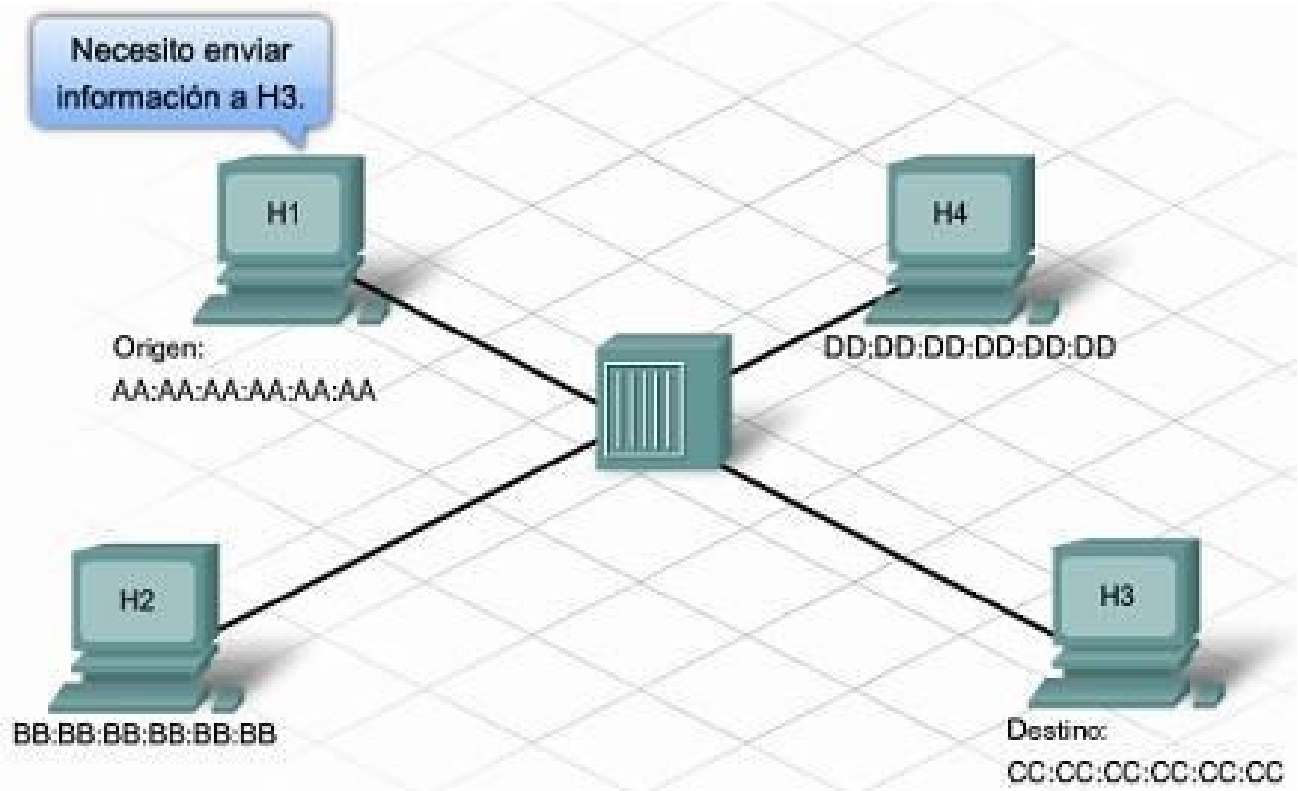
2. Prepara una trama con las direcciones físicas de origen y destino adecuadas.

3. El equipo remitente procesa la trama, el resto de equipos de la red a los que le llega la trama la desechan.

Direccionamiento físico

Ejemplo de comunicación

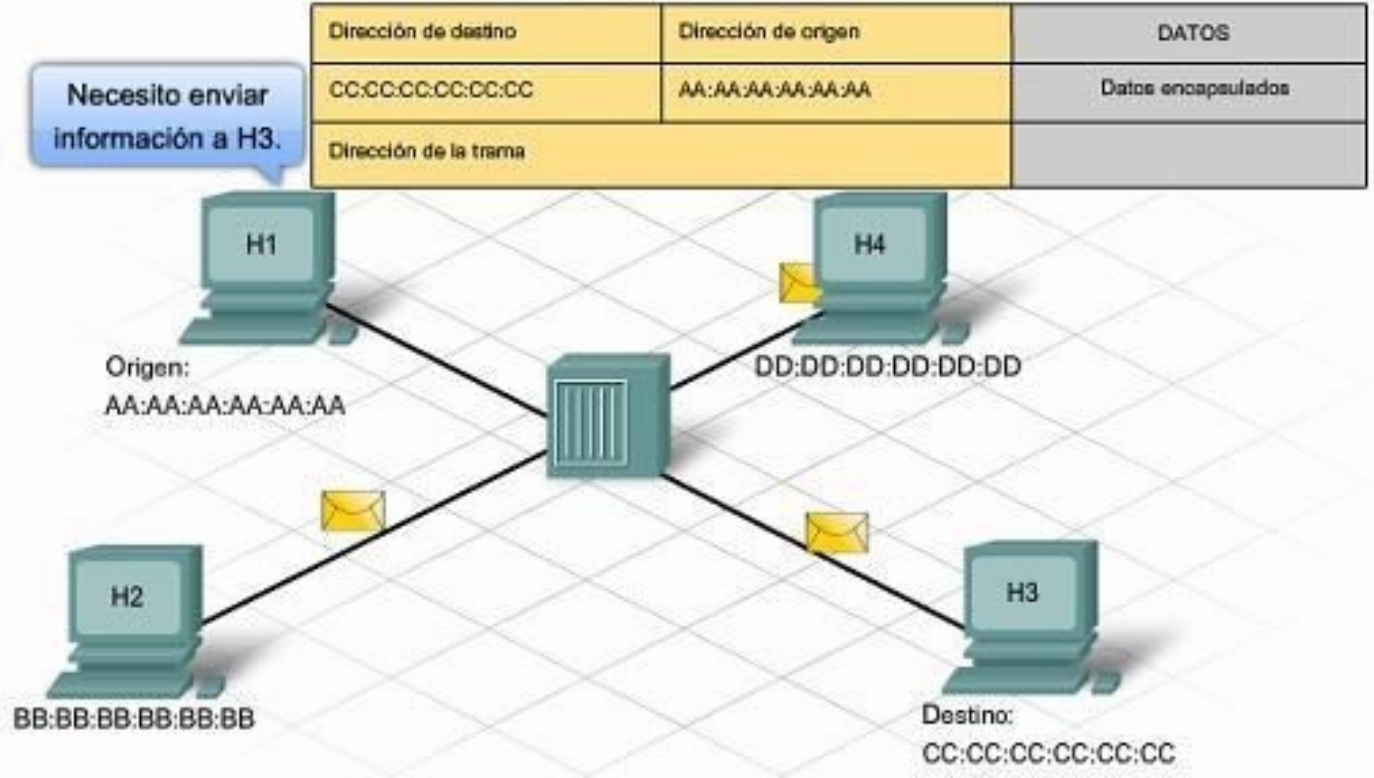
1. Un equipo de la red desea comunicarse con otro.



Direccionamiento físico

Ejemplo de comunicación

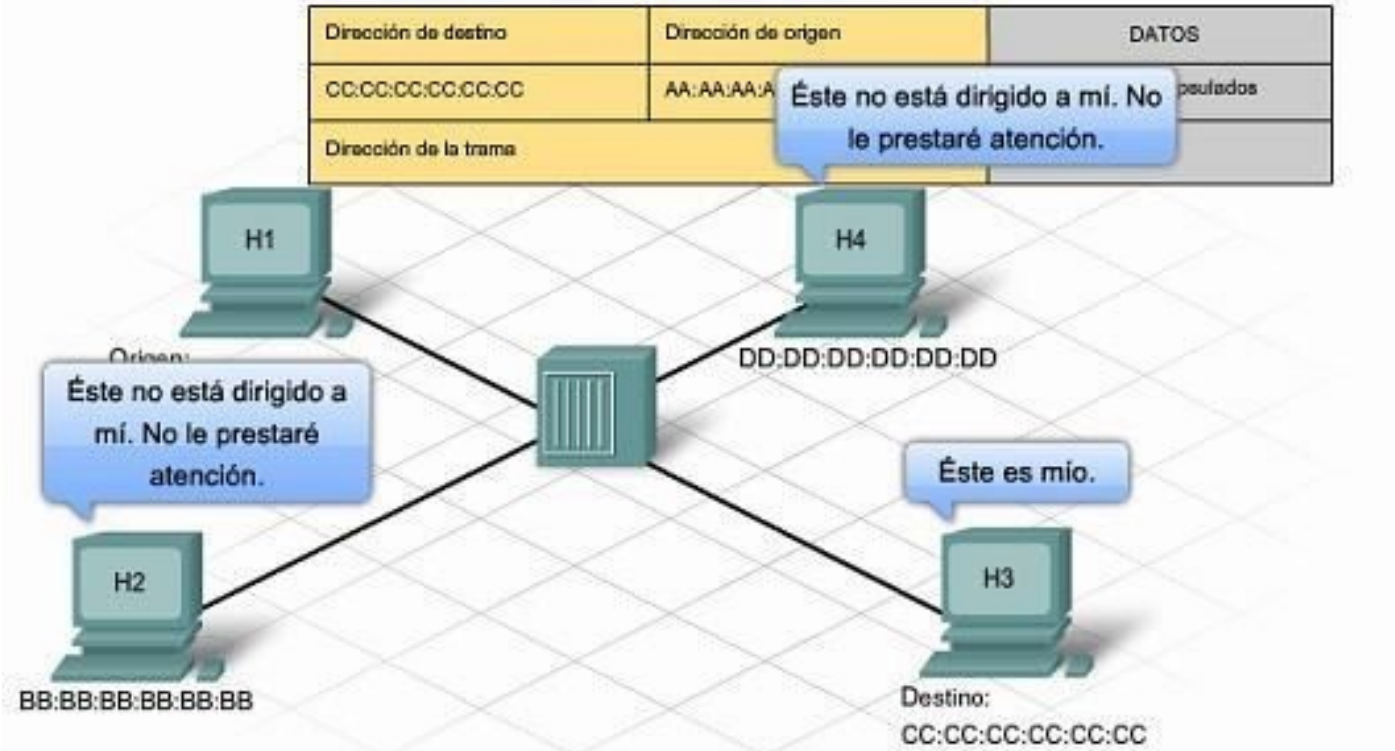
2. Prepara una trama con las direcciones físicas de origen y destino adecuadas



Direccionamiento físico

Ejemplo de comunicación

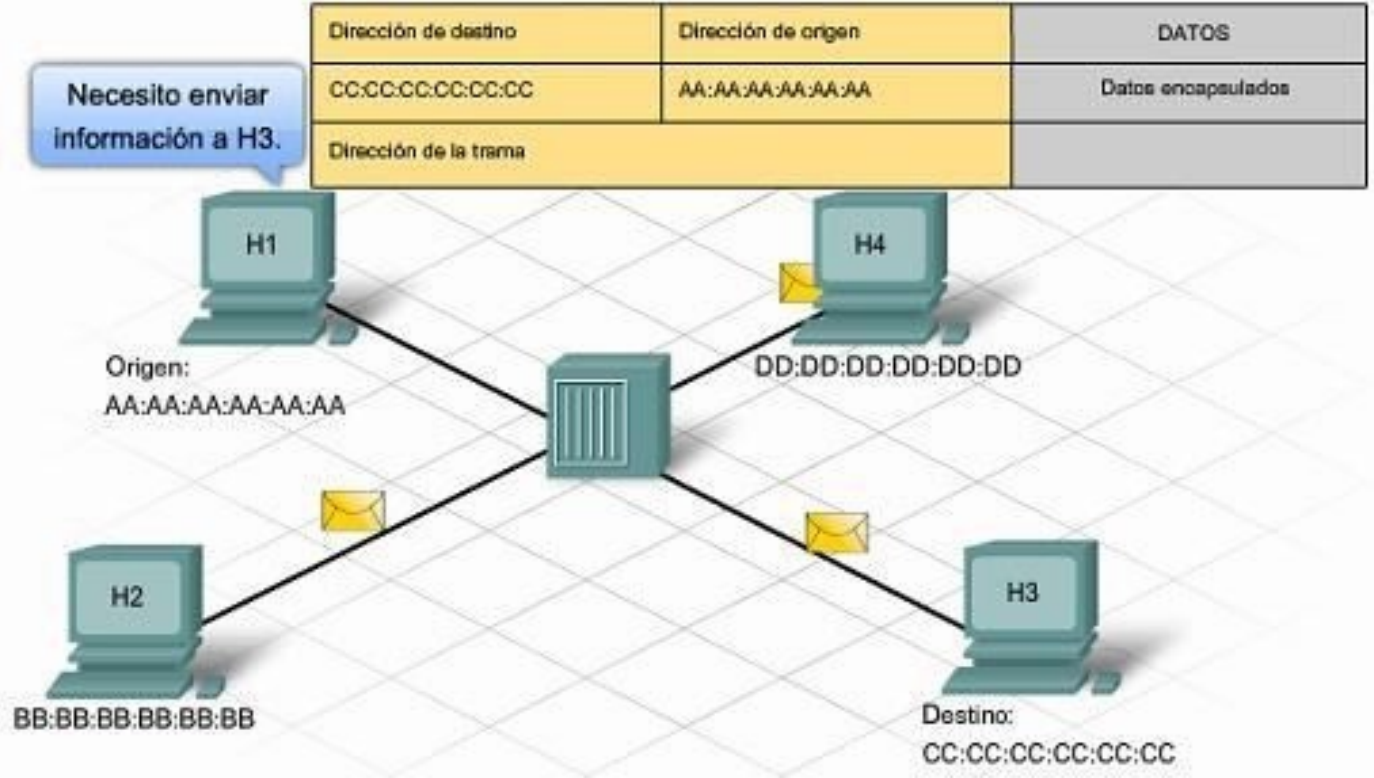
3. El equipo remitente procesa la trama, el resto de equipos de la red a los que le llega la trama la desechan.



Direccionamiento físico

Ejemplo de comunicación

3. El equipo remitente procesa la trama, el resto de equipos de la red a los que le llega la trama la desechan



Direccionamiento MAC de 48 bits

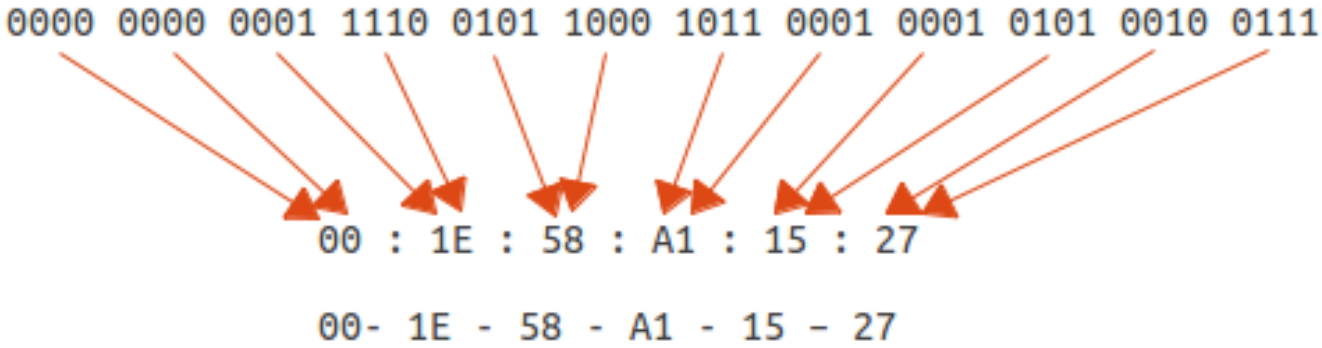
Debido a que la trama sólo se utiliza para transportar datos entre nodos a través del **enlace local**, la dirección de la capa de enlace sólo se utiliza para **entregas locales**. Las direcciones en esta capa no tienen significado más allá del enlace.

Los protocolos de enlace mayoritarios en las redes de área local son la familia de protocolos Ethernet (para las redes cableadas) y los protocolos IEEE 802.11 (para las redes inalámbricas). Todos estos protocolos utilizan un mismo tipo de direccionamiento físico: el direccionamiento MAC de 48 bits.

Dirección MAC unicast única global

Su principal uso es indicar en cada trama quiénes son su remitente y su destinatario de entre los diferentes dispositivos que comparten el medio.

Este tipo de dirección MAC consiste en un número binario de 48 bits que normalmente se representa de forma hexadecimal, agrupando los dígitos de dos en dos y separándolos mediante dos puntos (:) o un guión (-).



Dirección MAC unicast única global

Cada adaptador de red recibe una dirección MAC de fabrica que es **única** en el mundo. De esta forma se puede asegurar que, si no se modifican, nunca coincidirán dos dispositivos con una misma dirección MAC en una misma red.

La entidad encargada de controlar que las direcciones MAC de fabrica no se repitan es el IEEE. Para llevar a cabo esto, la dirección se divide en dos partes:

- Los **24 primeros bits** son el Identificador Único de la Organización (OUI, Organizationally Unique Identifier) > identifica al **fabricante** del NIC.
- Los **últimos 24 bits** los asigna el fabricante teniendo en cuenta la obligación de que sean distintos para cada **adaptador** NIC fabricado.

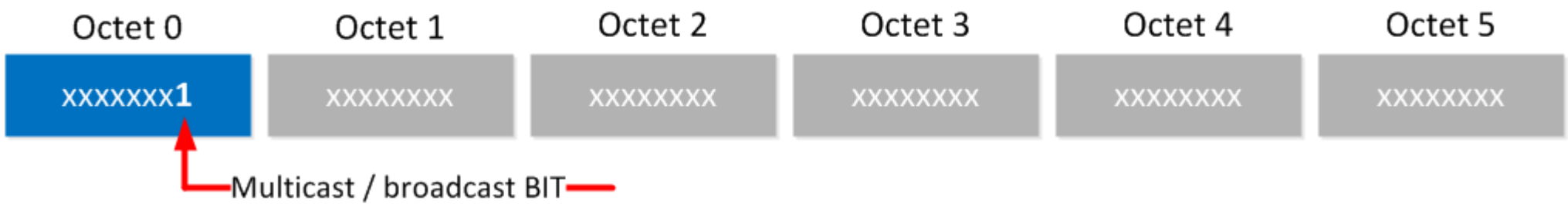
En https://standards-oui.ieee.org/oui/oui.txt podemos localizar el fabricante según los primeros 3 bytes de la MAC (en hexadecimal).

Direcciones MAC de multidifusión o de multicast

Su funcionamiento es similar al de la dirección MAC de difusión, ya que la **trama** puede ser **aceptada por varios dispositivos** a la vez.

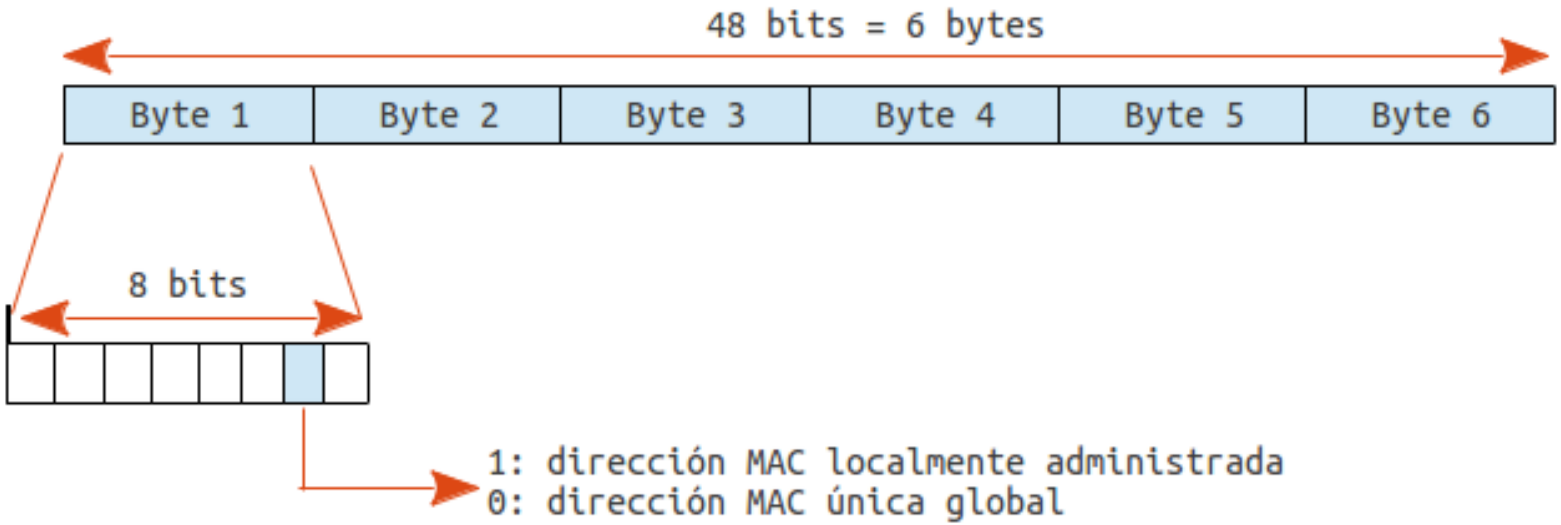
Este tipo de direccionamiento es útil cuando se quiere **difundir** datos **selectivamente** a algunos dispositivos de la red, por ejemplo cuando se quieren clonar algunas máquinas (pero no todas) a través de la red. O en aplicaciones de gestión de la red para informar a varios dispositivos a la vez de algún cambio.

Las MAC reservadas para este propósito son las que el **bit menos significativo del primer octeto está a 1**.



Direcciones MAC localmente administradas

Cuando queremos cambiar la dirección MAC de nuestro adaptador por otra arbitraria es importante que esta no coincida con la de ningún otro adaptador. Por ello se han reservado para **uso local** aquellas direcciones MAC que tienen el **segundo bit del primer byte a 1**.



Dirección MAC de broadcast o difusión

La dirección de difusión (broadcast) en Ethernet es una dirección MAC especial en la que todos los bits son 1:

FF:FF:FF:FF:FF:FF

Esto significa que cualquier trama enviada a esa dirección es **recibida por todas las NIC de la red**, independientemente de su MAC o de si están suscritas a algún grupo multicast.

Dirección MAC de broadcast o difusión

Características

- Es una dirección de grupo (bit I/G = 1).
- No se puede usar como identificador de host individual.
- No pertenece a ningún fabricante.
- No se puede asignar manualmente a un dispositivo.

¿Cuando se usa?

- ARP request → “¿Quién tiene la IP X?”
- DHCP Discover → “¿Hay algún servidor DHCP disponible?”
- Algunos protocolos de descubrimiento de servicios

Detección y corrección de errores

Las interferencias en la línea de comunicación puede provocar errores en la trama, cuando no la desaparición de la misma.

El nivel de enlace se encarga de **solicitar el reenvío de tramas erróneas**, **recomponer el orden** de las tramas desordenadas y duplicarlas. El nivel de red no debe enterarse de esto.

Para ello el nivel de enlace puede utilizar dos estrategias:

- **Detectar el error** en la transmisión y solicitar el reenvío, en la mayoría de los casos es la estrategia preferible.
- **Detectar y corregir el error** si el retardo en la transmisión es muy alto, como en el caso de las transmisiones vía satélite.

Tipos de errores

- **Error de bit**: Significa que únicamente **un bit** de una unidad de datos determinada (byte, carácter, unidad de datos o paquete) cambia de 1 a 0 o de 0 a 1.

  Enviado: `0100000001000011`

  Recibido: `0**0**00000001000011`

- **Error de ráfaga**: Significa que **dos o más bits** de la unidad de datos han cambiado de 1 a 0 ó de 0 a 1. Habitualmente seguidos, pero no tiene porqué.

  Enviado: `0100000001000011`

  Recibido: `010**11111**01000011`

Redundancia

Un mecanismo exacto de detección de errores sería enviando dos veces la misma información y realizar una comprobación bit a bit. También sería muy lento.

El concepto de **incluir información extra** es bueno, pero en lugar de incluir todo el flujo, se añade un grupo más pequeño. A esta técnica se le denomina **redundancia** porque los bits añadidos son redundantes, se descartan tan pronto como se ha comprobado la exactitud de la transmisión.

Redundancia vertical

Es el mecanismo de detección de errores más frecuente, se usa en los caracteres ASCII de 7 bits. Si hay errores en los datos el receptor los descarta y solicita su retransmisión.

Se le denomina **verificación de la paridad** y puede ser de dos tipos.

- Paridad Par
- Paridad Impar

Paridad Par

Se añade un bit de redundancia (bit menos significativo), denominado bit de paridad, al final de cada unidad de datos, de forma que el **número total de unos** en la unidad (incluyendo el bit de paridad) **sea par**.

Datos a enviar: `1100001` (3 unos)

Datos enviados: `1100001`**1** (4 unos)

Paridad Impar

Se añade un bit de redundancia (bit menos significativo), denominado bit de paridad, al final de cada unidad de datos, de forma que el **número total de unos** en la unidad (incluyendo el bit de paridad) **sea impar**.

Datos a enviar: `1100001` (3 unos)

Datos enviados: `1100001`**0** (3 unos)

Códigos de redundancia cíclica (CRC)

Los métodos anteriores sólo permiten la detección de errores simples. Para errores más complejos los CRC son los códigos más utilizados.

Se basan en la inclusión, al final de la palabra original, de una serie de dígitos redundantes que permiten detectar errores en varios dígitos.

Existen tres códigos CRC que se utilizan ampliamente:

- **CRC-12**: Su polinomio generador es X12+X11+X3+X2+X1+1 , es decir, “1100000001111”
- **CRC-16**: Su polinomio generador es X16+X15+X2+1, es decir, “11000000000000101”
- **CRC-32** Ethernet: Su polinomio generador es X32+X26+X23+X22+X16+X12+X11+X10+X8+X7+X5+X4+X2+X+1, es decir, “100000100110000010001110110110111”

Uso de CRC

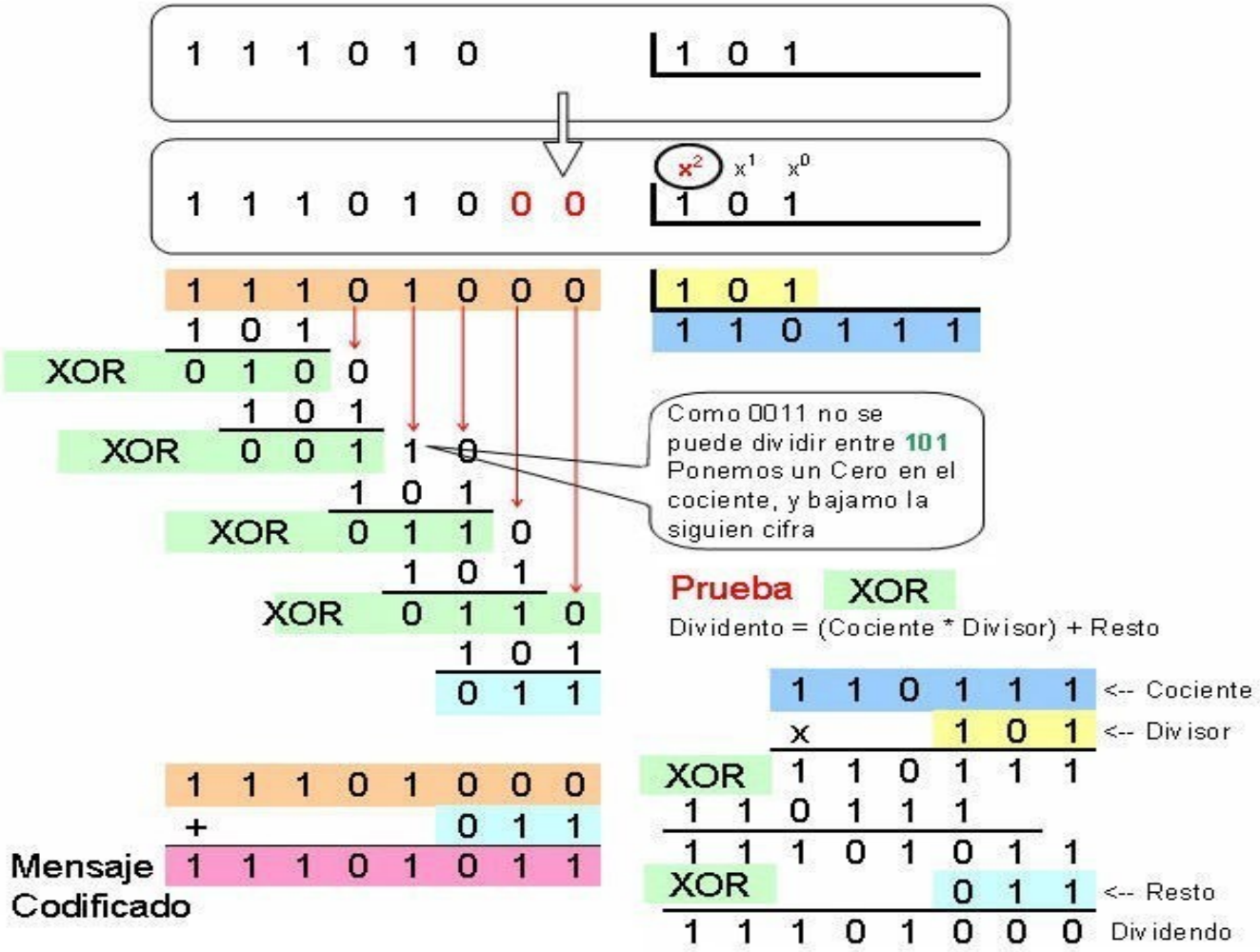
Para **transmitir** datos utilizando CRC, se siguen los siguientes pasos:

1. Dada una **palabra** de **N bits** y dado un **polinomio** generador de longitud **R** se le añaden **R-1 dígitos** al final de ella con el valor **0**.

2. La cadena anterior se **divide** (utilizando XOR) por el polinomio generador R.

3. A la cadena obtenida en el paso 1 se le **suma** el **resto** obtenido en el paso 2

Uso de CRC


1 1 1 0 1 0
1 0 1
1 1 1 0 1 0 0 0
x2 x1 x0
1 0 1
1 1 1 0 1 0 0 0
1 0 1
1 1 0 1 1 1
XOR 1 0 1
0 1 0 0
XOR 1 0 1
0 0 1 1 0
XOR 1 0 1
0 1 1 0
XOR 1 0 1
0 1 1 0
1 0 1
0 1 1
Como 0011 no se puede dividir entre 101 Ponemos un Cero en el cociente, y bajamo la siguien cifra
Prueba XOR
Dividento = (Cociente * Divisor) + Resto
1 1 0 1 1 1 <-- Cociente
x 1 0 1 <-- Divisor
XOR 1 1 0 1 1 1
1 1 0 1 1 1
1 1 1 0 1 0 1 1
XOR 0 1 1 <-- Resto
1 1 1 0 1 0 0 0 Dividendo
1 1 1 0 1 0 0 0
+ 0 1 1
Mensaje Codificado 1 1 1 0 1 0 1 1

Uso de CRC

Cuando se reciben datos con CRC, se hace lo mismo para comprobar los errores:

- **Dividir** la **palabra** codificada en CRC entre el **polinomio** generador.
  - Si el **resto** es **todo ceros**, quiere decir que no hay ningún error.
  - Si el **resto** de la división **no es todo ceros**, quiere decir que se ha producido un error en la transmisión.

Uso de CRC

Ejemplo

Queremos transmitir la palabra `1101011011` utilizando un código CRC cuyo polinomio generador es `100011` (x^5+x+1)

Seguimos los pasos:

1. Añadimos cinco ceros al final de la palabra `1101011011`**00000**
2. Dividimos la palabra anterior entre el polinomio generador. Esto nos da de resto `11001`
3. Sumamos ese residuo a la palabra `110101101100000` y nos queda la palabra `110101101111001`, que es la que se transmite.
4. El receptor dividirá la palabra recibida entre el polinomio generador `100011` y comprobará que el resto sea cero.

Sumas de comprobación (Checksum)

En este método, al enviar información, **se subdivide la unidad de datos en segmentos iguales de n bits**. Estos segmentos **se suman** y el **resultado** de la suma **se complementa** (se invierten unos por ceros y ceros por unos) y se añade al final de la unidad de datos original, como datos de redundancia.

El receptor subdivide las unidades de datos, suma todos los segmentos y complementa el resultado. El resultado obtenido si no ha habido errores debería ser 0. Si el resultado no es 0, el paquete contiene un error y el receptor lo rechaza.

Sumas de comprobación (Checksum)

Ejemplo

Se envía el siguiente bloque de 16 bits `1010100100111001` con una **suma de comprobación de 8 bits**.

```
    10101001
+   00111001
   ----------
    11100010
    00011101  (complemento de la suma)
```

El patrón enviado es: `10101001 00111001 00011101`

Sumas de comprobación (Checksum)

Ejemplo

Al llegar el paquete de datos al receptor, este suma cada segmento y obtiene el complemento, que si todo ha ido bien debería dar todo ceros.

En nuestro ejemplo el paquete de datos recibido es:

```
10101001 00111001 00011101
```

Suma de los segmentos:

```
    10101001
+   00111001
    00011101
   ----------
    11111111
    00000000
```

(complemento de la suma todo ceros, luego no ha habido errores)

Control de acceso al medio (MAC)

Cuando dos transmisiones coinciden en un medio, las señales que las forman se mezclan y dejan de ser interpretables, con lo que la información que contenían se pierde. Se dice entonces que se ha producido una **colisión** entre tramas.

Por ello cuando dos o más dispositivos están conectados a un mismo medio compartido, es necesario que **regulen** su método de acceso a dicho medio para que sus transmisiones no colisionen (como el tráfico de coches y los cruces).

Los **objetivos** de los métodos de acceso al medio son:

- Regular el acceso para impedir o reducir al máximo las **colisiones**.
- Utilizar el canal de forma **eficiente** aprovechando al máximo la capacidad.

MAC - Dominios de tráfico de red

Además de las colisiones que se producen en la transmisión en medios compartidos, las redes poseen mecanismos de **difusión** que permiten a los equipos comunicarse con todos los equipos de la red, pero ha de existir una **frontera** para que dichos mensajes **no se propaguen entre redes** y generen tráfico innecesario.

Por tanto, en el diseño de una red se debe tener especial cuidado, no hacerlo correctamente puede provocar que el rendimiento de la misma sea bajo.

MAC – Dominio de colisión

Es la región de una red donde dos tramas pueden llegar a colisionar. Reducir el número de colisiones es muy importante, ya que permite incrementar el rendimiento de la red y, por ello, la velocidad global de transmisión. Para ello hemos de tener en cuenta cómo nos afectan los dispositivos intermedios de red:

- Los **hubs** y los **repetidores propagan las colisiones**.
- Los **conmutadores**, los **puentes** y los **routers no propagan** las colisiones. Además, estos dispositivos, debido a que separan el tráfico y eliminan todo aquello que no consideran una trama válida, permiten eliminar gran parte de colisiones en la red.

MAC – Dominio de difusión

Es la región por donde se propaga una trama broadcast una vez lanzada a la red Cómo nos afectan los dispositivos intermedios de red:

- Los **repetidores**, los **hubs**, los **puentes** y los **switches propagan** las tramas de **difusión**.
- Los **routers no propagan** las tramas de difusión.

MAC – Métodos

El control de acceso al medio SÓLO es necesario en las redes **MULTIPUNTO**.

A la hora de compartir un medio tenemos dos grandes opciones:

- Reparto **estático** del canal:
  - Por **FDM** (Multiplexación en frecuencia) o **WDM** (Multiplexación en longitud de onda) en medios ópticos.
  - Por **SDMA** (Acceso Múltiple por División de Espacio) en comunicaciones por satélite o redes celulares.
  - Por **CDMA** (Acceso Múltiple por División de Código).
- Reparto **dinámico** del canal
  - Por **TDM** (Multiplexación en el tiempo)

    Y dentro de los TDM hay 2 tipos básicos de métodos de control de acceso:
    - **Controlados** o libres de colisiones
    - Basados en la **contención**

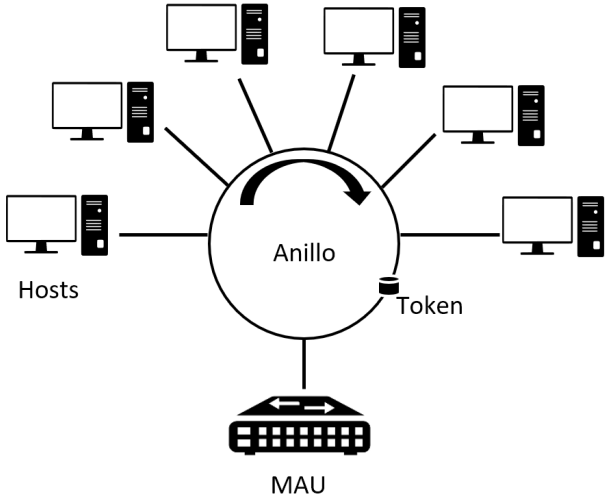
MAC – Métodos controlados

Método de paso de testigo

En esta técnica hay una **trama especial** de pequeño tamaño llamada **testigo** (token) que va siendo intercambiada entre los nodos según un orden preestablecido.

Un nodo sólo puede transmitir cuando tiene la trama testigo, si no deberá esperar.

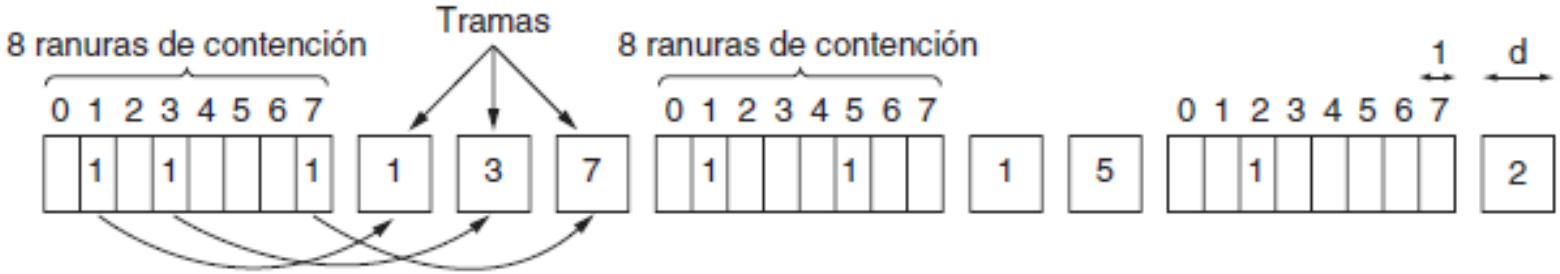
Ha sido muy utilizado en las topología de anillo.



MAC – Métodos controlados

Método de mapa de bits

En este protocolo hay un **periodo previo de contención** de tantas **ranuras** como estaciones a controlar, las cuales están **numeradas**. En este período, una estación puede **anunciar** que tiene una trama por enviar, para lo cual **inserta un bit 1 durante su ranura**. Una vez que han pasado las N ranuras, las estaciones empiezan a transmitir en orden numérico.



MAC – Métodos basados en contención

Método ALOHA

En Aloha **no hay control**, permitimos que los nodos transmitan siempre que tengan algo que emitir. Así que por supuesto se producirán colisiones cada vez que dos nodos emitan a la vez.

- Aloha se basa en el hecho de que podemos **detectar** esas colisiones **escuchando el canal**. Si lo que escucho no es lo que he emitido entonces ha habido una colisión.
- Detectada la colisión, se **desechan** las dos tramas que han colisionado.
- Los dos emisores **esperan un tiempo aleatorio** y emiten de nuevo sus trama. El tiempo de espera debe de ser aleatorio para impedir que se produzca una nueva colisión entre ellos.

MAC – Métodos basados en contención

Método CSMA/CD (Carrier Sense Multiple Access / Collision Detect)

El “Acceso Múltiple con Escucha de Señal Portadora” es una mejora sobre Aloha, consistente en que ahora, se dispone de una circuitería adicional que permite **escuchar** el canal antes de emitir para saber si está ocupado.

Esto **evita muchas colisiones**. Pero no las evita todas.

Durante la emisión las estaciones **sondean** el medio para **detectar** si se produce una **colisión** y en caso de producirse, todos los dispositivos interrumpen la transmisión y lo intentan después de un tiempo de espera. Este tiempo de espera se determina mediante **Binary Exponential Backoff**, donde cada estación espera un tiempo aleatorio entre 0 y $2^k - 1$ múltiplos del tiempo ranura (slot time), que en Ethernet clásico es 512 bit-times (~51,2 μs).

MAC – Métodos basados en contención

Método CSMA/CD (Carrier Sense Multiple Access / Collision Detect)

¿Qué hacemos si el canal está ocupado?

CSMA sin persistencia: Antes de mandar algo, se comprueba el medio. Si el canal está ocupado, **espera** un período **aleatorio** y vuelve a intentarlo. La utilización es mejor pero los retrasos para mandar tramas son más largos.

CSMA persistencia 1: Cuando una estación tiene datos para mandar, primero examina si alguien está usando el canal. Si el canal está ocupado, **sigue testeándolo hasta que se desocupa** y entonces transmite un marco. **Persistencia 1** significa que la estación transmite con una **probabilidad de 100%** cuando encuentra el canal desocupado.

CSMA de persistencia P: P es un número entre 0 y 1 que indica la **probabilidad** de que el nodo emita inmediatamente después de detectar el final de la última portadora. Ej: CSMA persistencia **0,3 indica 30% de posibilidad de emitir** inmediatamente después de detectar el final de la última portadora.

MAC – Métodos basados en contención

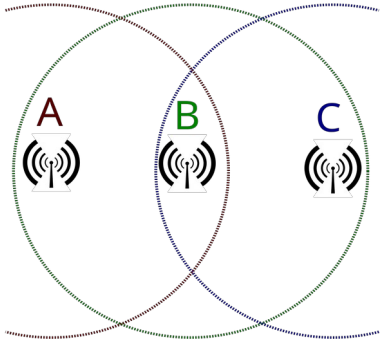
Método CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

Es un CSMA que usa el siguiente mecanismo para evitar colisiones.

Si el medio está libre:

- El dispositivo **envía una notificación** a través del medio, sobre su intención de utilizarlo realizando una especie de **reserva del medio**.
- El dispositivo luego envía los datos.

Este método es utilizado por las tecnologías de redes inalámbricas 802.11. Hay que tener en cuenta que este método evita muchas colisiones pero no todas principalmente por el **problema de nodos ocultos**.



MAC – Métodos basados en contención

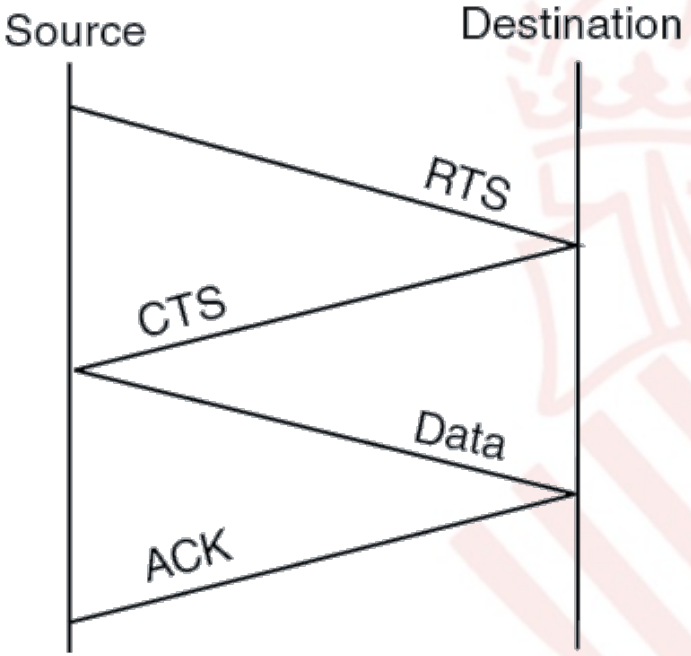
Método CSMA/CA

Funcionamiento:

Cuando una estación tiene una trama que transmitir antes de enviarla envía una trama

pequeña de aviso (de 30 bytes) denominada RTS (RequestTo Send). La trama RTS contiene información sobre la longitud de la trama que se pretende transmitir y la estación de destino.

Al recibir la trama RTS la estación de destino, si está en condiciones de recibir la transmisión, responde con otra trama denominada CTS (Clear To Send). La trama CTS también indica la longitud de la trama que se va a recibir.



Control de flujo

Cuando hablamos de control de flujo en el nivel de enlace, estamos hablando de la realización de dos funciones distintas:

1. Evitar que un emisor rápido **sature** a un receptor lento. Con el control de flujo se pretende que un emisor rápido no sature a un receptor lento y no se **pierdan las tramas** que no se pueden procesar. Si se da el caso contrario, un emisor más lento que el receptor, no habrá perdida de tramas.

2. Dar solución a las tramas que se detecten como **erróneas**:

   - Cuando un receptor detecta una trama errónea, hay que solicitar el **reenvío** al emisor.

   - Cuando un emisor, envía una trama, si tarda demasiado tiempo en recibir una respuesta, puede suponer que la trama se ha perdido, y puede reenviarla. Esto puede dar lugar a tramas **duplicadas** y también hay que controlarlo.

Métodos de control de flujo

Para realizar esta función de adecuación del ritmo el nivel de enlace provee una serie de mecanismos para detectar una posible saturación del receptor y “frenar” el envío de información.

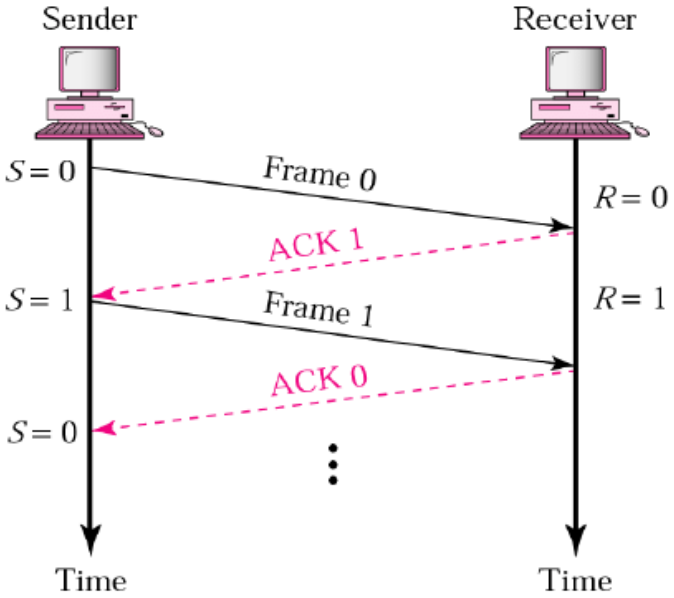
Los métodos más comunes son:

- Parada y espera
- Piggybacking
- Ventana deslizante

Método de Parada y espera

El emisor después de mandar una trama, **espera la confirmación** (ACK) del destino.

Una vez recibida continua enviando información.



Método de Piggybacking

Cuando una trama llegue, el receptor no tiene que mandar inmediatamente un acuse. Esperará hasta que el nivel de red le pase un paquete de datos para su transmisión. Cuando el paquete esté listo, le añadirá el acuse para la trama antes recibida. Así, **se combinan** en una única trama un **acuse** y una **trama** de datos.

Ventaja: un mejor uso del ancho de banda ya que una trama que consista solamente en un acuse ocupará mucho más espacio.

Es preciso que la línea sea **full-dúplex**.

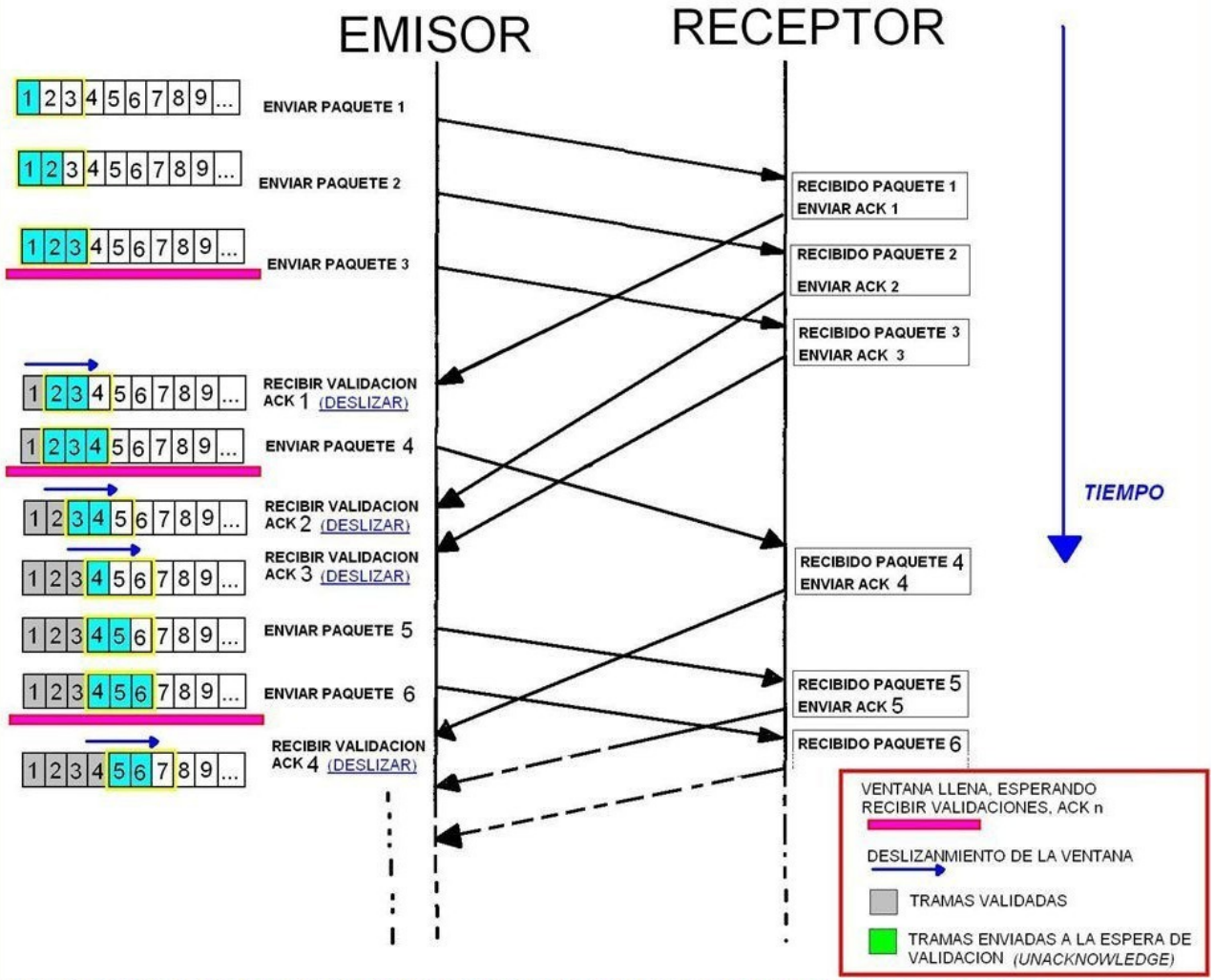
Método de Ventana deslizante

Hace posible ocupar el enlace no con una sino con **varias tramas** “en ruta” y permitir a la fuente emitir la trama n+1 antes de haber recibido la confirmación de la trama n.

Funcionamiento:

- Se asigna un **tamaño de ventana** (**N**) → cuántos paquetes se pueden enviar sin ACK.
- El emisor envía paquetes numerados de manera secuencial. Puede enviar hasta N paquetes sin necesidad de haber recibido los ACK.
- El receptor envía ACK indicando el último paquete recibido correctamente.
- Cuando llega un ACK, la ventana se desplaza y el emisor puede enviar el siguiente paquete pendiente.
- Si un paquete se pierde o llega corrupto:
  - el ACK no llega
  - o llega un ACK repetido
  - lo que provoca retransmisión.

Método de Ventana deslizante



Tarea

Realizar el boletín 2 de ejercicios del tema 4

Conmutación de tramas

La aparición de la conmutación (switching) fue un gran avance que desbancó a las tecnologías de interconexión de buses y concentradores.

DEFINICIÓN: La conmutación consiste en utilizar una topología física de **estrella** que centraliza la conexión a la LAN, en un punto en el que un dispositivo llamado conmutador redirige el tráfico del nivel de **enlace** hacia aquel enlace concreto en el que se encuentra el **destinatario** de la trama.

La conmutación de tramas ofrece una gran ventaja respecto a las redes basadas en buses y concentradores, ya que reduce drásticamente el número de colisiones en la red y el **tráfico** a través de los distintos enlaces y el **ancho de banda** está totalmente disponible para cada uno de los puertos.

Switch o conmutador

Un switch o conmutador es un dispositivo de acceso que opera en la capa 2 del modelo OSI y que posee múltiples puertos de conexión a los que se conectan los diferentes dispositivos de una red. Es el elemento central de las redes actuales con topología de estrella.

Es capaz de analizar las tramas a **nivel de enlace** para extraer la información de destino de las mismas y redirigirlas a través del puerto concreto del destinatario.

Poseen una **memoria intermedia** que les permite almacenar las tramas que llegan, lo que **impide que colisionen** los mensajes que reciben simultáneamente.

Son **interconectables** mediante un **cable cruzado**. Aunque actualmente la mayoría suelen tener puertos **Auto-MDI/MDI-X** que detectan el cable y hacen el ajuste automáticamente, de forma que se pueden conectar tanto con cable cruzado como con cable directo.

Switch - Tabla de direccionamiento MAC

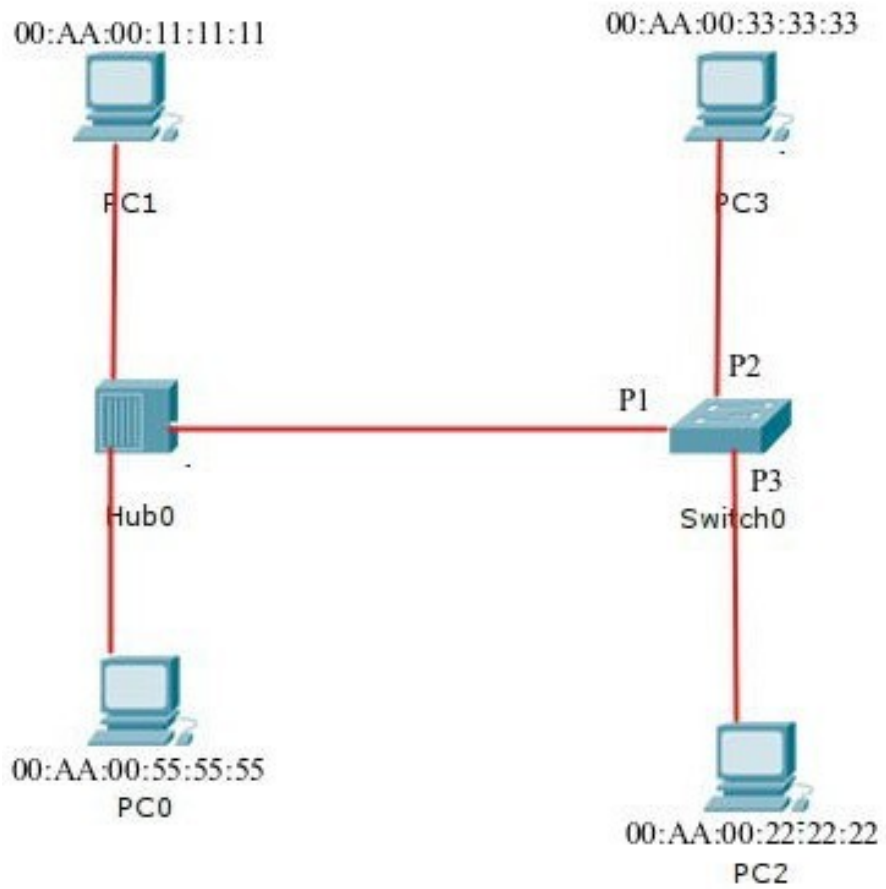
La memoria intermedia que incluyen los conmutadores, almacena una tabla llamada tabla de direccionamiento MAC o tablas ARP, que asocia las **direcciones MAC** de los dispositivos conectados directa o indirectamente al conmutador con el **número de puerto** al que se encuentran conectados dichos dispositivos.

Se generan **entradas** no sólo para los equipos conectados directamente a un puerto del switch, sino **también para los accesibles indirectamente** a través de dispositivos intermedios desde dicho puerto (podemos tener más de una entrada por puerto).

Switch - Tabla de direccionamiento MAC

Ejemplo de tabla de direccionamiento MAC de la red:

Puerto	Dirección MAC
P1	00:AA:00:11:11:11
P1	00:AA:00:55:55:55
P2	00:AA:00:33:33:33
P3	00:AA:00:22:22:22



Switch - Funcionamiento

Cuando un conmutador o switch recibe una trama a través de uno de sus puertos, realiza las siguientes acciones:

1. Detectar si la trama ha llegado con **errores** y, en caso afirmativo, descartarla o iniciar el procedimiento correspondiente.

2. Averiguar las direcciones **MAC** de **origen** y **destino** de la trama.

3. Conocida la **MAC origen** de la trama comprueba si **existe en la tabla** de direccionamiento MAC la entrada que asocia la MAC del dispositivo remitente con el puerto por el que ha sido recibida la trama. Si esta asociación no existe se crea y se almacena en memoria.

4. **Reenviar** la trama por el puerto que corresponda **según la MAC destino** (broadcast, multicast, unicast).

Switch - Funcionamiento

¿Qué ocurre si la MAC destino no está en la tabla?

Ocurre lo que se llama **flooding**, el switch envía la trama por **todos los puertos activos** excepto por el puerto por el que la recibió, solo dentro de la misma VLAN (lo veremos más adelante).

Esto se hace para intentar que el host destino reciba la trama y responda.

Cuando ese host responde, el switch aprende su MAC y ya no necesitará flooding para futuras tramas.

Switch - Funcionamiento

Aspectos a tener en cuenta

- Las MACs de **multicast** (bit menos significativo del primer byte) no se almacenan en la tabla de direccionamiento.
- Las entradas (filas) de la tabla tienen un **tiempo de vida** (timeout) definido. Pasado este tiempo sin que la entrada en la tabla haya sido renovada, esta es eliminada de la tabla.
- Las tablas se almacenan en la memoria del switch que tiene un determinado tamaño y por tanto puede almacenar una cantidad determinada de valores. Si la tabla se **llena** se van **eliminando las entradas más antiguas** para dejar espacio a los nuevos valores que se hayan de almacenar.
- En la actualidad se comercializan conmutadores que funcionan a **nivel 3** o superior que **incorporan funciones de enrutamiento** con la velocidad de la conmutación. Estos switchs tienen su propia configuración IP y suelen tener, para su administración, un servidor web interno.

Tipos de Switch

- **Compacto**: switch de configuración fija. Número de puertos, velocidad y funciones vienen definidos de fábrica.
- **Modular**: un chasis donde se insertan módulos: tarjetas de puertos, fuentes redundantes, ventiladores y supervisores.
- **Apilable**: varios switches conectados por enlaces de apilamiento, que funcionan como uno solo lógico.
- **Gestionable**: switch que permite ser configurado por web/CLI. Funciones habituales: VLANs, STP, SNMP, QoS, ACLs
- **PoE**: switch que alimenta dispositivos por Ethernet. Estándares: 802.3af, 802.3at, 802.3bt. Uso: cámaras IP, APs, teléfonos VoIP
- **Inteligente o multicapa**: switch que además de capa 2 opera en capa 3 (y a veces 4).

Puente de red o bridge

Un puente es un dispositivo de interconexión de redes que opera en la capa 2 del modelo OSI y **conecta segmentos** de red formando **una sola subred** (permite conexión entre equipos sin necesidad de routers).

Funciona a través de una **tabla de direcciones MAC** (forwarding table) detectadas en cada segmento al que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge **copia** la trama para la otra subred, teniendo la capacidad de **desechar** la trama (filtrado) en caso de no tener dicha subred como destino.

Incluye un mecanismo de aprendizaje automático (autoaprendizaje) por lo que no necesitan configuración.

Puente de red o bridge

Cuando un puente debe traspasar una trama de un segmento a otro de la red ejecuta las acciones siguientes:

- **Almacena** la trama recibida por cualquier puerto para su posterior análisis.
- Comprueba la **integridad** de la trama. Si es incorrecta la elimina.
- **Reconfigura** el **formato** de la trama al segmento de red destino.
- **Reexpide** la trama al segmento de red accesible por alguno de sus puertos.

Protocolo Spanning Tree (STP)

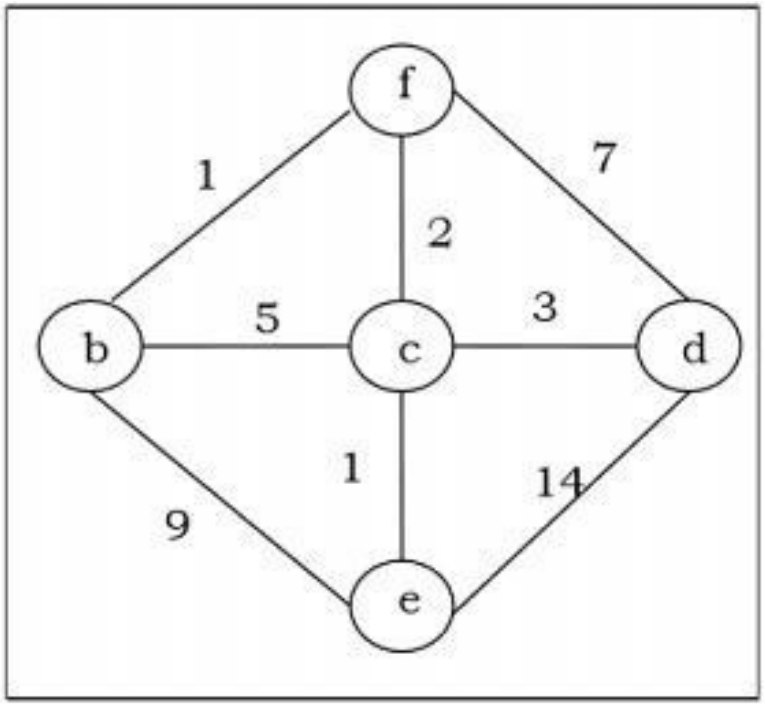
El protocolo STP (del inglés Spanning Tree Protocol) es un protocolo de red de nivel 2 OSI.

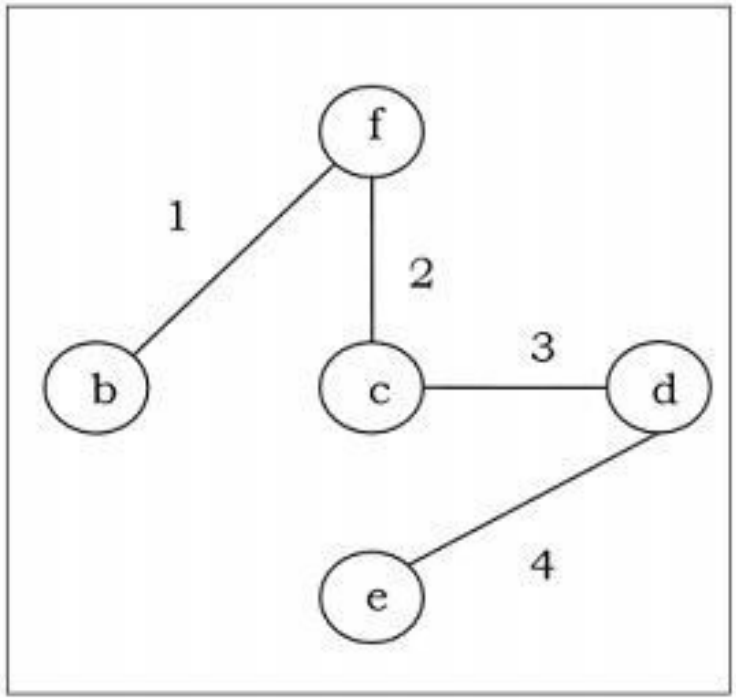
Su función es la de **gestionar la presencia de bucles** (que pueden multiplicar exponencialmente las tramas de difución generando las llamadas tormentas broadcast) en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones).

El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones de usuario.

Protocolo STP - Funcionamiento

El algoritmo debe **transformar** una red **física** con forma de **malla**, en la que existen bucles, a una red **lógica** en forma de **árbol** (libre de bucles).





Protocolo STP - Funcionamiento

Cuando los swtiches se encienden por primera vez tienen que realizar el una serie de pasos para poder converger a una red libre de bucles. En este proceso intercambian información utilizando unas tramas multicast especiales llamadas **BPDU** (Bridge Protocol Data Unit).

Los pasos que se realizan en el protocolo son los siguientes:

1. Escoger un **SWITCH RAÍZ** en la red.
2. Escoger un **PUERTO RAÍZ** por cada SWITCH NO RAÍZ.
3. Escoger un **PUERTO DESIGNADO** por cada ENLACE físico.
4. Bloquear el resto de **PUERTOS NO DESIGNADOS**.

Una vez se ha realizado el proceso, los switches envían cada 2 segundos tramas BPDU para informar si detecta algún cambio en la topología de la red.

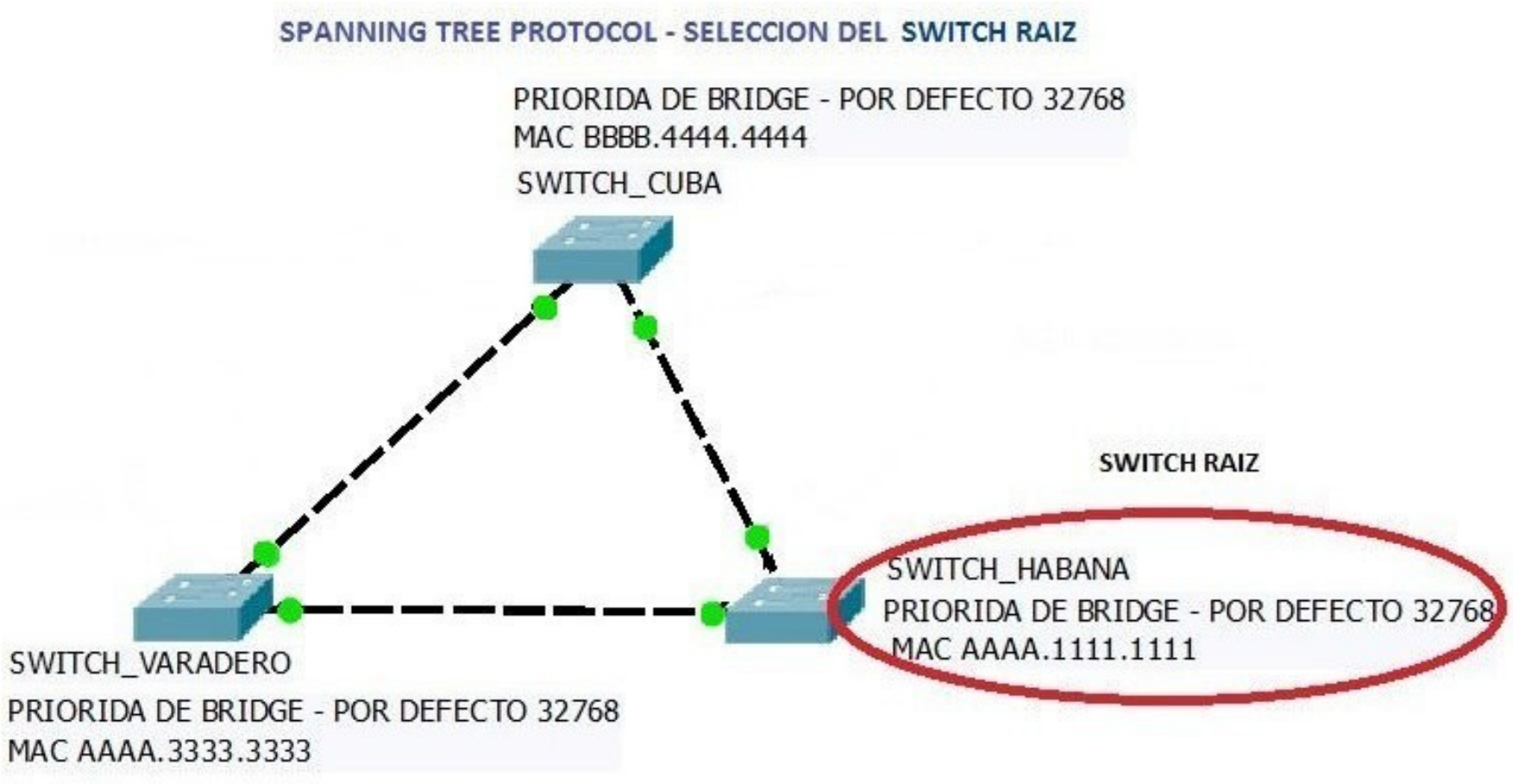
Protocolo STP – Escoger un Switch raíz

El **BRIDGE_ID (BID)** son 8 bytes compuesto por la **PRIORIDAD DEL BRIDGE**, que por defecto es igual en todos los switch (32.768 con incrementos de 4.096) y la direccion **MAC** del switch. El rango de la prioridad es [0 – 65535]. El administrador puede **modificar** el BRIDGE ID modificando la prioridad del bridge.

Al iniciar los swtiches de la red, todos comienzan a enviar BPDUs por todos sus puertos anunciando su BRIDGE_ID.

El SWITCH RAIZ será el switch con el **BID más bajo**.

Protocolo STP – Escoger un Switch raíz



Protocolo STP – Escoger un puerto raíz

Ahora le toca a cada switch NO RAÍZ escoger cuál será su único **PUERTO RAÍZ**, que será aquel que se utilizará para enviar el tráfico de datos y las BPDUs.

El **PUERTO RAÍZ** será el puerto del switch con la **ruta de menor COSTO** desde el switch no raíz hasta el switch raíz. En el caso de que haya dos o más puertos con el mismo costo hacia el puente raíz, se utiliza la dirección MAC que tenga menor valor para calcular el costo y establecer el puerto raíz.

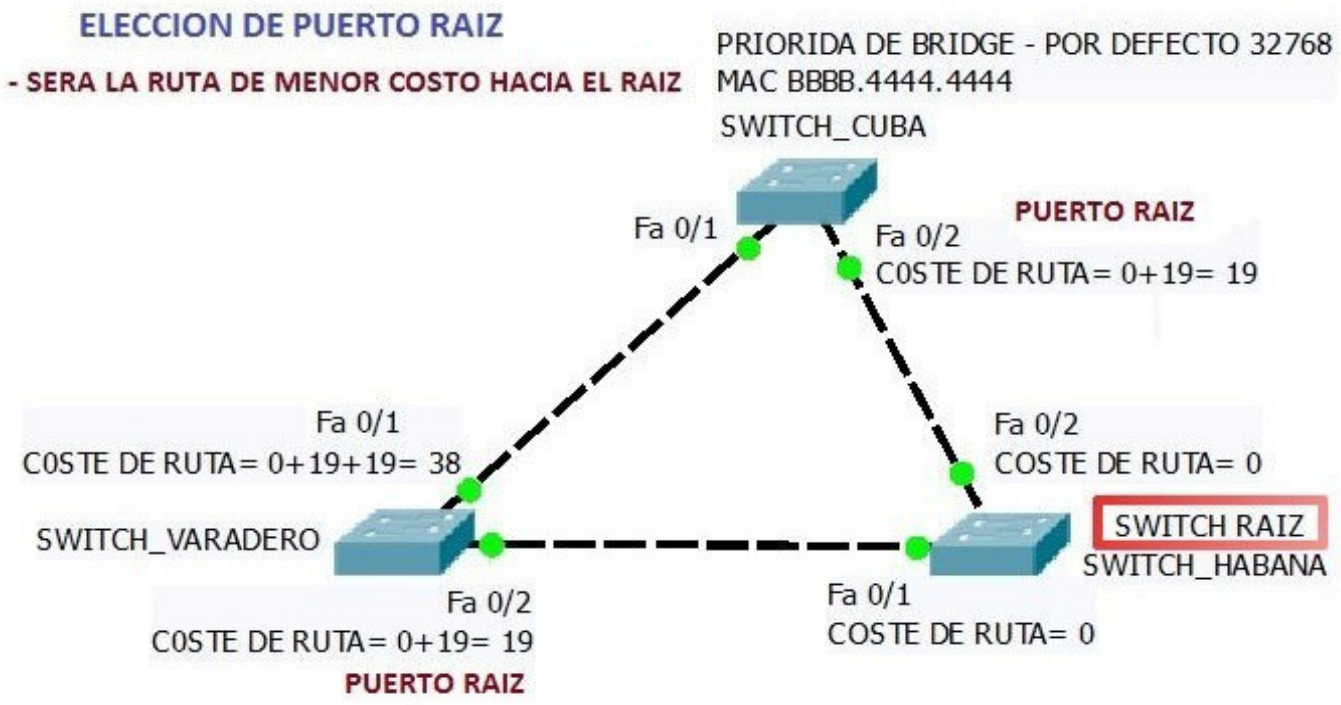
El **COSTO** está directamente relacionado con el **ANCHO DE BANDA** del enlace, en la siguiente tabla mostramos los valores de COSTE antiguo y nuevo revisado.

Protocolo STP – Escoger un puerto raíz

Ancho de Banda del Enlace	Coste STP Antiguo	Coste STP Nuevo
4 Mbps	250	250
10 Mbps	100	100
16 Mbps	63	62
45 Mbps	22	39
100 Mbps	10	19
155 Mbps	6	14
622 Mbps	2	6
1 Gbps	1	4
10 Gbps	0	2

Protocolo STP – Escoger un puerto raíz

Ejemplo:



En este caso todos los enlaces son de tipo Ethernet de 100 Mbps.

El SWITCH_VARADERO tiene 2 puertos y desde ellos:

- Del puerto Fa0/1 al RAÍZ ha de pasar por SWITCH_CUBA 19+19 = 38
- Del puerto Fa0/2 al RAÍZ va directo 19 = 19

Luego el puerto Raíz del SWITCH_VARADERO será el puerto Fa 0/2

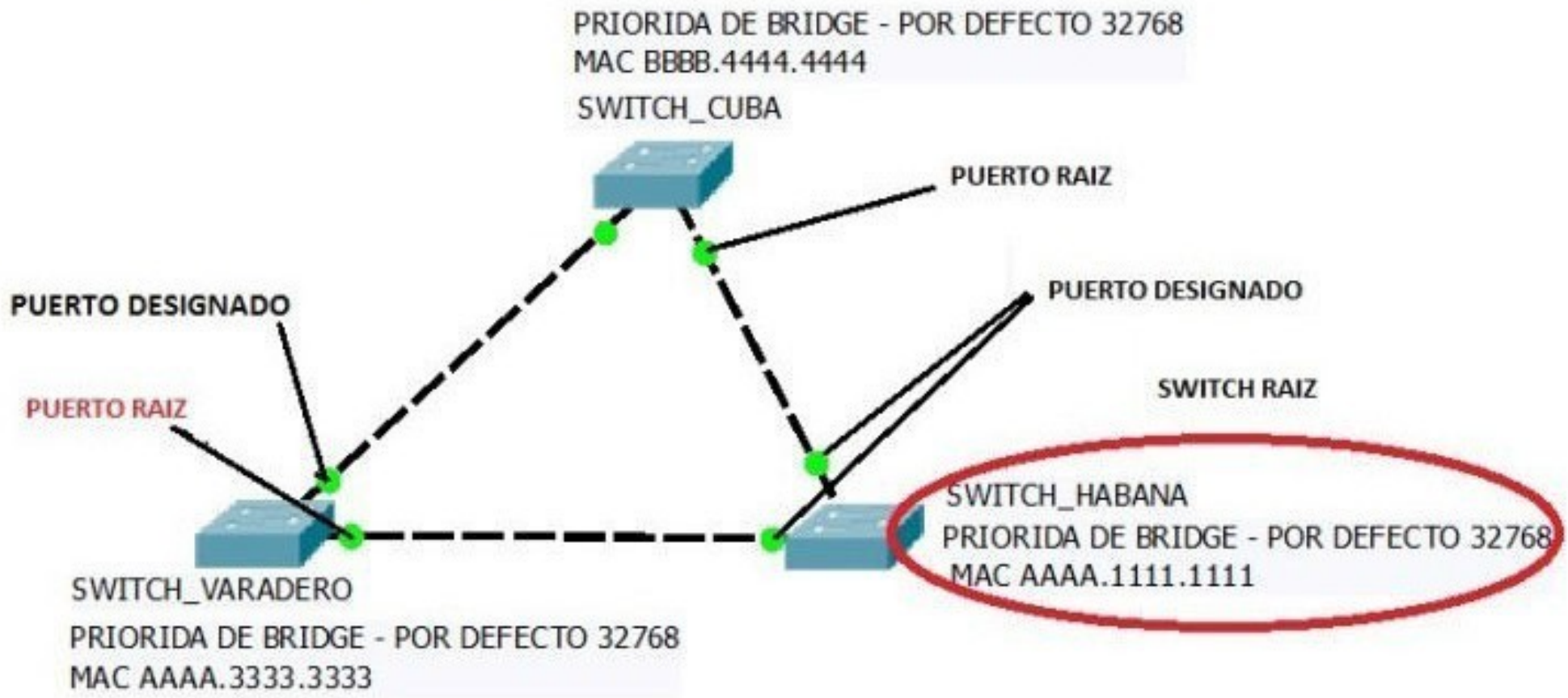
Protocolo STP – Escoger un puerto designado

En cada **segmento** habrá siempre un **PUERTO DESIGNADO** que se encargará de enviar y recibir tráfico y BPDUs. Su selección estará basada en el **COSTO ACUMULADO** hasta el SWITCH RAIZ. Si hubiese empate entre los costes administrativos que tienen los dos switches para llegar al root bridge, entonces se elegirá como Designated Port, el puerto del switch que tenga un menor BID.

En los segmentos conectados con el SWITCH RAIZ, los PUERTOS DESIGNADOS serán los propios puertos del SWITCH RAIZ.

Protocolo STP – Escoger un puerto designado

Ejemplo:



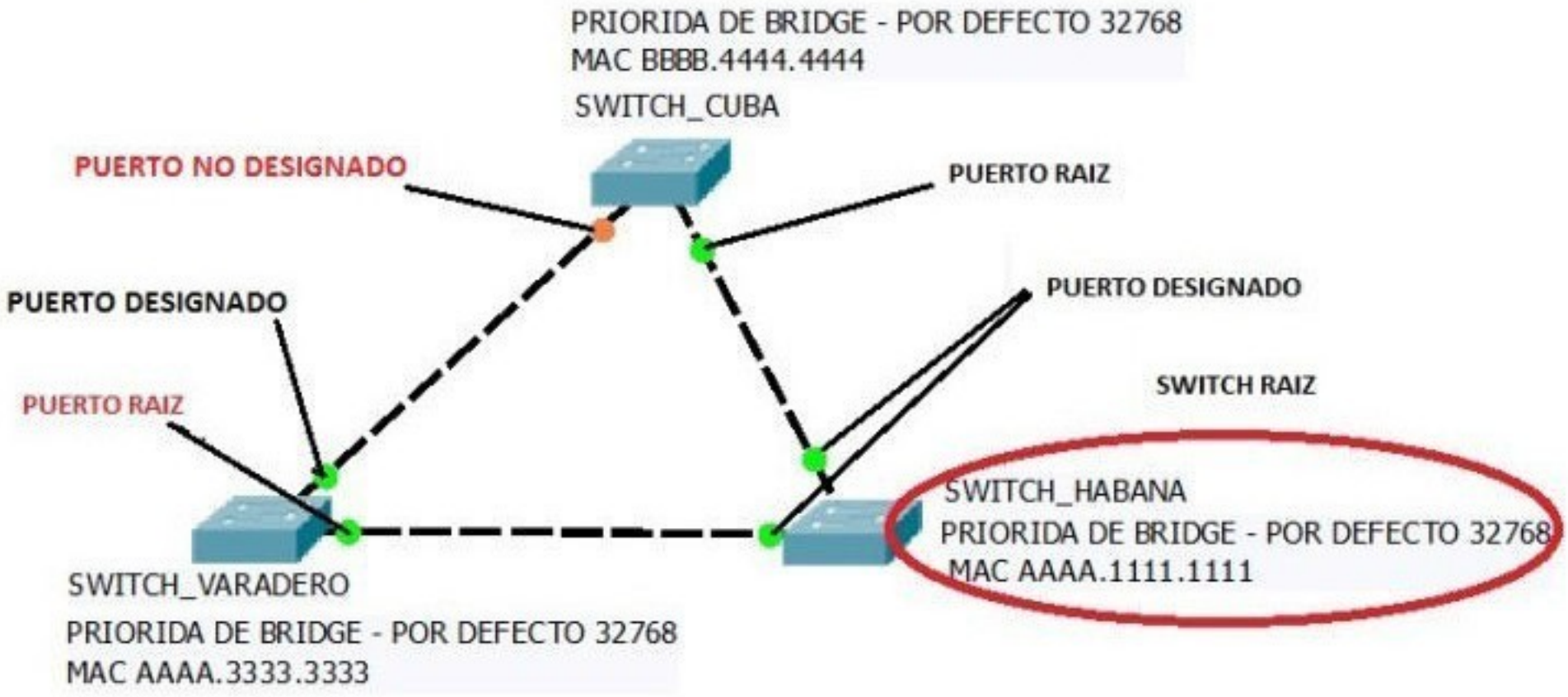
Protocolo STP – Bloquear resto de puertos

Aquellos puertos que no sean elegidos como RAÍZ ni como DESIGNADOS deben bloquearse. Estos puertos evitan los bucles.

Estos puertos **no participan** en el tráfico de datos pero **si reciben BPDUs** y si se producen cambios en la topología de la red este puerto **se puede activar** como PUERTO DESIGNADO ó PUERTO RAIZ.

Después de haber convergido, la red está en condiciones de comenzar a procesar el trafico de una manera eficiente. Este proceso no se repetirá hasta que no exista un cambio en la topología de la red.

Protocolo STP – Bloquear resto de puertos



En este caso, sólo el puerto Fa 0/1 del SWITCH_CUBA se bloquea quedando una topología sin bucles.

Tarea

Realizar el boletín 3 de ejercicios del tema 4

Ethernet

Es un **estándar** de comunicaciones que define las **características de cableado** y **señalización** de nivel físico y los **formatos de las tramas de datos** del nivel de enlace de datos del modelo OSI y del nivel de acceso al medio del TCP/IP.

La **primera LAN** del mundo fue la versión original de Ethernet. El primer estándar de Ethernet fue publicado por un consorcio formado por Digital Equipment Corporation, Intel y Xerox (conocido como DIX). Los primeros productos que se desarrollaron se vendieron a principios de la década de 1980.

Ethernet – Perspectiva histórica

En 1985, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN con la intención de garantizar la compatibilidad con los del modelo OSI, por lo que se realizaron pequeñas modificaciones al original.

Estos nuevos estándares se identifican con el número 802 o **IEEE 802**.

El **IEEE 802.1**: define la **interfaz con los niveles superiores** (el nivel de red)

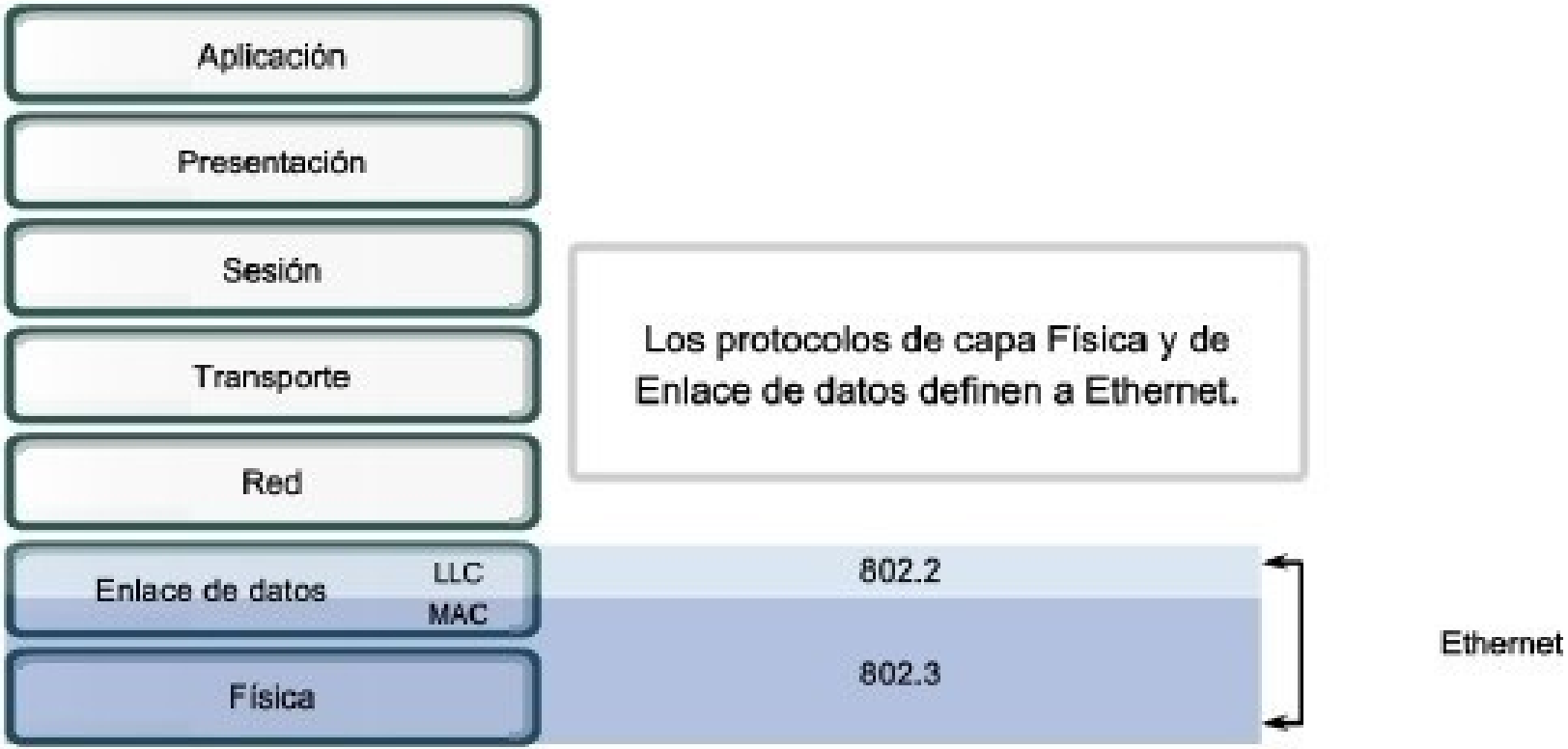
Ethernet – Características

El estándar redefine el nivel de enlace de datos dividiéndolo en dos partes:

- **Subcapa LLC** : **Control de enlace lógico**. Las características de esta parte se encuentran recogidas en el estándar **IEEE 802.2** y corresponden con las funciones de la capa de enlace independientes del medio físico y se se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware.

- **Subcapa MAC** : **Control de acceso al medio**. Esta parte es la encargada de gestionar el uso del medio físico, que debe ser compartido por todas las estaciones de la red local y que, por lo tanto, depende del propio medio. Las especificaciones se recogen del estándar **IEEE 802.3**

Ethernet – Características



Ethernet – Especificaciones IEEE 802

IEEE 802.3: El de las llamadas redes **Ethernet** para redes de área local de equipos conectados al mismo tipo de medio mediante cables basadas en topologías lógicas de bus demultiacceso. Tiene muchas evoluciones.

IEEE 802.4: Redes LAN **Token Bus** con protocolo de paso de testigo.

IEEE 802.5: Redes LAN **Token Ring** Econ topología de anillo.

IEEE 802.6: Las normas para las redes **MAN** de **fibra** óptica.

IEEE 802.8: La normativa para el uso de **fibra óptica** como medio.

IEEE 802.9: Las normativas para la transmisión de **voz** y **datos**.

IEEE 802.10: Referida a la **seguridad** informática en **redes** LAN.

IEEE 802.11: Para redes **inalámbricas** (Wi-Fi).

IEEE 802.14: Normativas para **módems de cable**.

IEEE 802.15: Para redes inalámbricas personales (**Bluetooth**).

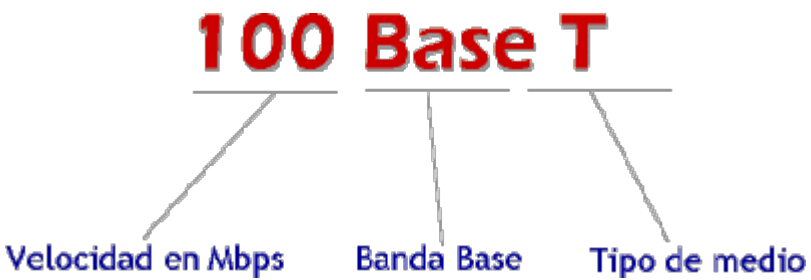
IEEE 802.16: Redes **metropolitanas** sin hilos de banda ancha (WIMAX).

Ethernet – Tipos

Se distinguen diferentes variantes de tecnología Ethernet según la velocidad, el modo de transmisión y el tipo de los cables utilizados.

A la hora de nombrar de forma abreviada los estándares Ethernet se suele utilizar una convención que incluye tres (o cuatro) partes

X Base Z



Ethernet – Tipos

- **X**: La velocidad de transmisión en Megabits por segundo sobre el canal (que no la velocidad disponible para datos, ya que no incluyen las PDU).
  - **10** → 10 Mbps. – Ethernet
  - **100** → 100 Mbps. - Fast Ethernet
  - **1000** → 1000 Mbps. - Gigabit Ethernet
  - **10G** → 10 Gbps. - 10 Gigabit Ethernet
- **Base**: o Baseband modulation, que es el método de modulación empleado. Indica el modo en que se transmite la señal.
  - **Base** → debido a que se transmite en bandabase (sin modular)
  - **Broad** → la señal es modulada (desplazada en frecuencia). Este modo apenas es utilizado actualmente.
- **Z**: Indica el medio utilizado (o a veces la longitud máxima del cable en centenares de metros).
  - **T** → par trenzado (Twisted pairs).
  - **F** → Fibra óptica (Fiber)
  - **5** → coaxial grueso.
  - **2** → coaxial fino.

Ethernet – Tipos

Ejemplo **10GBASE-TX**

nTIPO-LLLm

Tasa de transferencia de datos

10:	10 Mbits/s
100:	100 Mbits/s
1000:	1000 Mbits/s
10 G:	10 Gbits/s
40 G:	40 Gbits/s
100 G:	100 Gbits/s

Tipo de modulación

BASE: Banda base

Número final

"":	1 par de líneas
4:	4 pares de líneas
10:	10 pares de líneas o 10 kilómetros

Primera letra: medio o longitud de onda

C:	Cable coaxial
E:	Longitud de onda extra-larga
F:	Fibra óptica
L:	Longitud de onda larga
S:	Longitud de onda corta
T:	Par trenzado

Segunda letra: especificaciones de la capa de codificación física (PCS)

R:	Código 64B/66B
X:	Códigos 4B5B, 8B10B

Tercera letra:

M:	Multimodo

Nota: En las especificaciones de Ethernet más antiguas, como 10BASE2 o 10BASE5 (sobre cable coaxial), no se sigue esta nomenclatura y el último número se refiere a la longitud que se puede alcanzar (2 para 200 metros, 5 para 500 metros).

Ethernet – Tipos

Tipo	Velocidad	Cable	Dist. máx	Topología
10Base5	10 Mbit/s	Coaxial grueso	500 m	Bus (Conector AUI) – Thick Ethernet
10Base2	10 Mbit/s	Coaxial fino	185 m	Bus (Conector BNC) – Thin Ethernet
10BaseT	10 Mbit/s	UTP Cat 3-5	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbit/s	Fibra óptica 2f	2 km	Estrella (Hub o Switch)
100BaseT4	100 Mbit/s	UTP Cat 3-5 4p	100 m	Estrella H-duplex (hub) / F-duplex (switch)
100BaseTX	100 Mbit/s	UTP Cat 5+ 2p	100 m	Estrella H-duplex (hub) / F-duplex (switch)
100BaseFX	100 Mbit/s	Fibra óptica 2f	2 km	No permite el uso de hubs
1000BaseT	1 Gbit/s	UTP Cat 5e-6 4p	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1 Gbit/s	FO multimodo 2f	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1 Gbit/s	FO monomodo 2f	5 Km	Estrella. Full Duplex (switch)
10GBaseT	10 Gbit/s	Par Trenzado Cat 6a o 7	100 m	Estrella. Full Duplex (switch)
10GBaseLR	10 Gbit/s	Fibra óptica (monomodo)	10 km	Estrella. Full Duplex (switch)
10GBaseSR	10 Gbit/s	Fibra óptica (multimodo)	300 m	Estrella. Full Duplex (switch)
25GBaseSR	25 Gbit/s	FO multimodo 2f (OM3/OM4)	70 m (OM3), 100 m (OM4)	Estrella. Full Duplex (switch)
25GBaseLR	25 Gbit/s	FO monomodo 2f	10 km	Estrella. Full Duplex (switch)
40GBaseSR4	40 Gbit/s	FO multimodo 8f	100 m (OM3), 150 m (OM4)	Estrella. Full Duplex (switch)
40GBaseLR4	40 Gbit/s	FO monomodo 2f	10 Km	Estrella. Full Duplex (switch)

Ethernet – Trama

Hay dos estilos de tramas de Ethernet:

- El estándar DIX Ethernet, que ahora es **Ethernet II** (el más utilizado actualmente)
- El estándar IEEE 802.3, que ha sido actualizado varias veces para incluir nuevas tecnologías

Las diferencias entre las tramas son mínimas.

Ethernet – Trama

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

Los campos Preámbulo y Delimitador de inicio de trama no se incluyen en la descripción del tamaño de una trama.

Ethernet – Campos trama Ethernet II

Formato de la trama Ethernet II o DIX								
Capa	**Preámbulo**	**SFD**	**Dir. Destino**	**Dir. Origen**	**Tipo**	**Datos + Relleno**	**FCS**	**IFG**
	8 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 – 1500 bytes	4 bytes	12 bytes
Enlace								
Físico								

Campos de la trama Ethernet II

- **Dir. Destino**: Identifica el receptor de la trama. Puede ser unicast, multicast o broadcast.
- **Dir. Origen**: Dirección del dispositivo transmisor de la trama.
- **Tipo**: Indica qué protocolo se encapsula en la trama. Ej: 0x0800 = IPv4, 0x86DD = IPv6, 0x0806 = ARP.
- **Datos + Relleno**: La información que se transmite. Si es menor de 46 bytes, se rellena con padding.
- **FCS**: CRC32 calculado por el emisor para verificación de integridad

Campos de la capa Física

- **Preámbulo**: Patrón 10101010… que permite al receptor sincronizar el reloj con el transmisor antes de la trama real.
- **SFD**: Valor 10101011 que marca el final del preámbulo y señala el inicio de la trama MAC. El siguiente byte será la MAC destino.
- **IFG**: Tiempo de silencio obligatorio entre tramas para permitir procesamiento y evitar saturación.

Ethernet – Trama inalámbrica

El estándar IEEE 802.11, denominado comúnmente como “Wi-Fi”, utiliza el **mismo LLC** de 802.2 y el mismo esquema de direccionamiento de **48 bits** que las demás LAN 802.

Sin embargo, existen muchas diferencias en la subcapa MAC y en la capa física.

En un entorno inalámbrico, el entorno requiere consideraciones especiales. No hay una conectividad física definible; por lo tanto, factores externos pueden interferir con la transferencia de datos y es difícil controlar el acceso. Por ello los estándares inalámbricos tienen controles adicionales.

Ethernet – Trama inalámbrica

Se utiliza protocolo **CSMA/CA** de acceso al medio.

Las redes 802.11 también utilizan **acuses de recibo** de enlace de datos para confirmar que una trama se recibió correctamente. Si la estación transmisora no detecta la trama de reconocimiento, ya sea porque la trama de datos original o el reconocimiento no se recibieron intactos, se retransmite la trama. Este reconocimiento explícito supera la interferencia y otros problemas relacionados con la radio.

Otros servicios admitidos por la 802.11 son la **autenticación**, **asociación** (conectividad a un dispositivo inalámbrico) y **privacidad** (encriptación).

Tarea

Realizar el boletín 4 de ejercicios del tema 4