

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.

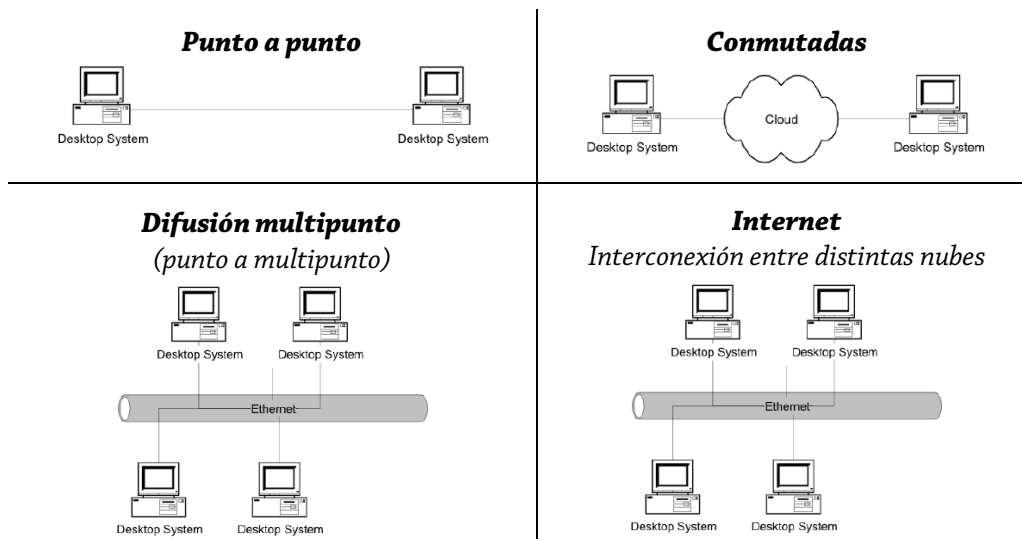
Las señales digitales permiten integrar todas las redes.

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



Clasificación de las redes

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

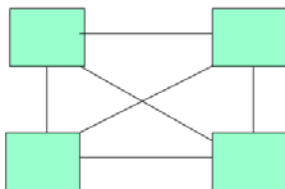
	LAN	WAN
Distancias	Cortas.	Grandes.
Velocidades de transmisión	Alta.	Baja.
Calidad de enlaces	Mayor (bajo BER).	Menor (alto BER).
Uso de canales	... de difusión.	... punto a punto.
Seguridad	Mayor (menos vulnerable).	Menor (más vulnerable).
Afectación por restricciones externas	NO se ven afectadas.	SÍ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

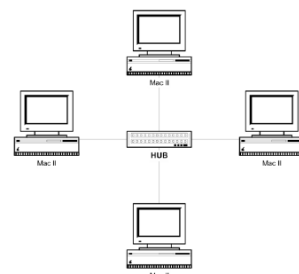
Topología de las redes → se manejan en Capa Física (1).

Malla



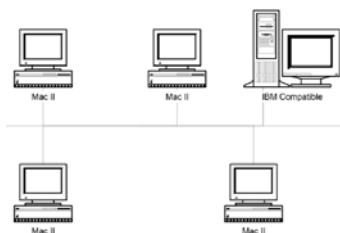
- Más común con pocos nodos.
- La cantidad de enlaces queda determinada por la cantidad de nodos:
$$N_{enlaces} = \frac{n_{nodos} \cdot (n_{nodos} - 1)}{2}$$
- Tiene mayores costos (debido a los enlaces).

Estrella

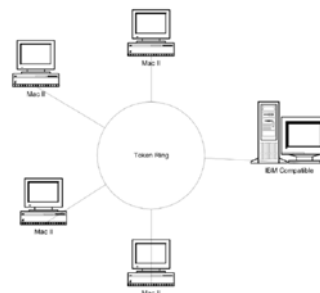


- Más común con muchos nodos → la poca confiabilidad se resuelve agregando redundancia.
- Hay tantos enlaces como terminales.
- Un SWITCH en el medio.

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.

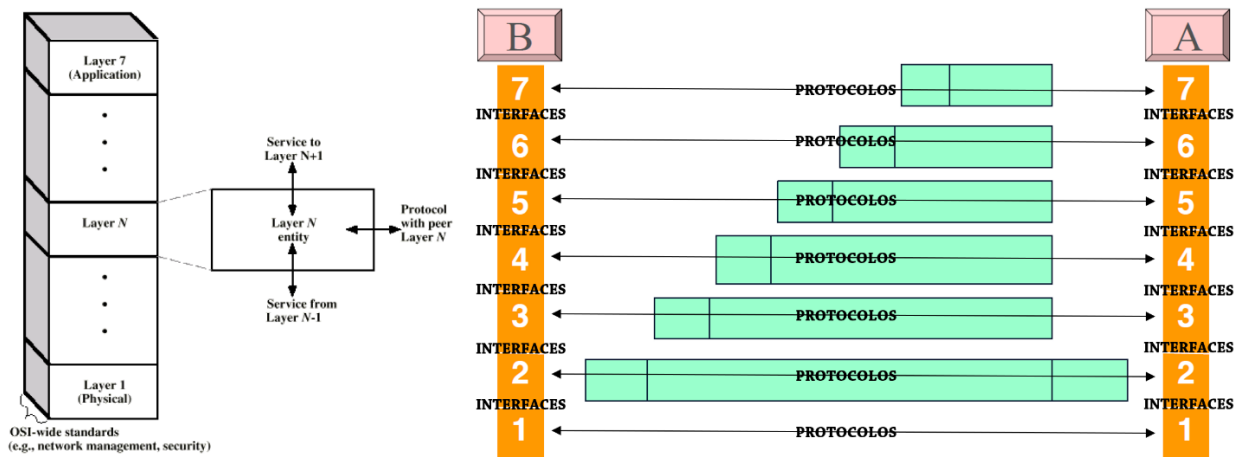
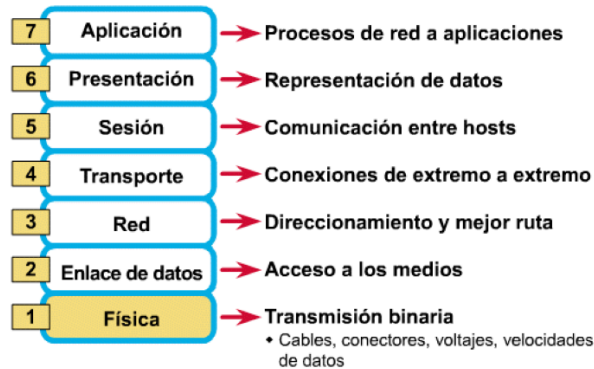
★ → Bajo.

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 desarmado 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-outs*.
 - Variantes:
 - **ARQ Stop-and-Wait** → 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.
 - **ARQ Sliding Windows** → 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 **ventana** → 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.

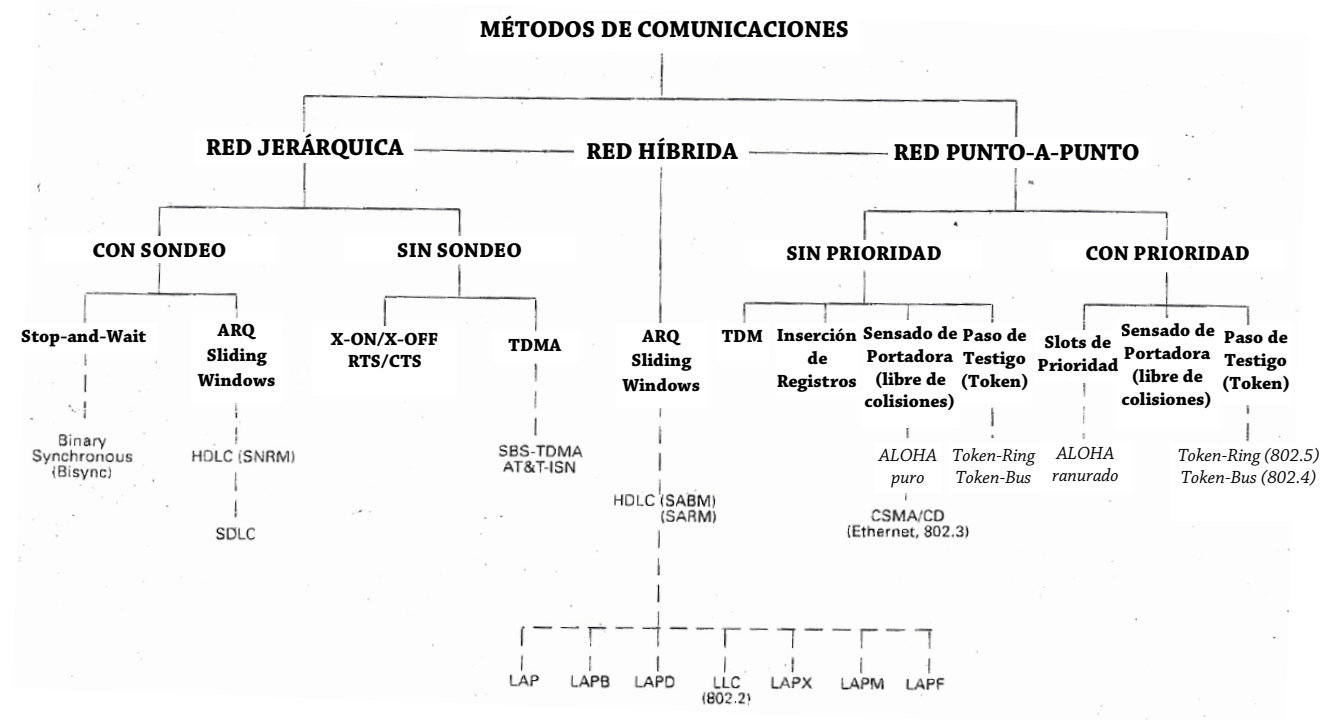
Sistema sin sondeo – Técnicas de control de flujo

- 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

<i>Modelo OSI</i>		<i>Modelo IEEE 802 (redes LAN)</i>	
Aplicación		<i>Protocolos de capas superiores</i>	
Presentación			
Sesión			
Transporte			
Red			
Enlace de Datos		[LLC] Control de Enlace Lógico	} <i>Alcance del Modelo IEEE 802</i>
		[MAC] Control de Acceso al Medio	
Física		Física	
MEDIO		MEDIO	

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

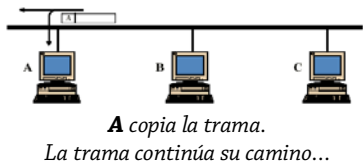
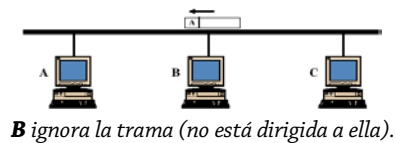
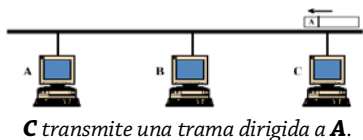
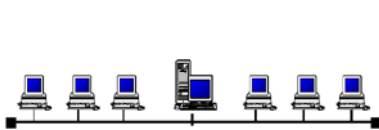
- DCE por defecto.
- Componentes genéricos:
 - Controladora:
 - Formateo de tramas (PDU de Capa 2).
 - Generación de FCS (Frecuencia de Control de Trama) → alguna técnica de detección de errores como CRC.
 - Sincronismo de bit → *clock* de transmisión y recepción.
 - Codificación → código de línea (Manchester o Manchester Diferencial).
 - Transreceptor:
 - 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

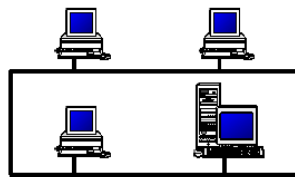
- Dirección física impregnada en el hardware o en la electrónica del dispositivo de red.
- Identifica unívocamente al dispositivo → cada interfaz tiene una dirección MAC.
- Son 48 bits repartidos en 6 grupos de 2 dígitos hexadecimales cada uno.
Formato → F0:E1:D2:C3:B4:A5.
Los primeros 24 bits identifican al fabricante. Los últimos 24 bits identifican a cada placa de red del fabricante.
- Dirección de broadcast (dirección especial: son todos 1s) → 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



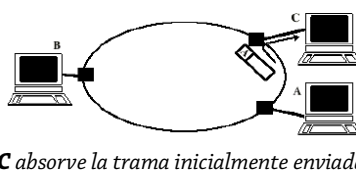
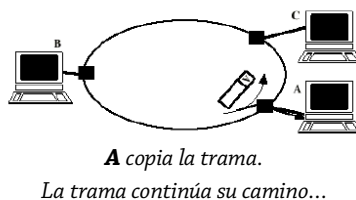
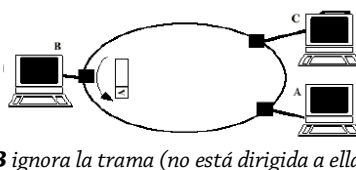
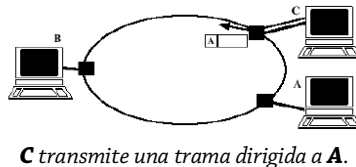
Ring o Anillo



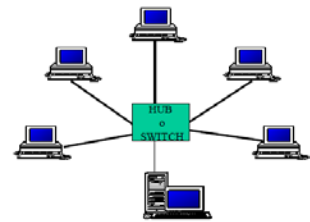
Paso de testigo:

Una vez que transmitió **C**, **C** le pasa el *token* a **B**, quien ahora, tiene el permiso para transmitir.

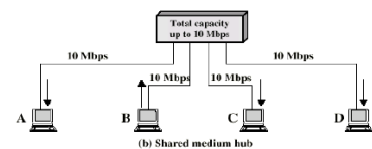
Luego de transmitir **B**, **B** le pasará el *token* a **A** y así...



Estrella



Estrella con HUB (Capa 1)

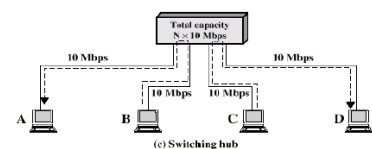


B transmite una trama.

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.
- $v_{\text{máx Tx}} = 10 \text{ MBps}$ 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.
- $v_{\text{máx Tx}} = 20 \text{ MBps}$ 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 Coaxial → 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:

Información							
1	2	3	4	5	6	7	8
0	N(S)			P/F	N(R)		

Supervisión							
1	2	3	4	5	6	7	8
1	0	S		P/F	N(R)		

No numeradas							
1	2	3	4	5	6	7	8
1	1	M		P/F	M		

- 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:

Información																
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
0	N(S)								P/F	N(R)						

Supervisión															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	S			0	0	0	0	P/F	N(R)					

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.

$$RTT = 2 \cdot T_{\text{propagación}}$$
 RTT_{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.

$$T_{\text{propagación}} \sim P_{(\text{colisión})} \quad RTT \sim P_{(\text{colisión})} \quad T_{\text{transmisión}} \sim \frac{1}{P_{(\text{colisión})}}$$

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 $RTT_{máx}$ 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.

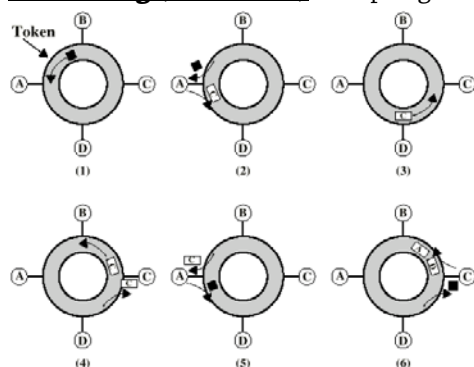
- Usa varias técnicas para evitar colisiones (una de ellas es la posicional, que establece prioridades de acuerdo a posiciones de las estaciones).

- **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.

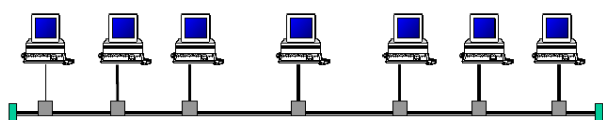
- Tipos:

- **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.

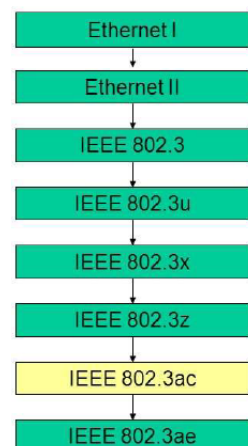
DISPOSITIVOS

- 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

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

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 $T_{\text{transmisión}}$ bajos como $T_{\text{propagación}}$ 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: $i \rightarrow \text{Número de ranuras entre 0 y } (2^i - 1)$.*
Red a 10 Mbps → Ranura de tiempo de espera = 51,2 μs .
Red a 100 Mbps → Ranura de tiempo de espera = 5,12 μs .
Cantidad máxima de ranuras = 1023.
La 1ª colisión se elige un número de ranura en forma aleatoria entre 0-1 (1 ranura).
La 2ª 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

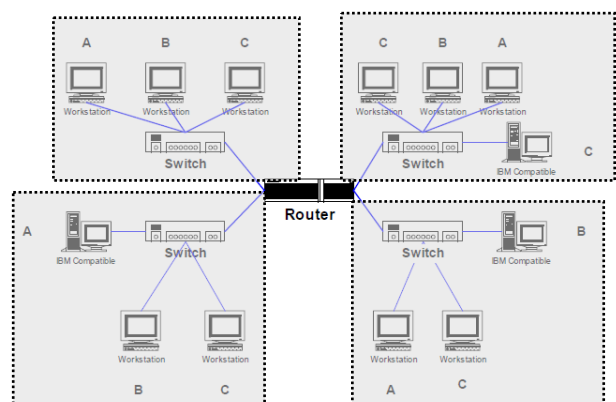
- 10B2 · Cable Coaxil Fino:
 - A menor sección transversal → mayores resistencia y atenuación.
 - Topología → bus/lineal.
 - Conector → T-BNC.
Tarjeta de red → incluye controladora y transreceptor.
 - Longitud máxima → 185m por segmento.
Cantidad máxima de nodos por segmento → 30.
Cantidad máxima de 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, 1^{ra} ventana), hasta 300m.
 - Opción 10 G B-L → FO monomodo (1310nm, 2^{da} ventana), hasta 10km.
 - Opción 10 G B-E → FO monomodo (1550nm, 3^{ra} ventana), hasta 40km.
 - Opción 10 G B-LX4 → FO monomodo o multimodo (1310nm, 2^{da} 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

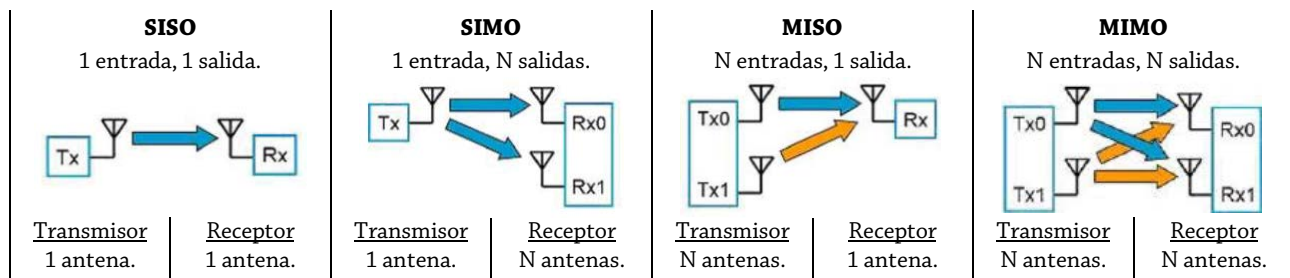
Aplicaciones LAN inalámbricas

- 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



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 encriptación.
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.

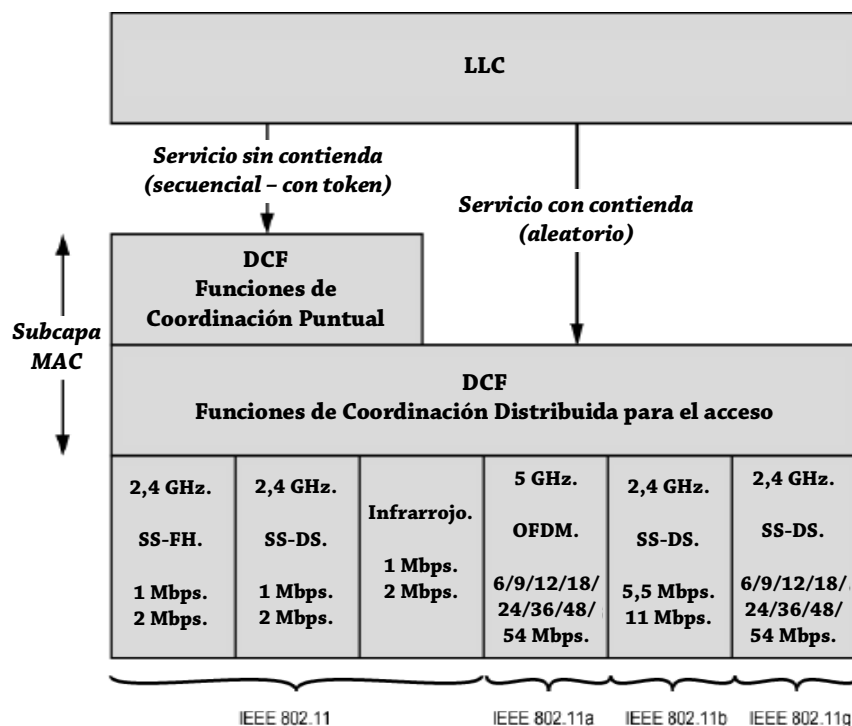
A mayor frecuencia, mayor atenuación → a mayor atenuación, menor alcance.

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



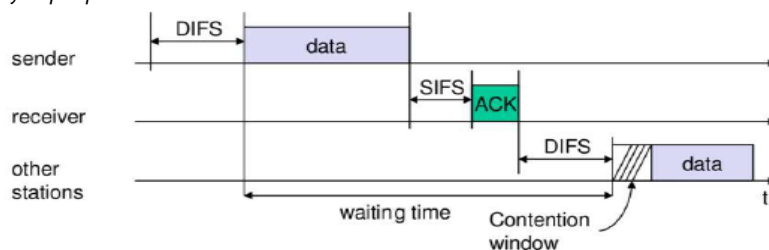
Modelo de Capas IEEE 802.11

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

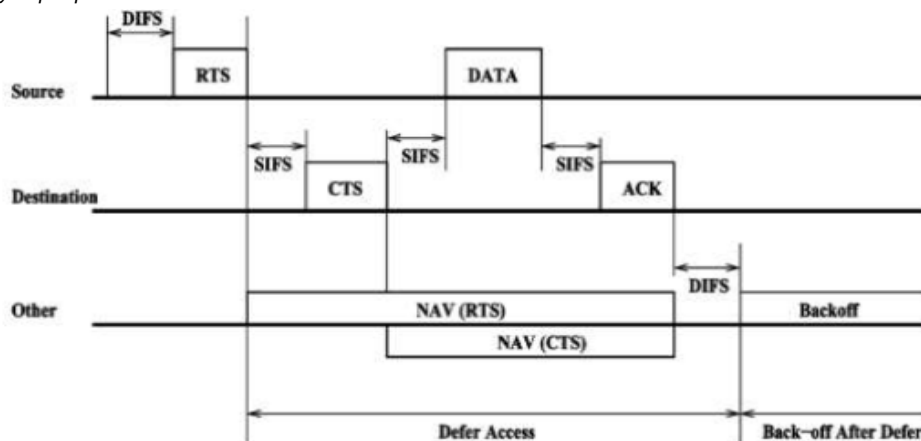
Subcapa MAC 802.11 – Funciones:

- Fiabilidad en la entrega de 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 colisión 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:

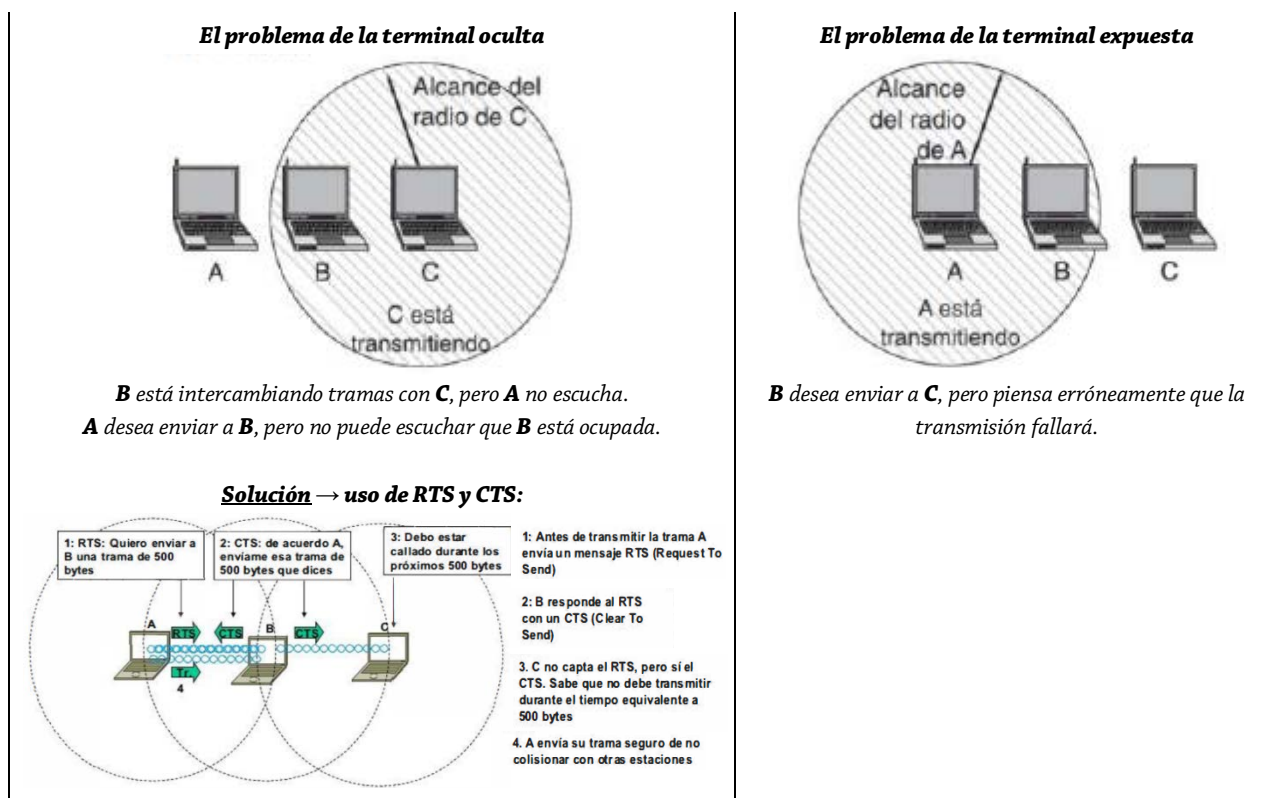
- DIFS → tiempo previo a la ocupación del canal (transmisor) y envío de datos.
- SIFS → tiempo posterior de espera (receptor) para responder conformidad, luego de haber recibido los datos.
- Backoff → tiempo en donde otras estaciones pueden competir para ocupar el medio.
- Protocolo de acceso centralizado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



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		
Presentación		FTP, TELNET, SMTP, NSP, SNMP.
Sesión		
Transporte	4	TCP, UDP.
Red	3	IP, ICMP, IGMP.
Enlace de Datos	2	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.

HEADER 20 B + ...	Versión 4 bits	Longitud del HEADER 4 bits	Tipo de Servicio 8 bits	Longitud Total 16 bits		1 ^{ra} palabra
	Identificación 16 bits			Banderas 3 bits	Desplazamiento de Fragmento 13 bits	2 ^{da} palabra
	Tiempo de Vida 8 bits		Protocolo 8 bits	Suma de Verificación del HEADER 16 bits		3 ^{ra} palabra
	Dirección IP del Origen 32 bits					4 ^{ta} palabra
	Dirección IP del Destino 32 bits					5 ^{ta} palabra
MTU 65.515 B máximo	Opciones + Relleno Longitud variable					6 ^{ta} palabra ...
	PAYLOAD Longitud variable					... Última palabra

1^{ra} 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.

2^{da} 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 acarreos en el fragmento.

3^{ra} 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.

4^{ta} palabra:

- **Dirección IP del Origen.**

5^{ta} palabra:

- **Dirección IP del Destino.**

6^{ta} 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 1s → difusión limitada en red local.
Si todos los bits son 0s → identificador del host en red local.
Si todos los bits del campo de host son 1s → difusión dirigida a una red.
Si todos los bits del campo de host son 0s → identificador de una red.
- Se prevén 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 → 0XXXXXXXX.XXXXXXXXX.XXXXXXXXX.XXXXXXXXX.

Clase B → 10XXXXXXXX.XXXXXXXXX.XXXXXXXXX.XXXXXXXXX.

Clase C → 110XXXXXXXX.XXXXXXXXX.XXXXXXXXX.XXXXXXXXX.

Clase D → 1110XXXX.XXXXXXXXX.XXXXXXXXX.XXXXXXXXX → dirección multifusión.

Clase E → 11110XXX.XXXXXXXXX.XXXXXXXXX.XXXXXXXXX → 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 1s y todos 0s).

- **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	<i>Hop-by-hop Options HEADER</i>	<i>Routing HEADER</i>	<i>Fragment HEADER</i>	<i>Destination Options HEADER</i>	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 manejo.
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 <u>control de flujo</u> .	<u>Control de flujo</u> → extremo a extremo, (mediante <i>sliding windows</i>). El problema puede aparecer en los extremos. <u>Control de congestión</u> → 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 <u>datagrama UDP</u> y también en el <u>pseudoHEADER del datagrama IP</u> .	SÍ (Checksum): en el <u>segmento TCP</u> y también en el <u>pseudoHEADER del datagrama IP</u> .
Corrección de Errores	NO.	NO: no corrige ni recupera.	SÍ (ARQ): En el <u>segmento TCP</u> y también en el <u>pseudoHEADER del datagrama IP</u> .

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	<i>Protocolo de Transferencia de Correo Simple.</i> 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. <ul style="list-style-type: none">• 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	<i>Sistema de Nombre de Dominio.</i> 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	<i>Protocolo de Configuración Dinámica de Host.</i> 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	<i>Protocolo de Administración de Red Simple.</i> 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 puertos 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).

UNIDAD 6 · REDES WAN

Composición de una Red WAN

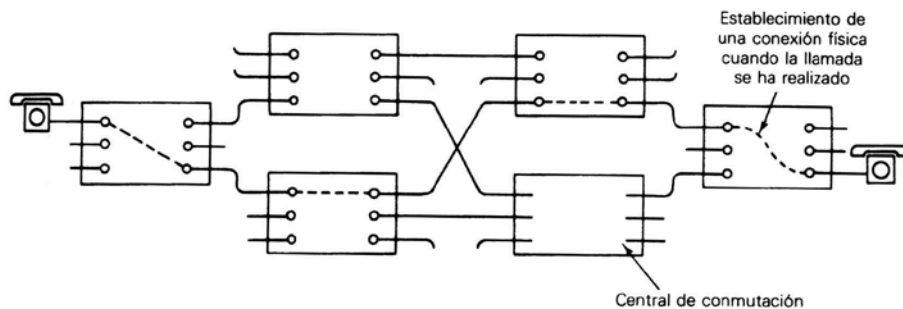
- Equipos terminales.
- Nodos de red.
- Enlaces de comunicaciones.

Tipos de Enlaces de comunicaciones

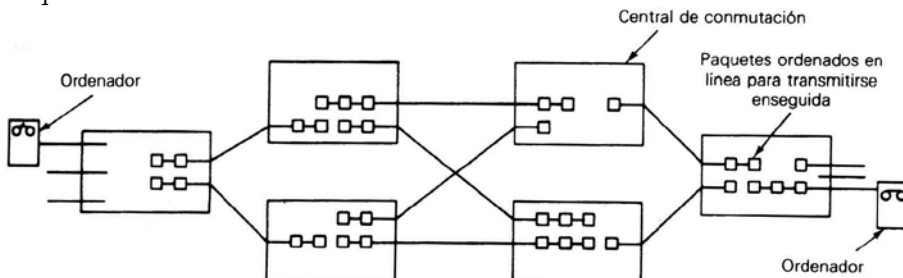
- Según los puntos que une:
 - Punto a Punto → ejemplos: ARQ, FEC.
 - Punto a Multipunto → ejemplo: FEC.
- Según las características:
 - Dedicados → el medio no se comparte → no hay intermediarios entre transmisor y receptor.
 - Conmutados → el medio se comparte → hay estaciones intermedias entre transmisor y receptor.

Tipos de Conmutación → según la forma en que se conmutan los nodos

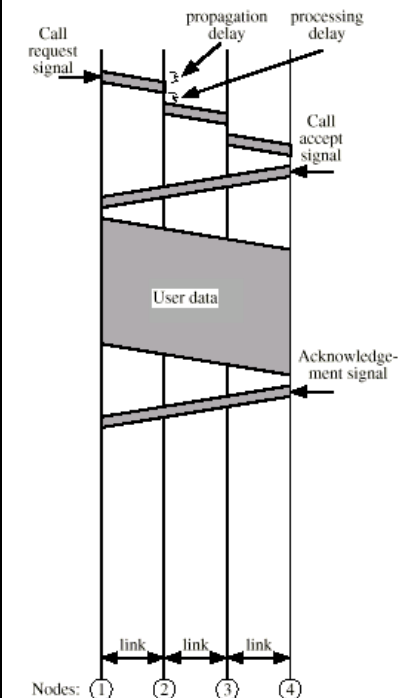
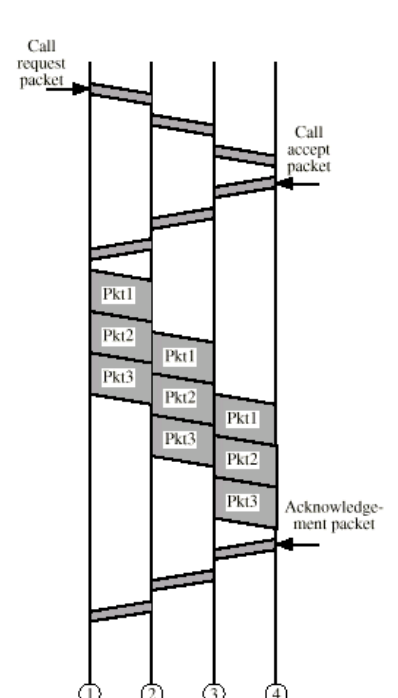
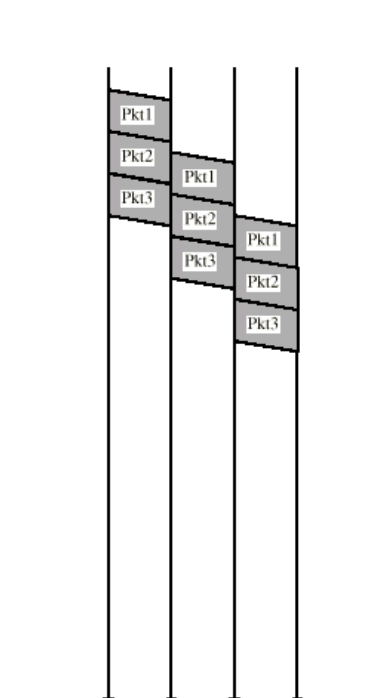
- **Conmutación de Circuitos** → cada conmutador establece una conexión y, así, queda definido un camino:
 - Hay monopolio de recursos → el recurso de conmutación y el enlace quedarán reservados para la comunicación entre A y B → solamente habrá paquetes de A y B en ese enlace.
 - Es con conexión → se establece una conexión entre A y B, la cual debe ser luego mantenida y liberada.
 - Esquema:



- **Conmutación de Paquetes** → entre paquete y paquete quedan espacios/tiempos que pueden ser aprovechados por otros paquetes de otras comunicaciones:
 - No hay monopolio de recursos → los recursos de conmutación y los enlaces se comparten.
 - Esquema:



- Modos de Operación:
 - **Circuito Virtual** → es con conexión → se establece un único camino (virtual) por el cual viajan todos los paquetes de una misma comunicación.
 - Protocolo que trabaja con circuitos virtuales → TCP.
 - **Datagrama** → es sin conexión → no se establece ningún camino único → cada paquete (que tiene suficiente información para poder enrutarse solo) puede ir por cualquier camino.
 - Protocolos que trabajan con datagramas → UDP, IP.

Conmutación de Circuitos	Conmutación de Paquetes (Circuitos Virtuales)	Conmutación de Paquetes (Datagramas)
Con conexión física.	Con conexión virtual.	Sin conexión virtual.
Ruta dedicada.	Ruta no dedicada.	No hay ruta.
La ruta se establece para toda la transmisión.		Cada paquete tiene su propio encaminamiento.
El encaminamiento es más rígido, ya que siempre es un único camino.	El encaminamiento es por la ruta menos costosa en retardos y cantidad de saltos.	
Los datos transmitidos llegan en orden.		Los datos transmitidos no llegan en orden.
Transmisión en forma continua.	Transmisión paquetizada.	
En general, uso eficiente para voz, pero ineficiente para datos.	En general, uso eficiente para datos, pero menos eficiente para voz.	
Se cobra por tiempo y distancia.	Se cobra por cantidad de paquetes y tiempo. La distancia, en general, no pesa.	
El mensaje no se almacena.	Los paquetes se almacenan hasta su envío.	Los paquetes se pueden almacenar hasta su envío.
Puede haber retardo en el establecimiento de la conexión.	Puede haber retardo durante la transmisión de paquetes.	
La congestión bloquea el establecimiento de la conexión.	La congestión aumenta el retardo de la transmisión de paquetes.	
Ancho de banda fijo.	Uso dinámico del ancho de banda. Mejor aprovechamiento del ancho de banda.	
 <p>Una señal de solicitud de llamada inicia el establecimiento de la conexión, mantenida durante la transmisión de datos de usuario, y finalmente liberada.</p>	 <p>La conexión se establece, se mantiene y finalmente se libera. Hay múltiples canales compartidos.</p>	 <p>Como es no orientada a la conexión, los paquetes se transmiten directamente.</p>

Al definir tamaño del paquete en un protocolo, hay que considerar la eficiencia y la tasa de errores (BER):

- Paquetes grandes → más eficientes (hay menos encabezados) → recomendables en canales de bajo BER bajo.
- Paquetes chicos → menos eficientes (hay más encabezados) → recomendables en canales de BER alto.

RED DE CONMUTACIÓN DE CIRCUITOS

→ una vez establecido el circuito, se convierte en un canal dedicado.

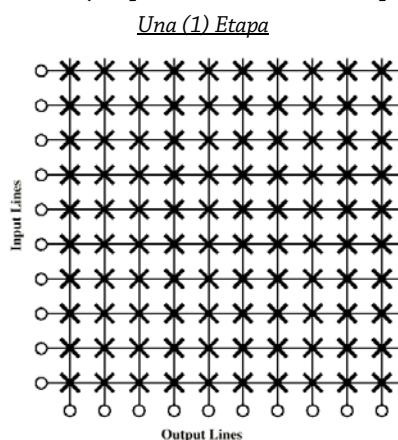
Fases → establecimiento del circuito, transferencia de datos y desconexión del circuito.

Componentes

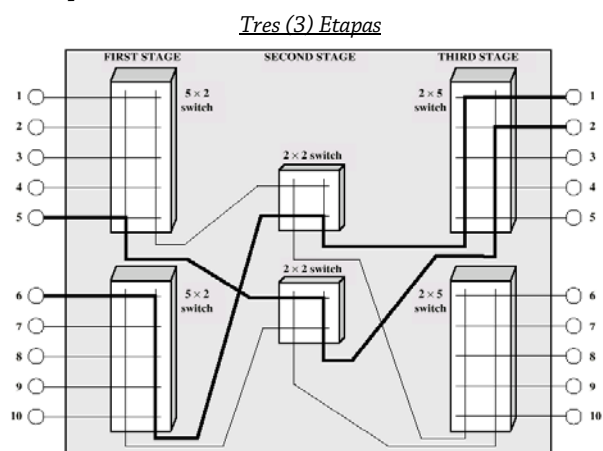
- Centrales → tienen los conmutadores; de ellas dependen los abonados.
- Abonados.
- Líneas principales o Troncales → unen a las centrales mediante fibra óptica, radioenlace, etcétera.
- Bucle local → lazo de abonado.

Tipos de Conmutación por Circuitos

- Por División en el Espacio → antiguo:
 - Las rutas que se establecen son físicamente independientes entre sí.
 - Ejemplos de Conmutadores por División en el Espacio:

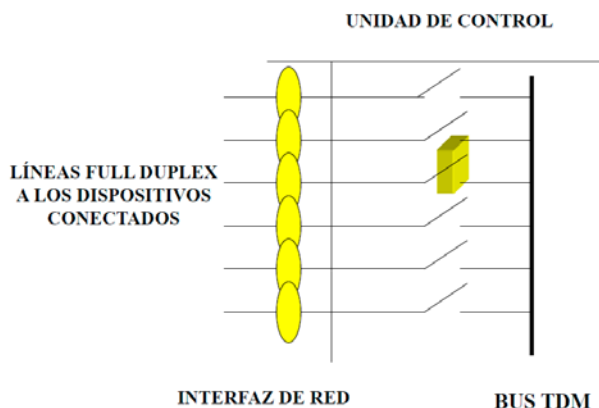


La cantidad máxima de comunicaciones simultáneas es, en el mejor de los casos, igual a la cantidad de líneas de entradas/salidas.



Hay concentración en los conmutadores, lo cual reduce la cantidad máxima de comunicaciones simultáneas.

- Por División en el Tiempo → más actual:
 - Los canales de menor velocidad son muestreados a una mayor velocidad para integrarse en un bus TDM → las etapas para digitalizar una señal analógica son: muestreo, cuantificación y codificación.
 - Se basa en sistemas digitales y multiplexación por división de tiempo (TDM).
 - Ejemplo de Conmutador por División en el Tiempo:



PPP · Point to Point Protocol → protocolo para enmarcar el Protocolo IP cuando se envía mediante una línea serial.

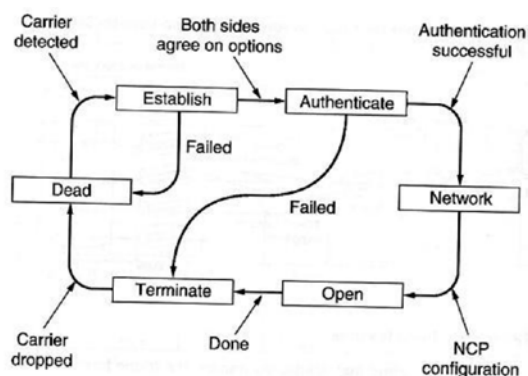
- Útil para la transferencia entre dos dispositivos → *Point-to-Point*.
- Es de Capa (2) de Enlace.
- Derivado del HDLC.
- Usado para formar VPNs.
- Funciones:
 - Transporte de datos.
 - Asegura el enlace y la recepción ordenada.
 - Provee control de errores → detección y corrección (usa ventana deslizante o *sliding windows*).
 - Provee autenticación.
 - Provee asignación dinámica de direcciones IP.

PDU

8 b	8 b	8 b	16 b	0 a N b	16 b o 36 b	8 b
Bandera de Inicio	Campo de Dirección (*)	Campo de Control (*)	Identificador de Protocolo	INFO	FCS	Bandera de Cierre

- **Bandera de Inicio** → elementos para el sincronismo de bloque; símil “preámbulo” de la trama Ethernet.
- **Campo de Dirección** → lleva siempre la dirección estándar de difusión (son dos estaciones)
 - Este campo puede ser eliminado por negociación, de acuerdo a la implementación que se realizará.
- **Campo de Control** → tipo de trama no numerada.
 - Este campo puede ser eliminado por negociación, de acuerdo a la implementación que se realizará.
- **Identificador de Protocolo** → puede asociarse a varios: IP, LCP, PAP, CHAP, etcétera.
- **INFO** → información de usuario.
- **FCS · Secuencia de Control de Trama** → mediante CRC 16 o CRC 32.
- **Bandera de Cierre** → elemento para el sincronismo de bloque.

Funcionamiento



- **Establecimiento de la conexión** → una computadora contacta con la otra y negocian los parámetros relativos al enlace (como el tamaño de los datagramas, el método de autenticación a usar, etcétera) usando el protocolo LCP, el cual es una parte fundamental de PPP.
- **Autenticación** → no obligatoria.
 - Hay dos protocolos: PAP (la contraseña se envía sin cifrar; no recomendado) y CHAP (la contraseña se manda cifrada).
- **Configuración de Red** → se negocian parámetros dependientes del protocolo de red que se esté usando.
- **Transmisión** → se manda y se recibe la información de red.
- **Terminación** → la conexión puede ser finalizada en cualquier instante y por cualquier motivo.

Comparación con SLIP

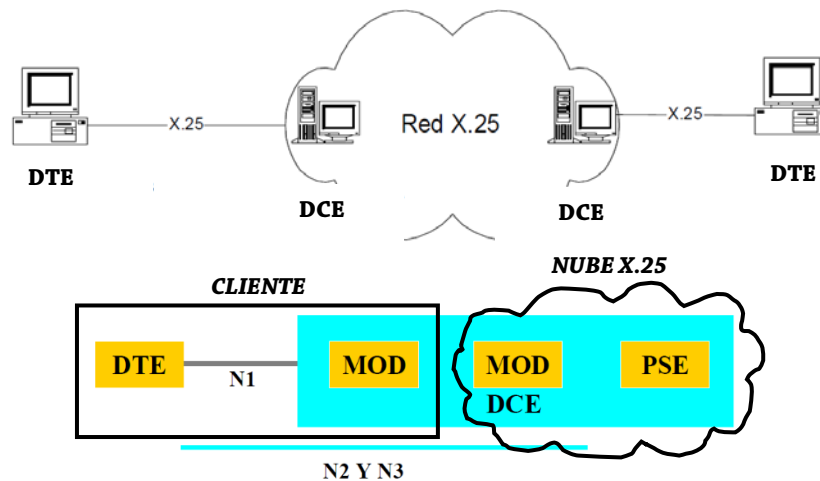
- **SLIP (Serial Line IP)** → protocolo de proceso de tramas usado antaño para envíos IP a través de una línea serial.
- Encapsula datagramas IP.
- Ventajas del PPP:
 - Permite la conexión tanto mediante líneas síncronas como asíncronas.
 - Permite la asignación dinámica de direcciones IP en ambos extremos de la conexión.
 - PPP permite el transporte de varios protocolos de red sobre él. SLIP permite IP solamente.
 - Implementa un mecanismo de control de red NCP.
 - PPP se puede usar también para crear VPN tanto cifradas como no cifradas, pero si se la desea cifrada se debe implementar por debajo de PPP.

UNIDAD 7a · PROTOCOLO X.25

El protocolo X.25 es un protocolo (de WAN) de conmutación de paquetes → Capas 1/2/3 del Modelo OSI.

- La transmisión es sincrónica → se tienen “bloques” (PDUs).
- Pensado para trabajar con enlaces poco confiables.
- Define una interfaz entre usuario y red, mediante DTE y DCE.
- Provee servicios con conexión o orientados a la conexión (con circuitos virtuales).

Estructura – Esquema



1. Se define una interfaz (Capa 1) entre el DTE y el DCE.
2. Se definen los módems [MOD]: uno del lado del cliente (forma parte del DCE que define la norma) y otro del lado de la red o nube X.25. Además, se definen los equipos conmutadores de paquetes.

X.25 resuelve la falta de confiabilidad en los enlaces con: detección de errores (Capa 2) y corrección de errores (Capa 3), vía ARQ.

Empaquetamiento

Capa Modelo OSI	Nombre PDU						
3	<i>Paquete</i>			Cabeza	Datos		
2	<i>Trama</i>	Bandera de Inicio	Campo de Dirección	Control Operativo	Información	Control de Errores	Bandera de Cierre
1	<i>Secuencia de Bits</i>	Secuencia de Bits					

CAPA 1 · FÍSICA → define características mecánicas/eléctricas/funcionales para conectar físicamente DTE con DCE.

- PDU → “Secuencia de bits”.
- Comprende las normas complementarias X.21 y X.21 bis:

	X.21	X.21 bis
Trabaja con ...	enlaces digitales, señales balanceadas.	... enlaces analógicos, señales desbalanceadas.
Velocidad máxima	64 Kbps.	20 Kbps.
Conector utilizado	DB-15 (15 pines).	DB-25 (25 pines)

PROTOCOLO HDLC · High-Level Data Link Control → protocolo de Capa 2 del Modelo OSI.

- Asegura el enlace de comunicación sin errores.
- Pensado para arquitecturas jerárquicas (primaria-secundaria: cliente-servidor, por ejemplo), en donde hay órdenes y respuestas.
- Del HDLC derivan varios protocolos, entre ellos: LLC, PPP, LAP, etcétera.
- Detecta y corrige errores en Capa 2.
- Corrección de errores → ARQ *sliding windows* (ventana deslizante).

Formato de la Trama → 1080 bits (135 B) máximo.

8 bits	8 bits	8 o 16 bits	Entre 0 y N bits	16 o 32 bits	8 bits
Bandera	Dirección de Destino	Campo de Control	INFO	FCS	Bandera

- **Banderas** → usadas para el sincronismo de bloque.
- **Dirección de Destino** → identifica al destino → puede ser un campo innecesario.
- **Campo de Control** → puede ser de 8 bits o de 16 bits:

○ 8 bits → hay 3 tipos:

De Información								De Supervisión								No numeradas							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0	N(S)				P/F	N(R)		1	0	S	P/F	N(R)		1	1	M	P/F	M					

N(S): número de secuencia de envío – P/F: bit de sondeo/final – N(R): número de secuencia de recepción.

○ 16 bits, aumentando la cantidad de números de secuencia → hay 2 tipos:

De Información																De Supervisión															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	N(S)								P/F	N(R)							1	0	S	0	0	0	0	P/F	N(R)						

N(S): número de secuencia de envío – P/F: bit de sondeo/final – N(R): número de secuencia de recepción.

- **FCS (Secuencia de Control de Trama)** → se usa CRC.

Tipos de Tramas

	No Numeradas	De Información	De Supervisión
Descripción	Establecimiento y Desconexión.	Para envío de datos.	Control de Errores. Control de Flujo.
Número de secuencia	No tiene.	Sí tiene.	Sí tiene.

Configuraciones

- Órdenes → de la estación primaria a la estación secundaria.
Respuestas → de la estación secundaria a la estación primaria.
- Balanceada → hay 2 estaciones primarias.
No balanceada → hay 1 estación primaria solamente → permite un enlace.

Modos de Operación

	NRM Respuesta Normal	ARM Respuesta Asíncrona	ABM Balanceado Asíncrono
Configuración	No balanceada.	No balanceada.	Cada estación se puede comportar como primaria y secundaria alternadamente.
La Transmisión se realiza sólo cuando lo indica la estación primaria.	... sin permiso de la estación primaria.	
Tipo de Enlace	Punto-a-Punto. Punto-a-Multipunto.	Punto-a-Punto.	Punto-a-Punto.
Tipo de Comunicación	<i>Half-Duplex.</i>	<i>Full-Duplex.</i>	<i>Full-Duplex.</i>

No balanceada → permite un enlace punto-a-punto o bien un enlace punto-a-multipunto.

Asíncrono/Asíncrona → no requiere el permiso de la estación primaria → no se puede tener multipunto.

Delimitación → elemento de sincronismo de bloque → dada por la bandera (1 octeto):

- 01111111 → línea inactiva, aún no activada.
- 01111110 → bandera.

Método de transparencia → inserción o eliminación de bit en secuencia similar a la bandera:

Si en el campo INFORMACIÓN hay una secuencia de bits 01111110, el receptor la interpretará erróneamente como bandera y no como información enviada. Este problema se evita con el **bit stuffing**, donde ante el quinto 1 consecutivo [11111] en el campo INFORMACIÓN, se le inserta un bit 0 (bit de inserción) en el lado del transmisor (→ si el receptor espera recibir X cantidad de bits –según lo indicado en el Campo de Control– pero luego recibe $X+3$ bits, el receptor sabrá que debe eliminar 3 bits de inserción).

El problema que acarrea el **bit stuffing** es el siguiente: si en el campo de información se tiene una secuencia 111110, donde ese 0 forma parte de la información enviada, el receptor lo interpretará erróneamente como bit de inserción y no como bit de información. Este segundo problema es solucionado por la capa superior.

FCS → CRC-16 → método para detectar errores.

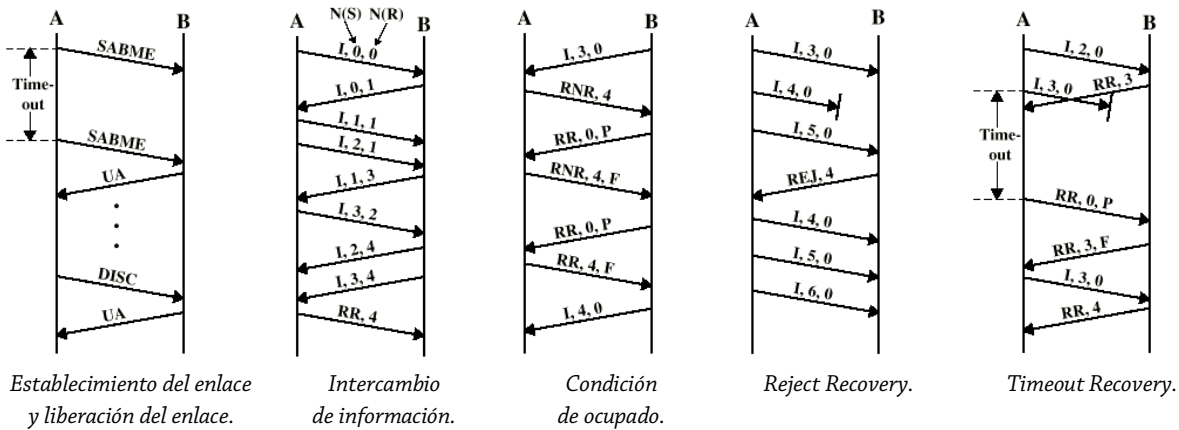
Métodos de direccionamiento

- Única para cada estación secundaria → no tiene sentido si se trabaja en punto-a-punto.
- De grupo → enlace multipunto (*multicast*).
- De difusión → enlace multipunto (*broadcast*).

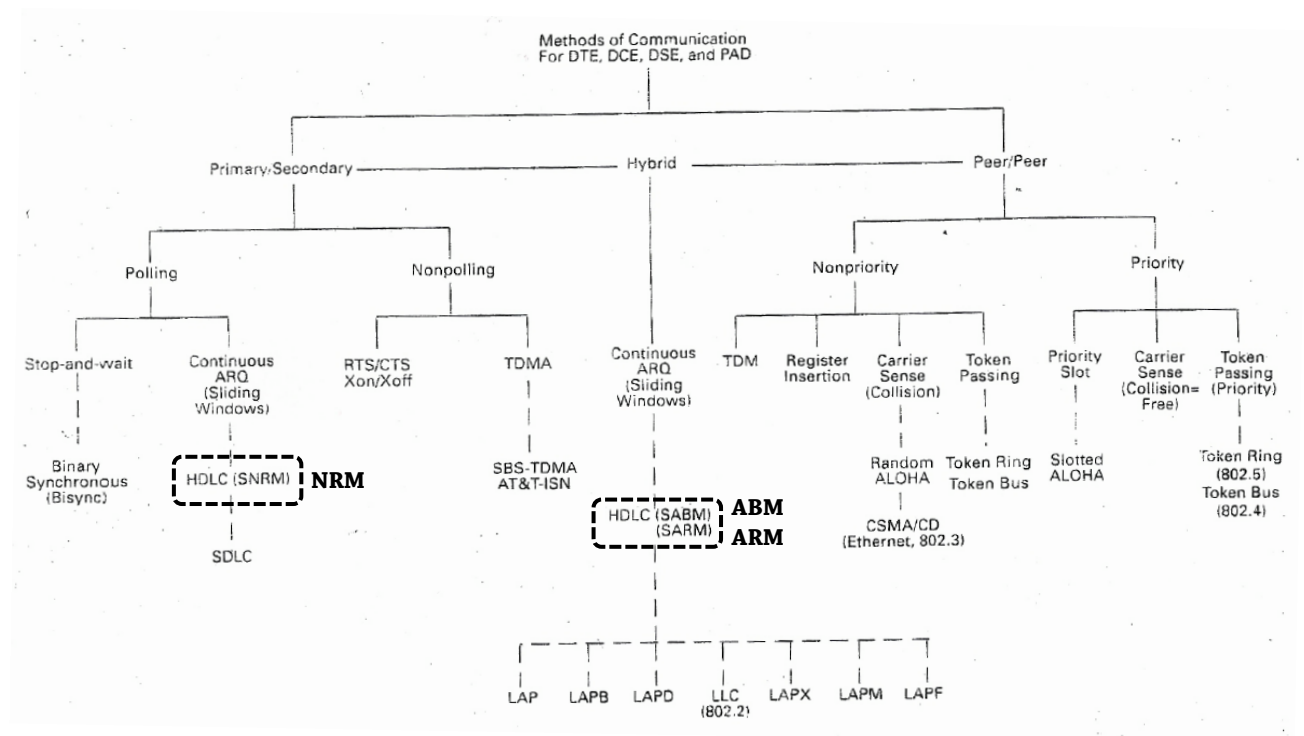
Bit P/F → usado para sondeo o escrutinio (*polling*).

- Si la trama va de la estación primaria a la secundaria → modo de pedir confirmación.
Si la trama va de la estación secundaria a la primaria → modo de dar confirmación.
- Bit=1 en un comando, indica que el receptor debe confirmar (se pide confirmación).
Bit=1 en una respuesta, indica que el receptor está confirmando (da confirmación).

Ejemplo de Funcionamiento – Intercambio de tramas en Capa 2:



Clasificación de los protocolos de comunicaciones



CAPA 2 · ENLACE → define los procedimientos para tener un enlace libre de errores.

- PDU → “trama”.
- Protocolo HDLC, versión LAP-B → procedimiento de acceso al enlace, modo balanceado, punto a punto.
- La transmisión es *full-duplex*.
- Usa ARQ *sliding windows* (ventana deslizante).
- Usa confirmación superpuesta mediante *piggyback*.
- Usa modo balanceado asincrónico (ABM).

CAPA 3 · RED → gestiona circuitos virtuales y maneja la conmutación de paquetes.

- Define tanto el formato de los paquetes como los procedimientos para el intercambio de paquetes y el establecimiento o la supervisión entre el DTE y el DCE de los circuitos virtuales con los DTE remotos.
- Maneja circuitos virtuales [VCs] y canales lógicos [LCs]:
 - **Circuitos virtuales** → asociación lógica de múltiples LCs entre origen y destino.
 - Alcance de extremo a extremo (DTE-DTE).
 - Pueden ser permanentes [PVC] o conmutados [SVC]:
 - PVC → la comunicación entre A y B es permanente.
 - SVC → la comunicación entre A y B es temporal (a demanda).
 - **Canales lógicos** → multiplexación del enlace de Capa 2 en varios canales de Capa 3.
 - Se numeran con un LCI (identificador de LC).
 - Alcance local → entre dispositivo y dispositivo.
- PDU → “paquete”.

Formato del Paquete

HEADER						DATOS DE USUARIO
14 b	12 b	8 b				
GFI	LCI	TPI	ADD	FAC	*	-

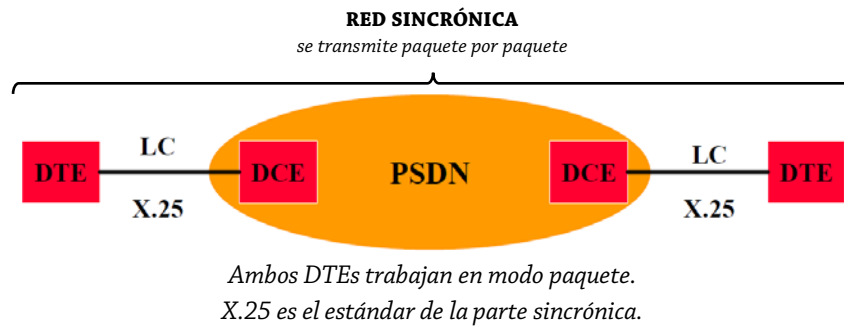
- GFI · Identificador de formato general → para numerar paquetes.
- LCI · Identificador de canal lógico → para numerar canales lógicos.
- TPI · Identificador de tipo de paquete → puede ser de llamada, de supervisión, de confirmación, de interrupción, de control de flujo y datos.
- ADD · Campo de Direcciones → opcional (en paquetes de llamadas):
 - Únicamente tiene sentido con SVC.
 - Plan de numeración → usado para número telefónico.
 - 15 dígitos como máximo → 4 para internacional, 9 para nacional, 2 para dispositivos.
 - Recomendación de norma → X.21.
- FAC · Campo de Facilidades → opcional (en paquetes de llamadas):
 - Cobro revertido.
 - Grupo cerrado de usuarios (CUG) → útil para seguridad, VPNs.
 - Selección rápida.
 - Negociación de tamaño de ventana, de paquete y de clase de tráfico.
- * · Campo de datos de usuario de llamada → opcional → identifica protocolo superior.

Parámetros de red a considerar – Facilidades

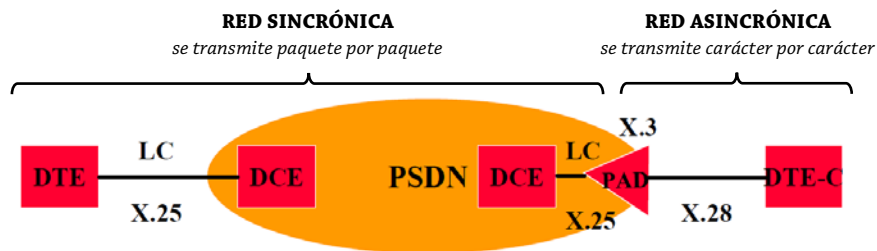
- Costos fijos y variables → no dependen de la distancia sino de paquetes (salvo en tarifa plana).
- Tamaños de paquete y de ventana.
- *Throughput* → velocidad real de transferencia de datos (sin errores) → $v_{Tx} > v_{realTx}$.
- Cantidad de LCs y tipo de LCs (entrante, saliente o bidireccional).
- Grupo cerrado de usuarios.
- Si se va a trabajar con PVC o SCV.
- Si se va a trabajar con selección rápida → “marcación rápida” en el teléfono.
- Cobro revertido → no se le cobra al transmisor sino al receptor.

Modos de Operación

- **Paquete** → modo síncrono total → VC (PVC o SVC).



- **Carácter** → modo síncrono/asíncrono.



Trabaja con un PAD → ensamblador/desensamblador de paquetes → vincula la parte síncrona con la parte asincrónica.
El PAD tiene 1 puerto síncrono y varios puertos asincrónicos.

UNIDAD 7b · PROTOCOLO FRAME RELAY

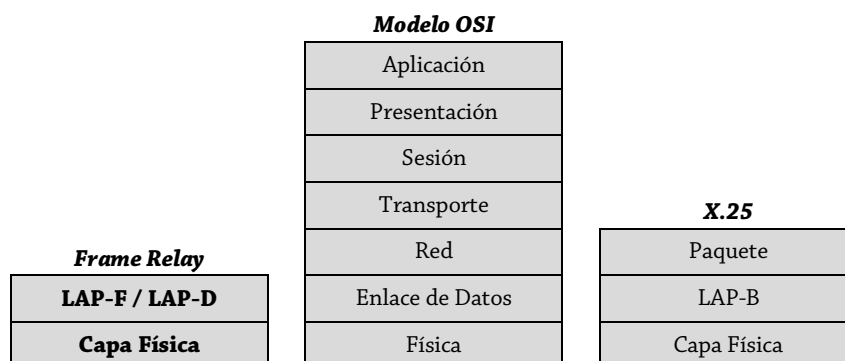
Frame Relay → **relevamiento de cuadro.**

- Técnica de conmutación de paquetes rápida.
- Trabaja sobre enlaces digitales de alta calidad → BER en el orden de los 10^{-7} (frente a los 10^{-4} de X.25).
- Se usa fundamentalmente para reemplazar líneas punto a punto dedicadas “LAN to LAN” (donde hay monopolio del recurso utilizado) por líneas conmutadas (donde los recursos se comparten, lo cual puede desencadenar en problemas de congestión); aunque se pueden usar ambas a la vez.
- Las estaciones terminales (los extremos) dan: detección de errores, corrección de errores (el cual no es problema de *Frame Relay* sino de las aplicaciones), control de secuencia y control de flujo.
- Las estaciones intermedias retransmiten información.

Características

- Alta velocidad respecto de X.25.
- Baja latencia → menor retardo en el procesamiento.
- Se basa en circuitos virtuales de Capa 2 → hay menor procesamiento.
X.25 se basa en CVs de Capa 3 permanentes (PVC) o conmutados (SVC).
- Trabaja con circuitos virtuales permanentes (PVC) → no hay opción para conmutar CVs.
X.25 trabaja con circuitos virtuales permanentes (PVC) y conmutados (SVC).
- El CLI (identificador de canal lógico) de X.25 ahora se llama DLCI (identificador de canal de enlace de datos).
- El CV es una asociación lógica de DLCIs.
Cada enlace tiene varios DLCIs → de la asociación de esos enlaces nace el CV que une extremo con extremo.
- El DLCI tiene significador local.
- La conmutación se produce en Capa 2 a nivel de cuadro (en X.25 se produce en Capa 3, a nivel de paquete).
- Uso dinámico del ancho de banda → la red da servicio en función del tráfico que hay, adaptándose de manera que todo el tráfico de todas las redes pueda pasar. En X.25 el uso del ancho de banda era estático.
- Orientado a tráfico por ráfagas (tipo LAN).
- Se define una interfaz entre CPE (equipo en la instalación del cliente) y POP (punto de presencia).
 - CPE → *routers* o FRADs (dispositivos de acceso a *Frame Relay*; símil PAD).
 - POP → nodos, conmutadores rápidos que ofrecen puertos de acceso a la red *Frame Relay*.
- Divide el tráfico en dos vías: la información de las aplicaciones de los usuarios (se usa el protocolo LAP-F) y, por el otro lado, los datos de red (se usa el protocolo LAP-D).
- Es soportado sobre ISDN (red digital de servicios integrados → consiste en dar servicio hasta varios dispositivos simultáneamente por una misma línea) banda angosta.

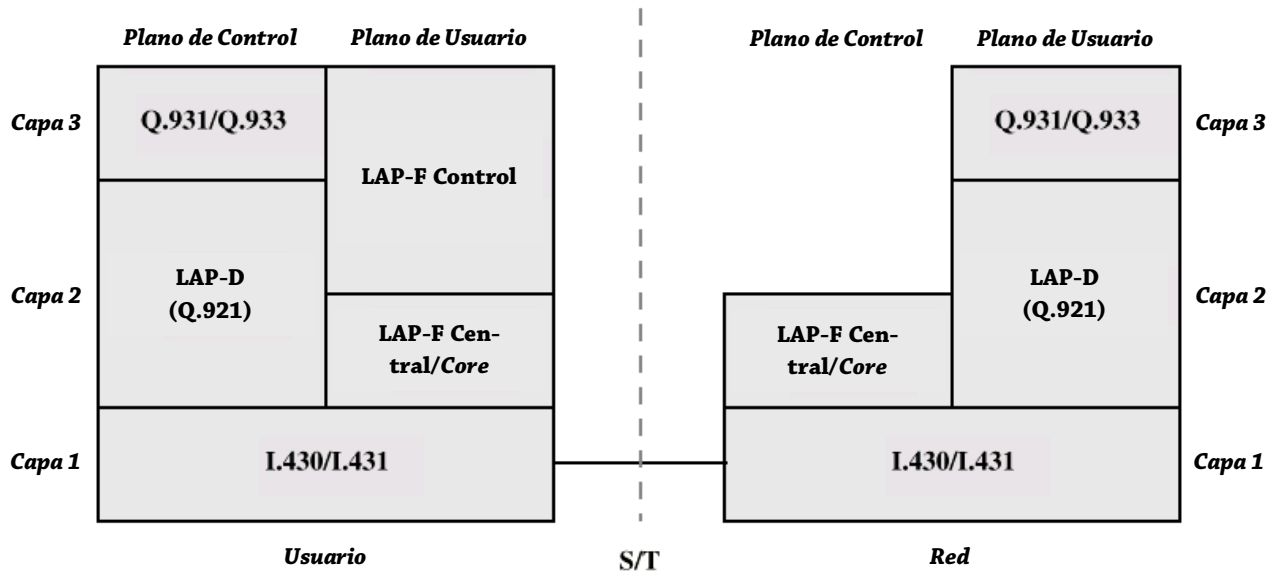
Ubicación respecto al Modelo OSI



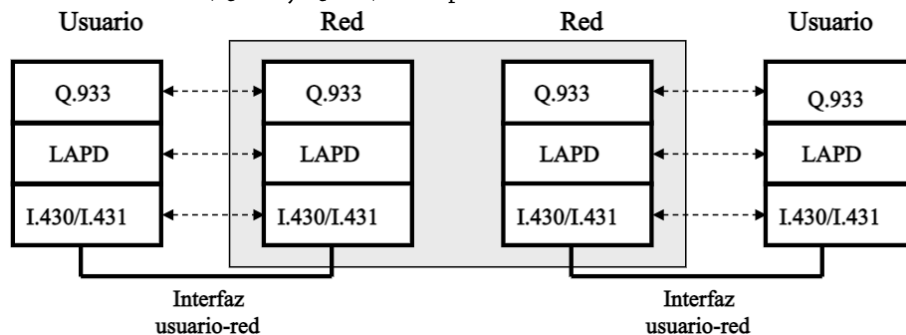
Arquitectura de Protocolos – Transferencia de Datos

Hay dos planos de operación:

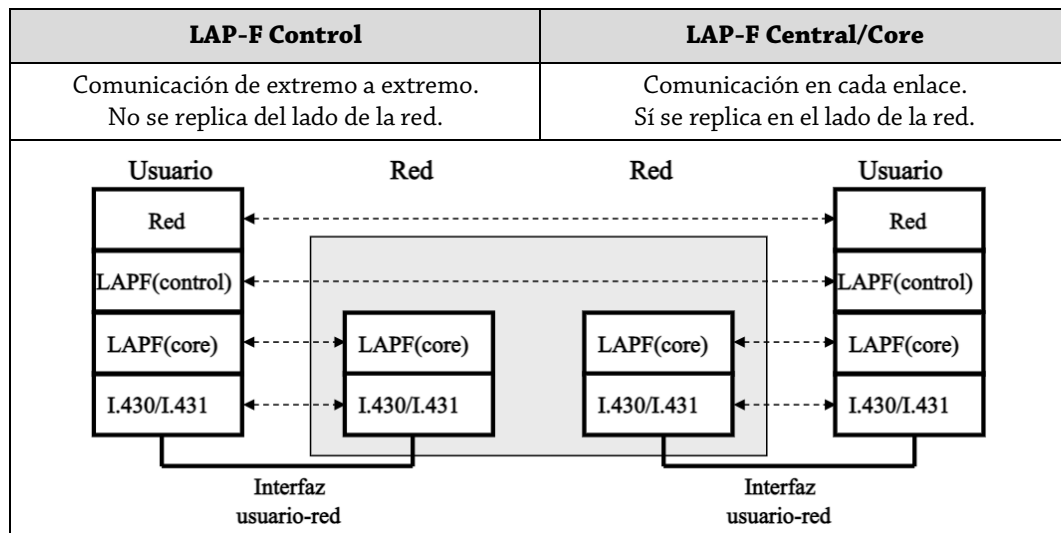
- Plano de Control → establecimiento/liberación de conexiones lógicas → se implementa entre usuario y red.
 - Trabaja con LAP-D.
- Plano de Usuario → transferencia de datos de usuarios → funcionalidad de extremo a extremo.
 - Trabaja con LAP-F.



- I.430 y I.431 → protocolos para ISDN.
- El **Plano de Control**, sobre el canal D, usa:
 - LAP-D (estándar Q.921) en Capa 2 → tanto en el lado del usuario como en el lado de la red.
 - Otros estándares (Q.931 y Q.933) en Capa 3 → tanto en el lado del usuario como en el lado de la red.



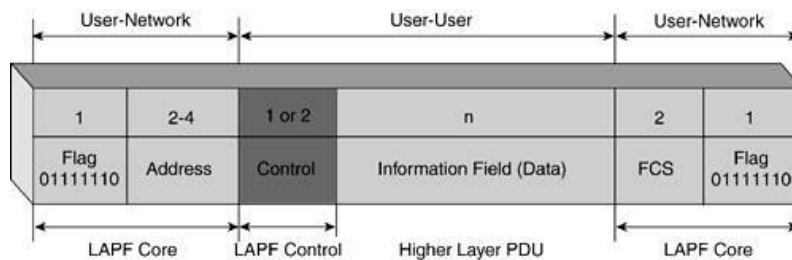
- El **Plano de Usuario** trabaja sobre canales B con **LAP-F Control** o **LAP-F Central/Core**:



Trama LAP-D → formato equivalente a la trama LAP-B y a la trama HDLC.

SD	destino	control	info	FCS	ED
----	---------	---------	------	-----	----

Estructura PDU para LAP-F Central/Core y LAP-F Control



- El Campo de Control está presente únicamente en LAP-F Control → en LAP-F Central/Core, no está.
- El LAP-F Central/Core maneja otras cosas en el Campo de Dirección.

Formato del Cuadro para LAP-F Central/Core → entre 1600 B y 4096 B.

1B	2B, 3B o bien 4B	2B	1B
Bandera	Campo de Dirección	INFORMACIÓN	FCS

• Campo de Dirección de 2B:

6 bits	1 bit	1 bit	4 bits	1 bit	1 bit	1 bit	1 bit
DLCI	C/R	EA0	DLCI	F	B	DE	EA1

- **DLCI** → identificador de canal de enlace de datos.
- **C/R** → comando/respuesta (uso por la aplicación).
- **EA0/EA1** → bit de extensión del campo de dirección (ubicado siempre al final de cada byte):
 - EA = 0 → hay otro byte para campo de dirección; éste no es el último byte.
 - EA = 1 → éste es el último byte del campo de dirección.
- **F · FECN** → notificación de congestión explícita hacia adelante:
 - F = 1 → hay congestión hacia adelante.
 - F = 0 → no hay congestión hacia adelante.
- **B · BECN** → notificación de congestión explícita hacia atrás:
 - B = 1 → hay congestión hacia atrás.
 - B = 0 → no hay congestión hacia atrás.
- **DE** → elegido para descarte:
 - DE = 1 → si hay congestión en la red, el cuadro se descartará.
 - DE = 0 → el cuadro no está elegido para descarte, no se descartará.

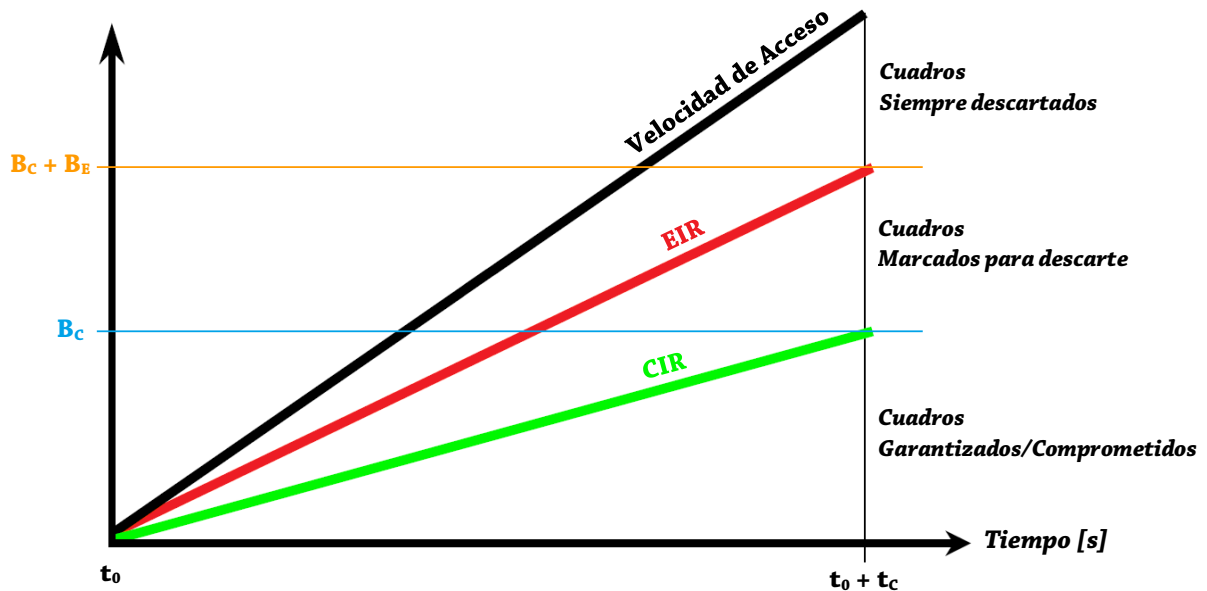
Campo de Dirección de 2B	Campo de Dirección de 3B	Campo de Dirección de 4B																																																																																																
10 bits para direccionar DLCIs.	16 bits para direccionar DLCIs.	23 bits para direccionar DLCIs.																																																																																																
<table><tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr><tr><td colspan="6">Upper DLCI</td><td>C/R</td><td>EA 0</td></tr><tr><td colspan="4">Lower DLCI</td><td>FECN</td><td>BECN</td><td>DE</td><td>EA 1</td></tr></table>	8	7	6	5	4	3	2	1	Upper DLCI						C/R	EA 0	Lower DLCI				FECN	BECN	DE	EA 1	<table><tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr><tr><td colspan="6">Upper DLCI</td><td>C/R</td><td>EA 0</td></tr><tr><td colspan="4">DLCI</td><td>FECN</td><td>BECN</td><td>DE</td><td>EA 0</td></tr><tr><td colspan="6">Lower DLCI or DL-CORE control</td><td>D/C</td><td>EA 1</td></tr></table>	8	7	6	5	4	3	2	1	Upper DLCI						C/R	EA 0	DLCI				FECN	BECN	DE	EA 0	Lower DLCI or DL-CORE control						D/C	EA 1	<table><tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr><tr><td colspan="6">Upper DLCI</td><td>C/R</td><td>EA 0</td></tr><tr><td colspan="4">DLCI</td><td>FECN</td><td>BECN</td><td>DE</td><td>EA 0</td></tr><tr><td colspan="6">DLCI</td><td></td><td>EA 0</td></tr><tr><td colspan="6">Lower DLCI or DL-CORE control</td><td>D/C</td><td>EA 1</td></tr></table>	8	7	6	5	4	3	2	1	Upper DLCI						C/R	EA 0	DLCI				FECN	BECN	DE	EA 0	DLCI							EA 0	Lower DLCI or DL-CORE control						D/C	EA 1
8	7	6	5	4	3	2	1																																																																																											
Upper DLCI						C/R	EA 0																																																																																											
Lower DLCI				FECN	BECN	DE	EA 1																																																																																											
8	7	6	5	4	3	2	1																																																																																											
Upper DLCI						C/R	EA 0																																																																																											
DLCI				FECN	BECN	DE	EA 0																																																																																											
Lower DLCI or DL-CORE control						D/C	EA 1																																																																																											
8	7	6	5	4	3	2	1																																																																																											
Upper DLCI						C/R	EA 0																																																																																											
DLCI				FECN	BECN	DE	EA 0																																																																																											
DLCI							EA 0																																																																																											
Lower DLCI or DL-CORE control						D/C	EA 1																																																																																											

Tráfico por Ráfagas – Definiciones y Parámetros

- Puertos → permiten el ingreso a la red.
 - Los POPs proveen puertos
 - De los puertos nacen los PVC.
- t_c [s] → tiempo comprometido; intervalo de medición (con o sin actividad).
- B_c [bit] → cantidad comprometida/garantizada de ráfaga.
 - Cantidad mínima de bits que se transmiten por un PVC en un tiempo t_c en condiciones normales.
- B_E [bit] → cantidad en exceso de ráfaga.
- AR [bps] → velocidad de acceso, velocidad de puerto → velocidad máxima de entrada a la red *Frame Relay*.
 - Rango: entre 64 Kbps y 2 Mbps.
- CIR [bps] → velocidad de información comprometida/garantizada para el PVC en condiciones normales.
- EIR [bps] → velocidad de información en exceso para el PVC en condiciones normales.

$$CIR = \frac{B_c}{t_c} \quad EIR = \frac{B_E}{t_c} \quad v_{puerto} = \frac{B_c + B_E}{t_c} = CIR + EIR$$

Cantidad de Bits



<p>“Full CIR”</p> <p>$CIR = 100\%$ de v_{puerto}</p>	<p>$CIR = 50\%$ de v_{puerto}</p> <p>$CIR < v_{puerto}$</p> <p>$v_{puerto} = \frac{B_c + B_E}{t_c}$</p> <p>$v_{puerto} = CIR + EIR$</p>	<p>$v_{puerto} > \frac{B_c + B_E}{t_c}$</p> <p>$v_{puerto} > CIR + EIR$</p>	<p>$B_c = 0$</p> <p>$CIR = 0$</p>
<p>No hay cantidad en exceso.</p> <p>No hay cantidades que se descarten en forma directa.</p>	<p>No hay descarte directo.</p>	<p>El proveedor garantiza algo.</p> <p>Algo queda marcado para descarte y el resto queda para descarte directo.</p>	<p>El proveedor no garantiza nada.</p> <p>Todo lo que pase está marcado para descarte.</p>

Control de Errores, de Congestión y de Flujo

- Control de Errores → solamente detección de errores (campo FCS) en las estaciones terminales (los extremos).
 - Las capas superiores se ocupan de la corrección de errores.
 - En el LAP-F Central/Core, no se lleva secuenciamiento de cuadros, que sí lo hace LAP-F Control.
- Prevención de Congestión → mediante FECN y BECN.
 - Cuando la congestión es en el mismo sentido que va el cuadro, se setea el FECN.
 - Cuando la congestión es en el sentido opuesto en que va el cuadro, se setea el BECN.
 - Estos bits son: seteados por los POP, y detectados por los CPEs y el administrador de la red.
- Control de Congestión → hecha por el LAP-F Central/Core.
 - La congestión, que se produce en la nube, puede producirse por retardos en la comunicación o cuando no se establece la comunicación.
 - Se rechazan cuadros mediante datos elegidos para descarte (campo DE).
- Control de Flujo → hecha por el LAP-F Control.
 - Se produce en los extremos de la comunicación.

Sobresuscripción → ocurre cuando la suma de los CIR de cada PVC supera la velocidad de puerto.

VoFR · Voz sobre Frame Relay → se prioriza el tráfico y el uso de DLCI para voz.

- La voz es tolerante a pérdidas, pero no a retardos.
- Menores QoS (calidad de servicio) y costos frente a comunicaciones telefónicas convencionales.
- En teoría, VoFR es más eficiente que VoIP.
- Uso de voz sin comprimir (64 Kbps PCM) y comprimida.

La voz comprimida se resuelve: priorizando el tráfico y el uso de DLCI especial para voz; utilizando menor tamaño de cuadros (para evitar fragmentación); utilizando rutas con pocos saltos (para evitar retardos)

- Comparación VoFR vs VoIP:

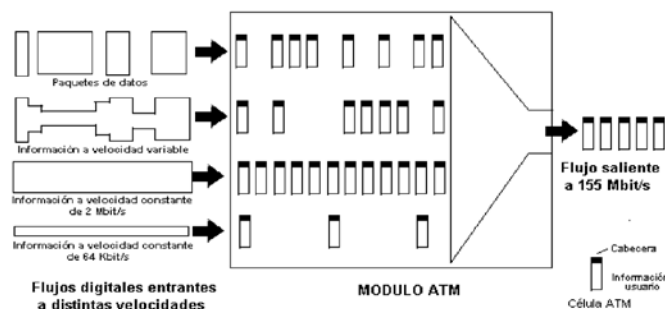
VoFR	VoIP
La voz viaja sobre cuadros <i>Frame Relay</i> .	La voz viaja sobre datagramas IP.
Trabaja en Capa 2.	Trabaja en Capa 3, generando mayor procesamiento.
VoFR es más confiable que VoIP.	VoIP tiene mayor alcance que VoFR.
Con conexión (CVs).	Sin conexión.

UNIDAD 8 · PROTOCOLO ATM

ATM → modo de transferencia asincrónico.

- Montado sobre redes ISDN banda ancha (B-ISDN), basadas en tecnología SDH.
- Enlaces de alta calidad → permiten velocidades binarias de más de 2,4 Gbps.
- Permiten transportar todo tipo de servicio → voz, video, datos y combinaciones entre ellos.
- Requiere capas de adaptación para integrar servicios.
- Trabaja con conmutación rápida con muy bajos retardos.
- Reducción de funcionalidades en los nodos → delegación de funciones a los extremos (estaciones terminales).
- Orientado a la conexión.
- PDU → “celda” o “célula”; son pequeñas y de tamaño fijo → 53 B.
- ¿Por qué “asincrónico”?
 - La red es sincrónica → las celdas se transportan sobre canales sincrónicos.
 - No hay sincronización con respecto a ningún usuario.
 - Las posiciones dentro de una ráfaga no son fijas, sino que se asignan a demanda.

Proceso de Adaptación



Todos los tipos de datos se van convirtiendo en celdas con sus respectivos HEADERS. Luego, estas celdas pasan por una tolva para finalmente quedar listas para viajar por la red.

Formato de la Celda → 53 B. Al ser de tamaño fijo y pequeño → procedimiento sencillo y menores retardos.



- **HEADER** → lleva información de enrutamiento y prioridad.

Su estructura depende si se aplica en una interfaz UNI o en una interfaz NNI:



UNI (interfaz usuario-red)						NNI (interfaz red-red)				
4 b	8 b	16 b	3 b	1 b	8 b	12 b	16 b	3 b	1 b	8 b
GFC	VPI	VCI	PT	CLP	HEC	VPI	VCI	PT	CLP	HEC

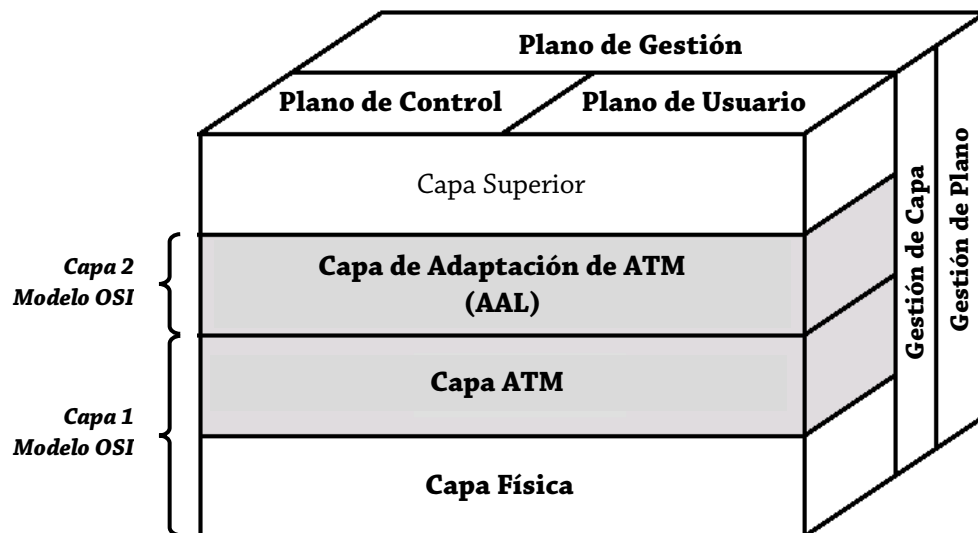
- **GFC** → control de flujo genérico → únicamente está presente en UNI (no está en NNI).
 - **VPI** → identificador de trayecto virtual.
 - **VCI** → identificador de circuito virtual.
 - **PT** → tipo de carga útil (de usuario o de gestión de red / mantenimiento).
 - **CLP** → prioridad de pérdida de celda → CLP=0, alta; CLP=1, puede descartar la red.
 - **HEC** → control de errores de HEADER (detección y, a veces, corrección error simple).
- **PAYLOAD** → información en sí (video, voz o datos) e información de operación y mantenimiento.

Trayectos y Canales Virtuales

- Los circuitos virtuales (de X.25 y *Frame Relay*) se llaman canales virtuales [CVs].
 - La fuente, con uno más destinos → puede ser punto-a-multipunto.
 - Los VCI (identificadores de canal virtual) sí se pueden repetir.
 - Los VCI son para conectar → la conexión está dada por los VCI (son la esencia).
- Los trayectos virtuales [VPs] son agrupamientos de canales virtuales que tienen los mismos destinos.
 - Los VPIs son para gestión y conmutación.
 - Los VPIs (identificadores de trayecto virtual) no se pueden repetir.

Arquitectura de Protocolos WAN – Capas y Subcapas

- Hay tres planos de operación:
 - Plano de Usuario → transferencia de información de usuarios y controles de flujo y errores.
 - Plano de Control → controles de llamada y de conexión.
 - Plano de Gestión/Administración:
 - Gestión/Administración de Plano → coordinación entre planos y como un todo.
 - Gestión/Administración de Capa → recursos y parámetros de protocolos.

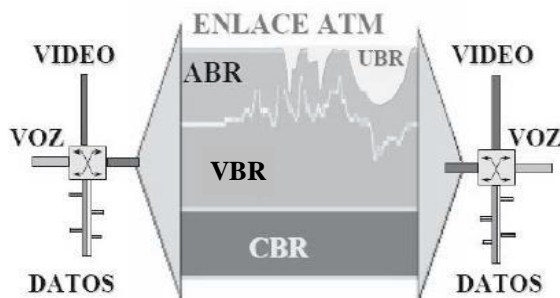


Modelo OSI	Capas ATM	Subcapas ATM	Acciones
	Altas		
Capa 2	AAL	Convergencia	Homogeniza las diferencias que recibe de las capas superiores. Identifica mensajes. Recupera señal de reloj.
		Segmentación y Reensamblado	Segmenta la información de capas superiores (el emisor segmenta, el receptor reensambla). Permite manejar cuadros de mayor longitud que las celdas, adaptando la información a los 48 B del PAYLOAD.
Capa 1	ATM		Arma/Desarma las celdas colocando/retirando el HEADER. Hace la conmutación. Control de Congestión y de Flujo.
	Física	Convergencia de Transmisión	Regula las velocidades con que llega al medio físico (al trabajar con distintos servicios). Convierte el flujo de celdas ATM en flujos de bits.
		Medio Físico	Controla las funciones que dependen del medio físico: tipos de cable, conectores, niveles de señales, etc.

Altas	Tramas de Aplicación	AAL	Carga de Celdas	ATM	Celdas	Física	Bits
-------	----------------------	-----	-----------------	-----	--------	--------	------

Clases de Servicio

Servicio	Velocidad	Acrónimo	Ejemplo
En tiempo real (sensible a retardos)	Constante	CBR	Velocidad constante fija durante toda la conexión y retardo máximo estable. Audio y video sin comprimir. Circuito E1 videoconferencia.
	Variable	rt-VBR	Fuertes restricciones al retardo y a su variación. Transmisión de video (no voz → velocidad variable). Con compresión.
En no tiempo real (no hay criticidad en tener respuesta)	Variable	nrt-VBR	Requisitos críticos en respuestas. Correo electrónico multimedia.
	Disponible	ABR	Reserva con conocimiento de AB necesario. Interconexión de LANs. Transmisión por ráfagas.
	No especificada	UBR	Aprovecha la capacidad sin usar. FTP en segundo plano. IP (best effort).
	De tramas garantizada	GFR	Servicio a subredes troncales IP.



En un tráfico puede haber distintas combinaciones.

Protocolos de AAL



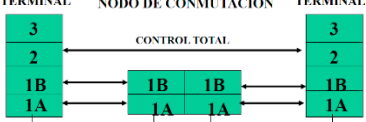
Requerimiento	Clase A	Clase B	Clase C	Clase D
Tiempo entre Fuente y Destino	Requerido (sensible a demoras). rt		No requerido (no sensible a demoras). nrt	
Velocidad (Bit Rate)	Constante CBR	rt-VBR	Variable nrt-VBR	
Modo de Conexión	Con conexión	Sin conexión		
Protocolo	AAL 1	AAL 2	AAL 3	AAL 4
Tipos de Datos Transmitidos	Audio y Video sin comprimir	Video comprimido	Datos en general	

- **AAL 5** es otro protocolo → servicio con menor *overhead* y mejor detección de errores.
 - Emulación LAN, *Frame Relay*, ATM, IP sobre ATM.

Cuadro comparativo de tecnologías

	X.25	Frame Relay	ATM
Niveles de Protocolos	1, 2 y 3 del Modelo OSI.	1 y 2 del Modelo OSI.	Medio Físico, ATM y AAL.
Velocidad bin. máxima	64 Kbps.	2 Mbps o más.	622 Mbps ~ 2,4 Gbps.
Control de Errores	Detección y Corrección salto por salto. LAP-B (HDLC).	Nodos intermedios RTX. Los extremos detectan. Las capas superiores corrigen. LAP-D y LAP-F (HDLC).	Sólo de extremo a extremo hay control de HEADER y de CELDA: detecta y a veces corrige. Las capas superiores corrigen. Detecta en el HEADER solamente.
Soporte de Comunicaciones	Red analógica y digital. Baja calidad.	ISDN. Mejor calidad.	B-ISDN. Alta calidad.
BER	$\sim 10^{-4}$.	$\sim 10^{-7}$.	$\sim 10^{-12}$.
Nombre PDU	Trama y Paquete.	Cuadro.	Celda o Célula
Longitud PDU	Grande y variable. 16 B / 1024 B.	Grande y variable. 1600 B / 4096 B.	Pequeño y fijo. 53 B.
Longitud MTU	128 B (Capa 3).	4090 B.	48 B.
Tipo de Tráfico más adecuado	File Transfer, Batch, Correo electrónico.	Ráfagas (LAN), voz.	Información en tiempo real, voz, video.
Tipo de Servicio	Con conexión.	Con conexión.	Con conexión.
Conmutación	En Capa 3. Por software. Mayor procesamiento.	En Capa 2. Por software. Menor procesamiento.	Por hardware. Menor retardo.
Multiplexación e Identificadores	LC (canal lógico). VC (circuito virtual). LCI.	VC (circuito virtual). DLCI.	VP (camino virtual). VC (circuito virtual). VPI y VCI.
Eficiencia	Asignación fija.	Asignación por demanda.	Asignación por demanda.

Comparación de Control de Errores por Niveles

X.25	Frame Relay	ATM
Control total, capa por capa, con detección y corrección.	Sólo detección en todo el cuadro.	Sólo detección en la celda.
		

UNIDAD 8 · PROTOCOLO MPLS

MPLS → *conmutación de etiquetas multiprotocolo*.

- Tecnología que busca simplificar o mejorar la eficiencia de las redes.
- Puede considerarse como un protocolo para acelerar el encaminamiento de los paquetes.
Puede considerarse como un protocolo para hacer túneles.
- Integra Capas 2 y 3 del Modelo OSI → combina ventajas de control de enrutamiento (Capa 3 – protocolo IP) y ventajas de una conmutación rápida (Capa 2).
Constituye la evolución de las tecnologías de integración de Capas 2 y 3 → IP sobre ATM y conmutación IP.
- Funciona sobre cualquier tecnología de Capa 2 → PPP, LAN, *Frame Relay*, ATM, etcétera.
- Proporciona QoS e ingeniería de tráfico a una red global que soporte todo tipo de tráfico.
- Es una solución con grandes posibilidades de éxito debido a la facilidad a la hora de migrar una red actual (*Frame Relay*, ATM, Ethernet, ...) a MPLS, siendo el primer paso para la coexistencia entre ellas mediante software añadido a equipos actuales.
- Facilita la migración a IPv6, en la que se acortará la distancia entre el nivel de red IP y la fibra óptica.
- Permite nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino).

Componentes

- **LSRs (*Label Switching Router*)** → ROUTERs con capacidad de conmutación de etiquetas.
 - ROUTERs de alta velocidad especializados en el envío de paquetes etiquetados por MPLS.
 - Pueden ser internos o externos:
 - LSR internos → sacan una etiqueta y ponen otra y arman túneles, mejorando la conmutación y el procesamiento, reduciendo la latencia.
 - LSR externos → agregan/sacan etiquetas → se ocupa de manejar la clasificación por FEC.
- **Etiqueta** → identificador corto (de longitud fija).
 - Se analiza en cada salto (solamente la etiqueta se analiza).
 - La PDU transferida puede tener una o varias etiquetas, pudiendo jerarquizarlas.
- **FEC (*Forwarding Equivalence Class*)** → clase de servicio con la cual se facilitan los intercambios.
 - Atributo por el que se clasifican los paquetes que ingresan.
 - Se asigna en el momento en que el paquete entra a la red (al LSR externo).
 - Todos los paquetes que tienen el mismo FEC van a viajar por el mismo LSP.
- **LSP (*Label Switched Path*)** → camino de conmutación de etiquetas.
 - Ruta a través de uno o más LSRs en un nivel de jerarquía que sigue un paquete de un FEC en particular.

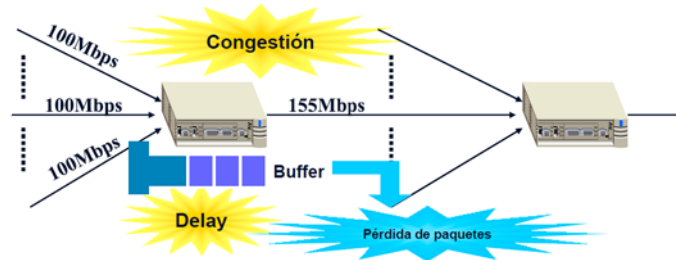
Formato del HEADER (genérico) → 34 b.

Datos de Usuario	HEADER IP	8 b	1 b	3 b	20 b	HEADER Capa 2
		TTL	S	EXP	Etiqueta	
		HEADER MPLS				
	Capa 3	Capas 2 y 3				Capa 2

- **TTL (*Time To Live*)** → contador de tiempo de vida → funcionalidad estándar TTL de las redes IP.
- **S** → bit de pila, usado para indicar el apilado de etiqueta de forma jerárquica.
 - S=1 → hay otra etiqueta a continuación.
 - S=0 → hay una única etiqueta.
- **EXP** → identificador de las clases de servicio (CoS).
- **Etiqueta**.

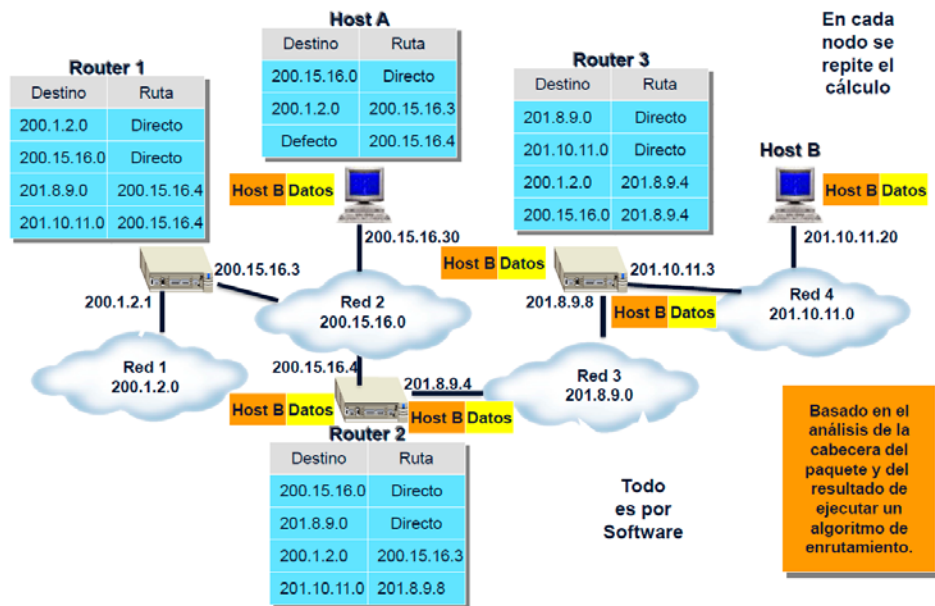
Problemas en las redes que MPLS busca resolver

- Calidad de Servicio (QoS):



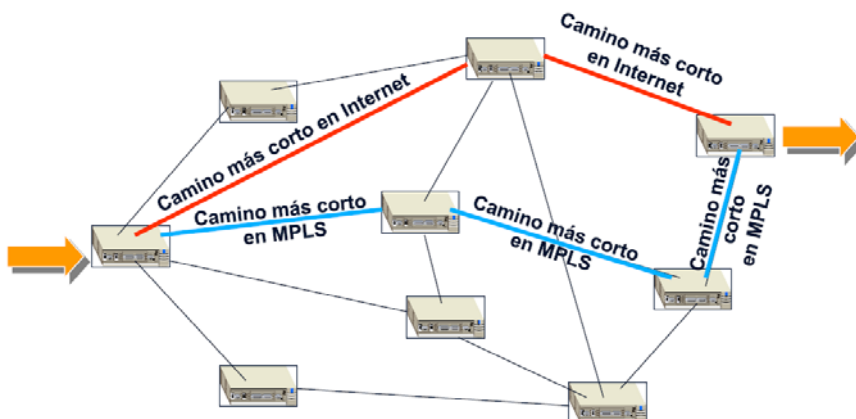
La calidad de servicio se ve afectada por retardos (delay), congestiones y pérdida de paquetes.
Cada router debe estar analizando el datagrama IP, su HEADER y eso genera retardos.

- IP Routing:



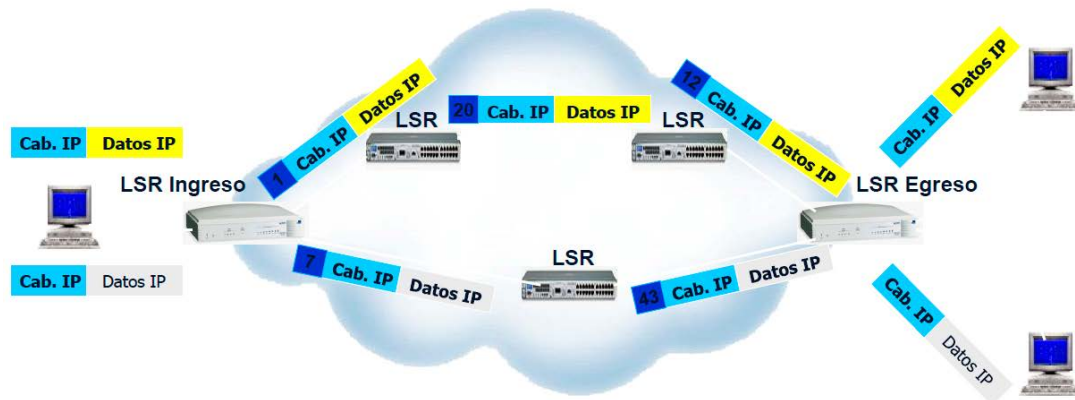
El proceso de análisis de direcciones y enrutamiento se debe hacer en cada nodo perteneciente a una red IP.
Cada terminal y ROUTER tiene su tabla de enrutamiento.

- El Camino Más Corto:



MPLS busca el camino más óptimo, independientemente de la cantidad de ROUTERs que atraviesa.

Funcionamiento – Esquema General



1. Los datagramas IP ingresan al LSR de ingreso, donde se determina el FEC. Asignado el FEC, se determina el LSP (camino). Y en función del LSR, se aplican las etiquetas. Ya en la nube, cada datagrama IP tiene una etiqueta.
2. Cuando el datagrama IP llega a un LSR, se cambia la etiqueta... y se van pasando.
3. Cuando el datagrama IP llega al LSR de egreso, éste le saca la etiqueta. Y ahí finaliza el proceso.

Control de Información

- Generación de tablas de envío que establecen los LSPs.
 - Uso de protocolos de enrutamiento internos IGP → OSPF, ISIS, RIP.
- Distribución de la información sobre las etiquetas a los LSRs.
 - Uso de diversos protocolos con variaciones en el intercambio de etiquetas, como:
 - LDP → mapea los destinos IP (*unicast*) en etiquetas.
 - RSVP, CR_LPD → usado para ingeniería de tráfico y reserva de recursos.
 - BGP → para etiquetas externas (VPN).

Servicios de Voz sobre MPLS

El protocolo MPLS permite sostener distintas redes:

- Voz sobre MPLS.
- Voz troncalizada sobre MPLS.
- IP sobre MPLS.
- ATM sobre MPLS.

UNIDAD 9 · SEGURIDAD EN REDES DE DATOS

Conceptos Generales

- Confidencialidad o Privacidad → acceso a la información sólo mediante autorización, de forma controlada.
- Autenticidad → asegurarse que la persona sea quien dice ser que es.
- Integridad de datos → modificación de la información sólo mediante autorización; evitar pérdida de datos.
- Ataques informáticos que afectan la seguridad: interceptación, virus, modificación/destrucción de archivos, ...

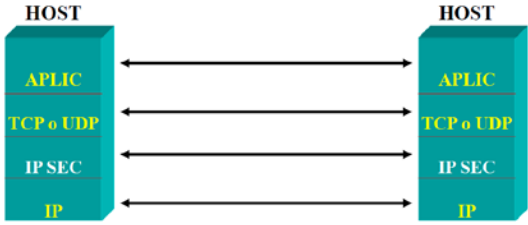
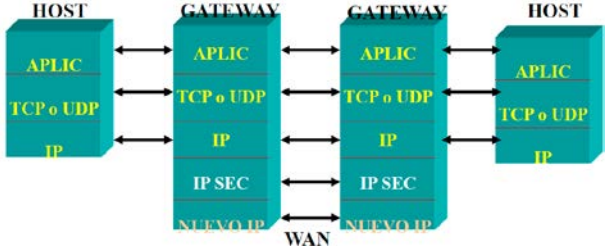


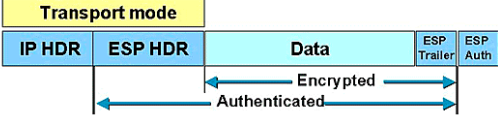


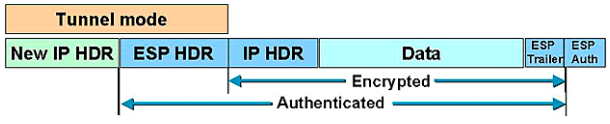
Estrategias/Métodos de Seguridad → lo mejor es superponer métodos, no limitarse a solamente uno:

- Control de acceso → se usan claves (y hasta sistemas biométricos) para acceder al sistema o a recursos.
- Encriptado de datos → preserva la confidencialidad de los datos.
- Seguridad física de los dispositivos → deben estar en sitios seguros y condiciones adecuados.

Muy vinculado a los Data Center, donde se guardan servidores con varios sistemas de segurización. Los Data Center tienen varias categorías de seguridad → TIER I, TIER II, TIER III (ARSAT tiene TIER III) y TIER IV.

- **Firewall** → componente que crea una barrera segura entre una red interna/privada y red externa/pública.
 - La configuración del *firewall* debe ser la adecuada → depende del tipo de organización, de la sensibilidad de los datos que maneja y del uso que se le da.
 - Se compone de hardware y software.
 - Beneficios:
 - Concentra seguridad en un único punto.
 - Da control de acceso → habilita o no el acceso.
 - Regula el uso de la red exterior → impide salidas innecesarias hacia afuera desde el interior.
 - Registra el empleo de la red interna y externa → se puede saber qué hizo cierto dispositivo.
 - Da protección frente a ataque externos.
 - Limita el tráfico de servicios vulnerables.
 - Mejora la privacidad → ejemplo: ocultando direcciones IP internas o bloqueando servicios.
 - Decisiones al implementar un *firewall*:
 - Política de seguridad de la organización:
 - Negación de todos los servicios, excepto algunos autorizados.
 - Permitir libre uso de todo, excepto lo expresamente prohibido.
 - Medir y auditar el uso de la red.
 - Nivel de seguridad deseado:
 - Análisis de necesidades con niveles de riesgo aceptables.
 - Nivel de seguridad que satisface → solución de compromiso.
 - Evaluación de costos → mejor relación costo-beneficio.
 - Se aplican en distintas capas:
 - Capa de Red → direcciones IP y números de puerto. Ejemplo: router.
 - Capa de Aplicación → no permiten tráfico directo entre las redes. Ejemplo: servidor proxy.
- **Firma digital** → técnica de seguridad aplicada sobre cierta información digital que se intercambia en una red:
 - Basada en criptografía asimétrica (uso de claves - pública y privada- de un usuario) y en función matemática (hash → la salida siempre es de longitud fija).
 - Requiere de una autoridad que certifique la autenticidad del documento enviado con firma digital.
 - Provee autenticidad → el mensaje llegó de parte de quien dice ser que lo envió.
 - Provee integridad → el mensaje llega sin que se pierda nada en el camino.
 - Provee no repudio → el transmisor no puede negar que fue enviado por él (su procedencia).
 - Puede adicionarse (no es la esencia) el encriptado → se provee confidencialidad (privacidad).
- **Capacitación de usuarios y administradores** → es importante y necesario que los RRHH estén preparados.
- Red Privada Virtual (VPN) → se logran con enlaces debidamente segurizados, basados en IP Sec.

- **IP Sec** → protocolos de seguridad que permiten agregar encriptado y autenticación a las comunicaciones.
 - Es de Capa 3 → resulta totalmente transparente para las aplicaciones.
 - Uso frecuente en VPN.
 - Modos de aplicación → modo transporte o modo túnel.

Modo Transporte	Modo Túnel
 <p><i>Se implementa de host a host, sin que la red intervenga.</i></p>	 <p><i>No se implementa de host a host, sino entre gateways. La securización se agrega a nivel gateway.</i></p>
 <p>(a) Paquete IP original</p>  <p>(b) Modo transporte</p>  <p><i>Se encripta solamente el PAYLOAD. Se autentican el PAYLOAD y el HEADER del ESP. Se mantienen las direcciones IP originales.</i></p>	 <p>(a) Paquete IP original</p>  <p>(c) Modo túnel</p>  <p><i>Se encripta el PAYLOAD y el HEADER del IP. Se autentican el PAYLOAD, el HEADER del IP y el HEADER del ESP. Se usa una nueva dirección IP que será la única legible en toda la red pública, enmascarando la dirección IP original.</i></p>
<p><i>Más rápido (menor procesamiento) que el modo túnel. Menor latencia que el modo túnel. Menor protección que el modo túnel.</i></p>	<p><i>Más lento (mayor procesamiento) que el modo transporte. Mayor latencia que el modo transporte. Mayor protección que el modo transporte.</i></p>

Seguridad por Capas/Niveles del Modelo OSI – Aspectos a Considerar

Aplicación	<ul style="list-style-type: none"> • Auditoría de: servidores, accesos remotos, <i>firewall</i>, correos electrónicos, DNS, etcétera. • Control de archivos .LOG.
Presentación	<ul style="list-style-type: none"> • Criptografía.
Sesión	<ul style="list-style-type: none"> • Control de acceso.
Transporte	<ul style="list-style-type: none"> • Auditoría del establecimiento de sesiones y de los puertos (cuáles están habilitados). • Operación con conexión (TCP) o sin conexión (UDP).
Red	<ul style="list-style-type: none"> • Auditoría de las rutas y direcciones. • Trabajo en el ROUTER sobre: contraseñas, configuración, protocolo de ruteo, listas de control de acceso, archivos .LOG, alarmas, etcétera. • Auditoría en ARP y direccionamiento IP (estático o dinámico).
Enlace de Datos	<p>Es la última capa que encapsula a las capas anteriores.</p> <ul style="list-style-type: none"> • Uso de analizadores de protocolos → para control de direcciones MAC, de configuraciones, análisis de tráfico (<i>Wireshark</i>) y de colisiones, evaluación de accesos WiFi, etcétera.
Física	<ul style="list-style-type: none"> • Auditoría del canal que se use. • Plano de la red. • Análisis de la topología. • Puntos de acceso físico. • Potencias, frecuencias utilizadas.

Análisis de Riesgos de Seguridad → Riesgos basados en el comportamiento humano:

- Fugas de información → errores humanos o acciones accidentales por exceso de confianza.
- Ataques de virus → error humano producto de priorizar beneficios sobre los riesgos.
- Análisis de archivos .LOG (almacenan la actividad del usuario en el dispositivo) → usado en análisis forenses.

Seguridad en Redes Inalámbricas

- WPS (*WiFi Protected Setup*) → mecanismos para facilitar la conexión de dispositivos a una red inalámbrica.
 - El más usado es el intercambio de PIN.
- WEP (*Wired Equivalent Privacy*) → ofrece seguridad similar a la red cableada mediante una encriptación.
- WPA (*WiFi Protected Access*) → agrega seguridad usando claves dinámicas proporcionadas a cada usuario.
 - WPA2 → usa algoritmo de encriptación AES (*Advanced Encryption Standard*).
 - WPA2 PSK (*Pre-Shared Key*) → para uso doméstico o de oficinas pequeñas donde se comparte la clave.
 - WPA2 TKIP → usa un protocolo de seguridad de clave temporal que cambia las claves de un sistema dinámicamente a medida que se utiliza.
 - WPA3 → puede verse en equipos WiFi 5 y WiFi 6.
- Comparación entre WEP, WPA y WPA2:

	WEP	WPA	WPA2
Encriptación	RC4.		AES.
Rotación de clave	Ninguna.	Claves de sesión dinámicas.	
Distribución de clave	Tipeadas manualmente en cada dispositivo.	Distribución automática disponible.	
Autenticación	Usa clave WEP.	Puede usar 802.1x & EAP.	

- Escala de segurización de protocolos, ordenados de los más seguros a los menos seguros:
WPA2-AES → WPA2-TKIP → WPA-PSK → WEP 128 → WEP 64 → MAC Auth → (sin seguridad).
- Otros recursos de seguridad:
 - SSID → nombre de la red.
 - Filtrado de direcciones MAC.