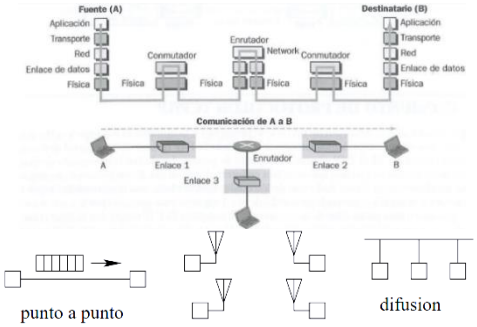
TEMA 5: CAPA DE ENLACE

INTRODUCCIÓN



- La CAPA DE ENLACE es la encargada de la transmisión de bloques de bits entre los extremos de un enlace.
  - Su PDU (unidad de datos de protocolo) son las **tramas**/marcos/frames.
  - Está implementada en los **sistemas finales**, los **routers intermedios** y en los **conmutadores.**
  - Se implementa en la **tarjeta**/adaptador **de red**.

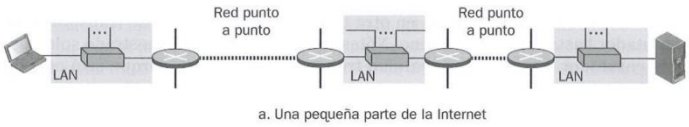
TIPOS DE ENLACE

- Enlace **punto a punto** → un único emisor y receptor a ambos extremos del enlace.
- Enlace por **difusión** → varios emisores y receptores conectados al mismo enlace.
  - ↳ Se necesita determinar cómo se realiza el acceso al medio.

NODOS Y ENLACES

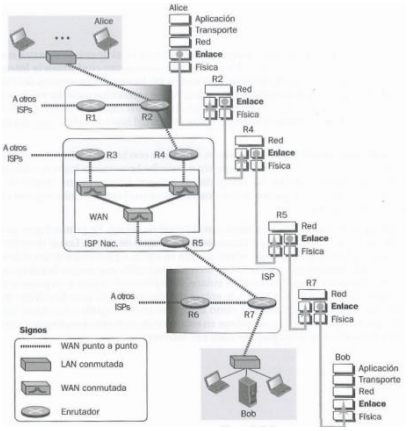
En la capa de enlace, consideraremos:

- **Nodos** → cualquier dispositivo que ejecute un protocolo de la capa de enlace (hosts origen y destino, routers y conmutadores).
- **Enlaces** → redes que conectan nodos adyacentes (LANs y redes punto a punto).



a. Una pequeña parte de la Internet

b. Nodos y enlaces



PROTOCOLOS DE LA CAPA DE ENLACE

- Los protocolos de la capa de enlace definen { el formato de las tramas. / las acciones de los nodos al recibir o enviar tramas.

SERVICIOS MÍNIMOS

- Proporciona servicios a la capa de red en el ámbito **nodo a nodo**.
- **Encapsulado** y **desencapsulado** de datagramas en tramas mediante la adición o eliminación de la **cabecera de capa de enlace**

SERVICIOS POSIBLES

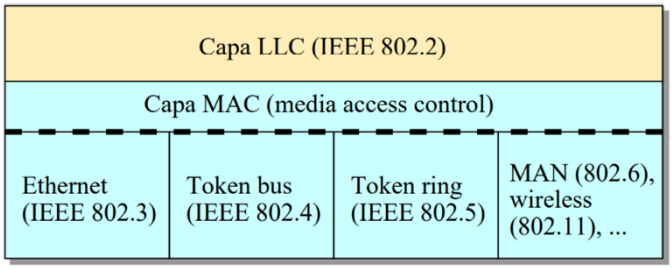
- **Entramado** o **delimitado** de tramas → encapsulado de datagramas de manera que permita identificar donde acaba una trama y donde empieza otra.
- **Acceso al enlace** → en las redes de difusión, establece cómo se accede al medio (MAC).
- **Entrega fiable** → se retransmite cuando la transmisión falla y se envía una confirmación cuando es exitosa.
- **Control de flujo** → el receptor limita la tasa de envío de tramas.
- **Detección de errores** → mecanismos para detectar errores en las tramas.
  - ↳ Más sofisticada que en capas superiores.
- **Corrección de errores** → mecanismos para corregir errores en las tramas (códigos de paridad, sumas de comprobación, CRC, etc.).
- Comunicación **half-duplex** → transmisión en ambos sentidos de manera no simultánea.
- Comunicación **full-duplex** → transmisión en ambos sentidos de manera simultánea.

MODELO IEEE 802

- El MODELO IEEE 802 establece un modelo para la capa de enlace de las principales LANs (ethernet, token bus, token ring, etc.).

En este modelo, se divide la capa de enlace en 2 subcapas:

- Capa de **control de enlace lógico** (LCC) → independiente del medio.
- Capa de **control de acceso al medio (MAC)** → depende del medio.
  - ↳ Por tanto, puede haber distintas opciones MAC para el mismo LLC.



Capa de enlace en LAN

CAPA LLC

- La **capa LLC** es la interfaz de la capa de enlace con las capas superiores.
- Puede tener mecanismos de control de errores y de flujo.

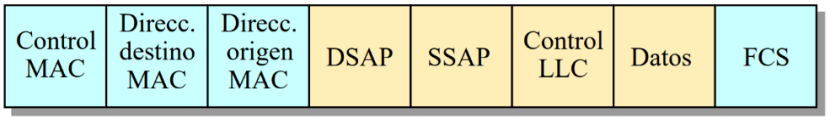
Puede ofrecer 3 tipos de servicio:

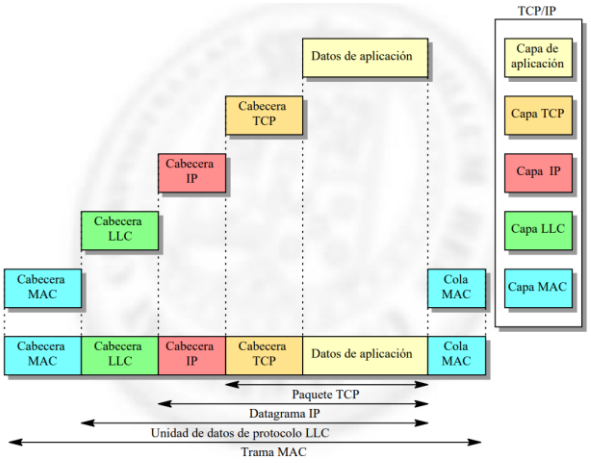
- Sin conexión ni confirmaciones.
  - ↳ No incluye mecanismos de control de errores ni de flujo.
  - ↳ No garantiza la recepción de los datos, delega su control en las capas superiores.
- Sin conexión, pero con confirmaciones.
  - ↳ Se confirman las tramas que llegan, pero no se establece una conexión previamente.
- Con conexión y confirmaciones.
  - ↳ Se establece conexión lógica y hay control de errores y de flujo.

CAPA MAC

- La **capa MAC** se encarga de:
  - En el **origen** → añade la cabecera MAC (identificación de comienzo de trama y direcciones físicas) y la cola MAC (comprobación de errores).
  - En el **destino** → desembala las tramas interpretando su cabecera para reconocer sus direcciones y comprobar si la trama tiene errores.
  - Realizar el **control de acceso** al medio de transmisión.

FORMATO DE UNA TRAMA



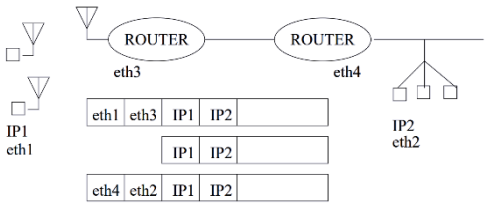


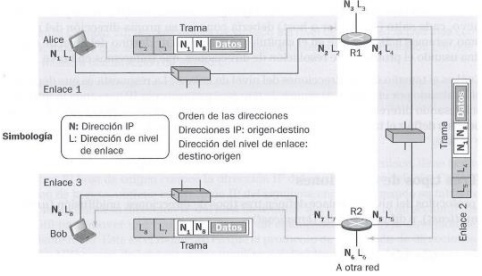
DIRECCIONES MAC ETHERNET

La arquitectura TCP/IP considera dos direcciones **para cada adaptador de red**:

- La **dirección IP**, que tiene sentido en Internet.
- La **dirección MAC**, que tiene sentido en el enlace o LAN.

↳ En la LAN, los adaptadores usan las direcciones MAC, pero fuera de la LAN se eliminan las cabeceras MAC y el paquete viaja usando las direcciones IP.





DIRECCIONES ETHERNET

- Cada nodo Ethernet tiene una dirección MAC única que lo identifica. Son **propias del adaptador** Ethernet y suelen estar fijadas en alguna memoria ROM.
- Están formadas por 6 bytes expresados en hexadecimal. `00:08:74:4A:BA:4B`
  - ↳ Para asegurar que no se repitan, cada fabricante tiene un código único para el comienzo de las direcciones de sus dispositivos.

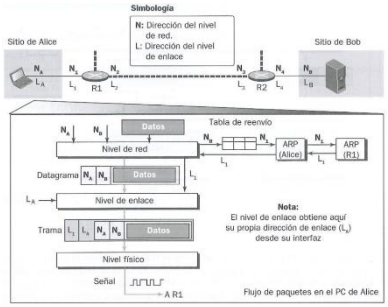
`08:00:20` → Sun
`08:00:5A` → IBM
`00:20:18` → Realtek
`00:80:9F` → Alcatel

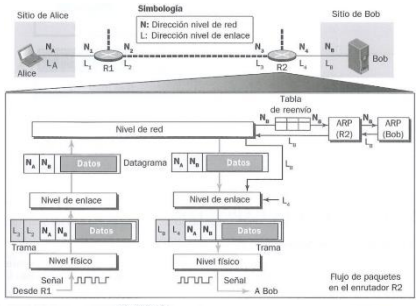
- Hay 2 **direcciones Ethernet especiales**:
  - **Broadcast** (se dirige la trama a todos los nodos de la red)→ todos los bits a 1.
  - **Multicast** (se dirige la trama a un grupo de nodos de la red) → LSB del primer byte a 1.
- Un nodo acepta las tramas cuya dirección destino sea:
  - Su propia dirección Ethernet (unicast).
  - Dirección de broadcast.
  - Dirección de multicast.
  - Cualquier valor cuando está en modo **promiscuo**.

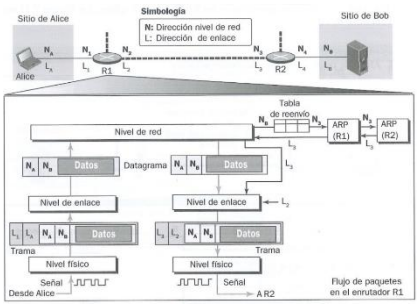
ARP

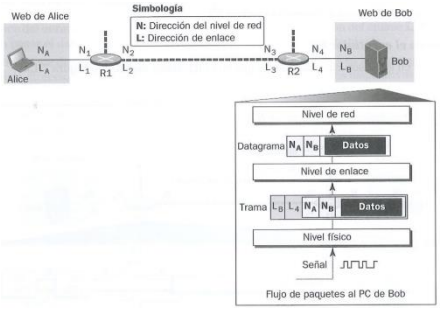
Las tarjetas de red manejan direcciones MAC, pero el software de los nodos maneja direcciones IP, por lo que se necesita poder obtener la MAC de un nodo a partir de su IP.

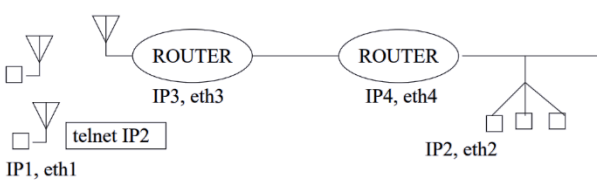
- El **protocolo ARP** (protocolo de resolución de direcciones) se encarga de traducir las direcciones IP a direcciones MAC.
  - Para lograr esto, almacena en cada nodo una tabla, la **caché ARP,** con correspondencias entre direcciones IP y MAC.
    - ↳ Sus entradas se borran cada varios minutos.
- Cuando ARP recibe una IP, la busca en su caché.
  - Si la encuentra → devuelve la MAC correspondiente.
  - Si no la encuentra:
    1. Emite una trama broadcast indicando esa IP.
    2. El adaptador al que le corresponde esa IP responde con su MAC.
    3. Se almacena la respuesta en la caché del peticionario.
    4. Se envía la trama.











1) Se consulta en la tabla de rutas la gateway

tabla rutas del host IP1

destino	gateway
default	IP3

2) Se pregunta la Ethernet de IP3 (si no esta en la tabla ARP) Se anade a la tabla ARP

consulta:	ARP	?IP3?	
respuesta:	ARP	IP3	eth3

3) Se hace la transmision

eth1	eth3	IP1	IP2	

tabla ARP

IP	Ethernet	Tiempo
IP3	eth3	9:40

ETHERNET

- La red ETHERNET es el tipo de LAN más sencilla y común.
  - Ofrece un servicio **no fiable**.
  - Es una red de **difusión** que acepta **distintas topologías** (bus, estrella, etc.).
  - Funciona sobre cable coaxial, par trenzado y fibra óptica.
  - Acepta muchas velocidades: 10Mbps, 100Mbps, etc.

FORMATO DE TRAMA MAC ETHERNET

- **Cabecera** (7 bytes) → 7 bytes iguales, 10101010, para indicar que empieza una trama.
- **SDF** (delimitador de comienzo de trama) (1 byte) → byte 10101011 para indicar el comienzo real de la trama.
- **Dirección destino y origen** (6 bytes cada una).
- **Long** (2 bytes) → tiene distintos usos en distintos tipos de tramas Ethernet. En el más común, **Ethernet DIX**, es un campo **tipo** que indica el protocolo de capa de red (IP o ARP).
- **Datos LLC** → cabecera LLC y datagrama.
  - Su tamaño tiene que estar entre 46 y 1500 bytes.
  - Por tanto, el tamaño de la trama sin cabecera ni SFD tiene que estar entre 64 y 1518 bytes.
- **Relleno** → asegura que los datos tienen un tamaño mínimo de 46 bytes.
- **FCS** (secuencia de comprobación de trama) (4 bytes) → código CRC (código de redundancia cíclica) para corrección de errores.

CONTROL DE ACCESO AL MEDIO

- Como Ethernet es una red de difusión necesita un mecanismo de acceso al medio para controlar qué dispositivo transmite en cada momento.
  Se usa el CSMA/CD (acceso múltiple con escucha de portadora y detección de colisiones).

Su funcionamiento se basa en:

- Para **recibir**, todos los dispositivos de la red escuchan (sondean) el medio constantemente, aceptando sólo las tramas dirigidas a ellos e ignorando las demás.
- Para **transmitir**, se observa primero el estado del medio:
  - Si el medio está **libre** (no está transmitiendo ningún dispositivo) → se transmite.
  - Si el medio está **ocupado** (está transmitiendo algún dispositivo) → se espera hasta que esté libre, dejando un pequeño **intervalo de seguridad**, y luego se transmite.

ORIGEN DE COLISIONES

- Existe un **tiempo de vulnerabilidad** al comienzo de una transmisión debido a que esta tarda un cierto tiempo en alcanzar al resto de nodos.
  Durante ese tiempo, otros nodos observarán que el medio está libre, por lo que puede ser que ellos comiencen a transmitir también.
  - Entonces, se produciría una **colisión**, es decir, aparecería en el medio más de una señal en el mismo instante, lo cual lleva a errores en los datos transmitidos.

DETECCIÓN DE COLISIONES

- Para detectar cuándo se producen colisiones, **el nodo transmisor escuchará el medio mientras transmite**.
  - Si la señal observada es **igual** a la señal transmitida → no se produjo colisión.
  - Si la señal observada **no** es **igual** a la señal transmitida → se produjo una colisión.
- Para que el transmisor tenga el suficiente tiempo para comparar la señal recibida con la enviada, el tiempo que pasa transmitiendo la trama (y por tanto comparándola con la señal recibida) tiene que ser lo suficientemente amplio como para que la señal vaya al punto más lejano de la red y vuelva.
  Es decir, se tiene que cumplir que $t_{trans\ trama} > 2t_{prop\ trama}$.
  - Para conseguir esto, o bien la **trama** tiene un **tamaño mínimo** o bien el **enlace** tiene una **longitud máxima**.

RESPUESTA A LAS COLISIONES

Cuando un nodo detecta una colisión:

1. Acaba de transmitir la cabecera de la trama.
2. Emite una secuencia concreta de 32 bits denominada **jamming sequence**.
3. Detiene la transmisión.
4. Ejecuta el algoritmo de **espera exponencial binaria**.

EXPONENTIAL BACKOFF

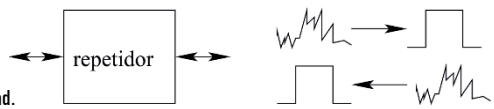
- Se divide el tiempo en ranuras discretas de longitud $T = 2t_{prop\ max}$.

1. Las estaciones que detectaron la colisión esperan 0 o T y vuelven a intentar transmitir.
2. Si se detecta otra colisión, el tiempo de espera se selecciona aleatoriamente entre $0, T, 2T$ y $3T$.
3. En general, durante las primeras 10 se escoge entre 0 y $(2^n - 1)T$.
4. A partir de la colisión 10, se escoge entre 0 y $1023T$.
5. Después de 16 colisiones, los transmisores desisten e informan a las capas superiores del fallo para que se encarguen ellas.

TECNOLOGÍAS ETHERNET

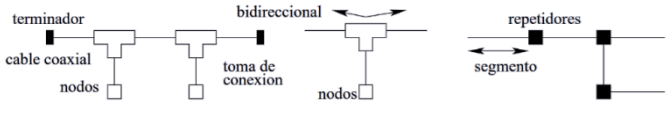
REPETIDORES

- Los REPETIDORES son dispositivos de la **capa física** que trabajan sobre **bits individuales**.
- Copian bits que le llegan por una interfaz en el resto de interfaces, reconstruyendo el **pulso de tensión**.
  - Siempre tienen **dos o más interfaces**.
- Se usan sobre todo en transmisiones a **largas distancias**, pues las señales van perdiendo intensidad y claridad.



TOPOLOGÍA BUS

- La TOPOLOGÍA BUS consiste en un único cable coaxial al que se conectan todos los adaptadores de red usando conectores en T.
- Se colocan **terminadores** a ambos extremos del cable.
- Como máximo, puede haber **4 repetidores** en toda la red.
- Hay un número **máximo de adaptadores** que se pueden conectar en cada **segmento** (sección entre 2 repetidores).
- Nomenclatura → [Mbps][Tipo de transmisión][Centenas de metros de la longitud máxima del segmento].
  - El tipo de transmisión puede ser base (se transmite la señal directamente) o broad (se transmite la señal modulada).
- Es una tecnología **obsoleta**.



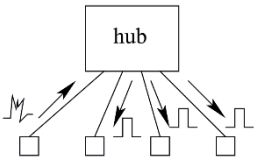
10base2: 10 Mbps, banda de base y segmento de 200 m
10base5: 10 Mbps, banda de base y segmento de 500 m
10broad36: 10 Mbps, banda ancha con modulación y segmento de 3600 m

10base-T: 10 Mbps, banda de base y longitud de 100 m
100base-TX (Fast Ethernet de par trenzado): 100 Mbps, banda de base y longitud de 100 m
100base-FX (Fast Ethernet de fibra óptica): 100 Mbps, banda de base y longitud de 400 m
1000base-T (Gigabit Ethernet de par trenzado)
1000base-SX y *1000base-LX* (Gigabit Ethernet de fibra óptica)
10Gbase-S, *10Gbase-L* y *10Gbase-E* (10 Gigabit Ethernet de fibra óptica)

TOPOLOGÍA ESTRELLA

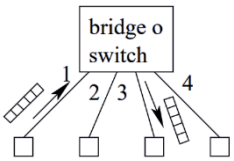
- La TOPOLOGÍA ESTRELLA consiste en un nodo central (que suele ser un conmutador) conectado al resto de nodos de la red.
- Cada nodo se conecta con un par trenzado o fibra óptica de entrada y otro par trenzado o fibra óptica de salida.
  - Se obtienen velocidades de 10Mbps o 100Mbps.
  - Cuando se usa par trenzado se limita la distancia a 100m.
- A partir de 1000Mpbs se necesita usar 4 pares trenzados.
- Nomenclatura → [Mbps][Tipo de transmisión][Tipo de enlace].
  - El tipo de transmisión puede ser base (se transmite la señal directamente) o broad (se transmite la señal modulada).
  - El tipo de enlace puede ser T (par trenzado) o F, S, L y E (fibra óptica).

CONCENTRADORES

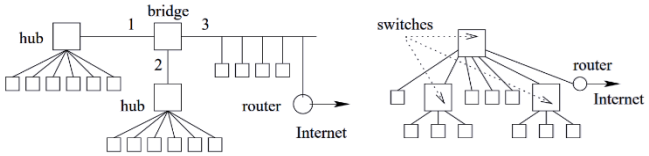


- Los CONCENTRADORES (hubs) son dispositivos de la **capa física** que trabajan sobre **bits individuales**.
- Copian los bits que le llegan por una interfaz en el resto de interfaces, reconstruyendo el **pulso de tensión**.
- Si llegan varias señales a la vez por distintas interfaces, informan a los adaptadores de que hubo colisión.
- Es una tecnología **obsoleta**.

PUENTES Y CONMUTADORES



- Los PUENTES (bridges) y CONMUTADORES (switches) son dispositivos de la **capa enlace** que trabajan sobre **tramas Ethernet**.
  - Los puentes tienen pocas interfaces y los conmutadores tienen muchas.
- **Procesan** los distintos **campos de las tramas Ethernet** (extraen la dirección destino, realizan la comprobación de errores, etc.).
- Tienen cierta **capacidad de almacenamiento**, con colas en las interfaces de salida para almacenar tramas que aún no han salido.
- En la actualidad los **puentes** están **obsoletos**, sólo se usan conmutadores.



AUTOAPRENDIZAJE

- Al igual que los routers, los conmutadores tienen capacidad de dirigir información a la interfaz apropiada, pero, en lugar de ejecutar algoritmos de encaminamiento para construir sus tablas, usan **algoritmos de autoaprendizaje** mediante los que aprenden la localización de los adaptadores.
- Para esto, cada conmutador tiene una **tabla de conmutación** en la que almacenan una entrada por adaptador conectado. Los campos de estas entradas son: Dirección Mac ethernet del adaptador, interfaz de salida que lleva al adaptador, instante de creación de la entrada.
  1. Al principio, la tabla de reenvío está vacía.
  2. Cuando reciben una trama, crean una entrada en la que asocian su MAC origen a la interfaz por la que la recibieron.
  3. Si en la tabla no hay una entrada para la MAC destino de la trama, la enviarán por difusión a todas las interfaces.
  4. Si en la tabla sí hay una entrada para la MAC destino de la trama, la enviarán sólo por la interfaz asociada a esa entrada.
  5. Después de unos minutos, borran las entradas de la tabla.

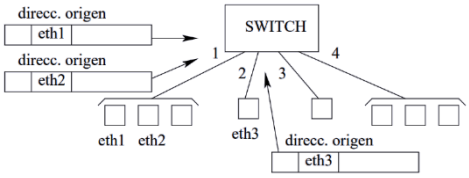
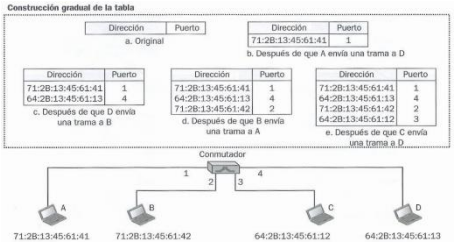


tabla del switch

host	interf.	tiempo
eth1	1	9:20
eth2	1	9:30
eth3	2	9:55



VENTAJAS

- ✓ **Aislamiento de tráfico** → aunque Ethernet sea una red de difusión, gracias a la tabla de reenvío los conmutadores reenvían las tramas sólo por la interfaz adecuada.
- ✓ **Evita colisiones** → como el resto de adaptadores apenas verán transmisiones que no están dirigidas a ellos, se evita que aparezcan varias en el medio.
- ✓ **Filtrado** → descartan las tramas cuya dirección de origen y destino es la misma.
- ✓ Permiten **múltiples transmisiones simultáneas** → siempre que las interfaces origen y destino sean distintas.
- ✓ **Tasa de transmisión agregada elevada** → como tienen muchas interfaces, la cantidad de bits transmitidos por unidad de tiempo es alta.

CONMUTADORES vs ROUTERS

- Ambos son dispositivos de **almacenamiento y reenvío**, es decir, primero reciben el paquete entero, examinan su cabecera y luego lo transmiten.

Los conmutadores:

- Trabajan en la **capa de enlace** con cabeceras de una determinada tecnología.
- Mantienen **tablas de conmutación** que crean con **algoritmos de autoaprendizaje**.

Los routers:

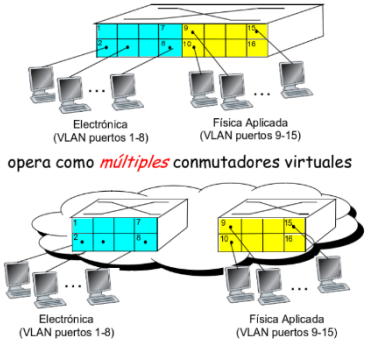
- Trabajan en la **capa de red** con **cabeceras IP**.
- Mantienen **tablas de reenvío** que crean con **algoritmos de encaminamiento**.

VLANs

- En el enfoque tradicional, cada conmutador definía una LAN formada por los adaptadores conectados a él. Esto provocaba muchos problemas:
  - × Un dispositivo no se puede mover físicamente muy lejos del conmutador si quiere seguir formando parte de la LAN.
  - × El dominio de broadcast es único, lo cual aumenta el tráfico en la red.
  - × Se desaprovechan muchos puertos de cada conmutador.
- Esto se soluciona usando conmutadores compatibles con **redes de área local virtuales** (VLANs), es decir, que soporten el estándar IEEE 802.1Q (añade unos campos en la cabecera).
- Estos conmutadores permiten definir múltiples VLANs sobre una única red física (sobre un único conmutador).

VLANs BASADAS EN PUERTOS

- En las **VLANs basadas en puertos** se dividen los puertos del conmutador en grupos de manera que cada uno se corresponde con una VLAN.
  - Se mantiene una **tabla** que asocia cada puerto a su VLAN.
  - A nivel de enlace, sólo se entregan tramas entre puertos de la misma VLAN.
  - Para entregar datagramas entre VLANs se utiliza encaminamiento a nivel de capa de red.
- ✓ **Aislamiento de tráfico** → sólo se entregan tramas entre puertos de la misma VLAN.
- ✓ **Pertenencia dinámica** → si se necesita reubicar un dispositivo de una VLAN a otra sólo se necesita realizar una reconfiguración de la tabla.
- También se pueden definir VLANs por MAC.

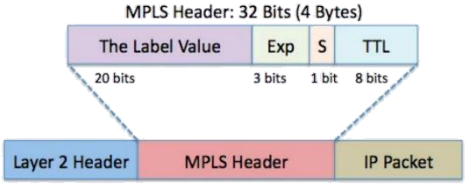


MPLS: CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO

- MPLS permite expandir la infraestructura existente para que actúe como si se tratase de una red de circuitos virtuales.
  - Desde un punto de vista **pedagógico** se podría decir que está **entre** la **capa de red** y la de **enlace**, pues define su propio { formato de paquete. / comportamiento de reenvío.
  - Desde el punto de vista de **Internet**, está en la capa de **enlace**, pues sirve para conectar dispositivos IP.

- A cada datagrama se le añade una **etiqueta** de longitud fija que los routers usarán para encaminarlo, ignorando la IP destino.
  - Funciona **conjuntamente con IP**, pues usa su direccionamiento y encaminamiento.
  - Por tanto, **mezcla técnicas** de redes de **circuitos virtuales** y de redes de **datagramas**.

CABECERA MPLS



- La cabecera MPLS está entre la cabecera de la capa de enlace y la de la capa de red.
  - **Etiqueta** (20 bits).
  - **Exp** (3 bits) → bits experimentales relacionados con la QoS.
  - **S** (1 bit) → en ocasiones aparecen varias etiquetas apiladas, este bit se pone a 1 si es la última de la jerarquía.
  - **TTL** (8 bits).

CÁLCULO DE RUTAS

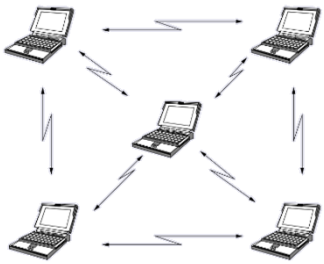
- Existen versiones extendidas de algoritmos de encaminamiento IP (como OSPF) para que los routers MPLS puedan obtener su tabla de etiquetas.
- Cada fabricante puede diseñar su propio algoritmo de encaminamiento.

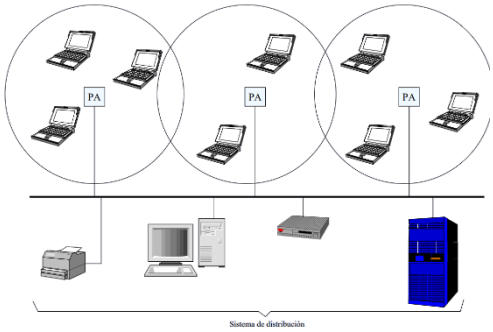
USOS

- **Ingeniería de tráfico** → anulan el encaminamiento IP normal, por lo que pueden dirigir el tráfico a su antojo.
- **Establecer VPNs**.
- **Aislamiento de recursos** → como pueden dirigir el tráfico, pueden aislar nodos para reservar sus recursos para otros usos.

WLAN: REDES DE ÁREA LOCAL INALÁMBRICAS

- Las redes inalámbricas están bajo la especificación IEEE 802.11.
  - 11b (en 2.4 GHz, DSSS, hasta 11 Mbps)
    - Interferencias, velocidad baja
    - Menor absorción, mayor alcance (120–460 m exterior, 30–90 m interior)
  - 11a (en 5 GHz, OFDM, hasta 54 Mbps)
    - Menos interferencias, pero mayor absorción y menor alcance (30–300 m exterior, 12–90 m interior)
    - En España, frecuencia reservada para uso militar
  - 11g (en 2.4 GHz, OFDM/DSSS, hasta 54 Mbps)
    - Misma velocidad que 11a con mayor alcance
    - Coexistencia con 11b (WiFi)
  - 11n (bandas 2,4 Ghz y 5 Ghz, hasta 600 Mbps teóricos)
    - Es la actual, en casi todos los productos
  - 11ac nuevo estándar (hasta 1 Gbps teórico)





- Una red inalámbrica puede ser:
  - Redes **ad-hoc**.
    - Se basan en conexiones de igual a igual.
    - Permiten comunicar 2 estaciones siempre que estén en su radio de alcance.
  - Redes **distribuidas**.
    - Usan una LAN cableada normal (**sistema de distribución**) que conecta los servidores con los puntos de acceso, AP, que cubren una determinada zona.
    - Cada AP da servicio a un número de estaciones móviles, que dependiendo de su localización en un momento dado estarán conectadas a un AP u otro.

PROTOCOLO MACA

- Como las WLAN comparten el medio de transmisión (el aire), necesitan un mecanismo de acceso al medio para controlar qué dispositivo transmite en cada momento.
  Se usa el MACA o CSMA/CA (acceso múltiple con escucha de portadora y avoidance de colisiones).

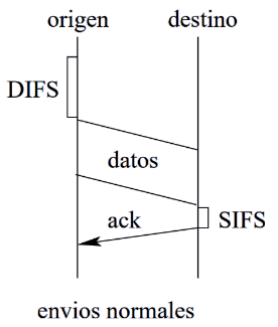
  Su funcionamiento se basa en:
  - Para **recibir**, todos los dispositivos de la red escuchan (sondean) el medio constantemente, aceptando sólo las tramas dirigidas a ellos e ignorando las demás.
  - Para **transmitir**, se observa primero el estado del medio:
    - Si el medio está **libre** (no está transmitiendo ningún dispositivo) → se espera un intervalo de seguridad grande, DIFS, y si sigue libre se transmite.
    - Si el medio está **ocupado** (está transmitiendo algún dispositivo) → se espera hasta que esté libre, se espera un DIFS, y si sigue libre transmite.
      - ↳ Si después del DIFS sigue ocupado utiliza un algoritmo de espera exponencial binaria.

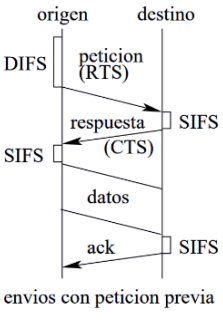
- Este método **no tiene detección de colisiones**.
  En su lugar, se usan los ACKs para evitarlas.

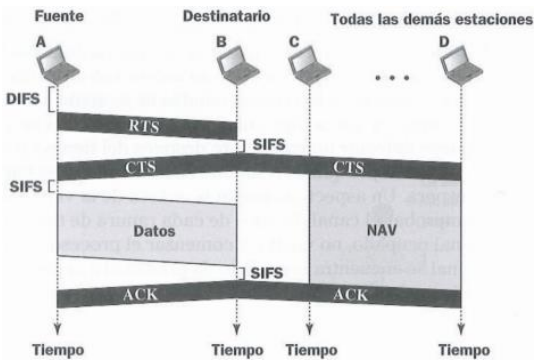
EVITAR COLISIONES

Envío **simple**:

1. Entre la recepción de la trama y el envío del ACK se espera un intervalo de seguridad corto, SIFS.
2. Todos los hosts que deseen transmitir tendrán que esperar a que llegue el ACK.







Envío con **tramas de control** para asegurar la transmisión:

1. El origen envía una trama de petición de envío, RTS.
2. El destino espera un SIFS y responde con una trama de reserva del canal, CTS.
3. El origen espera un SIFS y envía los datos.
4. Entre la recepción de la trama y el envío del ACK se espera un SIFS.
5. Todos los hosts que deseen transmitir tendrán que esperar a que llegue el ACK.
   - En las tramas RTS se incluye el tiempo calcula el origen que necesitará la transmisión. En las tramas CTS se incluye ese mismo valor.
   - El resto de estaciones que reciban la RTS o CTS (es decir, aquellas que están en rango pero no se está transmitiendo para ellas) crean un **temporizador NAV** (vector de asignación de red), que será el tiempo que esperen antes de volver a sondear el medio.

   PROBLEMAS
   - Dos estaciones pueden intentar enviar tramas RTS a la vez.
     - Solución → el emisor detectará la colisión si no recibe la trama CTS del receptor. Entonces usará el algoritmo de espera binaria para decidir cuándo lo vuelve a intentar.
   - Problema de la estación oculta:
     1. La estación A envía a la B una trama RTS.
     2. B envía a A una CTS.
     3. La estación C, que está en el alcance de B pero no el de A sólo recibe la trama CTS, que también incluye el tiempo de ocupación.
     4. Entonces, C sabe que alguna estación oculta está usando el canal, así que no transmite a D hasta que acabe su NAV, pese a que podría.

REDES ATM

- Las redes ATM (modo de transferencia asíncrono) son el tipo de red con la que trabajaban las compañías telefónicas.
  - Se usaban en redes telefónicas y en las redes troncales de Internet.
- El modelo ATM cubre la **capa física**, la **capa de enlace** y la **capa de red.**
- Son redes de **circuitos virtuales** (canales virtuales en nomenclatura ATM) y por tanto están **orientadas a conexión**.
- Se **integran** con facilidad en la **arquitectura TCP/IP**.
- Están diseñadas para operar a **alta velocidad** (los conmutadores pueden operar a terabits por segundo).
  - Pueden transmitir datos, audio y vídeo.

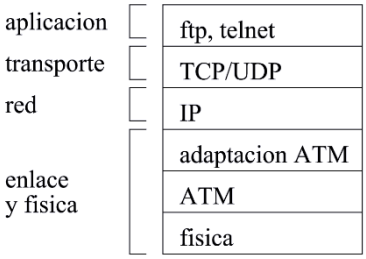
TIPOS DE SERVICIO

- **Tasa de bits constante** (CBR):
  - La tasa de transmisión se reserva durante el establecimiento de conexión y se garantiza durante toda la transmisión.
  - Se acotan los retardos y pérdidas bajo ciertos límites garantizados.
  - Adecuado para audio y vídeo.
- **Tasa de bits disponible** (ABR):
  - La tasa de transmisión varía en función de los recursos disponibles.
    - Siempre se garantiza un mínimo.
  - No se acotan los retardos o pérdidas.
- **Tasa de bits no especificada** (UBR):
  - Solo se transmite cuando el resto de los servicios de la red dejan recursos.
- **Tasa de bits variable** (VBR).
  - Se usan en aplicaciones de tiempo real (VBR-rt) o no en tiempo real (VBR-nrt).

CARACTERÍSTICAS

- **Paquetes pequeños y sencillos** → se llaman **celdas**. Están formados por 53 bytes (5 de cabecera y 48 de datos) para garantizar su conmutación a altas velocidades.
- **Red de CV orientada a conexión** → las celdas llevan en su cabecera su CVI, que los conmutadores buscarán en su **tabla de CV** para colocarlos en la interfaz de salida apropiada.
- **Las celdas llegan en orden** → como todas las celdas de una transmisión siguen la misma ruta, no se adelantan.´
- **No hay ACKs ni retransmisiones**.
- **Control de errores** → las celdas tienen mecanismos de control de errores en la cabecera.

MODELO DE CAPAS ATM

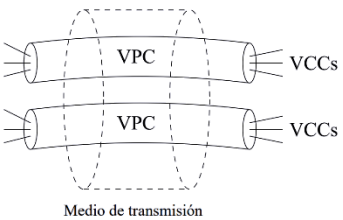


- ATM puede funcionar sobre cualquier capa física.
- Para que ATM funcione bajo varias capas de red, tiene una capa de adaptación a ATM (AAL).
  La AAL será distinta en función de la capa de red que se use.
  - Para TCP/IP → a la entrada de la ATM se fragmentan los datagramas para que quepan en celdas y se reensamblan a la salida.
  - Para audio y vídeo → se agrupan los datos hasta rellenar una celda.

ESTRUCTURA DE LAS CELDAS

ATM contempla dos niveles de conexión:

- Canal virtual (VCC) → circuito virtual normal.
- Camino virtual (VPC) → conjunto de circuitos virtuales con los mismos extremos para facilitar la gestión de los VCCs.



- Hay dos formatos para las celdas, uno para la comunicación usuario-red (entre el origen y el destino) y otro para la comunicación red-red (entre conmutadores).

- **GFC** (control de flujo genérico) (4 bits) → para la QoS.
  - Sólo se usa en la interfaz usuario-red.
- **VPI** (identificador de camino virtual) (8 bits).
- **VCI** (identificador de circuito virtual) (16 bits).
- **Tipo de carga útil** → especifica si la celda es de control (establecimiento o fin de la conexión) o de datos.
  - También indica si se detecta congestión.
- **CLP** (bit de prioridad de la celda) (1 bit).
- **HEC** (byte de control de errores de la cabecera) (8 bits) → es un CRC de 8 bits.