

UNIDAD 6 · REDES WAN

Composición de una Red WAN

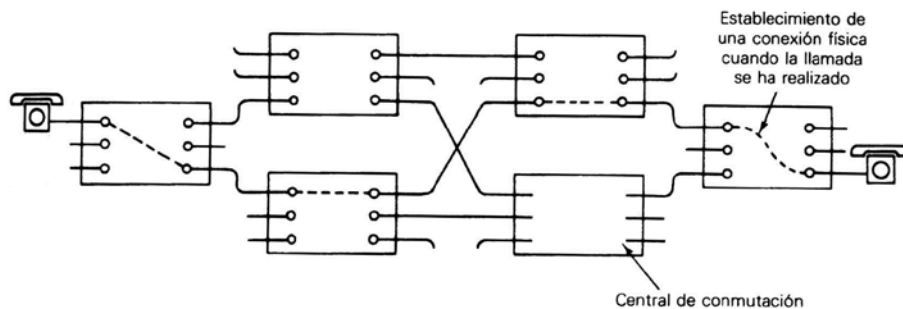
- Equipos terminales.
- Nodos de red.
- Enlaces de comunicaciones.

Tipos de Enlaces de comunicaciones

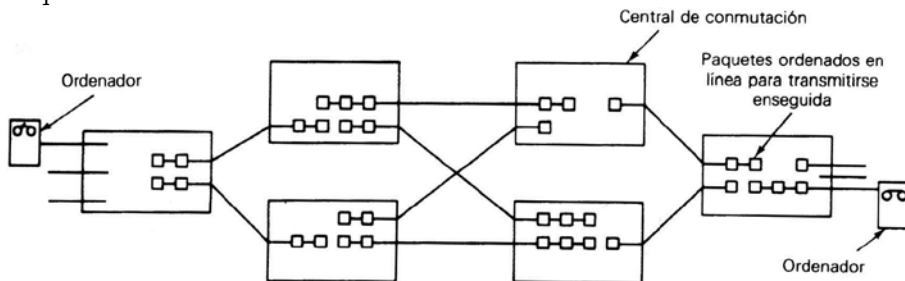
- Según los puntos que une:
 - Punto a Punto → ejemplos: ARQ, FEC.
 - Punto a Multipunto → ejemplo: FEC.
- Según las características:
 - Dedicados → el medio no se comparte → no hay intermediarios entre transmisor y receptor.
 - Conmutados → el medio se comparte → hay estaciones intermedias entre transmisor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

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

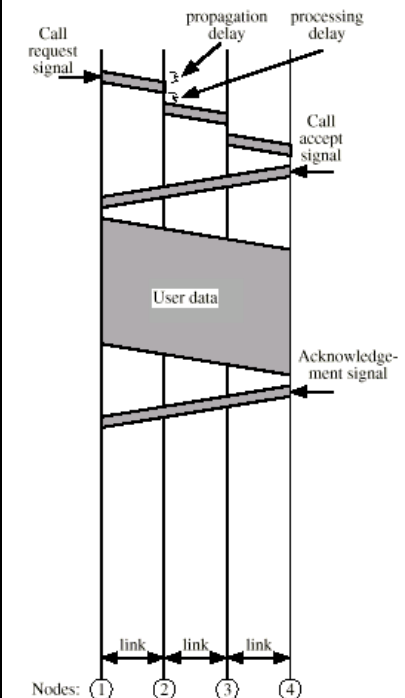
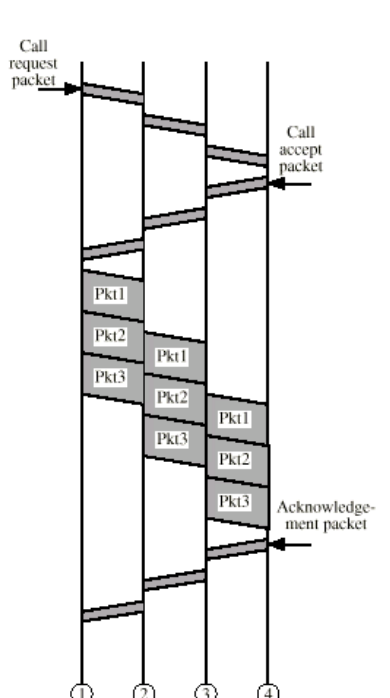
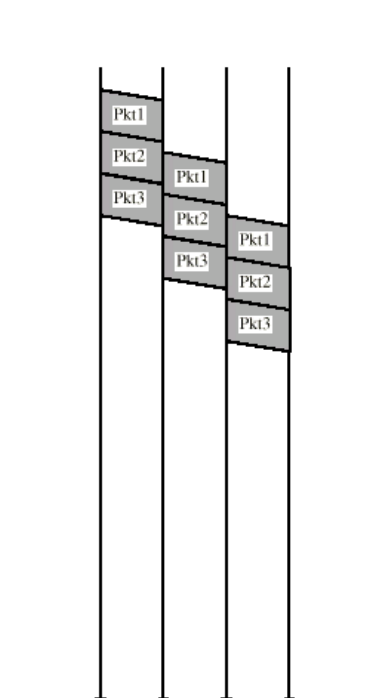
- **Conmutación de Circuitos** → cada conmutador establece una conexión y, así, queda definido un camino:
 - Hay monopolio de recursos → el recurso de conmutación y el enlace quedarán reservados para la comunicación entre A y B → solamente habrá paquetes de A y B en ese enlace.
 - Es con conexión → se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

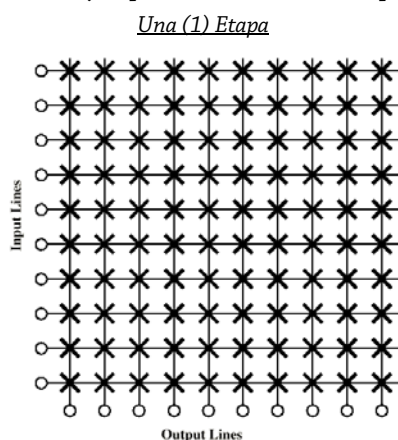
Fases → establecimiento del circuito, transferencia de datos y desconexión del circuito.

Componentes

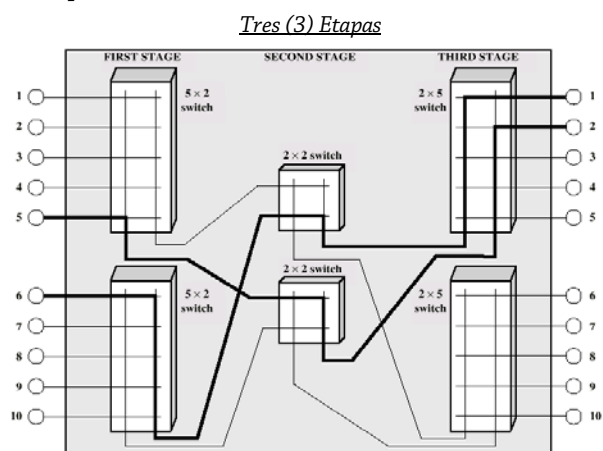
- Centrales → tienen los conmutadores; de ellas dependen los abonados.
- Abonados.
- Líneas principales o Troncales → unen a las centrales mediante fibra óptica, radioenlace, etcétera.
- Bucle local → lazo de abonado.

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:

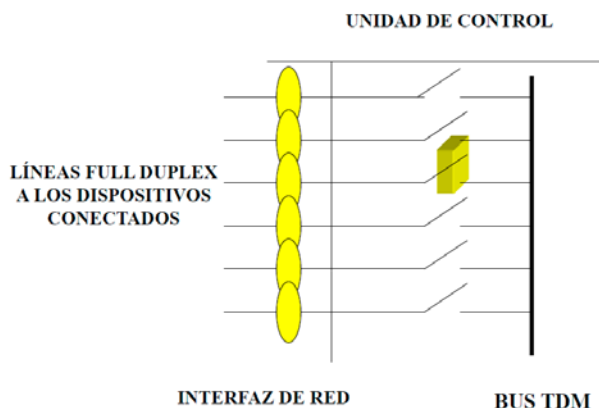


La cantidad máxima de comunicaciones simultáneas es, en el mejor de los casos, igual a la cantidad de líneas de entradas/salidas.



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.

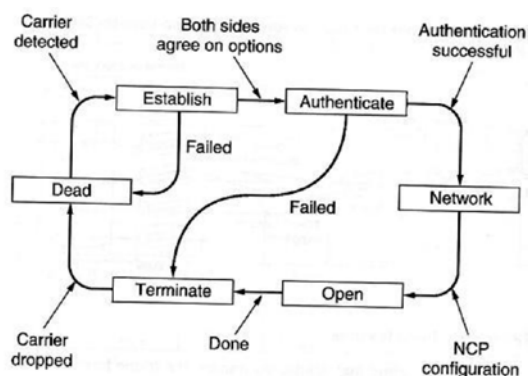
- Útil para la transferencia entre dos dispositivos → *Point-to-Point*.
- Es de Capa (2) de Enlace.
- Derivado del HDLC.
- Usado para formar VPNs.
- Funciones:
 - Transporte de datos.
 - Asegura el enlace y la recepción ordenada.
 - Provee control de errores → detección y corrección (usa ventana deslizante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

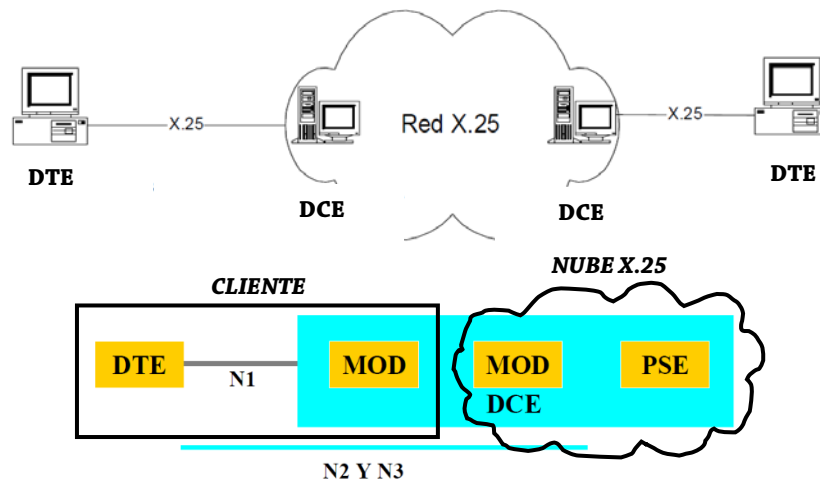
- **SLIP (Serial Line IP)** → protocolo de proceso de tramas usado antaño para envíos IP a través de una línea serial.
- Encapsula datagramas IP.
- Ventajas del PPP:
 - Permite la conexión tanto mediante líneas síncronas como asíncronas.
 - Permite la asignación dinámica de direcciones IP en ambos extremos 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	Paquete	Cabeza		Datos			
2	Trama	Bandera de Inicio	Campo de Dirección	Control Operativo	Información	Control de Errores	Bandera de Cierre
1	Secuencia de Bits	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.

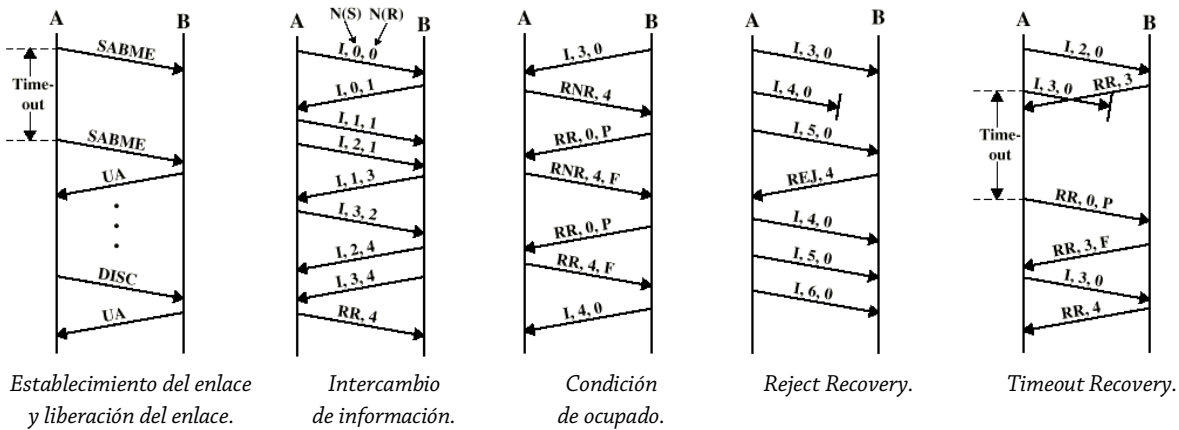
Métodos de direccionamiento

- 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*).

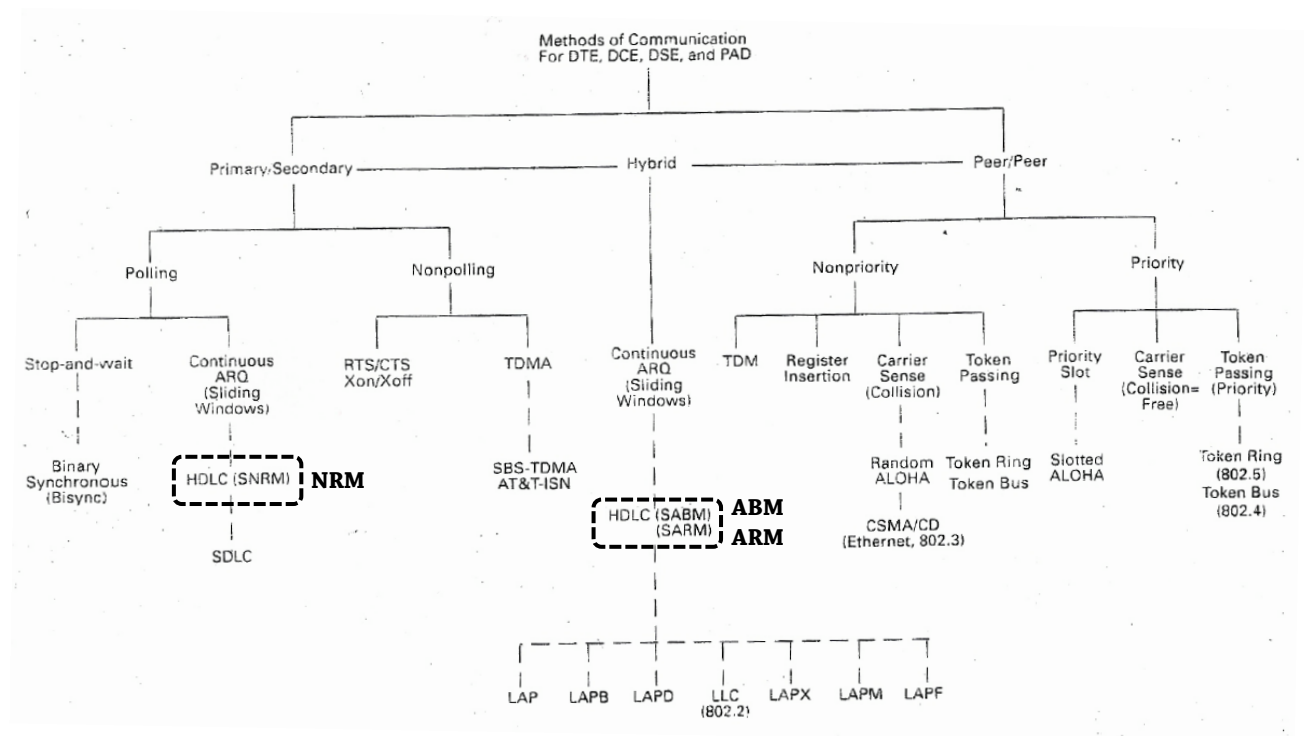
Bit P/F → usado para sondeo o escrutinio (*polling*).

- 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	*	-

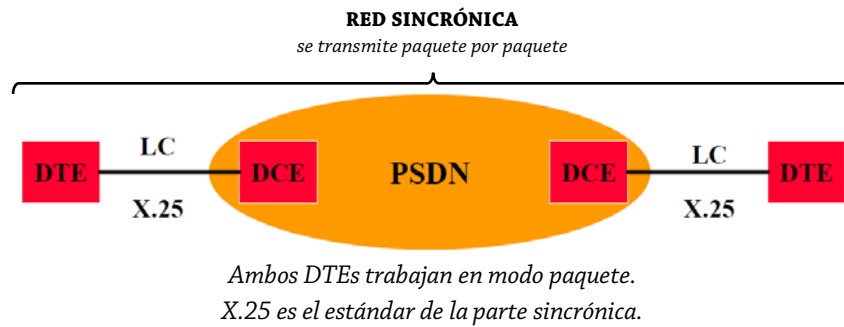
- GFI · Identificador de formato general → para numerar paquetes.
- LCI · Identificador de canal lógico → para numerar canales lógicos.
- TPI · Identificador de tipo de paquete → puede ser de llamada, de supervisión, de confirmación, de interrupción, de control de flujo y datos.
- ADD · Campo de Direcciones → 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

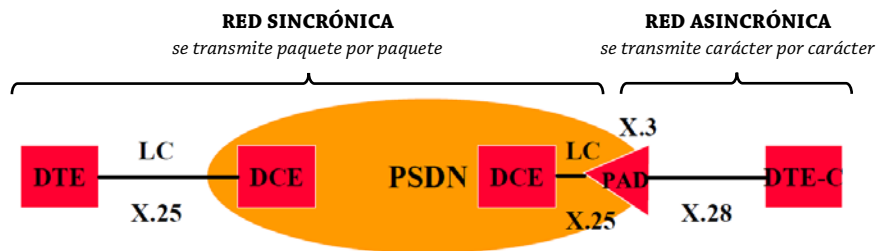
- Costos fijos y variables → no dependen de la distancia sino de paquetes (salvo en tarifa plana).
- Tamaños de paquete y de ventana.
- *Throughput* → velocidad real de transferencia de datos (sin errores) → $v_{Tx} > v_{realTx}$.
- Cantidad de LCs y tipo de LCs (entrante, saliente o bidireccional).
- 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.



UNIDAD 7b · PROTOCOLO FRAME RELAY

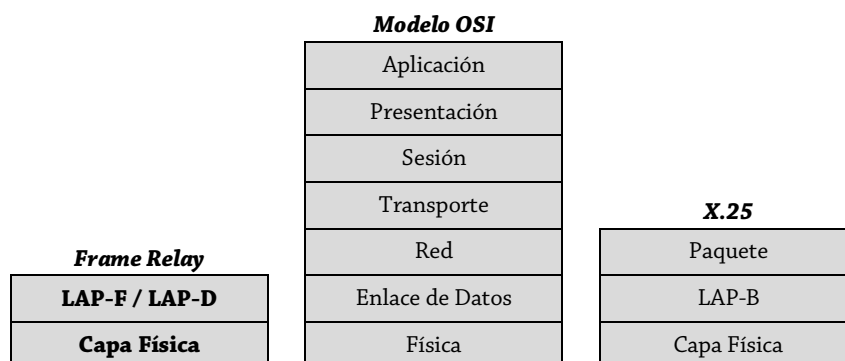
Frame Relay → **relevamiento de cuadro.**

- 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.

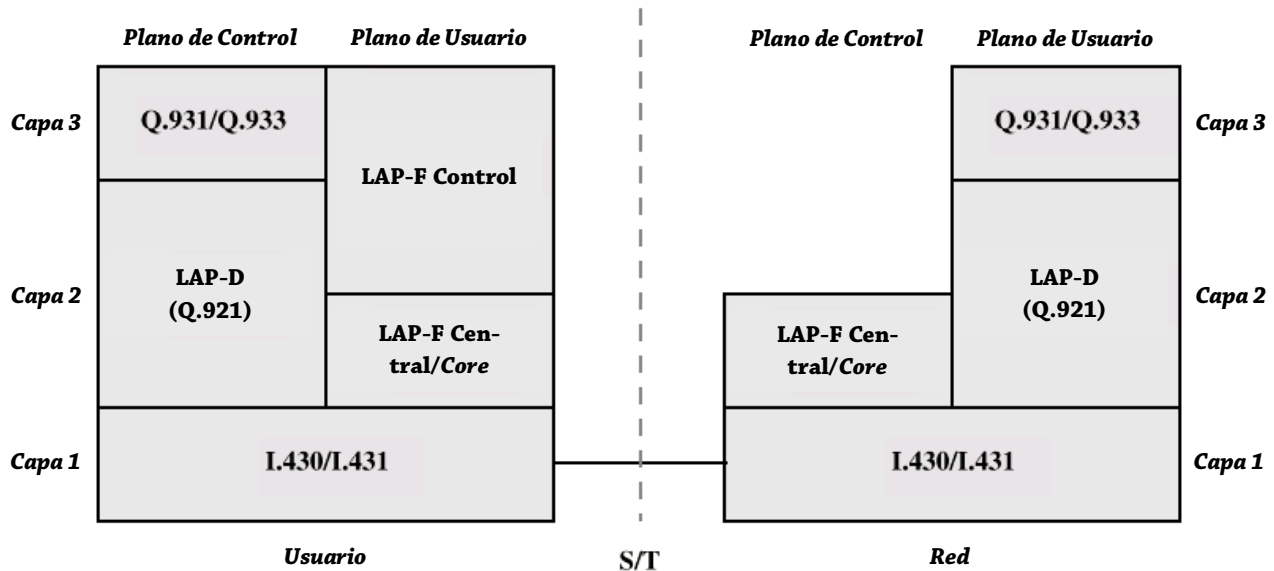
Ubicación respecto al Modelo OSI



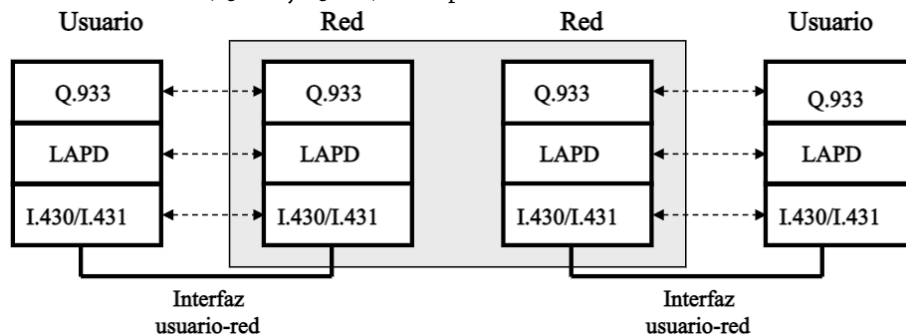
Arquitectura de Protocolos – Transferencia de Datos

Hay dos planos de operación:

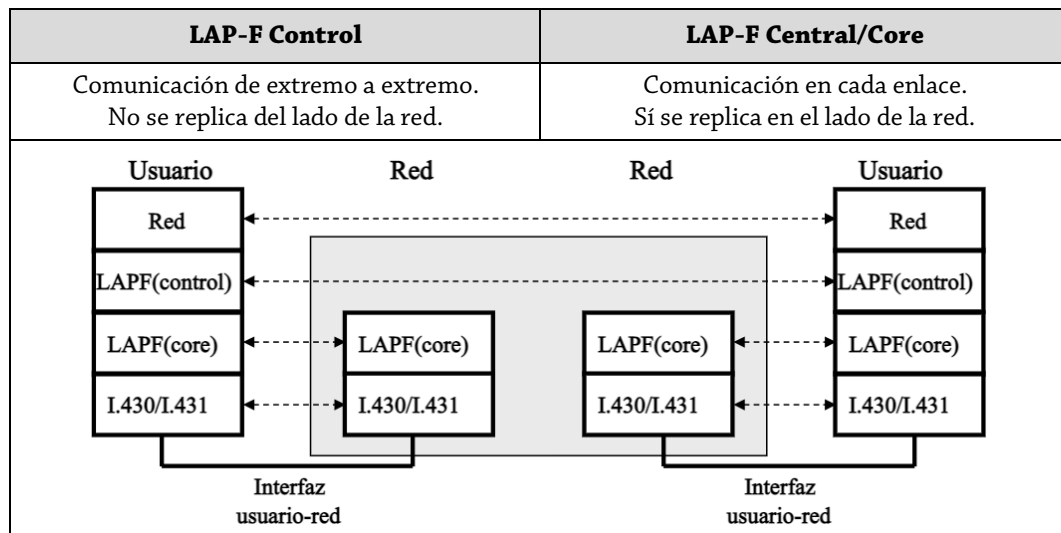
- Plano de Control → establecimiento/liberación de conexiones lógicas → se implementa entre usuario y red.
 - Trabaja con LAP-D.
- Plano de Usuario → transferencia de datos de usuarios → funcionalidad de extremo a extremo.
 - Trabaja con LAP-F.



- 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.



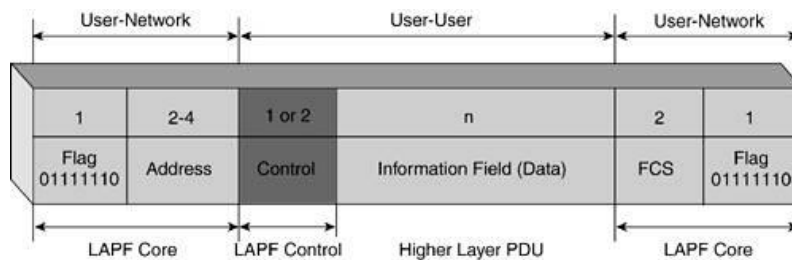
- El **Plano de Usuario** trabaja sobre canales B con **LAP-F Control** o **LAP-F Central/Core**:



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.

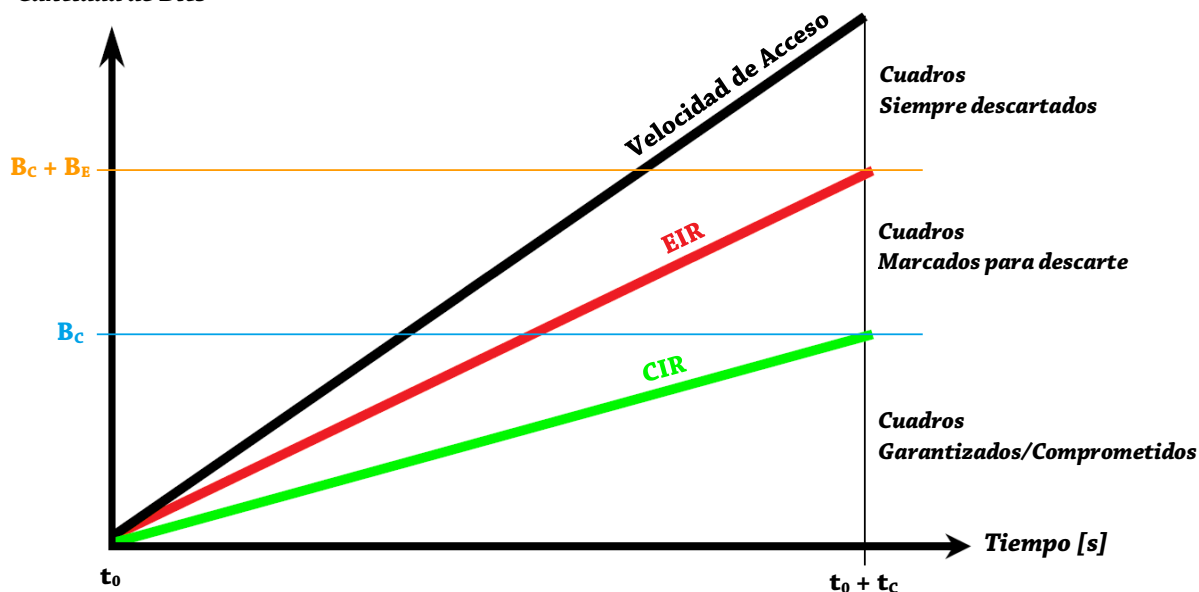
Campo de Dirección de 2B	Campo de Dirección de 3B	Campo de Dirección de 4B																																																																																																
10 bits para direccionar DLCIs.	16 bits para direccionar DLCIs.	23 bits para direccionar DLCIs.																																																																																																
<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 colspan="2">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:

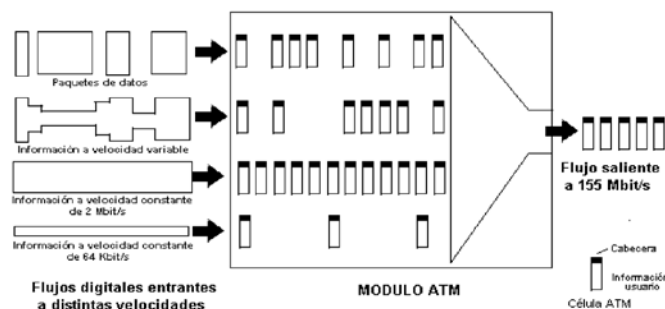
VoFR	VoIP
La voz viaja sobre cuadros <i>Frame Relay</i> .	La voz viaja sobre datagramas IP.
Trabaja en Capa 2.	Trabaja en Capa 3, generando mayor procesamiento.
VoFR es más confiable que VoIP.	VoIP tiene mayor alcance que VoFR.
Con conexión (CVs).	Sin conexión.

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

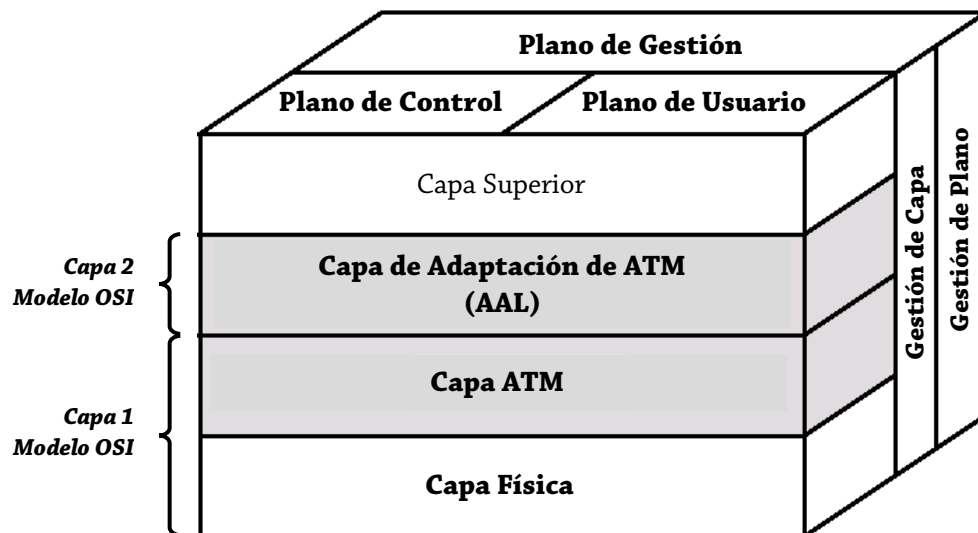
- **GFC** → control de flujo genérico → únicamente está presente en UNI (no está en NNI).
- **VPI** → identificador de trayecto virtual.
- **VCI** → identificador de circuito virtual.
- **PT** → tipo de carga útil (de usuario o de gestión de red / mantenimiento).
- **CLP** → prioridad de pérdida de celda → 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.

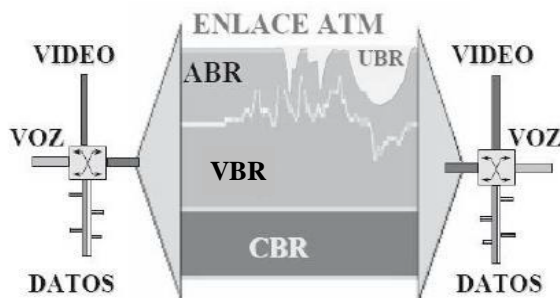


Modelo OSI	Capas ATM	Subcapas ATM	Acciones
	Altas		
Capa 2	AAL	Convergencia	Homogeniza las diferencias que recibe de las capas superiores. Identifica mensajes. Recupera señal de reloj.
		Segmentación y Reensamblado	Segmenta la información de capas superiores (el emisor segmenta, el receptor reensambla). 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



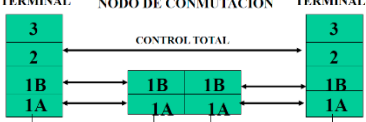
Requerimiento	Clase A	Clase B	Clase C	Clase D
Tiempo entre Fuente y Destino	Requerido (sensible a demoras). rt		No requerido (no sensible a demoras). nrt	
Velocidad (Bit Rate)	Constante CBR	rt-VBR	Variable nrt-VBR	
Modo de Conexión	Con conexión	Sin conexión		
Protocolo	AAL 1	AAL 2	AAL 3	AAL 4
Tipos de 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 (circuitos virtuales). LCI.	VC (circuitos virtuales). DLCI.	VP (camino virtual). VC (circuitos virtuales). 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.

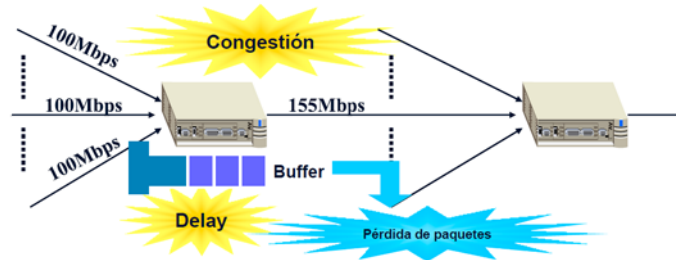
Formato del HEADER (genérico) → 34 b.

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**.

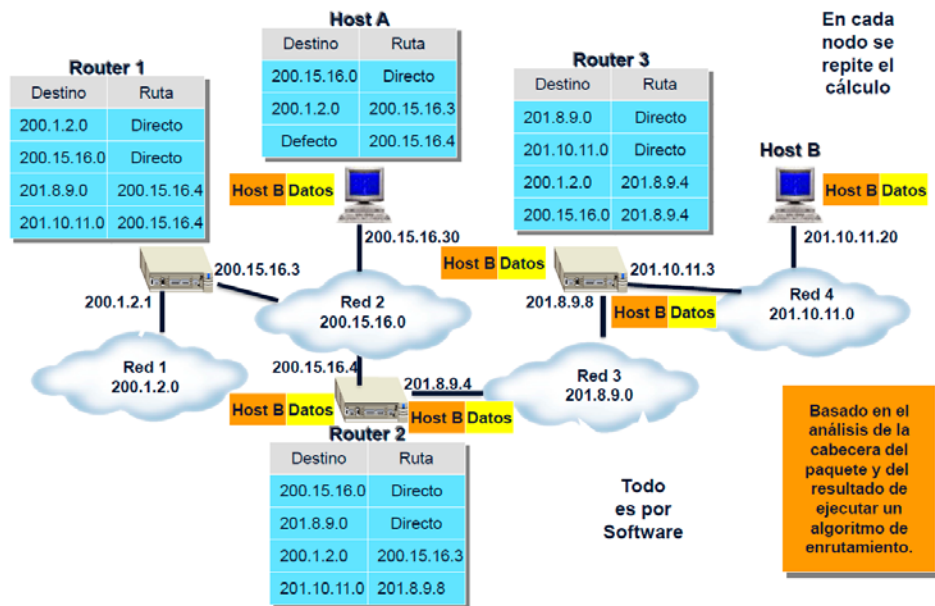
Problemas en las redes que MPLS busca resolver

- Calidad de Servicio (QoS):



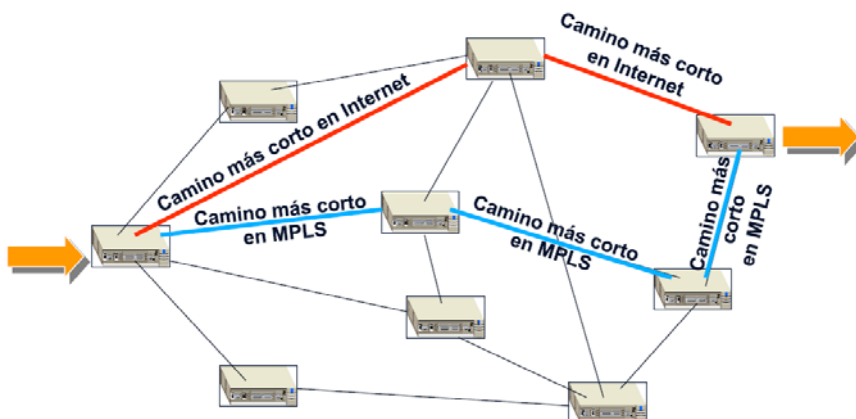
La calidad de servicio se ve afectada por retardos (delay), congestiones y pérdida de paquetes.
Cada router debe estar analizando el datagrama IP, su HEADER y eso genera retardos.

- IP Routing:



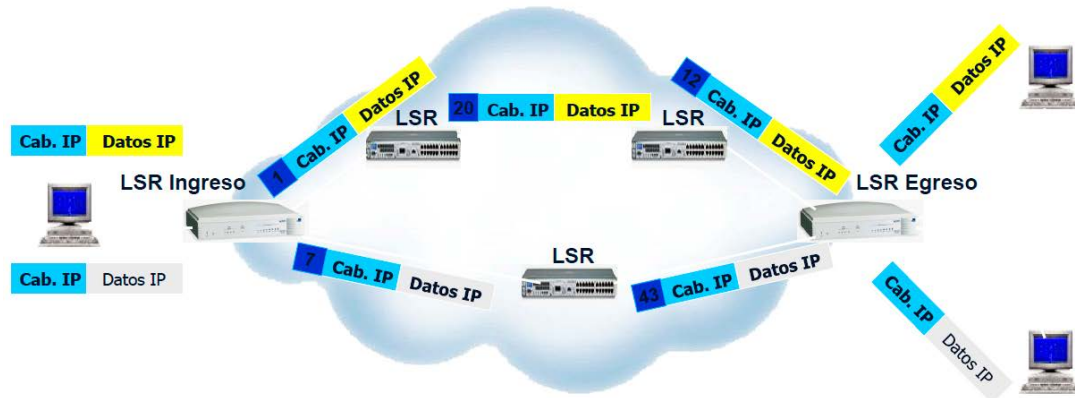
El proceso de análisis de direcciones y enrutamiento se debe hacer en cada nodo perteneciente a una red IP.
Cada terminal y ROUTER tiene su tabla de enrutamiento.

- 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, ...

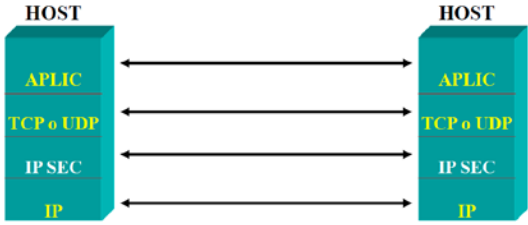
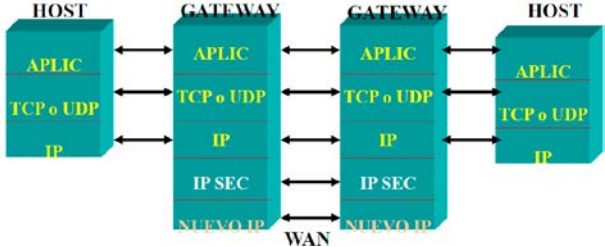


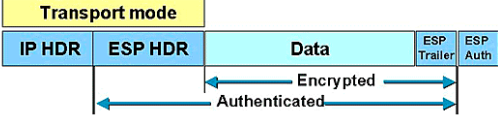


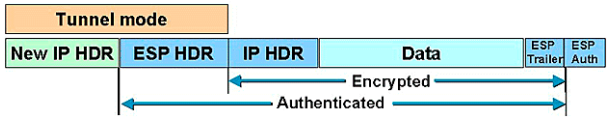
Estrategias/Métodos de Seguridad → lo mejor es superponer métodos, no limitarse a solamente uno:

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