UNIDAD 1 · INTRODUCCIÓN A LAS REDES DE DATOS

RED → conjunto de recursos de comunicaciones e informática que forman un sistema para transportar información.

- El objetivo principal es compartir recursos.

Antes, eran redes separadas → cada red (telefonía, TV por cable y datos) iba por separado.
Ahora, son redes integradas → **convergencia** entre todas las redes → todos los servicios van sobre una misma red.
Las señales digitales permiten integrar todas las redes.

Conforme las redes evolucionan (mainframe, stand alone, LAN, …), la seguridad se va extendiendo en múltiples ámbitos. Los problemas de seguridad pueden aparecer cuando uno no está aislado sino conectado a otra/s red/es.

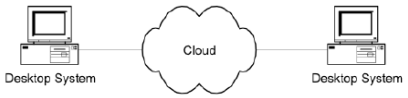
Composición de las redes

- Equipos terminales (DTE) → empleados por los usuarios que requieren disponer de esa red.
- Nodos de red → dispositivos que permiten el transporte de información.
- Enlaces de comunicaciones → vinculan equipos terminales con nodos de red.

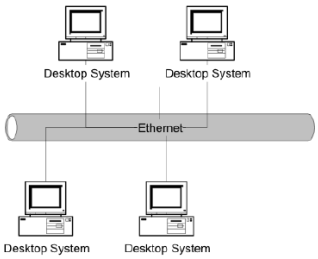
Tipos de redes

Punto a punto

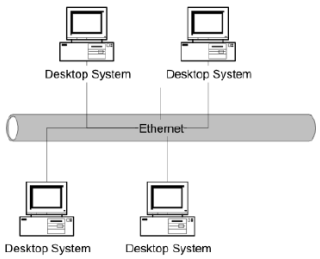
Conmutadas



Difusión multipunto
(punto a multipunto)



Internet
Interconexión entre distintas nubes



Clasificación de las redes

- Según el área geográfica:
  - Áreas locales → LAN (local).
  - Áreas extendidas → MAN (metropolitana), WAN (amplia/extendida) y GAN (global).

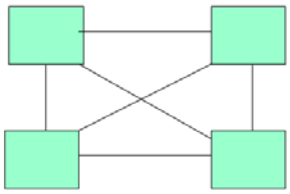
	LAN	**WAN**
Distancias	Cortas.	Grandes.
Velocidades de transmisión	Alta.	Baja.
Calidad de enlaces	Mayor (bajo BER).	Menor (alto BER).
Uso de canales	… de difusión.	… punto a punto.
Seguridad	Mayor (menos vulnerable).	Menor (más vulnerable).
Afectación por restricciones externas	NO se ven afectadas.	SÍ se ven afectadas.
Infraestructura/Recursos	Infraestructura privada.	Recursos públicos.

- Según el ámbito:
  - Públicas → PSDN y PSTN (redes de datos/telefonía de conmutación pública).
  - Privadas → RPV.

- Según modo de operación con conmutación de paquetes:
  - **Con circuitos virtuales (CVs)** → pueden ser CVs permanentes (PVC) o CVs conmutados (SVC).
  - **Con datagramas**.
- Según la tecnología:
  - Analógicas → no hay redes absolutamente analógicas hoy por hoy.
  - Digitales → no hay redes absolutamente digitales hoy por hoy.
- Según el ancho de banda [AB]:
  - Banda angosta → requieren menor AB.
  - Banda ancha → requieren mayor AB.
- Según la parte de la red donde actúa:
  - Red de acceso → interconexión entre centrales (troncales).
  - Red de transporte → interconexión con el usuario, "la última milla".

Topología de las redes → se manejan en Capa Física (1).

Malla

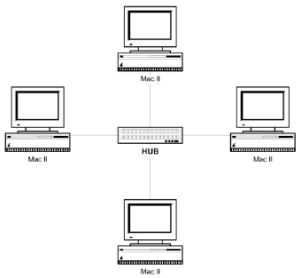


- Más común con pocos nodos.
- La cantidad de enlaces queda determinada por la cantidad de nodos:

$$N_{enlaces} = \frac{n_{nodos} \cdot (n_{nodos} - 1)}{2}$$

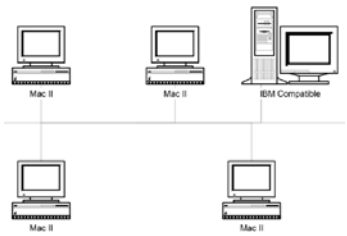
- Tiene mayores costos (debido a los enlaces).

Estrella

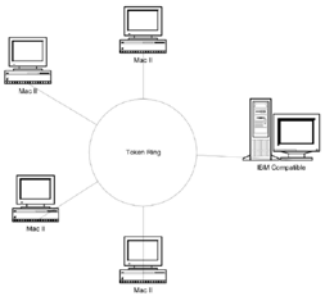


- Más común con muchos nodos → la poca confiabilidad se resuelve agregando redundancia.
- Hay tantos enlaces como terminales.
- Un SWITCH en el medio.

Bus o Lineal



Ring o Anillo



Híbridas
combinación de dos o más de las anteriores.

	Malla	Estrella	Bus o Lineal	Ring o Anillo
Cantidad de nodos	★★★★★	★★	★★★★	★★★★
Cantidad de enlaces necesarios	★★★★★	★★★★★	★	★
Confiabilidad	★★★	★★★	★★★	★
Facilidad de reconfiguración de la red	★★★★★	★	★★★★★	★
Facilidad de localización de las fallas	★	★★★★★	★	★★★★★

Referencias:

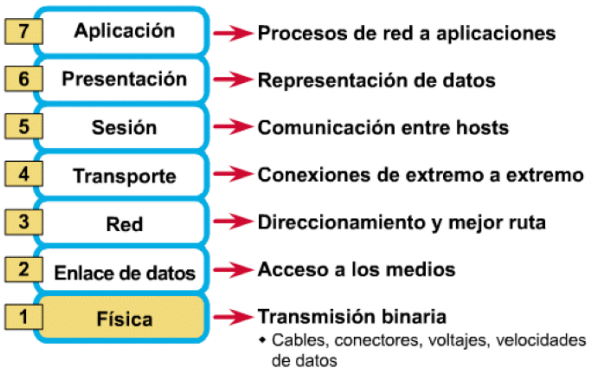
★★★★★ → Alto ★★★★ → Medio-Alto. ★★★ → Medio. ★★ → Bajo/Medio. ★ → Bajo.

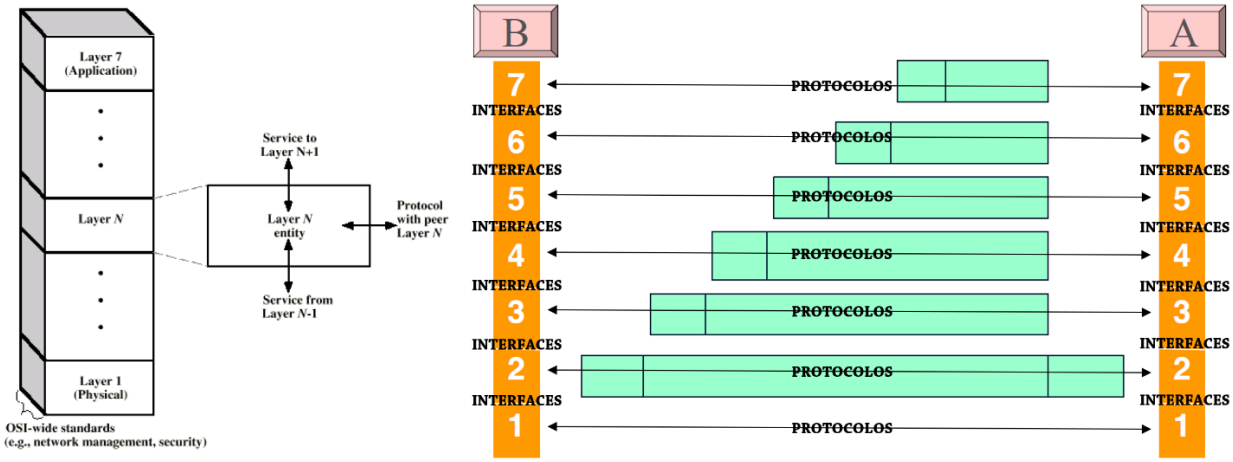
PROTOCOLOS → conjunto de reglas y procedimientos que regulan las comunicaciones entre dos o más dispositivos.

- Permiten intercambiar información entre capas que cumplen las mismas funciones.
- Gobiernan el formato y el significado de los elementos que se intercambian.
- Proveen información de HEADERs y TRAILERs.

HEADER	**PAYLOAD**	**TRAILER**
información de protocolo	*información a transmitir*	*información de protocolo*

Modelo OSI → modelo genérico de capas/niveles.





- Capa N provee servicios a la Capa N+1.
- Capa N accede a los servicios de la Capa N–1.
- El entendimiento entre capas de niveles adyacentes dentro de un mismo sistema es entre **interfaces**.
- El entendimiento entre capas del mismo nivel de distintos sistemas es entre **protocolos**.

Clasificación y características de los protocolos

- Según estructura:
  - Monolíticos → único protocolo.
  - Estructurados → conjunto de protocolos organizados con una estructura de capas.
- Según tipo de enlace o red:
  - Directos → punto a punto.
  - Indirectos → nodos como intermediarios para comunicar
- Según jerarquía:
  - Simétricos → punto a punto.
  - Asimétricos → estructuras jerárquicas (cliente-servidor, por ejemplo).
- Normalizados o no Normalizados:
  - Normalizados → se usa siempre el mismo protocolo para cualquier comunicación.
  - No normalizados → un protocolo para cada comunicación.

Servicios que brindan los protocolos	**Servicios CON conexión (orientados a la conexión)**	**Servicios SIN conexión (orientados a la no conexión)**
Monopolio de recursos	CON y SIN monopolio de recursos.	SIN monopolio de recursos.
Orden de llegada	CON orden de llegada.	SIN orden de llegada.
Encaminamiento	"Como un tubo" → un único camino.	Encaminamiento independiente por cada PDU.
Transferencia	Transferencia libre de errores.	Enfoque: mejor intento.
Modo de operación	CIRCUITO VIRTUAL.	DATAGRAMA.

Siempre que se trabaje con servicios con conexión (orientados a la conexión) es necesario:

Establecer la comunicación → Mantener la comunicación → Liberar la comunicación.

Tipos de conmutación		**Monopolio de Recursos**	**Conexión**
Conmutación de CIRCUITOS		CON	CON
Conmutación de PAQUETES	***modo CIRCUITO VIRTUAL***	SIN	CON
	modo DATAGRAMA	SIN	SIN

Funciones de los protocolos

- Control de flujo de datos → manejo entre terminales para evitar saturar la capacidad de procesamiento/almacenamiento del *buffer*.
- Control de la actividad en el canal de comunicaciones → para que pueda usarse sin problemas.
- Control de errores → garantizan que los bloques de datos lleguen a destino sin errores ni pérdidas.
    - CRC, CheckSum, ARQ (corrección hacia atrás), FEC (corrección hacia adelante), …
- Segmentación y Ensamblado → armado y desamblado de bloques de datos [PDU].
    - Según el tamaño de la PDU, se obtienen distintas características en la comunicación:
        - PDU más chicos → se tarda menos tiempo en enviarlos.
            - Más eficiente en el control de errores.
            - Mejor acceso a las transmisiones → permite que otros usuarios usen el medio.
            - Menos memoria (*buffer*).
            - Menos necesidad de interrupciones → no será necesario interrumpir el uso de un medio para evitar un monopolio de un usuario.
            - Menor eficiencia de transmisión → habrá mayor información relativa, aumentando el tiempo de latencia relativo.
        - PDU más grandes → se tarda más tiempo en enviarlos.
            - Mayor eficiencia de transmisión → habrá menor información relativa, disminuyendo el tiempo de latencia relativo.
            - Si la calidad de los enlaces no es buena, tendré problemas.
- Dar transparencia → garantiza que el uso de los datos agregados (los de protocolo) no afecte los datos originales (los que el usuario desea transmitir).
- Encapsulamiento → agregado de información de control a los datos, sin alterarlos.
    - *En el modelo OSI, se van encapsulando protocolo de capa 7 con el protocolo de capa 6, con el protocolo de capa 5, con el protocolo de capa 4, …*
- Sincronismo de bloque, de carácter o de bit.
- Control de la conexión → establecimiento, transferencia/mantenimiento y cierre/liberación.
- Direccionamiento → niveles, alcance, identificadores de conexión y modos (*unicast*, *broadcast* y *multicast*).
- Multiplexación → varios canales establecidos en un mismo enlace.

Sondeo y Selección → modalidad de trabajo en una red.

- Método para controlar las transmisiones en una línea compartida.

- **Sondeo**
  - La estación primaria [EP] gobierna el medio compartido entre varias estaciones secundarias [ESs].
  - La EP hace un "escrutinio": va consultando (sondeando) quién tiene tráfico…

  Cuando llega a la ES que tiene el mensaje, la EP solicita a la ES su envío.
  Luego, la EP sigue consultando (sondeando).

- **Selección**
  - La EP tiene un mensaje previamente enviado por una ES.
    La EP entrega el mensaje (lo selecciona) al destinatario correspondiente.

Sistema con sondeo y selección

- **[ARQ] Requerimiento automático de repetición:**
  - Es un método de:
    - Detección y Corrección de errores (hacia atrás).
    - Control de flujo.
  - Es punto a punto → se da entre dos estaciones (una EP y una ES).
  - Hace uso de:
    - Confirmación positiva [ACK] y confirmación negativa [NAK].
    - *Time-out*s.
  - Variantes:
    - **<u>ARQ Stop-and-Wait</u>** → se transmite mensaje a mensaje esperando un ACK o un NAK.
      - La operación es half-duplex → no requiere comunicación simultánea.
      - Hay ineficiencia si hay velocidades altas y grandes distancias.
      - Si el paquete es chico → $t_{propagación} > t_{transmisión}$.
        Si el paquete es grande → $t_{propagación} < t_{transmisión}$.
      - [A] envía paquete #1 a [B] → [B] hace detección de errores:
        1. → [B] envía un ACK a [A] → [A] envía paquete #2 a [B].
        2. → [B] envía un NAK a [A] → [A] envía paquete #1 nuevamente a [B].
      - Si luego de cierto tiempo (*time-out*) [A] no recibe ninguna confirmación de [B], entonces [A] asume que se recibió un NAK. Ergo, vuelve a enviar el paquete.
    - **<u>ARQ Sliding Windows</u>** → permite al emisor transmitir múltiples segmentos de información antes de comenzar la espera para que el receptor le confirme (con un ACK) la recepción de los segmentos. Esa validación contiene el número de la siguiente trama que espera recibir el receptor, o bien, el número de la última trama recibida con éxito (ACK **n**, siendo **n** el número de trama en cuestión). Con este aviso, el emisor podrá distinguir el número de envíos realizados con éxito, los envíos perdidos y los envíos que se esperan recibir.
      - Concepto de **<u>ventana</u>** → cantidad de paquetes que puede transmitir A sin esperar recibir conformidad de B:
        1. Se puede trabajar con un tamaño de ventana fijo o variable.
        2. Recibir un ACK permite liberar el *buffer* y deslizar la ventana.
      - Requiere número de paquete.
      - La operación es full-duplex → se requiere comunicación simultánea.

        Piggyback → transmisión de información y recepción de ACK/NAK al mismo tiempo.

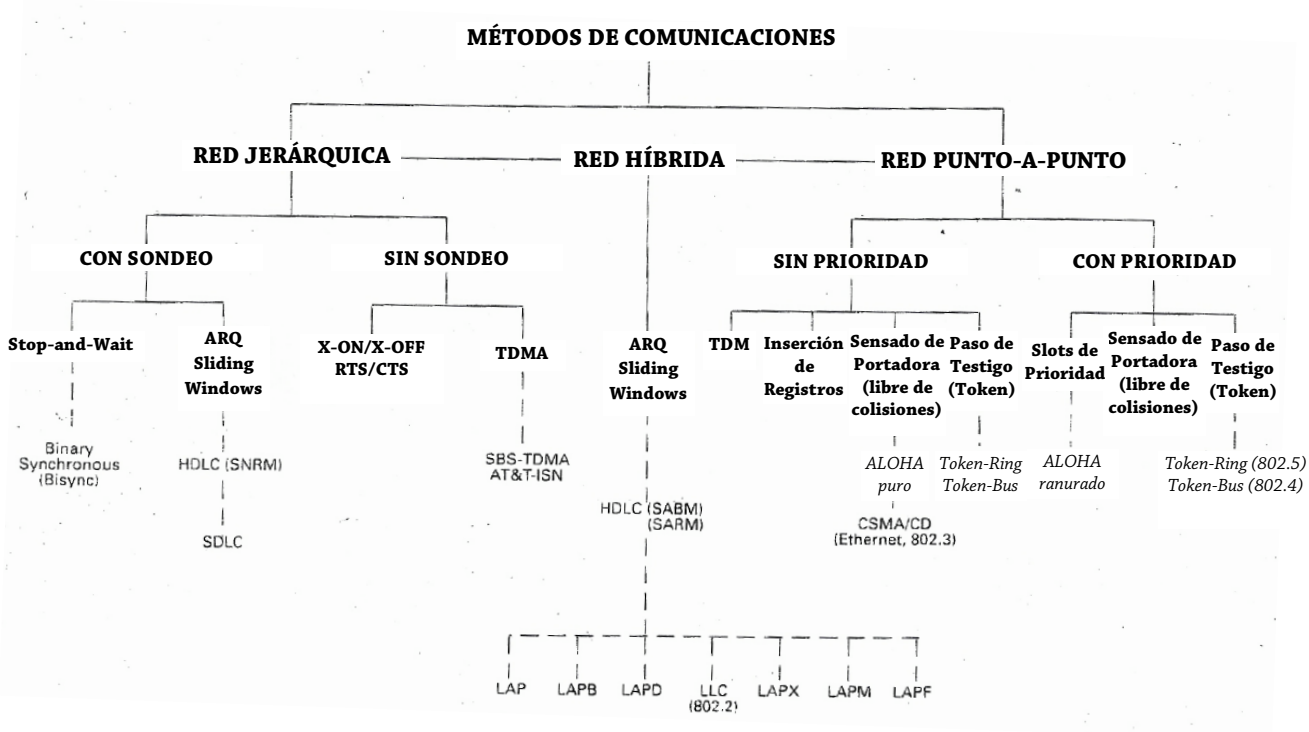
Sistema sin sondeo – Técnicas de control de flujo

- Caracteres de control de flujo (van dentro de códigos normalizados, como el ASCII):
  - **X-ON** → si la estación receptora no tiene *buffer* saturado, envía X-ON al otro extremo.
  - **X-OFF** → si la estación receptora tiene *buffer* saturado, envía X-OFF al otro extremo.
- Señales de interfaces digitales (método fuera de banda):
  - **RTS (*Request To Send*)** → el DTE requiere enviar algo al DCE.
  - **CTS (*Clear To Send*)** → el DCE envía un ACK al DTE.
- TDMA → método de acceso → acceso múltiple por división de tiempo.
  - TDM → método de multiplexación (por división de tiempo).

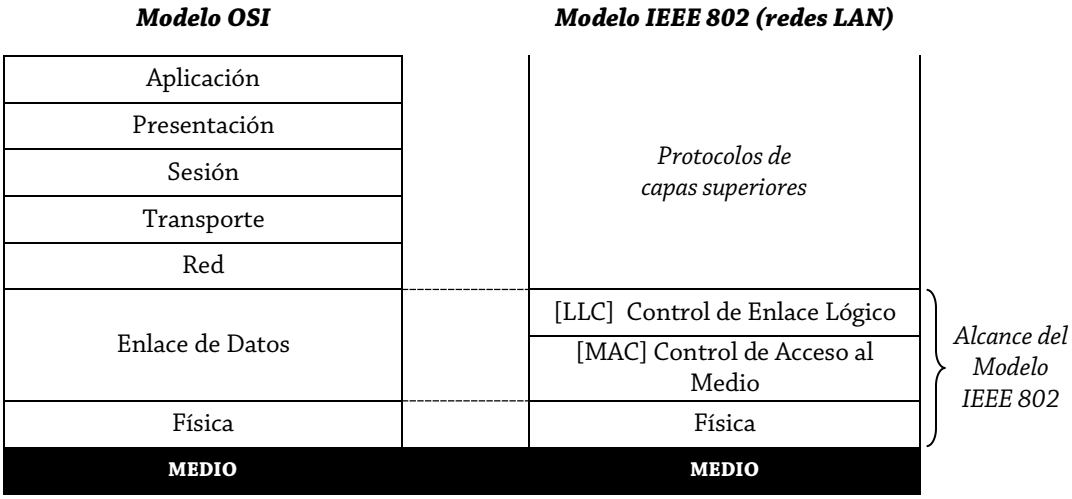
Sistema con manejo de prioridad

CON prioridad de uso del canal	SIN prioridad de uso del canal
Aloha ranurado.	Aloha puro/aleatorio.
Sensado de portadora.	
Paso de testigo/token.	

Clasificación de las redes según métodos de comunicación



UNIDAD 2 · LAN



Las subcapas LLC y MAC cubren, de alguna manera, las funciones que cubre el protocolo HDLC.

Los **protocolos de LAN** dependen:

- Según capa que se trate.
- Según el método de acceso al medio (*Contention*/Aleatorio o *Token Passing*/determinístico/secuencial).
- Según el medio de transmisión y la topología de red.

Placa de Red

- DCE por defecto.
- Componentes genéricos:
    - o <u>Controladora:</u>
        - Formateo de tramas (PDU de Capa 2).
        - Generación de FCS (Frecuencia de Control de Trama) → alguna técnica de detección de errores como CRC.
        - Sincronismo de bit → *clock* de transmisión y recepción.
        - Codificación → código de línea (Manchester o Manchester Diferencial).
    - o <u>Transreceptor:</u>
        - Modula/Demodula.
        - Sensado de la señal portadora:
            - El transreceptor detecta la señal portadora y luego, cuando se transmite información, detecta la señal modulada. Se alerta a todo el sistema para: recibir información, o bien, saber si el canal está ocupado:
                1. Si se escucha la portadora → el canal está ocupado.
                   Si no se escucha la portadora → el canal no está ocupado.

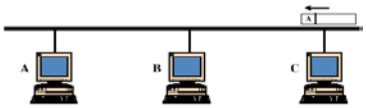
                   Señal portadora → no tiene información.
                   Señal modulada → sí tiene información.
        - Detección de colisiones:
            - Colisión → tipo de ruido que se superpone a la señal útil
            - Colisión → interferencia producida cuando dos o más estaciones de trabajo quieren usar el medio y colocan una trama.
              Si hay dos o más tramas dando vuelta en el medio, en algún momento colisionarán, generando una interferencia (reflexión por colisión) que se difunde por el medio.
- Según el protocolo usado, se puede tener sincronismo de bloque o de carácter.
  El sincronismo de bit está en todo tipo de protocolo.

Dirección MAC

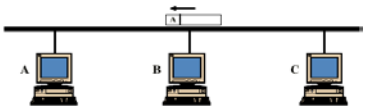
- Dirección física impregnada en el hardware o en la electrónica del dispositivo de red.
- Identifica unívocamente al dispositivo → cada interfaz tiene una dirección MAC.
- Son 48 bits repartidos en 6 grupos de 2 dígitos hexadecimales cada uno.
  Formato → `F0:E1:D2:C3:B4:A5`.
  Los primeros 24 bits identifican al fabricante. Los últimos 24 bits identifican a cada placa de red del fabricante.
- Dirección de broadcast (dirección especial: son todos `1`s) → `FF:FF:FF:FF:FF:FF`.
  - Permite la transmisión de datos simultánea a una multitud de nodos receptores en una misma subred
  - Útil cuando se desconoce la dirección MAC de destino.

Topología de LAN

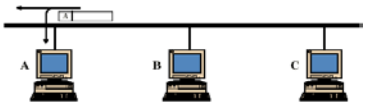
Bus o Lineal



***C** transmite una trama dirigida a **A**.*

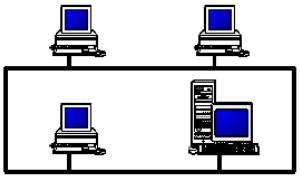


***B** ignora la trama (no está dirigida a ella).*

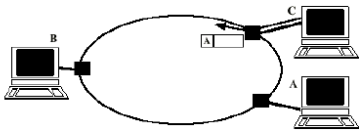


***A** copia la trama.*
La trama continúa su camino…

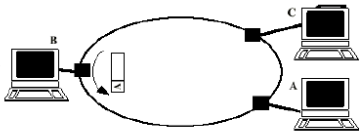
Ring o Anillo



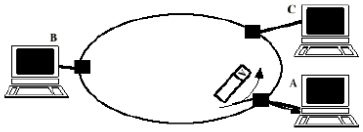
Paso de testigo:
Una vez que transmitió **C**, **C** le pasa el *token* a **B**, quien ahora, tiene el permiso para transmitir.
Luego de transmitir **B**, **B** le pasará el *token* a **A** y así…



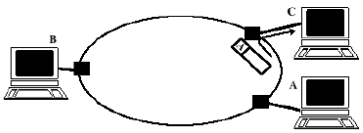
***C** transmite una trama dirigida a **A**.*



***B** ignora la trama (no está dirigida a ella).*

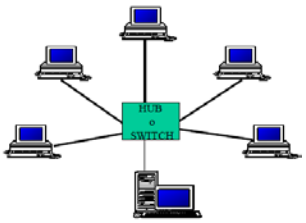


***A** copia la trama.*
La trama continúa su camino…

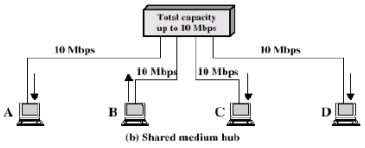


***C** absorve la trama inicialmente enviada.*

Estrella



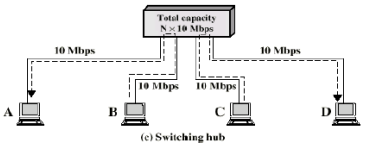
Estrella con HUB (Capa 1)



***B** transmite una trama.*
*El HUB reenvía la trama recibida a todos los puertos, por lo que la trama llega a todas las estaciones: **A**, **B**, **C** y **D**.*
Solamente la estación destinataria copia la trama (porque sí la usará).

- Se puede enviar hasta 1 única trama simultáneamente.
- $v_{máx\ Tx} = 10MBps$ *en este caso.*

Estrella con SWITCH (Capa 2)



***B** transmite una trama dirigida a **A**. El SWITCH recibe la trama y la direcciona solamente a **A**.*
*Análogamente, sucede lo mismo con **C** y **D**.*

- Se puede enviar tantas tramas simultáneamente como la mitad de la cantidad de puertos del SWITCH.
- $v_{máx\ Tx} = 20MBps$ *en este caso.*

Se puede tener físicamente una topología pero lógicamente es otra topología.

CAPA FÍSICA → Capa 1 del Modelo OSI y del Modelo IEEE 802 (redes LAN).

- Codifican y Decodifican → decide qué códigos de línea se usarán.
- Generan y eliminan preámbulo → el transmisor lo genera, el receptor lo elimina.
    - Preámbulo → forma parte del HEADER de la trama y brinda sincronismo de bloque.
- Transmiten y Reciben bits.
- Medios de transmisión utilizados:
    - Par trenzado → UTP (cableado estructurado) y STP.
    - Cable Coaxil → fino (mayor atenuación, menor alcance) y grueso (menor atenuación, mayor alcance).
    - Fibra Óptica → monomodo y multimodo (escalonado y gradual).
    - Inalámbrico → ondas electromagnéticas.

SUBCAPA MAC · CONTROL DE ACCESO AL MEDIO → Capa 2 del Modelo OSI y del Modelo IEEE 802 (redes LAN).

- Nombre PDU → **trama MAC**.
- Ensambla (Tx) y desensambla (Rx) tramas.
- Detecta errores (CRC).
- Maneja direcciones MAC.
- Procedimiento de control → centralizado o distribuido.
- Técnicas de Control de Acceso al Medio:
    - Síncronas (fijas).
    - Asíncronas (dinámicas):
        - Rotación Circular (*Token Passing*) o **Paso de Testigo** → secuencial/determinístico.
            - Adecuada cuando muchas estaciones generan tráfico.
        - Reserva:
            - Da cierto lapso de tiempo para transmitir (ranuras).
            - Adecuada cuando el tráfico es continuo.
        - **Contienda** (*Contention*) → aleatorio.
            - Adecuada cuando el tráfico es por ráfagas.

SUBCAPA LLC · CONTROL DE ENLACE LÓGICO → Capa 2 del Modelo OSI y del Modelo IEEE 802 (redes LAN).

- Nombre PDU → **PDU LLC**.
- Interfaz con capas superiores.
- Opcionalmente corrección de errores (mediante retransmisión) → uso de ARQ.
- Opcionalmente control de flujo → uso de técnicas como X-ON/X-OFF y RTS/CTS (son señales eléctricas).
    - El control de flujo se lleva a cabo entre las terminales, para evitar el problema de la capacidad de almacenamiento de los *buffers* y, así, no sobrescribir información.
    - El control de congestión se lleva a cabo en los nodos pertenecientes a la nube.
- Maneja direccionamiento en LLC (no MAC) → determina usuarios origen y destino que son protocolos en la capa superior.
- **Servicios** que brinda:
    - **No orientados a la conexión, sin confirmación** (datagrama) → más rápido, pero poco confiable.
    - **No orientados a la conexión, con confirmación** (datagrama confirmado, sin conexión lógica).
        - Cuando es con confirmación puede ser:
            - Sin avisar si llegó bien o no → solamente "*llegó*".
            - Avisando si la trama llegó bien o no → ACK ("*llegó bien*") o NAK ("*llegó mal*").
    - **Orientados a la conexión** (lógica, control de flujo y errores) → más lento, pero más confiable.

Formato genérico de una trama MAC y una PDU LLC

Trama MAC

Dirección MAC del Destino	Dirección MAC del Origen	Campo de Control MAC	**PDU LLC (*PAYLOAD*)**	CRC

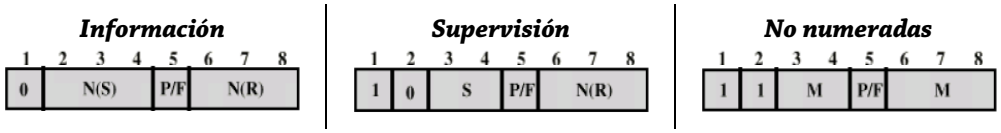
*La **PDU LLC** está encapsulada en la **trama MAC**.*

PDU LLC

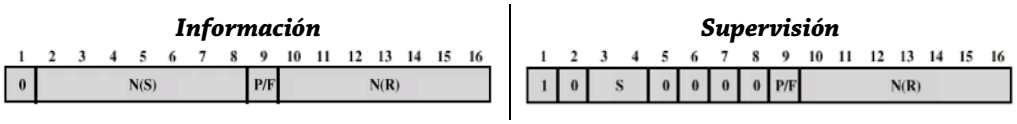
1 octeto	*1 octeto*	*1 octeto o 2 octetos*	*variable*
Dirección del Destino	Dirección del Origen	Campo de Control LLC	**Información (*PAYLOAD*)**

De acuerdo al servicio usado, el Campo de Control LLC puede tener 1 octeto o 2 octetos:

- 1 octeto (8 bits):
  - **Servicio no orientado a la conexión, sin confirmación**.
  - Hay 3 tipos de PDU LLC:



- 2 octetos (16 bits) → amplía cantidad de bits para numerar secuencias de envío y recepción.
  - **Servicio con conexión**.
    Servicio no orientado a la conexión, con confirmación.
  - Hay 2 tipos de PDU LLC:



Referencias:

- *N(S)* *Número de secuencia de envío.*
- *N(R)* *Número de secuencia de recepción.*
- *S* *Mensaje de información.*
- *M* *Mensajes específicos de bloques sin numeración.*

Normas LAN IEEE

Capas/Subcapas		***Técnicas de Acceso al Medio***				
		CSMA/CD	***Token-Bus***	***Token-Ring***	***WLAN CSMA/CA***	***Prioridad de Demanda***
Capas superiores		802.1				
2	*LLC*	802.2				
	MAC	802.3	802.4	802.5	802.11	802.16
1	*Física*	Coaxil fino/grueso. UTP.	Coaxil.	STP.	Radio. Wi-Fi.	Wi Max

Una **colisión** se produce cuando dos estaciones sensan canal desocupado y transmiten tramas simultáneamente.

Parámetros de análisis que determinan tamaños y longitudes de tramas para que las redes sean operativas:

- **Tiempo de propagación entre estaciones** → ligado a la distancia entre estaciones.
  RTT (*Round Trip Time*) → tiempo de ida y vuelta entre estaciones transmisora y receptora.

$$\mathrm{RTT} = 2 \cdot \mathrm{T}_{\mathrm{propagación}}$$

  $\mathrm{RTT}_{\mathrm{máx}}$ (*Round Trip Time* máximo - ventana de colisión) → tiempo de ida y vuelta de extremo a extremo.
- **Tiempo de transmisión de trama** → ligado a la cantidad de bits que tiene la trama.

$$\mathrm{T}_{\mathrm{propagación}} \sim P_{(colisión)} \qquad RTT \sim P_{(colisión)} \qquad \mathrm{T}_{\mathrm{transmisión}} \sim \frac{1}{P_{(colisión)}}$$

Dominio de colisión → área de red donde se propagan las colisiones producidas por ocupación del medio en forma simultánea por varios hosts.

Dominio de *broadcast* → área de red donde se propagan las tramas de difusión o *broadcast*.

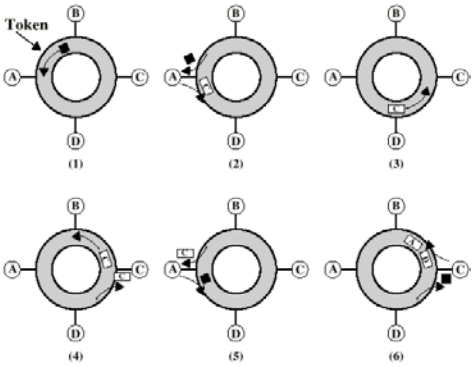
PROTOCOLOS DE ACCESO AL MEDIO → arbitran el uso del canal de difusión.

- **Contienda (aleatorio)** → los dispositivos "pelean" entre sí para acceder al medio.
  - **Aloha puro**:
    - No sensa ocupación del canal → el usuario transmite cuando quiere.
    - Detecta colisiones.
      En caso de darse una colisión, el usuario tendrá que esperar para volver a transmitir.
    - Menos eficiente → más probabilidades de colisión.

    Aloha ranurado:
    - Surge para solucionar el problema de la eficiencia del Aloha Puro.
    - Se establecen ranuras de tiempo dentro de cada cual solamente un usuario podrá transmitir.
      Cada usuario tendrá su ranura de tiempo para él solo.
    - Más eficiente → menos probabilidades de colisión.
  - CSMA → sensa permanentemente presencia de portadora en el medio para poder acceder:
    - Si el medio no está ocupado, se toma el medio.
    - Si el medio está ocupado, se establecen métodos respecto de persistencia
      - Persistente → espera un número entero de $\mathrm{RTT}_{\mathrm{máx}}$ para sensar.
      - No Persistente → no sensa continuamente el medio.
        Si está ocupado, espera un tiempo aleatorio.

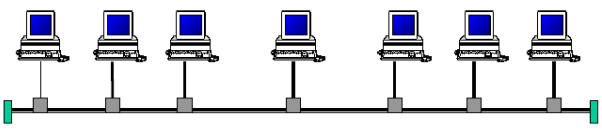
    CSMA/CD → además de sensar señal portadora en el medio para poder acceder, detecta colisiones.
    - Detecta colisiones mediante un algoritmo exponencial binario.
      Si detecta colisión, aborta transmisión y transmite señal de aviso de colisión.
      Espera un tiempo aleatorio para volver a transmitir.

    CSMA/CA → además de sensar señal portadora en el medio para poder acceder, evita colisiones.
    - Usa varias técnicas para evitar colisiones (una de ellas es la posicional, que establece prioridades de acuerdo a posiciones de las estaciones).
- **Paso de Testigo (determinístico/secuencial)**:
  - No se producen colisiones.
  - Monopoliza el medio mediante el uso de un *token* o testigo de control (trama pequeña que va circulando de manera secuencial y se va a ir pasando de un DTE a otro DTE).
    Únicamente se puede transmitir información si se tiene el *token*.
    Luego de transmitir información, se libera (se pasa) el *token* para que otro DTE tenga acceso.
  - Tipos:
    - **Token-Ring (IEEE 802.5)** → topología bus/lineal → acceso secuencial:



1. Se pasa el *token* a **A**.
2. **A** recibe el *token* (ahora sí puede transmitir) y envía la trama dirigida a **C**.
3. **D** ignora la trama (está dirigida a **C**).
4. **C** copia la trama y ésta sigue su camino.
5. La trama llega a **A** (quien la envió inicialmente) y le pasa el *token* a **D**. Pero **D**, como no tiene nada que transmitir, ignora el *token*.
6. **C** recibe el *token* y luego transmite…

    - **Token-Bus (IEEE 802.4)** → topología ring/anillo → acceso por difusión:



Se establece un anillo lógico entre los DTE.
El *token*/testigo se pasa a través del bus por el anillo lógico → todos reciben las tramas.
El DTE espera el *token* para transmitir una trama.
El DTE transmite todas las tramas y le pasa el *token* al DTE sucesor:

- Si recibe una trama, supone que todo está bien.
- Caso contrario, tiene que adoptar acciones correctivas.

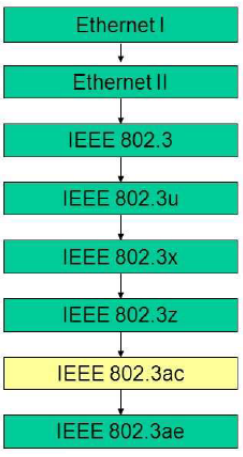
DISPOSITIVOS

- Capa 1 (Física) → **REPETIDOR** y **HUB**:
  - Al recibir una señal digital atenuada, primero la recomponen y luego la replican en cada puerto.
    No tienen inteligencia (no almacenan/procesan/reconocen) → sólo recomponen y replican señales.
  - Propagan tanto colisiones como *broadcast* MAC.
  - REPETIDOR → tiene 2 puertos.
    HUB → tiene N puertos.
- Capa 2 (Enlace de Datos) → **BRIDGE** y **SWITCH**:
  - Permiten establecer comunicaciones entre un puerto y otro (y no entre un puerto y todos los demás puertos, como hace un REPETIDOR o un HUB).
  - Almacenan tablas de direcciones MAC asociadas a cada puerto, posibilitando tales comunicaciones.
  - Almacena y hace control de errores antes de retransmitir tramas MAC.
  - Permiten interconectar una red LAN con otra red LAN.
  - No propagan colisiones, pero sí propagan *broadcast* MAC.
  - Al conectar varios SWITCHes entre sí, pueden aparecer problemas de bucles e inundación de tramas.
  - BRIDGE → tiene 2 puertos.
    SWITCH → tiene N puertos.
  - Tipos de SWITCHes:
    - *Store and Forward* → almacena tramas completas y reenvía.
      - Confiable.
    - *Cut Through* → fragmenta tramas a enviar.
      - No detecta tramas con errores.
      - Reduce latencia → es más rápido.
      - Variante: *Fragment Free* → no fragmenta tramas.
    - *Adaptive Cut Through* → modo adaptativo compatible con ambos (*Store and Forward* y *Cut Through*), según convenga.
- Capa 3 (Red) → **ROUTER**:
  - Tienen capacidad de enrutamiento o encaminamiento de paquetes.
  - Permiten interconectar redes LAN con redes WAN.
  - No propagan colisiones.
  - Limitan *broadcast* de MAC (Capa 2), pero no *broadcast* de IP (Capa 3).

Redes con CSMA/CD

- Evolución de las normas:
  - Ethernet DIX 1.0/2.0 → más antigua.
  - IEEE 802.3 → actual, en uso.
- Usan la misma tecnología de conectividad física.
- Conformación de la placa de red o interfaz:
  - Controladora → dsadsdas.
  - Transreceptor → modula/demodula.
- El formato de trama MAC sólo difiere en un campo.

Evolución de Ethernet



Tramas Ethernet y IEEE 802.3

$$\text{Tamaño máximo de la PDU} = 1518\text{B}$$
$$64\text{B} \leq \text{Tamaño total de trama} \leq 1518\text{B}$$

8B	6B	6B	2B	46B a 1500B	4B
Preámbulo	**Dirección Origen**	**Dirección Destino**	**Tipo/Longitud de Trama**	**Información (PAYLOAD)**	**Frecuencia de Control de Trama**

En el tamaño total de la trama no se contabiliza al preámbulo porque es de Capa 1.

- *Preámbulo Ethernet II* → `10101010`.
  Preámbulo IEEE 802.3 → `10101011` → el último bit (SFD, Secuencia Diferenciada) es un `1`, se usa para mejorar el sincronismo de bloque.
- Dirección Origen.
- Dirección Destino.
- Ethernet II → Tipo de Trama → qué tipo de información tiene cargada (por capa superior).
  IEEE 802.3 → Longitud de Trama → depende del PAYLOAD, dado que es un campo variable.
- Información (PAYLOAD) → campo de información.
  Si el tamaño de la trama es menor a 46B, se puede agregar un campo de relleno para alcanzar tal valor.
  Hay que evitar que las tramas sean cortas para evitar tanto $\mathrm{T}_{\text{transmisión}}$ bajos como $\mathrm{T}_{\text{propagación}}$ altos, lo cual aumentaría la probabilidad de colisiones.
- FCS · Frecuencia de Control de Trama → CRC-32 → alcanza a todos los campos menos al preámbulo, el cual (al igual que el propio FCS, no se tiene en cuenta para su cálculo).

Códigos de Línea

- Código Manchester Bifase:
  - Siempre hay transición en la mitad del intervalo.
    En las transiciones (en la mitad de cada intervalo) está la información:
    - 0 → transición de arriba hacia abajo.
    - 1 → transición de abajo hacia arriba.
  - Usado en redes *Ethernet*.
- Código Manchester Bifase Diferencial:
  - Siempre hay transición en la mitad del intervalo.
    Si se transmite:
    - 0 → hay otra transición en el inicio del intervalo (hay dos transiciones en total).
    - 1 → no hay transición en el inicio del intervalo (sólo hay una transición: en la mitad).
  - Usado en redes *Token-Ring*.

Detección de Colisiones

Algoritmo exponencial binario

- Permite gestionar cuándo y cómo reintentar acceder al medio en caso de detectarse colisiones.
- Fórmula y ejemplo:
- $Colisión: i \rightarrow Número\ de\ ranuras\ entre\ 0\ y\ (2^i - 1).$
  $Red\ a\ 10\ Mbps \rightarrow Ranura\ de\ tiempo\ de\ espera = 51{,}2\ \mu s.$
  $Red\ a\ 100\ Mbps \rightarrow Ranura\ de\ tiempo\ de\ espera = 5{,}12\ \mu s.$
  $Cantidad\ máxima\ de\ ranuras = 1023.$
  La 1ra colisión se elige un número de ranura en forma aleatoria entre 0-1 (1 ranura).
  La 2da colisión se elige un número de ranura en forma aleatoria entre 0 y 3 (3 ranuras: 0-1, 1-2 y 2-3).
- Cada estación tiene un contador de intentos, que se pone en 0 cuando consigue transmitir una trama.
- A mayor cantidad de ranuras → menor probabilidad de colisión → mayor tiempo de espera.

Tipos de Ethernet Básica

- 10B2 · Cable Coaxil Fino:
    - A menor sección transversal → mayores resistencia y atenuación.
    - Topología → bus/lineal.
    - Conector → T-BNC.
      Tarjeta de red → incluye controladora y transreceptor.
    - Longitud máxima → 185m por segmento.
      Cantidad máxima de nodos por segmento → 30.
      Cantidad máxima de repetidores → 3 → 4 segmentos máximo.
      Longitud máxima de todo el segmento → 740m = 4 segmentos de 185m cada uno.
    - Menos costoso, más flexible.
- 10B5 · Cable Coaxil Grueso:
    - A mayor sección transversal → menores resistencia y atenuación.
    - Topología → bus/lineal.
    - Conector → Vampiro, que incluye transreceptor.
      Tarjeta de red incluye controladora.
    - Usa interfaz AUI (cable con conector DB15) entre controladora y transreceptor → 50m máximo.
    - Longitud máxima → 500m por segmento.
      Cantidad máxima de nodos por segmento → 100.
      Cantidad máxima de repetidores → 4 → 5 segmentos máximo.
      Longitud máxima de todo el segmento → 2500m = 5 segmentos de 500m cada uno.
    - Máximo → 500m por segmento.
    - Más costoso, menos flexible.
- 10BT · Par Trenzado NO Blindado UTP → cableado estructurado (normas EIA/TIA 568 y 570):
    - Topología → estrella.
    - Conector → RJ-45.
      Tarjeta de red incluye controladora y transreceptor.
    - Cantidad máxima de repetidores → 4 (se pueden tener hasta 4 HUBs en cadena).
    - UTP 100 Ω:
        - Cat. 5 → actual → ancho de banda hasta 100 MHz (extiende hasta 100 Mbps).
        - Cat. 7 → actual → ancho de banda hasta 600 MHz (extiende hasta 10 Gbps).
        - Cat. 8 → futuro → ancho de banda hasta 1200 MHz (extiende hasta ¿40 Gbps?).
    - Menos costoso, más flexible.
    - El par trenzado se puede compartir con telefonía → de los 4 pares: 1 par se usa para transmitir datos, 1 par para recibir datos, quedando disponibles 2 pares para telefonía.
- 10 B-F · Fibra Óptica:
    - Hace uso de un par de cables de fibra por cada enlace.
    - Tipos:
        - 10 B-FP → estrella pasiva, con 1km por segmento.
        - 10 B-FL → enlace punto a punto entre estaciones/repetidores, a 2km máximo.
        - 10 B-FB → troncal → enlace punto a punto entre repetidores, a 2km máximo.

LAN de Alta Velocidad

- Ethernet Conmutada → no hay difusión a todos los integrantes del segmento.
  - Cada puerto constituye un dominio de colisión separado → no se producen colisiones.
  - El HUB/SWITCH aprende direcciones MAC para cada puerto, armando una tabla de ruteo.
  - No es necesario competir para acceder al medio compartido.

- Fast Ethernet → 100 Mbps.
  - El objetivo es aumentar la velocidad, manteniendo el cableado, MAC y los formatos.
  - IEEE 802.3 → 100BT4 (UTP3).
    IEEE 802.3 → 100B-TX (UTP5 o STP) y 100B-FX (FO).
  - Full-Duplex en lugar de Half-Duplex → duplicación teórica de la velocidad de transmisión.

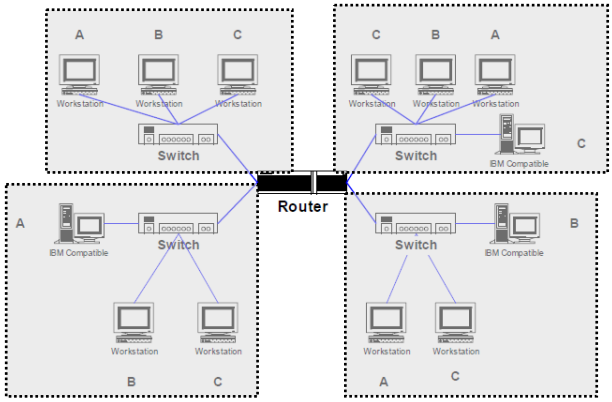
- Gigabit Ethernet → 802.3Z de 1 Gbps.
  - Opción 1000 B-SX → FO multimodo: 275m o 550m.
    Opción 1000 B-LX → FO: multimodo 550m o monomodo 5km.
    Opción 1000 B-CX → cable de cobre (unión PC-tablero), 25m.
    Opción 1000 B-T → cable UTP cat. 5 (pares no apantallados), 1000m.

- 10 Gigabit Ethernet → incremento del tráfico respecto de Gigabit Ethernet.
  - Uso de FO.
  - Modo Full-Duplex exclusivamente.
  - Distancias desde 300m hasta 40km.
  - Opción 10 G B-S → FO multimodo (850nm, 1ra ventana), hasta 300m.
    Opción 10 G B-L → FO monomodo (1310nm, 2da ventana), hasta 10km.
    Opción 10 G B-E → FO monomodo (1550nm, 3ra ventana), hasta 40km.
    Opción 10 G B-LX4 → FO monomodo o multimodo (1310nm, 2da ventana), hasta 10km.

- FDDI · Interfaz de Datos Distribuidos por FO:
  - Topología → doble anillo → si se llegara a caer una estación, se puede "puentear" (cerrar el lazo) para mantener la red. Es decir: se pasa de un doble anillo a un anillo simple.
  - Velocidad → 100 Mbps.
  - Longitud total → 100km.
  - Máxima cantidad de estaciones → 50.

VLAN (LAN Virtual) → asociación lógica de estaciones que componen una LAN, para reducir la difusión en la red.

- En el ejemplo de la imagen se ven 4 LAN físicas y 3 VLANs (asociando puertos)
- Cada VLAN es un dominio de *broadcast*.
- Tales asociaciones lógicas se pueden hacer de distintas maneras:
  - Por puertos (Capa 1).
  - Por direcciones MAC (Capa 2, Subcapa MAC).
  - Por tipo de protocolo (Capa 2, Subcapa LLC).
  - Por direcciones IP (Capa 3).
  - Por aplicaciones (Capas superiores).



- Protocolo IEEE 802.1Q → múltiples redes pueden compartir un enlace (modo *trunk*).
  Protocolo IEEE 802.1D → incluye el protocolo STP (*Spanning Tree Protocol*).
  - Impide bucles que se generan en los BRIDGEs/SWITCHes, por haber vínculos redundantes.
  - Transforma una red física de tipo malla con bucles en una red tipo árbol libre de bucles.

UNIDAD 4 · LAN INALÁMBRICAS

Aplicaciones LAN inalámbricas

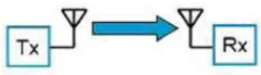
- Ampliaciones de redes → empleo de *Access Points* (APs) para aumentar alcance.
- Interconexión de edificios → uso de radioenlaces punto-a-punto que une redes LAN.
- Acceso nómade → acceso temporal de no todos los servicios que permite el acceso a un dispositivo móvil.
- Trabajo en red *ad-hoc* → sin servidor central, punto-a-punto.

Requisitos (aspectos a considerar) de LAN inalámbricas

- Rendimiento → capacidad para dar servicio.
- Cantidad de nodos → la cantidad es limitada → si están todos los canales ocupados, no se podrá acceder.
- Conexión a la LAN troncal (*backbone*).
- Área de cobertura → la potencia de la señal depende de las condiciones climáticas, de los horarios y de la presencia de obstáculos.
  La atenuación afecta la $v_{transmisión}$.
- Consumo de batería → asociado a la telefonía móvil, que forma parte de una red de datos.
- Robustez en la transmisión y seguridad (confidencialidad).
- Funcionamiento de redes adyacentes → convivencia entre varios APs.
- Funcionamiento sin licencia → se deben usar los canales habilitados por el ENACOM (hay con y sin licencia).
- Traspaso (*Handoff*) → cambio de celda (de una frecuencia) a otra adyacente a ella
  Itinerancia (*Roaming*) → cambio de una red a otra.

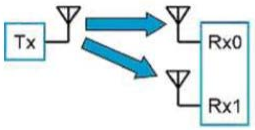
Tecnología de radio SISO, SIMO, MISO y MIMO

SISO
1 entrada, 1 salida.



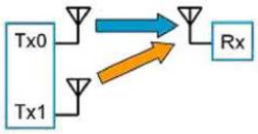
Transmisor	Receptor
1 antena.	1 antena.

SIMO
1 entrada, N salidas.



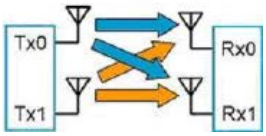
Transmisor	Receptor
1 antena.	N antenas.

MISO
N entradas, 1 salida.



Transmisor	Receptor
N antenas.	1 antena.

MIMO
N entradas, N salidas.



Transmisor	Receptor
N antenas.	N antenas.

Tecnologías inalámbricas para transmisión de datos

	WPAN	WLAN	WMAN y WWAN	WRAN
Nombre	**Bluetooth**	**WiFi**	**Wi Max**	**-**
Estándar	IEEE 802.15	IEEE 802.11	IEEE 802.16	IEEE 802.22
Banda	2,4 GHz.	2,4 GHz. 5,8 GHz.	2,3 GHz a 3,5 GHz.	54 MHz a 862 MHz.
Velocidad máxima	1 Mbps a 24 Mbps.	11 Mbps a 54 Mbps.	54 Mbps.	23 Mbps.
Alcance	10m.	~50m	60km.	33km ~ 100km.
Técnica y Método de Modulación	SS-FH. GFSK.	SS-FH y SS-DS.	-	OFDMA. Sin licencia.

Medios de comunicación inalámbrica – Tecnologías LAN inalámbricas

- De Infrarrojos → ondas electromagnéticas del espectro infrarrojo, próximas a la luz visible
  Puede ser: un haz dirigido, omnidireccional, o bien difusión (usando un reflector).

- **Radio por Espectro Expandido/Ensanchado (*Spread Spectrum* · SS):**
  - Usa un código denominado secuencia de expansión (pseudoaleatoria o pseudoruido) tanto en el transmisor como en el receptor.
  - Procedimiento:
    - En el transmisor se hace una expansión del espectro.
      - Cuando se combinan la señal original (la que contiene información) con la señal pseudoaleatoria, sale la señal modulada con el espectro expandido.
    - En el receptor se hace una compresión del espectro.
      - Se recibe la señal útil con el espectro expandido, la interferencia y la señal pseudoaleatoria.
      - La señal recupera su ancho de banda original.
        La interferencia amplía su ancho de banda → pero mediante filtros se puede eliminar el ruido, prevaleciendo la señal que interesa.
  - Provee seguridad en las comunicaciones → baja detectabilidad y capacidad de encripción.
    Todo procesamiento realizado con un código X sólo podrá ser recibido por quien tiene ese código X.
  - Permite varios usuarios en el mismo ancho de banda, con pocas interferencias.
    - CDM → muchos usuarios pueden usar el mismo canal y la misma frecuencia.
  - Uso difundido en Bluetooth y WiFi.
  - Hay dos técnicas para expandir el espectro:
    - **Secuencia Directa (*Direct Sequence* · SS-DS):**
      - Se expande el espectro y se vuelve al formato original.
    - **Salto de Frecuencia (*Frequency Hopping* · SS-FH):**
      - Es el mismo espectro, sólo que "se hace saltar" la frecuencia.
      - El atacante no puede interceptar una comunicación ya que la frecuencia está saltando permanentemente. La única manera de seguir los saltos es teniendo el mismo código pseudo-aleatorio que ya tienen el transmisor y el receptor.

- Radio de banda estrecha (microondas) → radioenlaces.
  Pueden ser: con licencia del ENACOM → banda 18 GHz, mayor alcance.
  sin licencia del ENACOM → menor 5,8 GHz, menor alcance

Bluetooth · IEEE 802.15 · WPAN → protocolo de bajo costo y poco alcance que depende de la clase/potencia.

Clase	Potencia Máxima permitida	Alcance
1	100 mW = 20 dBm.	~ 100m.
2	2,5 mW = 4 dBm.	5m a 10m.
3	1 mW = 0 dBm.	~ 1m.
4	0,5 mW = 0 dBm.	~ 0,5m.

Versión	Velocidad de Transmisión
1.2	1 Mbps.
2.0 +EDR	3 Mbps.
3.0 +HS	24 Mbps.
4.0	32 Mbps.
5	50 Mbps.

- Puede usar 23 o 79 canales (según el ente de comunicaciones de cada país) para los saltos de frecuencia (FH).
- Cantidad máxima de dispositivos → 8.
- Automatización de la conexión → código PIN para identificación inicial.
- Evita problemas de acople de señales de radio → usar cables para conectar parlantes en un sistema de audio puede provocar que se acoplen señales de audio, lo cual sucede porque el cable actúa como una antena.
- Puede recibir ataques por *bluejacking* → en los dispositivos Bluetooth se reciben mensajes anónimos.

WiFi · IEEE 802.11 · WLAN

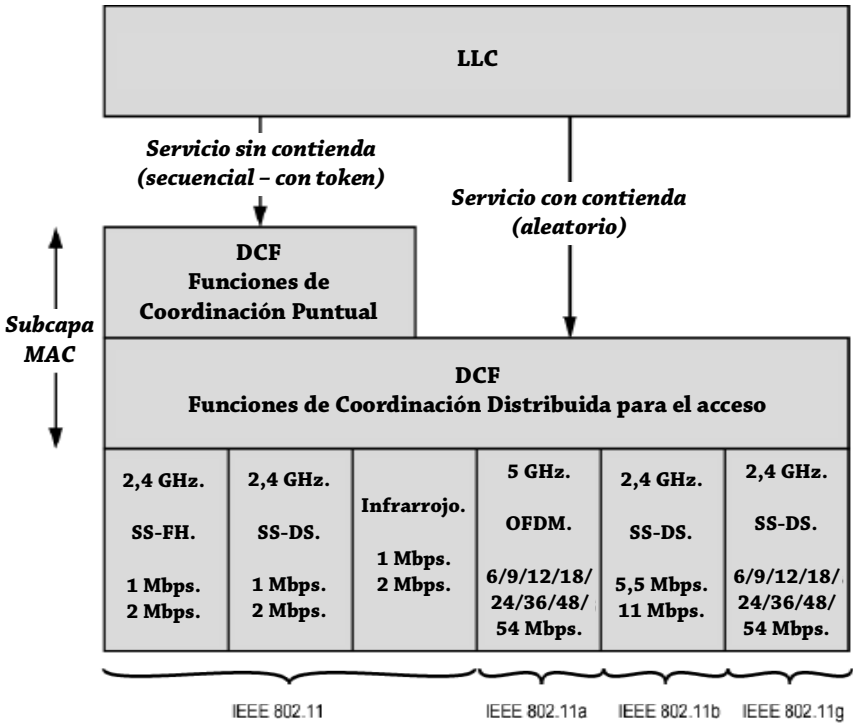
	802.11 Legacy	802.11a	802.11b	802.11g	802.11n WiFi 4	802.11ac WiFi 5	802.11ax WiFi 6
Uso-Cronología	Pasado.				Actual.		Futuro.
Características y Técnicas de Modulación	SS-DS. SS-FH. IR.	OFDM.	SS-DS.	OFDM.	OFDM. SU-MIMO. 64 QAM.	MU-MIMO. 256 QAM.	OFDM. MU-MIMO. 1024 QAM.
Alcance	-	-	-	-	70m.	30m.	-
Frecuencia de Operación	2,4 GHz.	5 GHz.	2,4 GHz.	2,4 GHz.	2,4 GHz. 5,8 GHz.	5,8 GHz.	2,4 GHz. 5,8 GHz.
Velocidad de Transmisión	2 Mbps.	54 Mbps.	11 Mbps.	54 Mbps.	300 Mbps. 600 Mbps.	7 Gbps.	10 Gbps.

A mayor frecuencia, mayor atenuación → a mayor atenuación, menor alcance.
A mayor ancho de banda, mayor velocidad de transmisión.

Funciones de los canales inalámbricos

- Optimizar la ocupación del ancho de banda → para evitar interferencia entre canales.
- Escaneo y cambio de canal → para pasar al canal más conveniente.
- Compartir frecuencias en las bandas → SS-DS permite compartir el canal con varios usuarios:
  - 2,4 GHz → 13/14 canales WiFi → menor AB, entonces menores velocidades de transmisión.
    - Trabaja con un AB de 20 MHz.
    - De los 13/14 canales, se pueden usar 3 canales a la vez como máximo.
      Si se usan más de 3 canales, se solapan los AB, afectando la velocidad de transmisión.
      Al ser tráfico de ráfagas, el canal no estará ocupado permanentemente.
  - 5,8 GHz → 14 canales WiFi → mayor AB, entonces mayores velocidades de transmisión.
    - Preparada para trabajar con un AB de 40 MHz.

Arquitectura IEEE 802.11



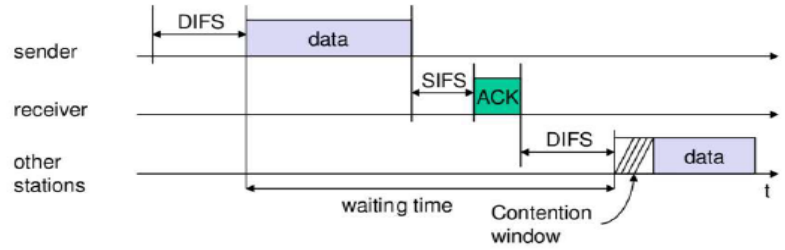
Modelo de Capas IEEE 802.11

LLC 802.2		
MAC 802.11		
IR (Infrarrojo)	**SS-FH**	**SS-DS**

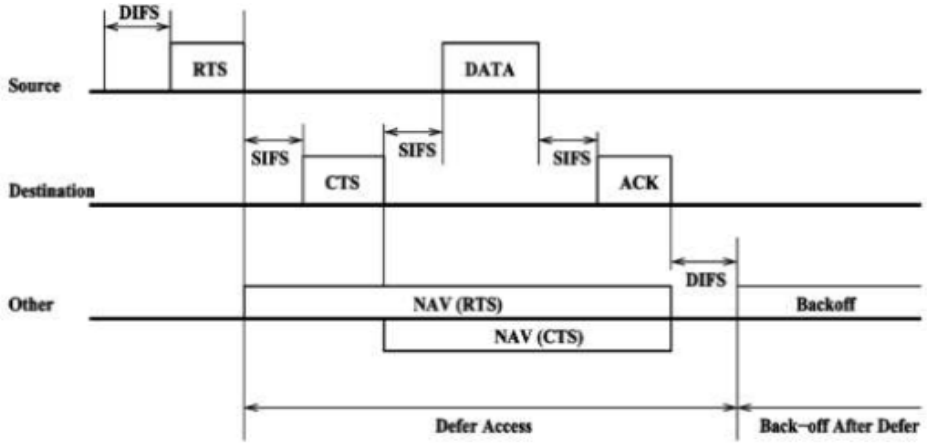
Subcapa MAC 802.11 – Funciones:

- Fiabilidad en la entrega datos → protocolo de intercambio de tramas:
  - Mecanismo de 2 tramas → más rápido, pero menos confiable:
    1. Trama de datos → enviada por el transmisor.
    2. Conformidad (ACK/NAK) → enviada por el receptor.
  - Mecanismo de 4 tramas: → más lento, pero más confiable.
    1. RTS → enviado por el transmisor.
    2. CTS → enviado por el receptor.
    3. Trama de datos → enviado por el transmisor.
    4. Conformidad (ACK/NAK) → enviada por el receptor.
- Control de acceso → regula el acceso al espectro radioeléctrico:
  - Protocolo de acceso distribuido → DCF (Función de Coordinación Distribuida):
    1. Algoritmo de prevención de contienda para el acceso a la totalidad del tráfico.
    2. Protocolo CSMA/CA (prevención de colisiones).

  Ejemplo para mecanismo de 2 tramas:



  Ejemplo para mecanismo de 4 tramas:



  Referencias:
  - *DIFS → tiempo previo a la ocupación del canal (transmisor) y envío de datos.*
  - *SIFS → tiempo posterior de espera (receptor) para responder conformidad, luego de haber recibido los datos.*
  - *Backoff → tiempo en donde otras estaciones pueden competir para ocupar el medio.*
  - Protocolo de acceso centralizado → PCF (Función de Coordinación Puntual):
    - Algoritmo centralizado para acceso libre de contienda.
    - Asegura acceso a usuarios.
- Seguridad → referidos a la autenticación y a la privacidad.

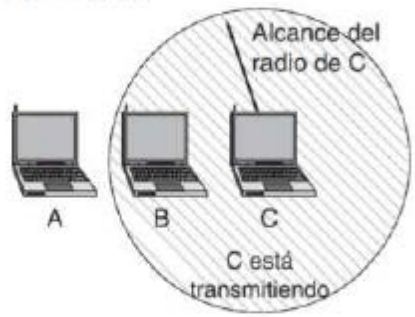
Subcapa MAC 802.11 – Formato de trama → se incrementan campos de direcciones y de control.

2 oct.	2 oct.	6 octetos	6 oct.	6 oct.	2 oct.	6 oct.	0 a 2312 octetos	4 oct.
FC	**D/I**	**Dirección del Destino**	**Dirección del Origen**	**Dirección del Receptor**	**SC**	**Dirección del Transmisor**	**PAYLOAD**	**CRC**

- **FC · Control de Trama** → indica el tipo de trama:
  - Control → sondeo de ahorro de energía, manejo de RTS/CTS/ACK/DIFS/SIFS.
  - Datos.
  - Gestión → manejo entre estaciones y puntos de acceso.
- **D/I · Duración/Conexión** → indica tiempo de reserva del canal para:
  - una transmisión satisfactoria; o bien
  - la identificación de una conexión.
- **Dirección del Destino** → siempre es la misma dirección desde que se sale del Origen hasta que llega a Destino.
- **Dirección del Origen** → siempre es la misma dirección desde que se sale del Origen hasta que llega a Destino.
- **Dirección del Receptor** → va cambiando de acuerdo al contexto.
- **Dirección del Transmisor** → va cambiando de acuerdo al contexto.
- **SC · Control de Secuencia** → fragmentación, reensamblado y número de tramas enviadas.
- **PAYLOAD** → información a enviarse.
- **CRC** → control de errores.

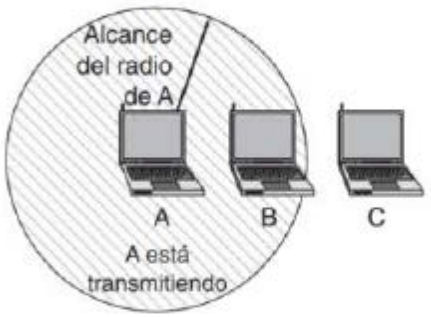
Problemas en la comunicación por radio que pueden generar colisiones

El problema de la terminal oculta



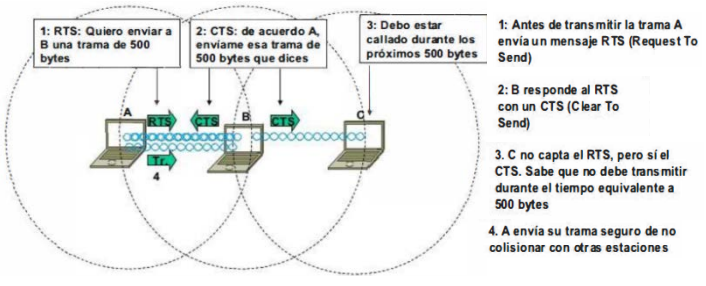
***B** está intercambiando tramas con **C**, pero **A** no escucha.*
***A** desea enviar a **B**, pero no puede escuchar que **B** está ocupada.*

El problema de la terminal expuesta



***B** desea enviar a **C**, pero piensa erróneamente que la transmisión fallará.*

Solución** → **uso de RTS y CTS:



Tecnologías incorporadas en WiFi 5

- *Beamforming* → tecnología que permite a un AP enfocar la señal hacia los destinos de interés.
  - Aumenta la eficiencia de la comunicación.
  - Usado en 5G.
- MU-MIMO → mejora de SU-MIMO.
  - SU-MIMO → WiFi a un dispositivo por vez.
  - MU-MIMO → WiFi a múltiples dispositivos a la vez, a la misma velocidad y mejor recepción.

Seguridad en WiFi

- Protocolos de seguridad usados:
  - WPS → mecanismos para facilitar la conexión de dispositivos a una red inalámbrica.
  - WEP → ofrece seguridad similar a la red cableada mediante una encriptación → débil.
  - WPA → agrega seguridad mediante el uso de claves dinámicas proporcionadas a cada usuario.
  - WPA2 → usa algoritmo de encriptación AES → el más seguro.
  - WPA2PSK → para uso doméstico o de oficinas pequeñas donde se comparte la clave.
- Otros recursos de seguridad:
  - Nombre de la red (SSID) → puede mostrarse/ocultarse.
  - Filtrado de direcciones MAC → lista de direcciones MAC permitidas y/o bloqueadas.

Wi Max · IEEE 802.16 · WMAN/WWAN → tecnología para comunicaciones punto a multipunto en banda ancha.

- Permite alcanzar mayores distancias e integrar distintas tecnologías.
- Preparado para trabajar sin colisiones.
- La transmisión de datos es sin contienda (a diferencia del WiFi).
- No está tan difundido actualmente.

	Wi Max 802.16	**802.16a**	**802.16b**	**Wi Max 2 802.16m**
Características	Con visión directa.	Sin visión directa.	Sin visión directa. Terminales en movimiento.	-
Sistema	Fijo.	Fijo.	Móvil.	Móvil.
Radio de celda	2km a 5km.	5km a 10km.	2km a 5km.	Hasta 50km.
Frecuencia de Operación	10 GHz a 66 GHz.	Menor a 11 GHz.	Menor a 6 GHz.	-
Velocidad de Transmisión	32 Mbps a 134 Mbps.	75 Mbps.	15 Mbps.	300 Mbps.

Los sistemas fijos permiten una instalación más perfeccionada.

UNIDAD 5 · PROTOCOLOS DE INTERCONEXIÓN TCP/IP

Internet → conjunto de redes heterogéneas, dispersas e interconectadas vía TCP/IP.

Protocolos → proporcionan reglas para la comunicación sin depender del hardware de red.

TCP/IP → conjunto de protocolos que permiten la interconexión entre redes heterogéneas, que no están asociados a un sistema operativo ni a un proveedor.

Comparación entre Modelo OSI y Modelo TCP/IP + Protocolos del Modelo TCP/IP

Modelo OSI		Modelo TCP/IP + Protocolos	
Aplicación		**Aplicación**	FTP, TELNET, SMTP, NSP, SNMP.
Presentación			
Sesión			
Transporte	4	**Transporte**	TCP, UDP.
Red	3	**Internet**	IP, ICMP, IGMP.
Enlace de Datos	2	**Acceso a la Red**	ARP, RARP.
Física			

ARP · Protocolo de Resolución de Dirección → permite conocer la dirección MAC por medio de su dirección IP.

- No es de Capa 2 ni Capa 3 → está en una capa intermedia "interfaz de red".
- Todo dispositivo conectado a una red necesita una tabla ARP, la cual relaciona dirección IP con dirección MAC. La tabla ARP reside en memoria → al apagarse el dispositivo, la tabla ARP se vacía.
- El transmisor envía un *broadcast* MAC con la dirección IP del Destino para que el destino responda con su dirección MAC y, de esa manera, ésta pueda registrarse en la tabla ARP del transmisor inicial.
- Comando de Windows para mostrar la tabla ARP → `arp -a`

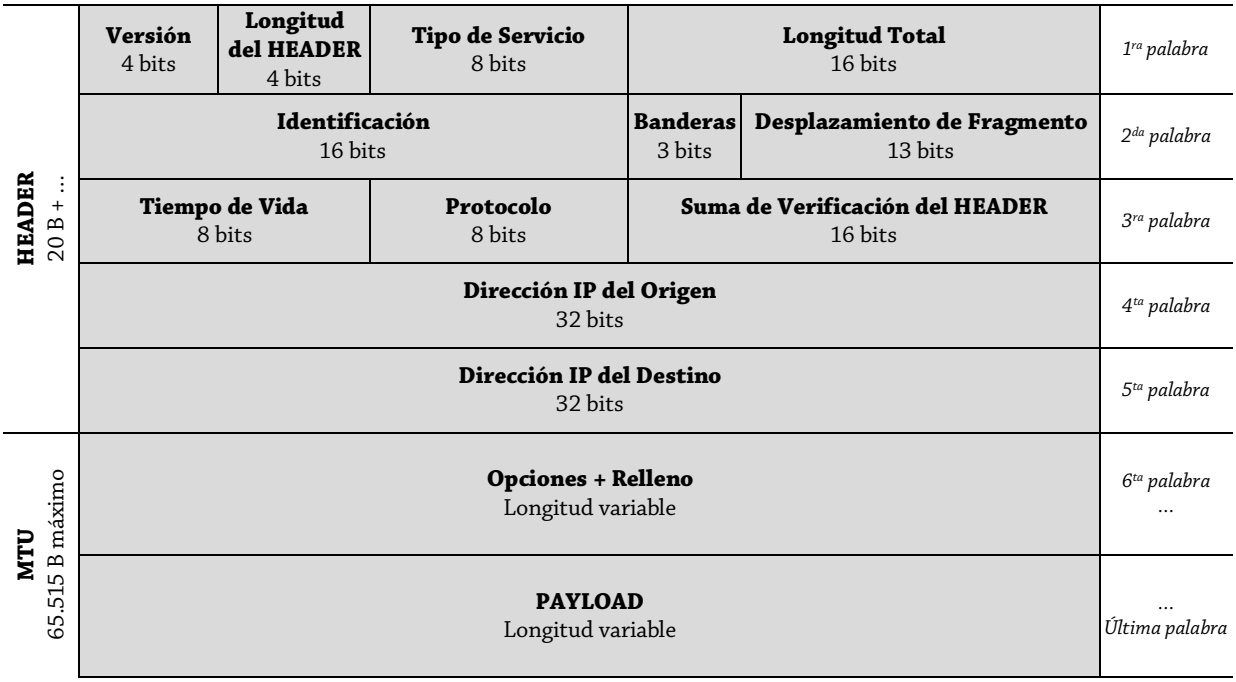
RARP · Protocolo de Resolución de Dirección Inversa → permite conocer la dirección IP con su dirección MAC.

- No es de Capa 2 ni Capa 3 → está en una capa intermedia "interfaz de red".
- Todo dispositivo conectado a una red necesita una tabla ARP, la cual relaciona dirección IP con dirección MAC. La tabla ARP reside en memoria → al apagarse el dispositivo, la tabla ARP se vacía.
- El transmisor envía un *broadcast* MAC de solicitud para que el Servidor RARP de la dirección IP correspondiente a la dirección MAC de la máquina solicitante
  El Servidor RARP, luego de recibir el *broadcast*, responde asignando una dirección IP para el transmisor.

IP · Protocolo de Internet → define: la unidad básica para la transferencia de datos, la selección de rutas (ruteo) y el conjunto de reglas para la entrega de paquetes no confiable.

- Inunda la red por todos los caminos con el objetivo de llegar a un destino.
  Si hay un error, será resuelto por la capa de arriba.
- Basado en el servicio no orientado a la conexión y no confiable → no garantiza que el datagrama llegue a destino
- Nombre PDU del Protocolo IP v4 → **datagrama**.
  Nombre PDU del Protocolo IP v6 → **paquete**.
  - Cada datagrama es independiente → no hay relación entre un datagrama y otro.
  - Cada datagrama lleva la suficiente información de encaminamiento (en su *header*) para viajar por cualquier camino sin limitación, en forma independiente.
  - Los datagramas viajan por distintas redes → Ethernet, FDDI, Token-Ring, etcétera.

Datagrama IP v4 → se estructura en palabras de 32 bits (4B) → tamaño máximo = 65.535 B.



1ra palabra → funciones de aspectos operativos y de formato:

- **Versión** → versión de la dirección IP → puede ser v4, v5 o v6.
- **Longitud del HEADER** → como no es de longitud fija sino variable, es necesario aclarar su tamaño.
- **Tipo de Servicio** → 6 bits de servicios diferenciados y 2 bits para notificación explícita de congestión.
- **Longitud Total** → como el datagrama IP no es de longitud fija sino variable, es necesario aclarar su tamaño.

2da palabra → dedicada a la fragmentación:

- **Identificación** → identifica unívocamente al datagrama → útil en la fragmentación.
- **Banderas** → brindan variedad de información de un datagrama (si puede o no ser fragmentado, por ejemplo).
- **Desplazamiento de Fragmento** → especifica el desplazamiento en el datagrama original de los datos acarreados en el fragmento.

3ra palabra → temas operativos:

- **Tiempo de Vida** → contador usado para que el datagrama no quede dando vueltas por la red indefinidamente.
- **Protocolo** → identifica al protocolo de la capa superior (Capa de Transporte).
- **Suma de Verificación del HEADER · *CheckSum* (no CRC)** → detecta errores solamente en el HEADER.

4ta palabra:

- **Dirección IP del Origen**.

5ta palabra:

- **Dirección IP del Destino**.

6ta palabra:

- **Opciones** → usado para pruebas de red o depuración → no siempre se utiliza.
  Relleno → usado para asegurar que el HEADER tenga una longitud múltiplo de 32 bits.

Direcciones IP v4 → identificador de una conexión de red de un dispositivo que use el Protocolo IP.

- Usa 32 bits (4B) → se representa en binario o en decimal, separando los octetos por puntos.
- La dirección IP de cada red debe ser única.
  La dirección IP de cada *host* debe ser única dentro de una misma red.
- Si un host se mueve de una red a otra, su dirección IP debe cambiar.
  No es como con la dirección MAC, que viene grabada.
- Si todos los bits son `1`s → difusión limitada en red local.
  Si todos los bits son `0`s → identificador del host en red local.
  Si todos los bits del campo de host son `1`s → difusión dirigida a una red.
  Si todos los bits del campo de host son `0`s → identificador de una red.
- Se preveen tres tipos de difusión → las direcciones IP de difusión son de Destino, nunca de Origen.
  - Difusión Dirigida → *broadcast* limitado a la red.
  - Difusión Limitada → limitada a la red local.
  - Multidifusión → se hace con clase D.

- **Direcciones IP especiales:**
  - `127.0.0.1` → refiere a este mismo dispositivo → se usa como dirección destino para pruebas.
    `127.0.0.0` hasta `127.255.255.255` → se comporta de la misma manera que `127.0.0.1`, sólo que las demás direcciones del rango no se usan.
  - `255.0.0.0` hasta `255.255.255.255` → reservadas.
    `224.0.0.0` hasta `239.255.255.255` → reservadas → clase D.
    `240.0.0.0` hasta `247.255.255.255` → reservadas → clase E.
  - Direcciones IP privadas:
    - `10.0.0.0` hasta `10.255.255.255` → reservada.
    - `169.254.0.0` hasta `169.254.255.255` → reservada.
    - `172.16.0.0` hasta `172.31.255.255` → reservada.
    - `192.168.0.0` hasta `192.168.255.255` → reservada.

- **Direcciones IP con clase:**
  - Direcciones (en binario):
    Clase A → `0XXXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX`.
    Clase B → `10XXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX`.
    Clase C → `110XXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX`.
    Clase D → `1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX` → dirección multifusión.
    Clase E → `11110XXX.XXXXXXXX.XXXXXXXX.XXXXXXXX` → reservado para uso posterior.
    Referencias de los colores: la parte de red en naranja, la parte de host en verde.
  - Regla del primer octeto (en decimal):
    Clase A → `1` hasta `126`.
    Clase B → `128` hasta `191`.
    Clase C → `192` hasta `223`.
    Clase D → `224` hasta `239`.
    Clase E → `240` hasta `247`.
  - Cuadro comparativo:

Clase	Cantidad de Redes	Cantidad de hosts	Rango de direcciones IP
A	$2^7 - 2 = 126$	$2^{24} - 2 = 16.777.214$	`1.0.0.0` hasta `126.0.0.0`.
B	$2^{14} - 2 = 16.382$	$2^{16} - 2 = 65.534$	`128.1.0.0` hasta `191.254.0.0`.
C	$2^{21} - 2 = 2.097.150$	$2^8 - 2 = 254$	`192.0.1.0` hasta `223.255.254.0`.
D	-	-	`224.0.0.0` hasta `239.255.255.255`.
E	-	-	`240.0.0.0` hasta `247.255.255.255`.

Las 2 direcciones que se restan son las direcciones prohibidas (todos `1`s y todos `0`s).

- **Subredes** → se piden prestados bits a la parte de host.
    - Usadas para el mejor aprovechamiento de las grandes redes (las cuales se dividen en *subredes*).
    - Concepto de direccionamiento jerárquico → primero: red; segundo: subred; y tercero: *host*.

- **Máscara de Subred (MS)** → da interpretación a la dirección IP → define qué parte es red y cuál es host.
    - Queda instalada en los dispositivos.
    - No viaja por el datagrama.
    - Se pueden escribir en 3 formatos:
        - Decimal.
        - Binario.
        - CIDR → sobre el final de la dirección IP se coloca un "/N", siendo N la cantidad de 1s.
    - Los 1s de la MS corresponden a la parte de red y a la parte de subred.
      Los 0s de la MS corresponden a la parte de *host*.

VER APUNTE APARTE DE DIRECCIONAMIENTO IP

- **Superredes** → uso de varias direcciones de red para una misma organización.
    - Normalmente son varias direcciones IP clase C que identifican a los *hosts* de una sola red.
    - Se toman direcciones IP contiguas y se identifica un número de conteo.
    - No es muy usado actualmente.

- Hay dos tipos de direccionamiento IP:
    - Direccionamiento IP Con Clase → aplico el concepto de subred cuando es necesario.
    - Direccionamiento IP Sin Clase → me salgo del concepto de subred; pudiendo tomar cantidades de bits a gusto y así incrementar combinaciones posibles.

- **VLSM (Máscara Variable)** → permite un uso más eficiente asignando distintas máscaras a las interfaces de un ROUTER.

- **CIDR (Direccionamiento Sin Clase)** → no necesito aplicar el concepto de subred.
    - Se asignan bloques de direcciones sin pertenecer a ninguna clase.

MTU → *unidad de transferencia máxima* de una red → capacidad de carga máxima del *payload* que tiene un protocolo.

- El MTU depende de la tecnología de red → para un datagrama IP, el MTU es de 65.515 B.
- Cada puerto del ROUTER tiene su propia MTU.

El PDU de Capa N se encapsula en un PDU de Capa N–1.

Fragmentación → división del datagrama en partes para que puedan encapsularse en MTUs más pequeñas.

- El ROUTER fragmenta de acuerdo al MTU de cada puerto.

IP v6 → mejora de IP v4.

- Usa 128 bits para representar una dirección IP (IPv4 usa 32) → aumenta la capacidad de direccionamiento.
- PDU IP v6 → **paquete**.
- El HEADER del datagrama IP v4 tiene 20B.
  El HEADER del paquete IP v6 tiene 40B mínimo (HEADER obligatorio) → se pueden agregar más HEADERs.

- **Estructura de un paquete IP v6:**

40 B	Variable	Variable	8 B	Variable	Opcional, Variable. 20 B	Variable
HEADER IPv6	*Hop-by-hop Options HEADER*	*Routing HEADER*	*Fragment HEADER*	*Destination Options HEADER*	HEADER TCP	Información
HEADER obligatorio	HEADERs opcionales				**PAYLOAD**	

- **Estructura del HEADER de un paquete IP v6:**

40 B **HEADER obligatorio**	**Versión** 4 bits	**Clase de Tráfico** 8 bits	**Etiqueta de Flujo** 20 bits
	Longitud del PAYLOAD 16 bits	**HEADER siguiente** 8 bits	**Límite de Saltos** 8 bits
	Dirección IP v6 Origen 128 bits = 16 B		
	Dirección IP v6 Destino 128 bits = 16 B		

  - **Versión** → número de versión.
  - **Clase de Tráfico** → identifica y distingue entre clases o prioridades de paquete.
  - **Etiqueta de Flujo** → etiqueta paquetes con tratamiento especial de encaminamiento/ruteo.
  - **Longitud del PAYLOAD** → medida en octetos de las cabeceras de extensión + PDU de transporte.
  - **HEADER siguiente** → cada HEADER tiene un campo que apunta al siguiente HEADER.
    - Puede ser de extensión o de TCP/UDP.
  - **Límite de Saltos** → símil "tiempo de vida".
  - **Dirección IP v6 Origen**.
  - **Dirección IP v6 Destino**.

- **Direcciones IP v6:**
  - Notación en hexadecimal con dos puntos → facilita el manejor.
    16B en total, con dos valores hexadecimales cada uno.
  - Un nodo tiene interfaces individuales → cada interfaz puede tener múltiples direcciones IP asociadas.
  - Permite agrupar por jerarquía de red, por proveedores de acceso, por proximidad geográfica, etc.
  - Tablas de encaminamiento/ruteo más pequeñas y consultas más rápidas → no se pone la dirección IP completa, sino los bits necesarios para rutear los datagramas.
  - Tipos de direcciones IP v6:
    - *Unicast* → identificador para una interfaz.
    - *Anycast* → identificador para un conjunto de interfaces.
      - Se entrega a una sola interfaz (la más cercana).
    - *Multicast* → identificador para un conjunto de interfaces.
      - Se entrega a un grupo de estaciones.
    - *Broadcast* → identificador para un conjunto de interfaces.
      - Se entrega a todas las estaciones de la red.

UDP · Protocolo de Datagrama de Usuario → *ver cuadro comparativo UDP vs TCP*.

Datagrama UDP:

Puerto Origen 16 bits	**Puerto Destino** 16 bits
Longitud del Mensaje UDP 16 bits	***CheckSum*** 16 bits
PAYLOAD 32 bits	

- **Puerto Origen** → opcional, puede valer 0 si no se usa.
- **Puerto Destino**.
- **Longitud del Mensaje UDP** → cantidad de octetos (HEADER y PAYLOAD).
- ***CheckSum*** → opcional, puede valer 0 si no se usa.
- **PAYLOAD.**

PseudoHEADER UDP → 3 palabras de 32b (4B) cada una, 96b = 12 B en total.

Dirección IP Origen 32 bits		
Dirección IP Destino 32 bits		
CEROS 8 bits	**Protocolo HEADER IP** 8 bits	**Longitud UDP** 16 bits

TCP · Protocolo de Control de Transmisión → *ver cuadro comparativo UDP vs TCP*.

Segmento TCP:

Puerto Origen 16 bits			**Puerto Destino** 16 bits
Número de Secuencia 32 bits			
Número de Acuse de Recibo 32 bits			
Longitud del HEADER 4 bits	**Reserva** 6 bits	**Banderas** 6 bits	**Tamaño de Ventana** 16 bits
CheckSum 16 bits			**Puntero de Urgencia** 16 bits
Opciones + Relleno 0 a 320 bits, variable.			
PAYLOAD N bits			

- **Puerto Origen** → opcional, puede valer 0 si no se usa.
- **Puerto Destino**.
- **Número de Secuencia** → para que llegue ordenado.
- **Número de Acuse de Recibo** → ACK.
- **Longitud del HEADER**.
- **Reserva**.
- **Banderas**.
- **Tamaño de Ventana**.
- ***CheckSum***.
- **Puntero de Urgencia** → relaciona a un protocolo de capa superior.
- **Opciones + Relleno**.
- **PAYLOAD**.

Congestionamiento en TCP → condición de retraso severo causada por una sobrecarga de segmentos en uno o más puntos de conmutación → se produce colapso por congestionamiento.

- Consecuencias:
  - Aumento de retrasos.
  - Descarte de segmentos por superar la capacidad de almacenamiento del ROUTER.
  - Retransmisión de datagramas por exceso de *time-out*.
- Acciones para evitar el colapso por congestionamiento que se produce:
  - Uso de algoritmos.
  - Uso de técnicas de disminución multiplicativa (disminución del tráfico) y arranque lento.

UDP vs TCP → Protocolo de Datagrama de Usuario vs Protocolo de Control de Transmisión.

Protocolo	**UDP**	**TCP**
Nombre PDU	Datagrama UDP.	Segmento TCP.
Tipo de Servicios	Sin conexión (orientados a la no conexión). Los datagramas UDP viajan por caminos distintos.	Con conexión (orientados a la conexión). Los segmentos TCP viajan por un único camino.
Confiabilidad en la Entrega de Datos	Entrega de datos no confiable. No garantiza ni confirma la entrega de datos. Pueden haber pérdidas, duplicaciones y retrasos.	Entrega de datos confiable. Garantiza la entrega de datos vía confirmación.
Orden de Llegada de los Datos	La entrega de datos no es secuenciada. Los datos no llegan en orden.	La entrega de datos es secuenciada. Los datos llegan en orden.
Velocidad	Rápido. Tiene requisitos de carga pequeños.	Lento. Tiene requisitos de carga mayores.
Establecimiento de Sesión entre Hosts	No se establece.	Sí se establece.
Comunicaciones Admitidas	Punto-a-punto. Punto-a-multipunto.	Solamente punto-a-punto (usa ARQ).
Controles de Flujo y de Congestión	No hace control de flujo.	Control de flujo → extremo a extremo, (mediante *sliding windows*). El problema puede aparecer en los extremos. Control de congestión → en sistemas intermedios. El problema puede aparecer en la nube.
Corrección y Detección de Errores	(*) Las aplicaciones que corren sobre UDP requieren corrección/detección de errores.	(*) Las aplicaciones que corren sobre TCP no requieren corrección/detección de errores.
Uso de IP y Capa de Residencia	Ambos usan IP como Capa 3. Ambos residen en la Capa 4 (Transporte).	
Multiplexado y Demultiplexado	Ambos realizan direccionamiento, multiplexado y demultiplexado mediante puertos.	
Otras características	Características similares al Protocolo IP.	Maneja conexiones Full-Duplex. Usa CheckSum

(*) → ver cuadro "Control de Errores según Protocolos IP/UDP/TCP".

Control de Errores según Protocolos IP/UDP/TCP

Protocolo	**IP**	**UDP**	**TCP**
Detección de Errores	**SÍ (*CheckSum*):** *en el HEADER.*	**SÍ (*CheckSum*):** *en el datagrama UDP y también en el pseudoHEADER del datagrama IP.*	**SÍ (*Checksum*):** *en el segmento TCP y también en el pseudoHEADER del datagrama IP.*
Corrección de Errores	**NO.**	**NO:** *no corrige ni recupera.*	**SÍ (ARQ):** *En el segmento TCP y también en el pseudoHEADER del datagrama IP.*

Puertos UDP y TCP → se usan números de puerto de protocolo para identificar el destino final.

- Para definir un punto extremo → se define el par (dirección IP, número de puerto).
- El número de puerto en una misma máquina puede ser compartido por varias conexiones.
- La conexión TCP se identifica por un par de puntos extremos.
- Los números de puertos apuntan a los protocolos de capa superior.
  El protocolo de transporte es quien direcciona los puertos.

Protocolos de Aplicación	FTP	TELNET	SMTP	DNS	TFTP	SNMP
Número de Puertos	**21**	**23**	**25**	**53**	**69**	**161**
Protocolos de Transporte	TCP			UDP		

ICMP · Protocolo de Mensajes de Control de Internet → Capa 3 → siempre se encapsula en el protocolo IP.

- Es parte de la Capa IP → se empaqueta dentro de un datagrama, pero no es Capa de Transporte.
- Verifica e informa eventos en red IP.
- Informa cuando el TTL (*Time To Live* – tiempo de vida) llega a cero.

IGMP · Protocolo de Administración de Grupo en Internet → Capa 3 → siempre se encapsula en el protocolo IP.

- Genera mensajes que se encapsulan en el datagrama IP.
- Gestiona la multidifusión → transmite datagramas IP a un conjunto de máquinas (grupo de multidifusión).
- Intercambia información entre ROUTERs.

Protocolos de Aplicaciones

Protocolo	Corre sobre…	Características
PING	ICMP	Envía solicitud de eco, captura la respuesta y realiza estadísticas.
TELNET	TCP	Permite el manejo de un terminal en forma remota a través de Internet. Con autenticación.
FTP	TCP	Permite la descarga de archivos de un servidor (FTP). Con autenticación.
SMTP	TCP	*Protocolo de Transferencia de Correo Simple.* Especifica formato de mensajes haciendo uso del ASCII. SMTP → permite el envío de mensajes o e-mails. POP3 e IMAP → permiten la recepción de mensajes o e-mails. • POP3 → el mensaje, luego de leerse, no reside en el servidor POP3. • IMAP → el mensaje, luego de leerse, no reside en el servidor POP3.
TFTP	UDP	Similar a FTP, pero más económico y vulnerable. Sin autenticación.
DNS	UDP	*Sistema de Nombre de Dominio.* Maneja la traducción de nombres pronunciables por seres humanos a direcciones IP. Usa servidores (que usan bases de datos) con la información necesaria.
BOOTP	UDP	Mejora el RARP → especifica aspectos de arranque.
DHCP	UDP	*Protocolo de Configuración Dinámica de Host.* Protocolo de tipo cliente-servidor, donde un servidor DHCP asigna dinámicamente una dirección IP a cada dispositivo en una red de acuerdo a los requerimientos. El administrador puede supervisar y distribuir en forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva dirección IP si el dispositivo es conectado en un lugar diferente de la red.
SNMP	UDP	*Protocolo de Administración de Red Simple.* Hace administración de la red → administración de routers y distintos dispositivos.

Toda aplicación que corre sobre UDP/TCP debe poder trabajar con determinados puertos asignados a TCP/UDP.

El puerto es la vía de comunicación entre ellos protocolos de Transporte y de Aplicación.

ROUTERs y Ruteo

- **ROUTER** → dispositivo de Capa 3 del Modelo OSI.
  - Posee puertas de enlaces LAN, WAN y para consola.
  - Cada ROUTER tiene en su configuración una tabla de ruteo que vincula redes entre sí usando puertos.
  - Aprende direcciones IP.
  - Provee seguridad a la red.
  - Se encarga de hacer el ruteo.
- **Ruteo** → encaminamiento de los datagramas de una red a la otra.
  - Se pueden definir rutas estáticas o dinámicas:
    - Rutas estáticas → ingresadas por el administrador de red → menos flexibles, más seguras.
    - Rutas dinámicas → ajustadas automáticamente mediante protocolos de ruteo.
  - Los protocolos de ruteo proveen información sobre accesibilidad, retardos y tablas de ruteo. Algunos protocolos son: RIP, IGRP, OSPF, EGP.
  - Hay dos tipos de protocolo de ruteo, según el sistema autónomo (red que tiene un administrador):
    - IRP · Protocolo de Ruteo Interior → distribuye información de ruteo (más detallada) dentro de un sistema autónomo.
    - ERP · Protocolo de Ruteo Exterior → distribuye información de ruteo (menos detallada, más simple) entre diferentes sistemas autónomos
  - Hay tres estrategias de ruteo:
    - Por Vector Distancia → intercambio de información con ROUTERs vecinos.
      - Es una estrategia para protocolos internos.
      - Ejemplo: RIP.
    - Por Estado de Enlace → intercambio de información de costos de enlace (esfuerzo en la comunicación entre un ROUTER y otro) con todos los routers dentro de un sistema autónomo.
      - Es una estrategia para protocolos internos.
      - Ejemplo: OSPF.
    - Por Vector Camino → no incluye estimación de distancia ni de costo.
      - Es una estrategia para protocolos externos.
      - Minimiza la información que se intercambia.

VoIP · Voz sobre IP → la voz se digitaliza para que viaje en el datagrama IP.

- Gran conjunto que comprende muchas aplicaciones (como Zoom, Meet, Skype, etcétera).
- La telefonía VoIP (digital; no es la voz natural) tiene menor calidad que la telefonía convencional (analógica; es la voz natural).

ToIP · Telefonía IP → comunicación sobre una red telefónica.

- Forma parte de VoIP.
- Los aparatos deben trabajar con el concepto de señalización de la telefonía.
- Puertos usados:
  - Puerto FXS → para conectar un terminal o suscriptor (un teléfono, por ejemplo).
    - Pone un lazo de corriente.
  - Puerto FXO → para conectar una central telefónica.
    - Recibe un lazo de corriente (de una oficina de conmutación).