

Redes de Datos

Finales

≡ Redes - Finales

U1. Introducción a las Redes de Datos

Red: conjunto de recursos de comunicaciones y de información que forman un sistema para el transporte de información.

Composición de las Redes

- Enlace de Datos.
- Nodos de Red.
- Equipos terminales.

Clasificación de las redes

Área Geográfica	Áreas Locales	LAN
	Áreas Extendidas	MAN WAN GAN
Ámbito	Públicas	PSDN PSTN
	Privadas	RPV
Modo de Operación	Circuitos Virtuales	PVC SVC
	Datagramas	
Tecnología	Analógicas	
	Digitales	
Ancho de Banda	Banda Angosta	
	Banda Ancha	

Parte de la Red donde Actúa	Red de Acceso
	Red de Transporte

Según el Área Geográfica

- Local Area Network
- Metropolitan Area Network
- Wide Area Network
- Global Area Network

	Área Local	Área Extendida
Distancias	Cortas	Grandes
Velocidad 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
- Privadas

Según Modo de Operación

- Con circuitos virtuales (CVs)
- Con datagramas

Según el Ancho de Banda

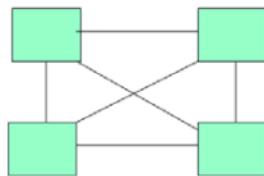
- Banda angosta
- Banda ancha

Según la parte de la red donde actúa:

- Red de Acceso
- Red de Transporte

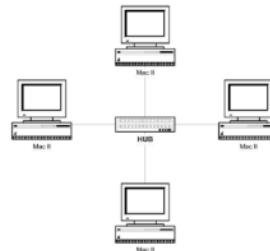
Topología de las Redes

Malla



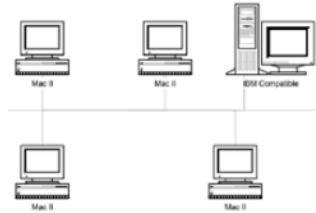
- Más común con pocos nodos.
 - La cantidad de enlaces queda determinada por la cantidad de nodos:
- $$N_{enlaces} = \frac{n_{nodos} \cdot (n_{nodos} - 1)}{2}$$
- Tiene mayores costos (debido a los enlaces).

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.

Protocolos

Protocolo -> 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.
- Permiten la interoperabilidad.
- Proveen información de HEADERS y TRAILERS.

HEADER <i>información de protocolo</i>	PAYOUT <i>información a transmitir</i>	TRAILER <i>información de protocolo</i>
--	--	---

Clasificación

- **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	Sin monopolio
Orden de llegada	Con orden de llegada	Sin orden de llegada
Encaminamiento	Un único camino	Encaminamiento independiente por cada PDU
Transferencia	Transferencia libre de errores	Enfoque: mejor intento
Modo de operación	Círculo virtual	Datagrama

Los servicios con conexión necesitan:

1. Establecer la comunicación.
2. Mantener la comunicación.
3. Liberar la comunicación.

Tipos de Conmutación

		Monopolio de Recursos	Conexión
De Circuitos		CON	CON
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, FEC, ...
- Segmentación y Ensamblado
 - Armado y desamblado de bloques de datos [PDU].
 - Según el tamaño de la PDU, se obtienen distintas características en la comunicación:
 - PDU más chicos
 - Se tarda menos tiempo en enviarlos.
 - Más eficiente en el control de errores.
 - Mejor acceso a las transmisiones (permite que otros usuarios usen el medio).
 - Menos memoria (buffer).
 - Menos necesidad de interrupciones: no será necesario interrumpir el uso de un medio para evitar un monopolio de un usuario.
 - Menor eficiencia de transmisión: habrá mayor información relativa, aumentando el tiempo de latencia relativo.
 - PDU más grandes
 - Se tarda más tiempo en enviarlos.
 - Mayor eficiencia de transmisión: habrá menor información relativa, disminuyendo el tiempo de latencia relativo.

- Si la calidad de los enlaces no es buena, tendré problemas.
- Dar transparencia
 - Garantiza que el uso de los datos agregados (los de protocolo) no afecte los datos originales (los que el usuario desea transmitir).
- Encapsulamiento
 - Agregado de información de control a los datos, sin alterarlos.
 - En el modelo OSI, se van encapsulando protocolo de capa 7 con el protocolo de capa 6, con el protocolo de capa 5, con el protocolo de capa 4, ...
- Sincronismo de bloque, de carácter o de bit
- Control de la conexión
 - Establecimiento, transferencia/mantenimiento y cierre/liberación.
 - Manejo de interrupciones y recuperación.
- Direccionamiento
 - Niveles, alcance, identificadores de conexión y modos (unicast, broadcast y multicast).
- Multiplexación
 - Varios canales establecidos en un mismo enlace.
- Entrega en orden
 - Uso de numeración secuencial.
- Servicios de transmisión
 - Prioridad
 - QOS
 - Seguridad

Sondeo y Selección

Proceso mediante el cual una **estación primaria** sondea a las **estaciones secundarias**, una a una, invitándolas a transmitir (**sondeo**) o solicita a una secundaria recibir datos (**selección**). Método para el control de las transmisiones en una línea compartida. A cargo del procesador central o primaria.

Las estaciones son:

- **Estación primaria**
 - Responsable de controlar el funcionamiento del enlace.
 - Las tramas que genera se denominan **órdenes**.
- **Estación secundaria**
 - Funciona bajo el control de la estación primaria.
 - Las tramas que genera se denominan **respuestas**.
 - La primaria establece un enlace lógico independiente con cada una de las secundarias presentes en la línea.

- **Estación combinada**

- Combina las características de las primarias y de las secundarias, pudiendo generar tanto órdenes como respuestas.

Requerimiento automático de repetición (ARQ)

Tiempo de transmisión: tiempo empleado por una estación para emitir todos los bits de una trama sobre un medio.

Tiempo de propagación: tiempo empleado por un bit en atravesar el medio desde el origen hasta el destino.

ARQ Stop and Wait

- La operación es *half-duplex*.
- La entidad origen transmite una trama. La entidad destino, después de recibirla, indica su deseo de aceptar otra mediante el envío de una confirmación (**ACK**). El origen debe esperar la confirmación antes de enviar la trama siguiente. El destino puede parar el flujo de los datos reteniendo las confirmaciones.
- Cuando $t_{transmisión} > t_{propagación}$, la trama es lo suficientemente larga para que los primeros bits lleguen al destino antes de que el origen haya concluido la transmisión. La línea se usa de forma ineficiente.
- Cuando $t_{propagación} > t_{transmisión}$, el emisor completa la transmisión de toda la trama antes de que el primer bit de la misma llegue al receptor. La línea está siempre infrautilizada.

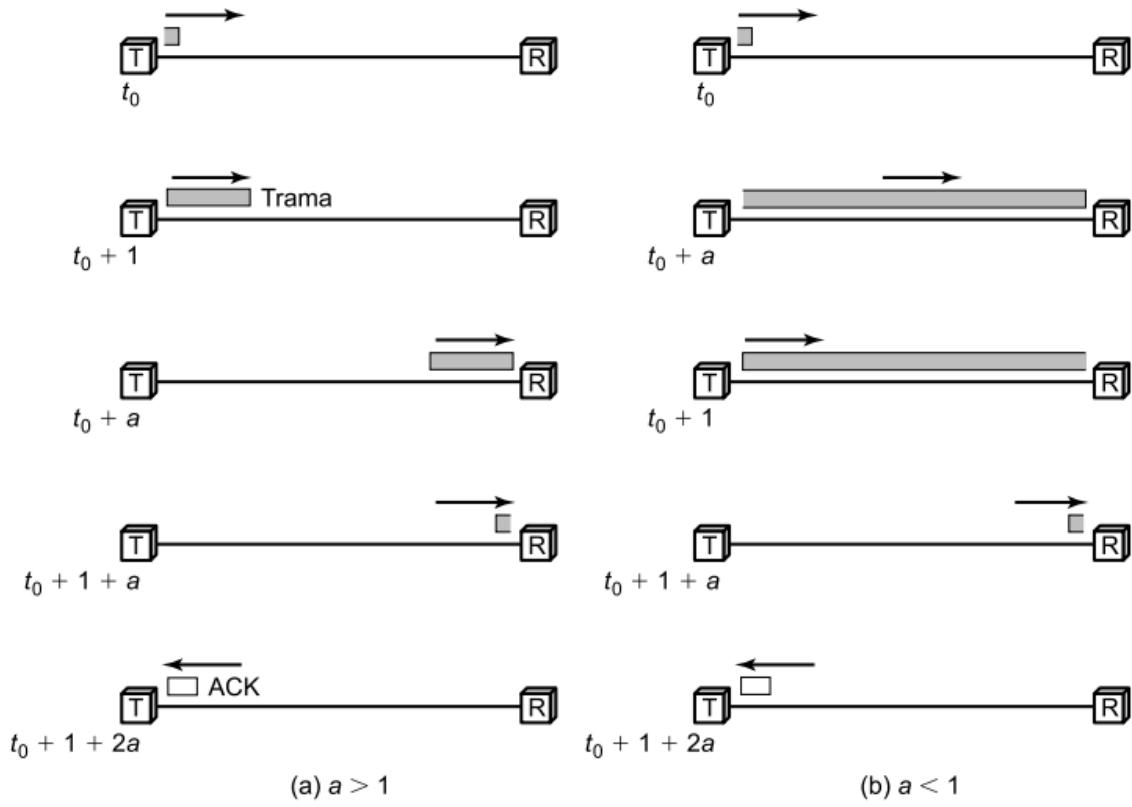
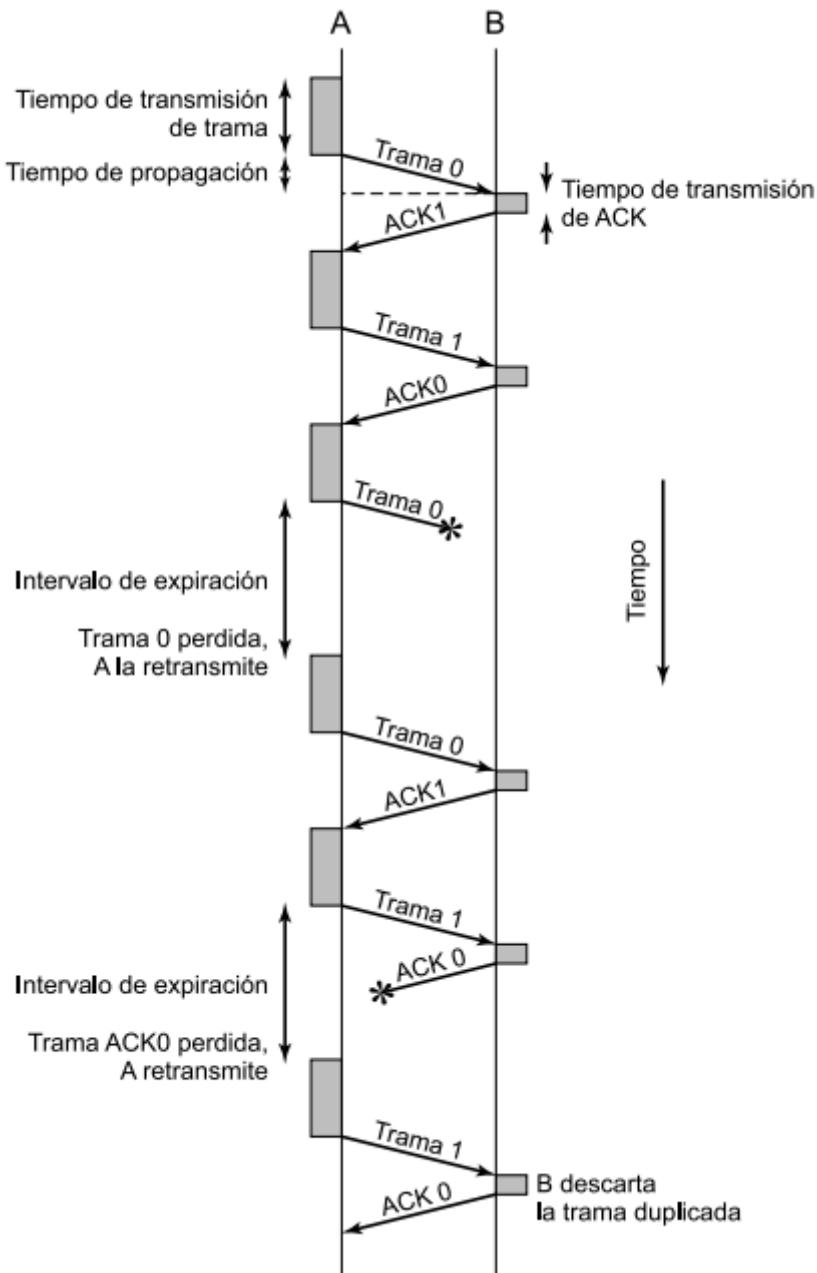


Figura 7.2. Utilización del enlace en parada y espera
(tiempo de transmisión = 1; tiempo de propagación = a).

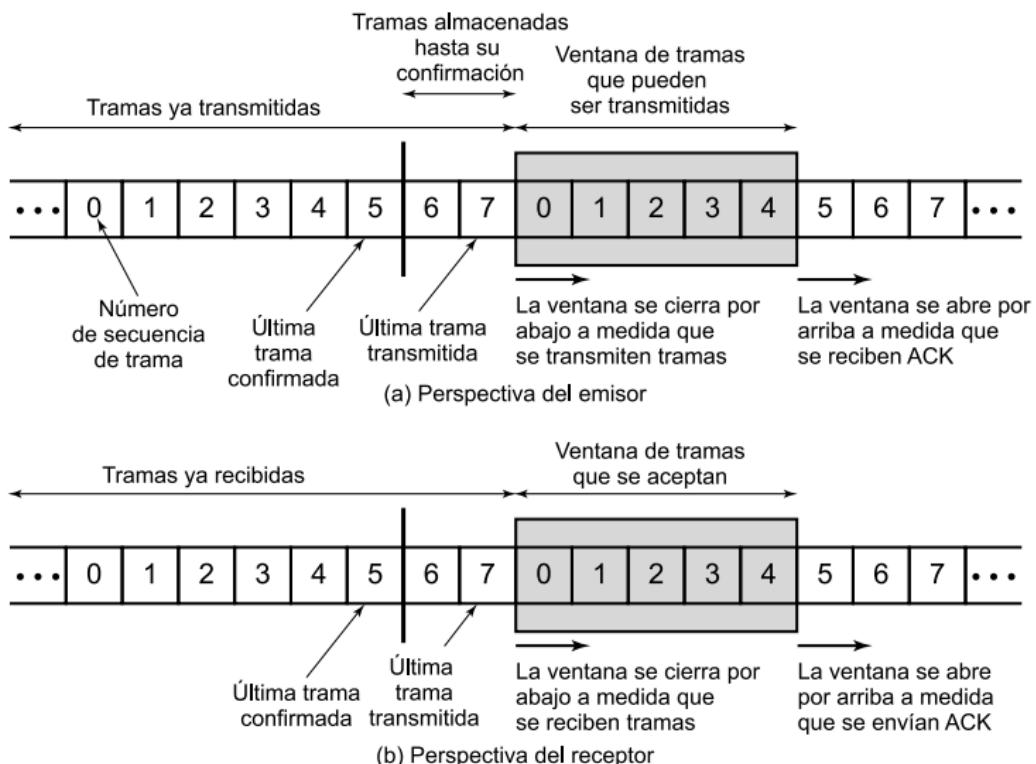
- Este procedimiento da lugar a una utilización ineficiente de la línea para el caso de velocidades de transmisión muy altas entre emisores y receptores que se encuentran separados a grandes distancias.
- Para el control de errores, se consideran dos tipos de errores:
 - Trama dañada** al llegar al destino. La estación fuente usa un temporizador. Si no se recibe ninguna confirmación antes de que el temporizador expire, se envía otra vez la misma trama.
 - Confirmación deteriorada**. La estación B envía un ACK, pero A no puede identificar la confirmación, causando una expiración del temporizador y el reenvío de la misma trama. La trama duplicada llega a B y se acepta otra vez. Para evitar ese problema, las tramas se pueden etiquetar de forma alternada con 0 o 1. La confirmación ACK0 confirma la trama 1 e indica que el receptor está preparado para aceptar la trama 0.



ARQ Sliding Window

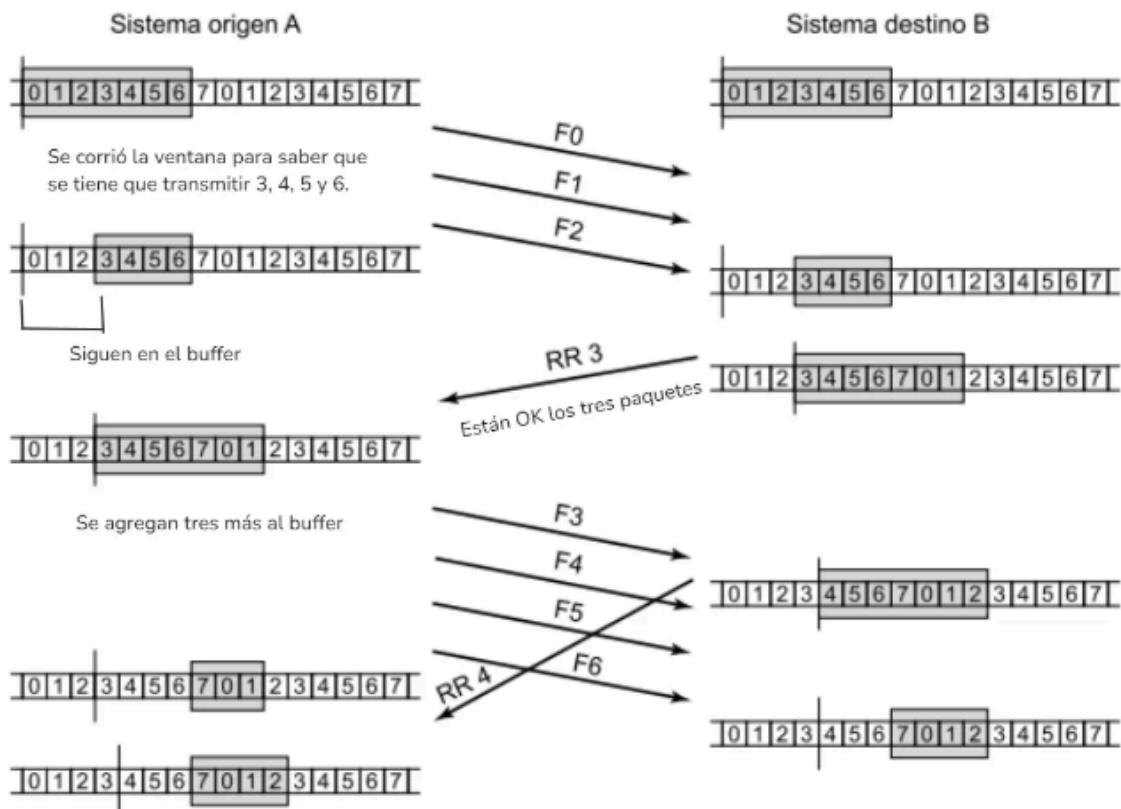
- Si se permite que varias tramas viajen al mismo tiempo sobre el enlace, la eficiencia mejorará significativamente.
- Funciona en un enlace *full-duplex*.
- Procedimiento entre dos estaciones A y B.
 - La estación B reserva un buffer suficiente para almacenar W tramas. B puede aceptar W tramas, permitiéndole a A enviar W tramas sin tener que esperar ninguna confirmación.
 - Para saber qué tramas se han confirmado, cada trama se etiqueta con un número de secuencia.

- B confirma una trama mediante el envío de una confirmación que incluye el número de secuencia de la siguiente trama que se espera recibir, informando (implícitamente) que está preparado para recibir las W tramas siguientes, comenzando por la del número especificado. Este esquema se puede utilizar también para confirmar varias tramas simultáneamente.
- A mantiene una lista con los números de secuencia que se le permite transmitir y B mantiene una lista con los números de secuencia que está esperando recibir. Cada una de estas listas es una **venta** de tramas.
- Por ejemplo: B recibe las tramas 2, 3 y 4, pero retiene la confirmación hasta que llegue la trama 4; cuando envía la confirmación, envía un 5, confirmando las tramas 2, 3 y 4.



- La trama **RR (Receive Ready) N** significa “recibí todas las tramas hasta N y estoy preparado para recibir la trama 3”
- La trama **RNR (Receive Not Ready) N** confirma las tramas anteriores pero prohíbe la transmisión de tramas adicionales. Significa “recibí hasta la trama número 4, pero no acepto más”.
- Cuando dos estaciones intercambian datos, cada una debe mantener dos ventanas (una para transmitir y otra para recibir), y enviar datos como confirmaciones. Para esto se usa **piggybacking**:
 - Cada **trama de datos** incluye un campo en el que se indica el número de secuencia de dicha trama más un campo que indica el número de

- secuencia que se confirma. Si una estación tiene para enviar una confirmación además de datos, lo hará conjuntamente utilizando una sola trama, ahorrando así capacidad del canal.
- Si la estación sólo tiene que enviar una confirmación, enviará una **trama de confirmación** (RR o RNR).
 - Si la estación sólo tiene datos para enviar, deberá repetir el último número de secuencia de confirmación enviado con anterioridad (debido a que el receptor espera un número de confirmación). Al ser repetido, el receptor simplemente lo ignora.



- Si la estación destino detecta un error en una trama, envía una confirmación negativa (REJ) para dicha trama. La estación destino descarta esta trama y todas las que reciba con posterioridad hasta que dicha trama errónea llegue correctamente. La estación origen, cuando reciba un REJ, debe retransmitir la trama errónea y todas las posteriores que hayan sido transmitidas tras ella.

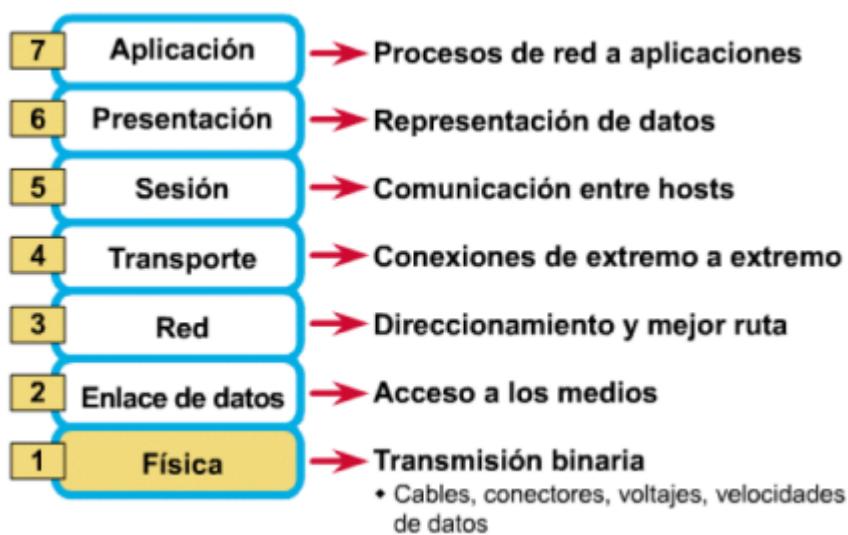
Sistema sin sondeo – Técnicas de control de flujo

- 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).

U1.B - Modelo OSI

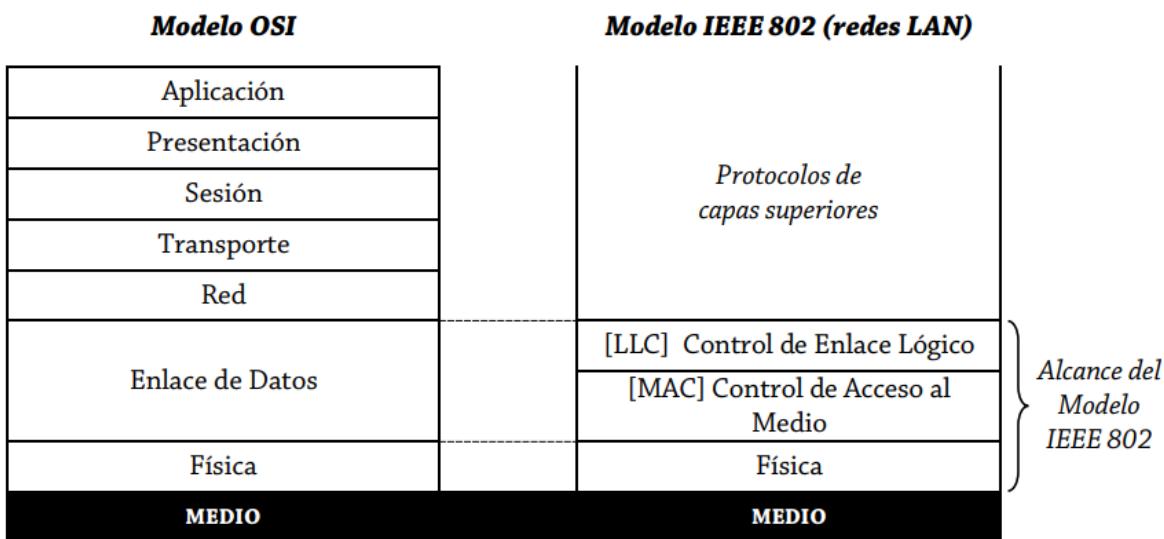
- Cada capa provee servicios a las capas superiores
- Cada capa utiliza servicios de las capas inferiores
- La comunicación entre capas adyacentes dentro de un mismo sistema se realiza mediante **interfaces**.
- La comunicación entre capas del mismo nivel de distintos sistemas se realiza mediante **protocolos**.



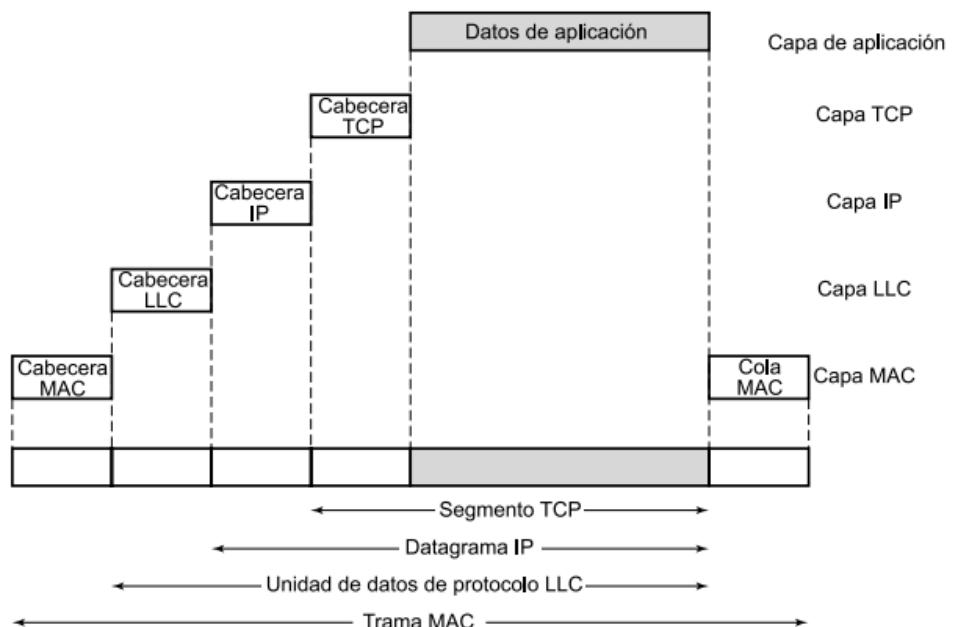
TODO: Completar con las capas

U2. LAN

Modelo OSI vs Modelo IEEE 802



- La capa inferior del modelo IEEE 802 es la capa física del modelo OSI.
- Las funciones se separan porque:
 - La lógica necesaria para la gestión del acceso a un medio compartido no se encuentra en la capa 2 de control de enlace de datos tradicional.
 - Se pueden ofrecer varias opciones MAC para el mismo LLC.



- La subcapa LLC añade una cabecera de información de control dando lugar a una unidad de datos de protocolo (PDU) LLC. Esta información se usa para el funcionamiento del protocolo LLC. La PDU se pasa a la subcapa MAC, que añade información de control al principio y al final del paquete creando una trama MAC.

Protocolos de LAN

- Según la capa que se trate (LLC, MAC).
- 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

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:
 - Si se escucha la portadora → el canal está ocupado.
 - Si no se escucha la portadora → el canal no está ocupado.
 - Detección de colisiones.
 - Una **colisión** es un tipo de ruido que se superpone a la señal útil. Se produce cuando dos o más estaciones de trabajo quieren usar el medio y colocan una trama. Si hay dos o más tramas viajando en un 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 siempre está presente.

Dirección MAC

Es la **dirección física o de hardware** que identifica de manera unívoca al dispositivo. Cada interfaz tiene una dirección MAC

3 B	3 B
Organizationally Unique Identifier (OUI)	Network Interface Controller (NIC) Specific

Está formada por 48 bits en 6 grupos de 2 dígitos hexadecimales.

- F0 : E1 : D2 : C3 : B4 : A5
- **OUI** identifica al fabricante
- **NCI Specific** identifica a la placa de red del fabricante.
- El primer bit de la dirección se denomina I/G (Individual/Group). Si es 0, es una transmisión **unicast**; si es 1, **multicast**.

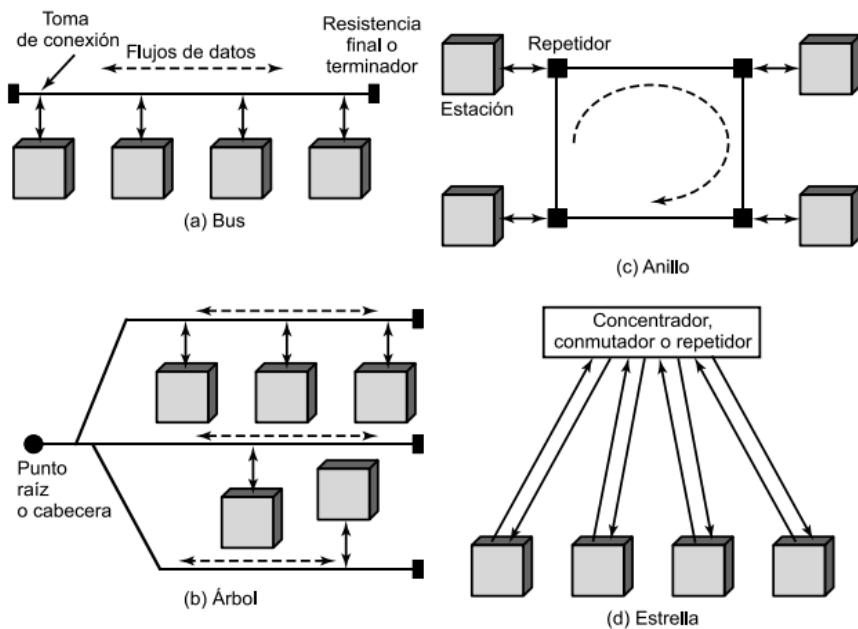
Dirección de broadcast

- 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.
- Son todos 1s - FF : FF : FF : FF : FF : FF .

Dirección de multicasting

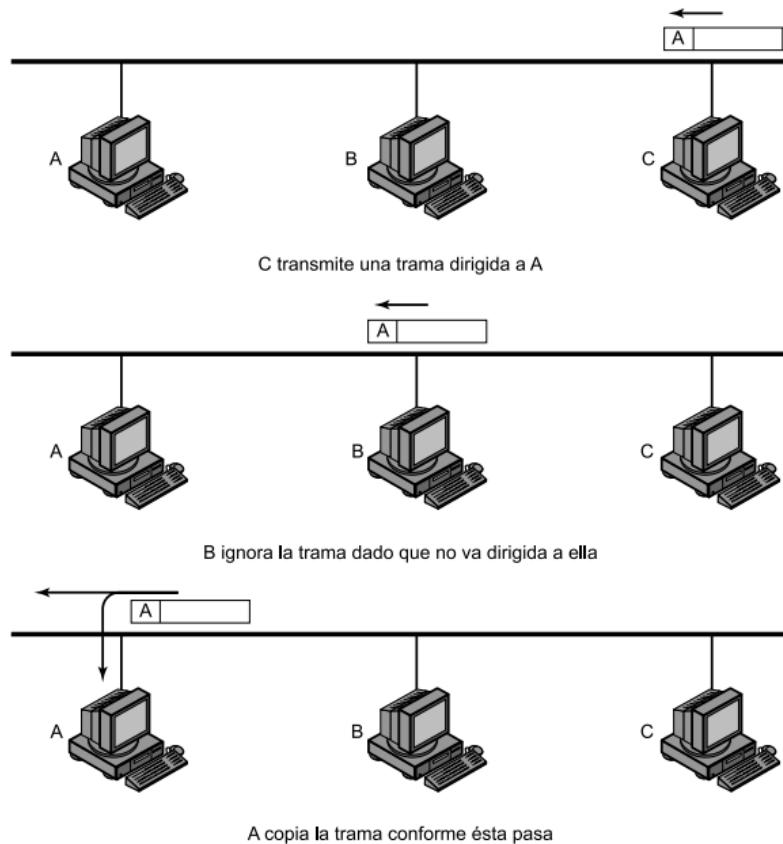
- Permite enviar una trama a todas las estaciones que forman parte de un grupo.
- Involucra el manejo de grupos para definir qué estaciones están en el grupo.

Topologías de LAN



Topología en Bus

- Caso especial de la topología en árbol, con un solo tronco y sin ramas.
- Se caracteriza por el uso de un medio multipunto.
- Todas las estaciones se encuentran directamente conectadas a un medio de transmisión, a través de interfaces físicas (**tomas de conexión - taps**).
- El funcionamiento full-duplex entre la estación y la toma de conexión permite la transmisión y la recepción de datos a través del bus.
- Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de las estaciones.
- En cada extremo del bus existe un terminador que absorbe las señales, eliminándolas del bus.
- Este esquema tiene dos problemas:
 - Se necesita algún método para indicar a quién va dirigida la transmisión, ya que todas las estaciones pueden recibir la transmisión.
 - Se necesita un mecanismo para regular la transmisión
 - Si dos estaciones intentan transmitir simultáneamente, sus señales se superpondrán y serán erróneas.
 - Una estación podría transmitir continuamente durante un largo período de tiempo.
- Los problemas se solucionan enviando en la cabecera de la trama la dirección de destino.



Topología en Árbol

- Generalización de la topología en bus.
- El medio de transmisión es un cable ramificado sin bucles cerrados que comienza en un punto conocido como *raíz* o *cabecera*. Uno o más cables comienzan en el punto raíz y cada uno puede presentar ramificaciones (y así sucesivamente).

Topología en Anillo

- La red está formada por un conjunto de *repetidores* unidos por enlaces punto a punto formando un bucle cerrado.
- Un repetidor es un dispositivo capaz de recibir datos a través del enlace y de transmitirlos, bit a bit, a través del otro enlace tan rápido como son recibidos.
- Los enlaces son unidireccionales. Los datos circulan alrededor del anillo en el sentido de las agujas del reloj (o en el contrario).
- Cada estación se conecta a la red mediante un repetidor, transmitiendo los datos hacia la red a través de él. Los datos se transmiten en tramas. Una trama que circula por el anillo pasa por las demás estaciones, de modo que la estación de

destino reconoce su dirección y copia la trama en una memoria temporal local. Cuando la trama alcanza la estación de origen, se elimina del medio.

- El anillo es compartido por varias estaciones, entonces se necesita una técnica de control de acceso al medio para determinar cuándo cada estación puede insertar tramas.
- Puede ser usada para proporcionar enlaces de muy alta velocidad sobre distancias largas. Tiene potencialmente un mejor rendimiento que el resto de las topologías.
- Desventaja: un fallo de un solo enlace o de un repetidor puede inutilizar la red entera.

Topología en Estrella

- Cada estación está conectada a un nodo central común, a través de dos enlaces punto a punto (transmisión y recepción).
- Existen dos alternativas para el funcionamiento del nodo central:
 - **En modo de difusión**
 - La transmisión de una trama por parte de una estación se retransmite sobre todos los enlaces de salida del nodo central.
 - El dispositivo central se denomina **concentrador (hub)**.
 - **En modo conmutación de tramas.**
 - Una trama entrante se almacena temporalmente en el nodo y se retransmite sobre un enlace de salida hacia la estación de destino.
 - El dispositivo es un **comutador (switch)**.
- Se aprovecha de la disposición natural del cableado de los edificios.
- Es mejor para distancias cortas y puede ofrecer velocidades elevadas a un número pequeño de dispositivos.

Capa Física

- Es la capa 1 del Modelo OSI y del Modelo IEEE 802 (redes LAN).
- Codificación/decodificación de señales.
- Generación/eliminación de preámbulo (para sincronización).
- Transmisión/recepción de bits.
- Especificación del medio de transmisión y de la topología.

Elección de la Topología

- Depende de factores como:
 - Fiabilidad de la topología
 - Capacidad de expansión.
 - Rendimiento

- No debe ser llevada a cabo independientemente de la elección del medio, la disposición del cableado y la técnica de control.
- Para una LAN en bus hay cuatro alternativas:
 - **Par trenzado:** ya no se usa porque no resulta práctico migrar a velocidades más altas.
 - **Cable coaxial en banda base:** el esquema original de Ethernet lo usaba.
 - **Cable coaxial en banda ancha:** ya no está en uso porque es más caro, difícil de mantener y de instalar que el cable coaxial en banda base.
 - **Fibra óptica.**
 - **Inalámbrico**

Elección del medio de transmisión

Los factores a tener en cuenta son:

- **Topología**
- **Capacidad:** debe soportar el tráfico de red esperado.
- **Fiabilidad:** debe satisfacer los requisitos de disponibilidad.
- **Tipos de datos soportados:** ajustados a la aplicación.
- **Alcance del entorno:** debe proporcionar servicio a la gama de entornos requeridos.

Subcapa MAC - Control de Acceso al Medio

Funciones

1. En transmisión, ensamblado de datos en tramas con campos de dirección y detección de errores.
2. En recepción, desensamblado de tramas, reconocimiento de dirección y detección de errores.
3. Control de acceso al medio de transmisión LAN.

Parámetros claves

- **Dónde:** Se refiere a si el control se realiza de forma **centralizada** o **distribuida**.
 - **Centralizada.** Un controlador tiene autoridad para conceder el acceso a la red. Las estaciones tienen que esperar para transmitir hasta recibir el permiso.
 - **Distribuida.** Las estaciones realizan conjuntamente la función de control de acceso al medio para determinar dinámicamente el orden en que transmitirán.
- **Cómo.**

- Viene impuesto por la topología y es un compromiso entre el costo, las prestaciones y la complejidad (entre otros).
- Técnicas **síncronas**. Se dedica una capacidad dada a una conexión. No son óptimas en redes LAN y MAN porque las necesidades de las estaciones son impredecibles.
- Técnicas **asíncronas**. Se reserva capacidad de forma dinámica más o menos en respuesta a solicitudes inmediatas. Hay tres categorías:
 - Rotación circular
 - Reserva
 - Contención

Técnicas asíncronas

- **Rotación circular**

- Cada estación tiene la oportunidad de transmitir, pudiendo rechazarla o transmitir hasta un límite superior (cantidad de datos o tiempo). Cuando la estación termina debe ceder el turno a la siguiente en la secuencia lógica. El control de secuencia puede ser centralizado o distribuido.
- Es eficiente cuando varias estaciones disponen de datos a transmitir durante un largo período de tiempo.
- Hay un costo alto en el paso del turno si pocas estaciones disponen de datos a transmitir durante un extenso período de tiempo (la mayoría solo cede el turno, no transmite).
- Conviene en tráfico continuo (transmisiones largas y continuas).
- Más común.

- **Reserva**

- Adecuadas para tráfico continuo.
- Se divide el tiempo en ranuras.
- Si una estación quiere transmitir, tiene que reservar futuras ranuras para un largo período de tiempo.
- Las reservas se pueden llevar a cabo de forma centralizada o distribuida.
- Menos común que el resto.

- **Contención**

- Adecuadas para tráfico a ráfagas.
- No se realiza control para determinar de quién es el turno; las estaciones compiten.
- Son distribuidas.
- Ventajas
 - Sencillas de implementar.
 - Eficientes en condiciones de carga baja o moderada.
- Desventaja
 - Ineficiente para cargas altas.

- Más común.

Control centralizado vs descentralizado

Las ventajas y desventajas de un esquema centralizado contra uno descentralizado

Ventajas	Desventajas
Proporciona prioridades, rechazos y capacidad garantizada.	Genera un punto de falla
Permite el uso de una lógica de acceso relativamente sencilla en cada estación.	Puede actuar como un punto de botella.
Resuelve el problema de coordinación distribuida entre entidades paritarias.	

Las ventajas y desventajas de uno descentralizado son las contrarias.

Subcapa LLC - Control de Enlace Lógico

- Funciones
 - Especificar los mecanismos para direccionar estaciones a través del medio y para controlar el intercambio de datos entre dos usuarios.
 - Interfaz con capas superiores.
 - Corrección de errores y de flujo (Opcional).
- Características no compartidas con otros protocolos de CE:
 - Debe admitir el acceso múltiple.
 - La capa MAC lo libera de algunos detalles del acceso al enlace.
- El direccionamiento necesita los usuarios LLC origen y destino.
 - Un usuario es un protocolo de una capa superior o una función de gestión de red en la estación.
 - Esas direcciones se denominan SAP (*Service Access Point*).

Servicios LLC

- **Servicio no orientado a conexión sin confirmación.**
 - De tipo datagrama.
 - No incluye mecanismos de control de flujo ni de errores (no está garantizada la recepción de los datos).
 - Es útil cuando el software de las capas superiores ofrece la fiabilidad y los mecanismos de control de flujo, y cuando el costo de establecimiento y mantenimiento de la conexión resulta injustificado (por ejemplo, en una aplicación de supervisión -sensores, cámaras, etc-).

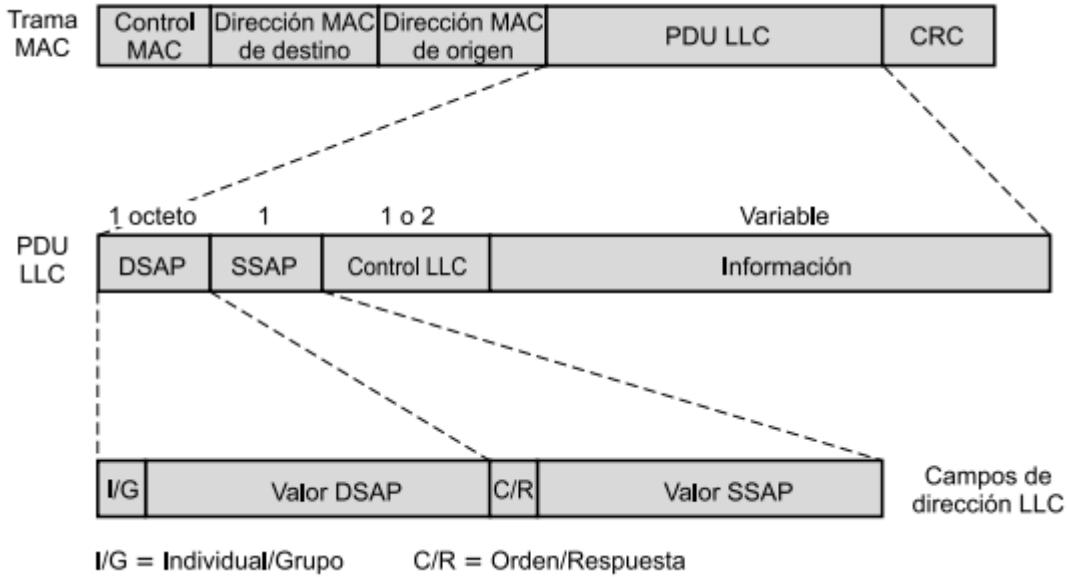
- **Servicio no orientado a conexión con confirmación.**
 - Similar al ofrecido por HDLC.
 - Se establece una conexión lógica entre dos usuarios que intercambian datos, existiendo control de flujo y de errores.
 - Útil cuando se necesita garantizar la recepción, pero existe un gran número de destinos para los datos (se necesitan demasiadas tablas con el estado de cada conexión), y en caso de señales de urgencia.
- **Servicio en modo conexión.**
 - Mezcla de los dos anteriores.
 - Los datagramas son confirmados, pero no se establece conexión lógica previa.
 - Se usa en dispositivos muy simples que disponen de poco software por encima de este nivel.

Protocolo LLC

El protocolo LLC básico presenta funciones y formatos similares a HDLC.

- **Operación tipo 1.** LLC presta un servicio no orientado a conexión sin confirmación usando la PDU de información no numerada, lo que se conoce como.
- **Operación tipo 2.** LLC usa el modo ABM de HDLC para dar soporte al servicio LLC en modo conexión. No se usan los otros modos.
- **Operación de tipo 3.** LLC ofrece un servicio no orientado a conexión confirmado haciendo uso de dos PDU no numeradas nuevas.
- LLC permite multiplexación mediante el empleo de puntos de acceso al servicio LLC (LSAP).

Los tres protocolos usan el mismo PDU. DSAP y SSAP contiene una dirección de 7 bits que especifica los usuarios LLC destino y origen. Un bit del campo DSAP indica si la dirección es individual o de grupo, mientras que un bit de SSAP indica si la PDU es una orden o una respuesta. El formato del campo de control LLC es igual al de HDLC.



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

Protocolos de Acceso al Medio

Arbitran el uso del canal de difusión. Pueden ser:

- **Contienda (aleatorio)**: los dispositivos pelean entre sí para acceder al medio.
- **Paso de Testigo (determinístico/secuencial)**: no se producen colisiones.

Contienda

Aloha

- **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 cuál solamente un usuario podrá transmitir.
 - Cada usuario tendrá su ranura de tiempo para él solo.
- Más eficiente → menos probabilidades de colisión.

CSMA

- Acceso Múltiple con Detección de Portadora (Carrier Sense Multiple Access).
- Una estación que quiere transmitir tiene que sentir la presencia de portadora en el medio para poder acceder.
 - Si el medio está siendo usado, tiene que esperar.
 - Si el medio está libre, puede transmitir.
- Para solucionar las colisiones, las estaciones guardan una cantidad de tiempo razonable después de transmitir en espera de una confirmación, teniendo en cuenta el retardo de propagación máximo del trayecto de ida y vuelta y el hecho de que la estación que confirma debe competir también por conseguir el medio para responder.
 - Si no hay respuesta, se asume una colisión y se retransmite.
- Es efectivo en las redes con tiempo de transmisión >> tiempo de propagación.
 - Habrá colisiones si más de un usuario comienza a transmitir dentro del mismo intervalo de tiempo.
 - Si no existen colisiones durante el tiempo de propagación hasta la estación más lejana, no se producirán colisiones para esa trama porque todas las estaciones están enteradas de la transmisión.
- **No Persistente**
 1. Si el medio se encuentra libre, transmite; en otro caso se aplica el paso 2.
 2. Si el medio se encuentra ocupado, espera una cierta cantidad de tiempo obtenida de una distribución de probabilidad (retardo de retransmisión) y repite el paso 1.
- **1-Persistente (IEEE 802.3)**
 - Reglas
 1. Si el medio se encuentra libre, transmite; en otro caso se aplica el paso 2.
 2. Si el medio está ocupado, continúa escuchando hasta que el canal se detecte libre, momento en el cual se transmite inmediatamente.
 - La capacidad se desaprovecha porque el medio permanece generalmente desocupado tras el fin de una transmisión.
 - El tiempo desaprovechado debido a las colisiones es muy pequeño (si las tramas son largas en comparación al retardo de propagación).

- No es probable que las dos estaciones involucradas en una colisión vuelvan a estarlo en sus siguientes reintentos.
- **p-persistente**
 - Reglas
 1. Si el medio se encuentra libre, se transmite con una probabilidad p y se espera una unidad de tiempo con una probabilidad $(1 - p)$. La unidad de tiempo es generalmente igual al retardo máximo de propagación.
 2. Si el medio está ocupado, se continúa escuchando hasta que se detecte libre y se repite el paso 1.
 3. Si la transmisión se ha retardado una unidad de tiempo, se repite el paso 1.
 - El parámetro p debe ser lo suficientemente bajo como para evitar la inestabilidad, resultando ocasionalmente en retardos enormes en condiciones de carga elevada.
- **Ineficiencia**
 - Cuando dos tramas colisionan, el medio permanece inutilizable mientras dure la transmisión de ambas tramas dañadas.
 - En **1-persistente**, si dos estaciones están listas a la mitad de la transmisión de una tercera estación, ambas van a transmitir exactamente al mismo tiempo cuando se libere el canal, provocando una colisión.

CSMA/CD

- CSMA con Detección de Colisiones (*with Collision Detection*)
- Soluciona la ineficiencia de CSMA haciendo que la estación siga escuchando el medio mientras dura la transmisión.
- Reglas
 1. Medio libre => transmite; medio ocupado => paso 2
 2. Medio ocupado => escucha hasta que el canal se libere.
 3. Colisión durante la transmisión => se transmite una pequeña señal de interferencia (**jam signal**) para asegurarse de que todas las estaciones constaten la colisión y se deja de transmitir.
 4. Tras la emisión de la señal de interferencia, la estación espera una cantidad aleatoria de tiempo conocida como **backoff**, intentando transmitir de nuevo a continuación (volviendo al paso 1).
 - Algoritmo exponencial binario.

CSMA/CA

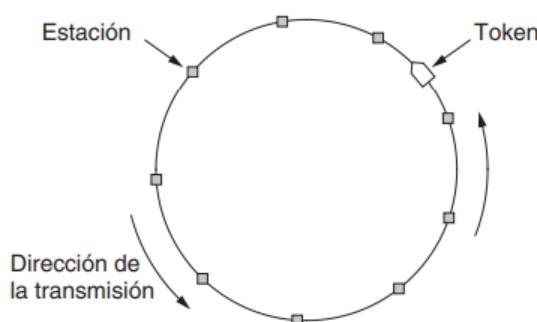
- Usa varias técnicas para evitar colisiones (una de ellas es la posicional, que establece prioridades de acuerdo a las posiciones de las estaciones).

Paso de Testigo

- Permite que cada estación transmita una trama por turno, en un orden predefinido. Se pasa un pequeño mensaje (**token**) de una estación a otra, en el mismo orden. Ese **token** representa el permiso para enviar. Cuando la estación recibe el token, puede enviar la trama que tiene en cola para transmitir, y después envía el token a la siguiente estación. Si no está esperando para enviar, simplemente pasa el token.
- **Ventaja**
 - Control de acceso flexible.
 - Equitativo.
 - Proporciona prioridad y servicios con ancho de banda garantizado.
- **Desventaja**
 - Necesita procedimientos para realizar el mantenimiento del anillo.
 - La pérdida del token impide posteriores utilizaciones del anillo.
 - Una duplicidad del token puede interrumpir el funcionamiento del anillo.
- **Tipos**
 - **Token-Ring (IEEE 802.5)**
 - **Token-Bus (IEEE 802.4)**

Token Ring

- La topología anillo se usa para definir el orden en el que las estaciones envían información. El token y las tramas se transmiten en la misma dirección. Para evitar que la trama circule indefinidamente, una estación la quita del anillo (puede ser la estación origen o destino).



Token Bus

- Físicamente, el canal es un bus; lógicamente, un anillo.
- Cada estación puede usar el bus para enviar el token a la siguiente estación en la secuencia predefinida.
- Al poseer el token, una estación puede usar el bus para enviar una trama.

Dispositivos

Dominio de Colisión: Es el área de red donde se propagan las colisiones producidas por ocupación del medio en forma simultánea por varios hosts.

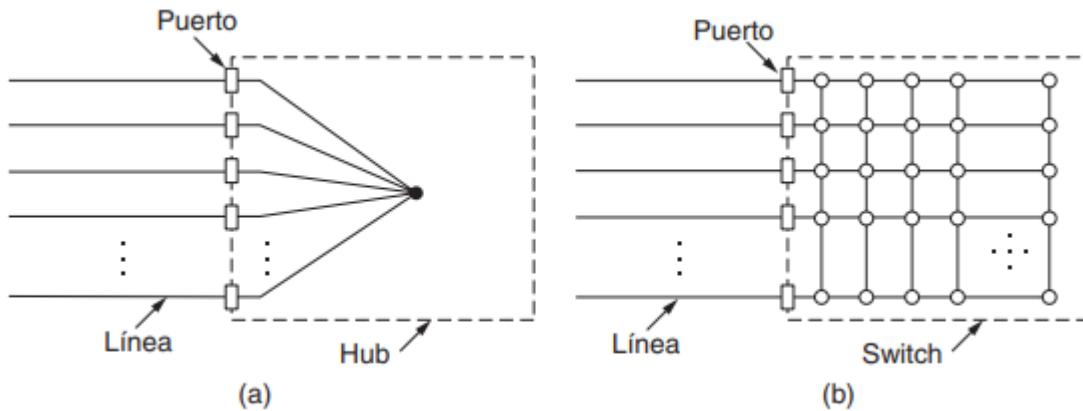
Dominio de Broadcast: Es el área de red donde se propagan las tramas de difusión o broadcast. Están limitadas por routers.

Capa	Dispositivos	Dominio de Colisión	Dominio de Broadcast
Red	Router	No	Sí
Enlace	Bridge - Switch	No	Sí
Física	Repetidor - HUB	Sí	Sí

Capa 1 (Física)

- **Repetidores**
 - Recibe datos sobre un enlace de comunicaciones y los transmite, bit a bit, sobre otro enlace tan rápido como se reciben los datos, sin utilizar almacenamiento temporal.
 - Son dispositivos analógicos que funcionan con señales de los cables a los que están conectados.
 - La señal se limpia, amplifica y se pone en otro cable.
 - Tiene dos puertos
- **HUB (Concentrador)**
 - Tiene N puertos que unen de manera eléctrica.
 - Cuando llega una trama por una línea, se envían por todas las demás.
 - Todas las líneas deben operar a la misma velocidad.
 - Todas las estaciones están en el mismo dominio de colisión

Capa 2 (De Enlace de Datos)



- **Bridge**
 - Interconecta dos LAN que usan la misma capa física y capa MAC.
 - Almacena y hace control de errores antes de retransmitir las tramas MAC.
 - Reenvía tramas MAC que corresponden al segmento.
 - Dispone de memoria, capacidad de direccionamiento y enrutamiento.
 - Debe conocer las direcciones de cada red para determinar qué tramas debe pasar.
 - Puede conectar más de dos LAN.
- **Switch (Conmutador)**
 - Aprenden y almacenan direcciones MAC de los dispositivos alcanzables a través de sus puertos.
 - Mejora de rendimiento y seguridad.
 - Pasan datos de un segmento a otro liberando la conexión al finalizar.
 - Problema de bucles e inundación.
 - Cada puerto es un dominio de colisión.
 - Tipos
 - **Store and forward (almacenamiento y reenvío).** Almacena en búfer, calcula CRC y tamaño de trama. Asegura sin errores y confiable. Demora. Uso en redes corporativas.
 - **Cut through.** Reduce latencia. Lee sólo los 6 bytes primeros y reenvían. No detecta tramas corruptas o con errores. Variante fragment free. Lee los primeros 64 bytes y reenvía. Evita corrupción de trama. Uso en pequeños grupos.
 - **Adaptive cut through.** Modo adaptativo compatible con ambos según convenga.

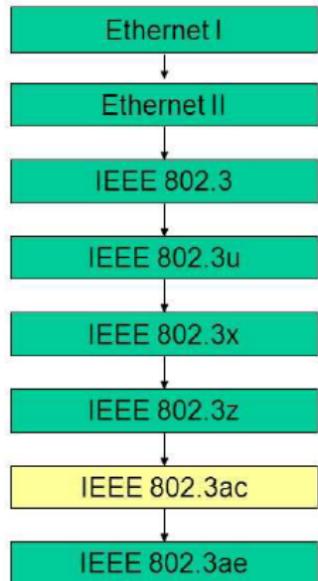
Capa 3 (De Red)

- **Router**
 - Tienen capacidad de enrutamiento o encaminamiento de paquetes.
 - Permiten interconectar redes LAN con redes WAN.
 - 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 → formateo, generación de FCS, codificación manchester, etc.
 - Transceptor → modula/demodula.
- El formato de trama MAC sólo difiere en un campo.

Evolución de Ethernet



Tramas Ethernet y IEEE 802.3

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

8B	6B	6B	2B	46-1500B	4B
Preámbulo	Dirección Destino	Dirección Origen	Tipo/Longitud de Trama	PAYLOAD	Frecuencia de Control de Trama

- 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_t bajos como T_p 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**
 - 0s → transición negativa en la mitad del intervalo del símbolo.
 - 1s → transición positiva en la mitad del intervalo del símbolo.
 - Usado en redes *Ethernet*.
- **Código Manchester Bifase Diferencial**
 - 0s → hay 2 (dos) transiciones: una al inicio del intervalo del símbolo y otra en la mitad.
 - 1s → hay 1 única transición en la mitad del intervalo del símbolo; al inicio no hay.
 - Usado en redes Token-Ring.

Detección de Colisiones

Para gestionar cuándo y cómo reintentar acceder al medio (determinar el intervalo aleatorio) en caso de detectarse colisiones, se utiliza el **algoritmo exponencial binario**.

Después de una colisión, el tiempo se divide en ranuras discretas cuya longitud es igual al tiempo de propagación de ida y vuelta ($2t_p$). Tomando en cuenta la ruta más larga permitida por Ethernet, el tiempo de ranura se estableció en 512 tiempos de bit. Después de la primera colisión, cada estación espera 0 o 1 tiempos de ranura al azar antes de intentar otra vez. Si dos estaciones entran en colisión y ambas eligen el mismo número aleatorio, habrá una nueva colisión. Después de la segunda, cada una escoge 0, 1, 2 o 3 al azar y espera ese tiempo de ranura. Si ocurre otra colisión, la próxima se elige un número de ranura entre $0 \text{ a } 2^3 - 1$

Al llegar a 10 colisiones, el intervalo de aleatorización se mantiene en un máximo de 1.023 ranuras. Después de 16 colisiones, la estación deja de intentar e informa un error.

Cuando una estación consigue transmitir la trama, su contador de intentos (colisiones) se pone a cero

Generalizado:

$$\text{Colisión } i \rightarrow \# \text{ranuras entre } 0 \text{ y } (2^i - 1)$$

$$\text{Ranura de tiempo de espera} = 512 / V_{RED}$$

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 Comutada

- Para tratar con el aumento de carga se usa un **switch** que contiene un **backplane** de alta velocidad que conecta a todos los puertos.
- En *full-duplex* no hay colisiones (el puerto y la estación pueden enviar una trama en el cable al mismo tiempo).
- En *half-duplex* la estación y el puerto deben competir por la transmisión con CSMA/CD.

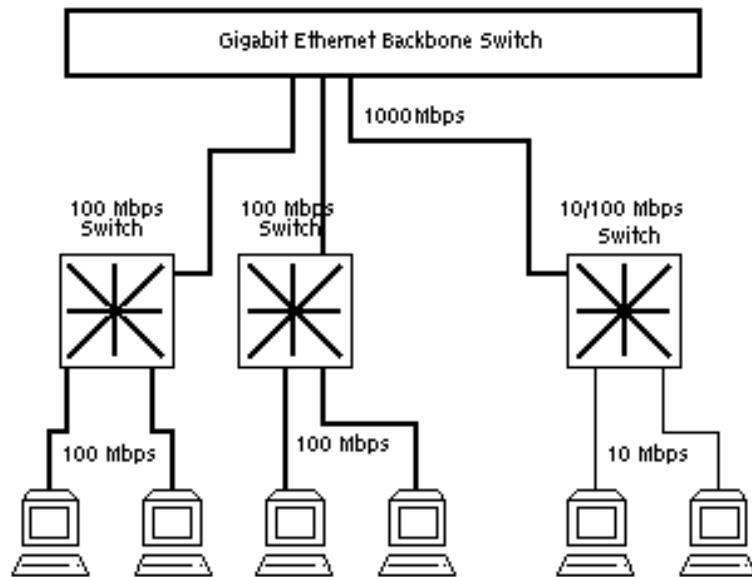
Fast Ethernet (802.3u)

- Se mantienen todos los formatos, interfaces y reglas de procedimientos anteriores, pero se reduce el tiempo de bits de 100 nseg a 10 nseg.

Nombre	Cable	Segmento máximo	Ventajas
100Base-T4	Par trenzado	100 m	Utiliza UTP categoría 3.
100Base-TX	Par trenzado	100 m	Full-dúplex a 100 Mbps (UTP cat 5).
100Base-FX	Fibra óptica	2000 m	Full-dúplex a 100 Mbps; distancias largas.

- Ethernet clásico es *semi-duplex*. En caso de operar en *full-duplex*, una estación puede transmitir y recibir al mismo tiempo. Una Ethernet a 100 Mbps en *full-duplex* alcanzaría (teóricamente) una velocidad de 200 Mbps.
- **Autonegociación**. Dos estaciones negocian de manera automática la velocidad óptima y la duplicidad (half-duplex o full-duplex). Esto facilita la actualización.

Gigabit Ethernet (80.3ab)



- Ofrece servicio de datagramas sin confirmación de recepción con unidifusión y multidifusión, utiliza el mismo esquema de direccionamiento de 48 bits y mantiene el mismo formato de trama.
- Soporta *full-duplex* y *half-duplex*
 - *Full-duplex*. Se utiliza cuando hay un switch central conectado. Todas las líneas se almacenan en el búfer con el fin de que cada estación o switch pueda enviar tramas cuando lo desee. No se utiliza CSMA/CD porque no hay colisiones y la longitud máxima del cable se determina en base a los aspectos relacionados a la fuerza de la señal. Los switches pueden mezclar las velocidades (autonegociación entre 10, 100 y 1000 Mbps)
 - *Half-duplex*. Se utiliza cuando la estación está conectada a un hub. El hub no almacena las tramas entrantes. Hay colisiones (se usa CSMA/CD).
- Mejoras en el esquema CSMA/CD
 - **Extensión de la portadora.** Se agregan símbolos al final de una trama MAC corta para que el bloque tenga una duración de 4.096 bits (mayor que los 512 exigidos a 10 y 100 Mbps). Esto es para que la longitud de trama (tiempo de transmisión) sea mayor que el tiempo de propagación a 1 Gbps.
 - **Ráfagas de tramas.** Se transmiten de forma consecutiva varias tramas cortas sin necesidad de dejar el control del CSMA/CD.

Nombre	Cable	Segmento máximo	Ventajas
1000Base-SX	Fibra óptica	550 m	Fibra multimodo (50, 62.5 micras)
1000Base-LX	Fibra óptica	5000 m	Monomodo (10 μ) o multimodo (50, 62.5 μ)
1000Base-CX	2 pares de STP	25 m	Par trenzado blindado
1000Base-T	4 pares de UTP	100 m	UTP estándar categoría 5

10 Gigabit Ethernet

- Solo soportan *full-duplex*.
- CSMA/CD no forma parte del diseño.
- Para la compatibilidad, las interfaces usan la autonegociación y cambian a la velocidad más alta soportada por ambos extremos de la línea.
- 10GB-LX4 usa WDM para multiplexar el flujo de bits sobre cuatro ondas de luz.

Nombre	Cable	Distancia Máxima
10GB-S	FO Multimodo (850 nm, 1° Ventana)	300m
10GB-L	FO Monomodo (1.310 nm, 2° Ventana)	10km
10GB-E	FO Monomodo (1.550 nm, 3° Ventana)	40km
10GB-LX4	FO Monomodo y Multimodo (1.310 nm)	10km

FDDI · Interfaz de Datos Distribuidos por FO

- Topología → doble anillo → si se llegara a caer una estación, se puede “puentejar” (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)

Es importante distinguir quién está en qué LAN (agrupar usuarios en redes LAN):

- Reflejar la estructura de la organización.
- Seguridad. Una LAN hospeda los servidores web, otra computadoras de uso público, etc).

- Carga. No todas las LAN tienen la misma carga (es conveniente separarlas para no saturar toda la red única).
- Tráfico de difusión. A medida que aumenta el número de computadoras en una LAN, aumenta el número de difusiones.
 - Tormenta de difusión. Una interfaz de red puede averiarse y generar flujos interminables de tramas de difusión. Algunas de esas tramas pueden provocar respuestas (generando más tráfico). Como consecuencia, las tramas de difusión ocupan toda la capacidad de la LAN y las máquinas se atascan sólo procesando y desechariendo las tramas difundidas.

VLAN surgió porque realizar cambios en el cableado no resulta muy flexible. VLAN es la asociación lógica de estaciones que constituyen la red. Cada VLAN es un dominio de broadcast.

Configuración

- Cantidad de VLANs
- Nombre de las VLAN
- Miembros de la VLAN
- Tablas de configuración. Indican qué VLANs se pueden acceder a través de qué puertos.

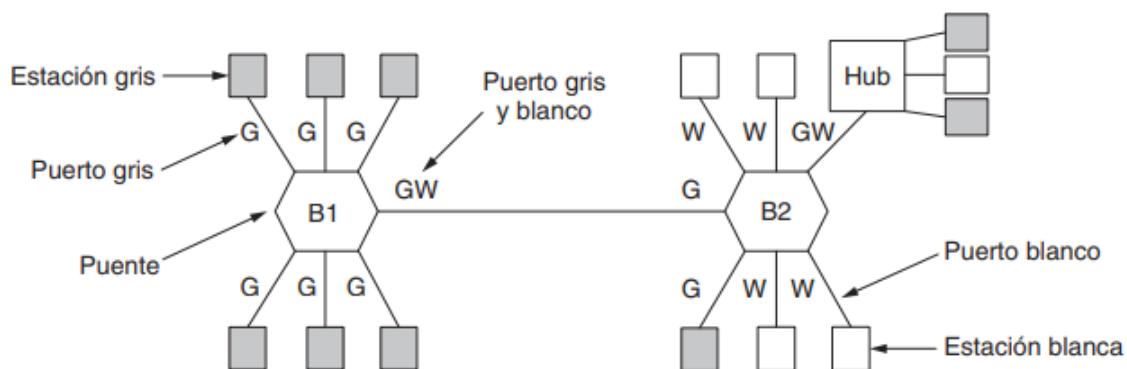


Figura 4-47. Dos redes VLAN, gris y blanca, en una LAN con puente.

- Formas de definir una VLAN:
 - Por puertos (Capa 1).
 - Por dir. MAC (Capa 2).
 - Por tipo de protocolo (Capa 2, LLC).
 - Por dir. IP (Capa 3).
 - Por aplicaciones superiores (Capas superiores).

IEEE 802.1Q

- Los puentes necesitan saber a qué VLAN pertenece una trama para poder reenviarla.
- Se agrega un nuevo campo con una etiqueta VLAN. Ese campo solo es utilizado por los puentes y los commutadores. Los puentes deben tener soporte para VLAN. Los que tienen soporte, agregan los campos VLAN; los que no, los eliminan.
- Múltiples redes pueden compartir un enlace (trunk)

Trama 802.1Q

Dir. Destino	Dir. Origen	TAG	Longitud /Tipo	Datos	Relleno	CRC
--------------	-------------	-----	----------------	-------	---------	-----

Tag

2 Bytes	3 bits	1 bit	12 bits
ID del protocolo de VLAN (0x8100)	Prioridad	CFI	Identificador de VLAN

- El identificador de VLAN es usado por el switch como índice de una tabla para averiguar a cuáles puertos enviar la trama.
- *Plug-and-play*. Los puentes con soporte VLAN se pueden autoconfigurar. Por ejemplo, si una trama etiquetada como VLAN 4 llega por el puerto 3, se asume que una máquina en el puerto 3 está en la VLAN 4.

IEEE 802.1D Spanning Tree

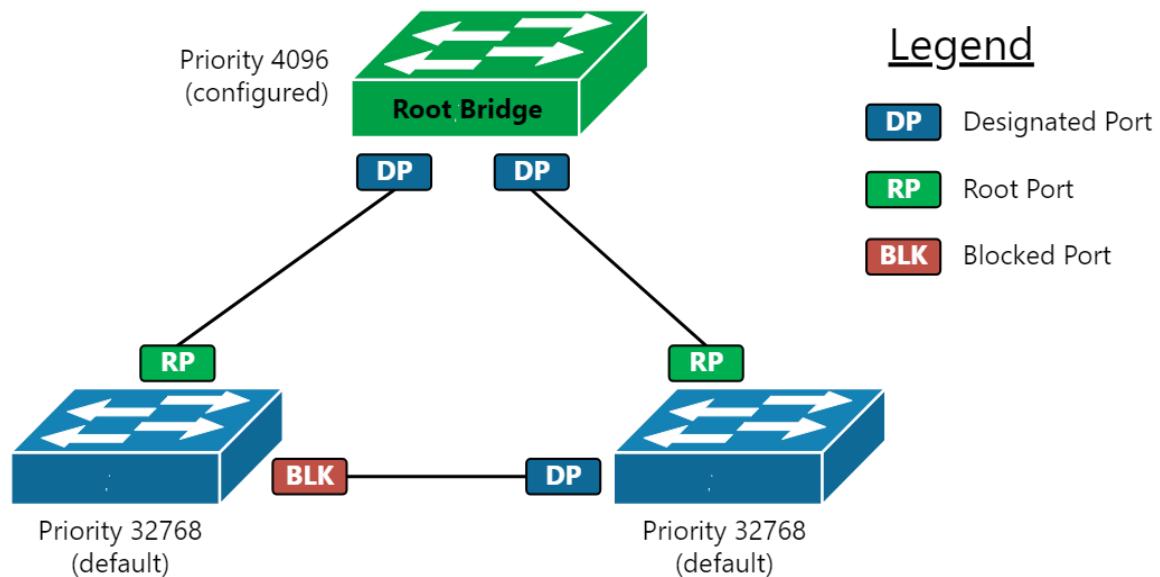
Estándar de puentes MAC que incluye el protocolo Spanning Tree (STP). Impide la acción de bucles que se generan en los puentes/switches, cuando existen vínculos redundantes. Transforma una red física de tipo malla con bucles, en una red lógica tipo árbol libre de bucles.

1. **Designación del root switch.** Los SWs intercambian BPDU cada 2 segundos. El BPDU contiene el BID (Bridge ID) del root SW que conocen en el momento y su propio BID. Al comienzo, cada switch dice "yo soy el root". El root se termina eligiendo mediante el menor BID (Bridge priority + MAC Address).
2. **Definir los puertos designados del root switch.** Todos los puertos que se conectan a un SW desde el root SW.
3. **Detectar loops.** Un switch entiende que hay un loop cuando recibe BPDUs del root desde más de una interfaz. Se tiene que bloquear uno de esos puertos.

4. **Definir los caminos de menor costo desde los SW al root SW.** Para encontrar las rutas más cortas, los SW incluyen la distancia desde la raíz en sus mensajes de configuración.
5. **Definir los puertos designados por tramos de los demás SW.**
6. **Definir los puertos bloqueados.**

Los puertos pueden ser:

- **Root Port.** Representa el mejor camino hacia el Root SW. No se envían BPDUs mediante este puerto. El switch aprende direcciones MAC en este puerto.
- **Designated Port.** Un puerto que apunta lejos del root. BPDUs son enviados mediante este puerto. Son los puertos que forman parte de la ruta más corta.
- **Blocked Port.** No se transmite tráfico. Son los puertos que no forman parte de la ruta más corta.



U3. LAN con Cableado Estructurado

Cableado Estructurado

- Permite tráfico de voz y datos en el mismo cableado.
- Basado en la Norma EIA / TIA 568
 - Estándar para el cableado de telecomunicaciones en edificios comerciales.
- **Características:**
 - Alta velocidad en la transmisión de datos.
 - Mejor calidad en las comunicaciones de voz aprovechando la capacidad instalada.
 - Compatibilidad con tecnologías actuales y futuras.
 - Flexibilidad y bajo costo de mantenimiento. Estética agradable.
- **Componentes del Cableado:**
 - Medio de Transmisión: UTP, STP, FO y Coaxil.
 - Bloques de Conexión.
 - Paneles de Interconexión.
 - Armario de Telecomunicaciones.
 - Armario de Distribución o Placas y Tomas de Pared.
 - Puesta a Tierra.
 - Abrazaderas.

Herramientas Utilizadas

- **Punch Tool:** para fijar cables en los conectores hembra.
- **Crimp Tool:** para fijar cables en los conectores RJ45. Asegura que placas conductoras penetren el conductor.
- **Medidor de Cables:** mapa de cableado, longitud de cables, atenuación, otras mediciones.

Atenuación

- Relación entre la potencia de la señal recibida en el extremo destino del cable y la potencia transmitida en el extremo origen.
- Cuanto menor es su valor, peor es. Lo ideal es una atenuación igual a 0.

Diafonía

- Es consecuencia del acoplamiento inductivo entre los pares de transmisión y recepción en un cable, por lo cual parte de la señal de un par aparece en el otro.
- La parte más importante es la paradiafonía o NEXT (Near End Crosstalk). El NEXT se produce en el extremo más próximo al receptor, causada por la señal emitida por el mismo.
- Ideal es una diafonía infinitamente negativa. Se minimiza con el trenzado de los cables.

Comparación de Cableados Estandarizados

Anónimo	Impedancia	Significado
STP	150 ohms	Par trenzado blindado
FTP	120 ohms	Par trenzado cubierto de pantalla de aluminio
SFTP	120 ohms	FTP con una malla de cobre adicional
SSTP	120 ohms	Par trenzado con una pantalla de aluminio independiente y una malla exterior de cobre.

U4 - LAN Inalámbricas

Aplicaciones

- **Ampliaciones de redes**
 - Una LAN inalámbrica está conectada en muchos casos a una LAN troncal cableada.
 - Existe un **módulo de control** (CM) que funciona como interfaz con la LAN inalámbrica. Incluye funciones propias de un puente o switch, y lógica de control de acceso.
 - Los hubs y otros módulos de usuario (UM) que controlan varias estaciones fuera de una LAN cableada pueden formar parte de la LAN inalámbrica.
- **Interconexión de edificios.**
 - Uso de enlace punto a punto inalámbrico entre dos edificios. Los dispositivos conectados son puentes o dispositivos de encaminamiento.
- **Acceso nómade.**
 - Proporciona un enlace inalámbrico entre un concentrador de una LAN y un terminal de datos móvil.
- **Trabajo en red *ad-hoc***
 - Red *ad-hoc*: red entre iguales (sin servidor central) establecida temporalmente para satisfacer alguna necesidad inmediata.

Modos

- **Modo infraestructura**
 - Cada cliente se asocia a un AP (*Access Point*). El AP está conectado a la otra red. El cliente envía y recibe sus paquetes a través del AP
 - Se pueden conectar varios puntos de acceso juntos mediante una red alámbrica (**sistema de distribución**).

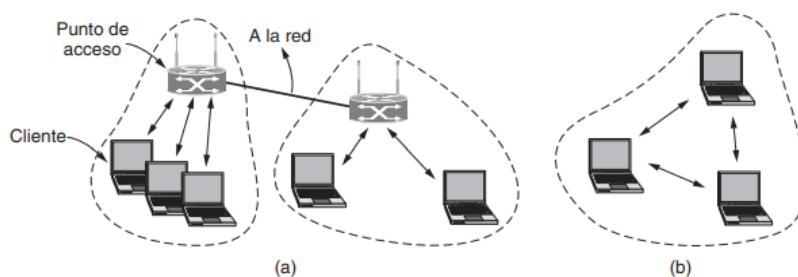


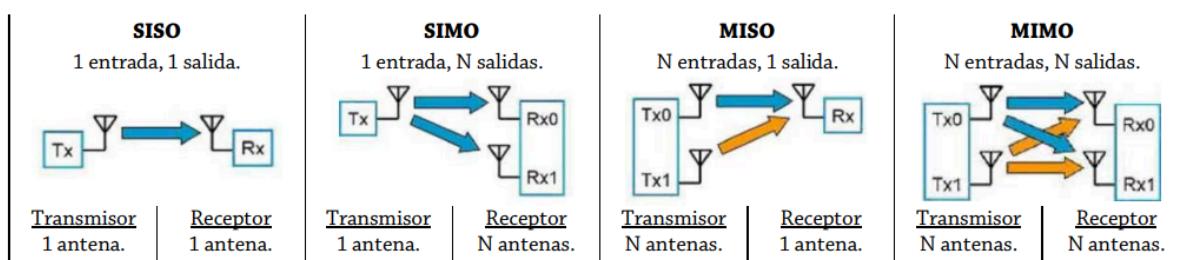
Figura 4-23. Arquitectura 802.11. (a) Modo de infraestructura. (b) Modo *ad hoc*.

- **Red *ad-hoc*.**

Requisitos

- Requisitos típicos de cualquier LAN
 - Alta capacidad, cobertura de pequeñas distancias, conectividad total entre las estaciones pertenecientes a la red y capacidad de difusión.
- **Rendimiento:** el protocolo de control de acceso al medio debería hacer un uso tan eficiente como fuera posible del medio inalámbrico para maximizar la capacidad.
- **Número de nodos:** poder dar soporte a cientos de nodos mediante el uso de varias celdas.
- **Conexión a la LAN tronca.**
- **Área de servicio:** cobertura de la red.
- **Consumo de energía.**
- **Robustez en la transmisión y seguridad:** confidencialidad
- **Funcionamiento de redes adyacentes:** evitar interferencias entre redes que operen en la misma zona.
- **Funcionamiento sin licencia.**
- **Traspasos (Handoff)/Itinerancia (Roaming):** el protocolo MAC usado en LAN inalámbricas debería permitir a las estaciones móviles desplazarse de una celda a otra.
- **Configuración dinámica:** los aspectos del direccionamiento MAC y de gestión de la red LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

Tecnología de radio SISO, MIMO, MISO y SIMO



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 a 3,5 GHz	54 a 862 MHz
Velocidad Máxima	1 a 24 Mbps	11 a 54 Mbps	54 Mbps	23 Mbps
Alcance	10m	50m	60km	33 - 100 km
Técnica y Método de Modulación	SS-FH. GFSK.	SS-FH y SS-DS.		OFDMA. Sin licencia.

Medios de comunicación inalámbrica – Tecnologías LAN inalámbricas

LAN de infrarrojo (Infrared - IR)

- Una celda individual en una LAN IR está limitada a una sola habitación.
- Ondas electromagnéticas del espectro infrarrojo, próximas a la luz visible.
- Técnicas
 - Haz dirigido
 - Omnidireccional
 - Difusión (usando un reflector).
- Ventajas
 - Espectro virtualmente ilimitado, permitiendo alcanzar velocidades de datos extremadamente altas.
 - La luz infrarroja no atraviesa objetos opacos, garantizando que no haya escuchas o interferencias desde otra habitación.
 - Equipos baratos y simples
- Desventajas
 - La radiación infrarroja debido a la luz solar y artificial causa ruido en el receptor, obligando a usar transmisores de mayor potencia.

LAN de Espectro Expandido

- Hace uso de una disposición de celdas múltiples. Las celdas adyacentes utilizan diferentes frecuencias dentro de la misma banda para evitar interferencias.
- Dentro de cada celda puede usarse una topología basada en un concentrador o bien una entre iguales.
- El espectro expandido permite que varios usuarios puedan utilizar el mismo ancho de banda con muy pocas interferencias entre sí.
 - CDM y CDMA
- **Ocultamiento y cifrado de señales.** Solo un usuario que conozca el código expansor podrá recuperar la información codificada.

Espectro Expandido

- La idea es expandir la señal de información en un ancho de banda superior con objeto de dificultar las interferencias y la intercepción.
- Esquema
 1. La entrada va a un codificador de canal que produce una señal analógica con un ancho de banda relativamente estrecho centrado en una frecuencia dada.
 2. La señal se modula haciendo uso de una secuencia de dígitos conocida como código o secuencia de expansión. Ese código se genera mediante un generador de números pseudoaleatorios. La modulación incrementa el ancho de banda (expansión del espectro) de la señal a transmitir.
 3. El receptor usa la misma secuencia pseudoaleatoria para demodular la señal de espectro expandido.
 4. La señal pasa a un decodificador de señal para recuperar los datos.

LAN de Radio de Banda Estrecha (Microondas)

- Se utiliza una banda de frecuencias de microondas de radio para la transmisión de la señal, siendo esta banda relativamente estrecha (el ancho suficiente para acomodar la señal).
- Puede ser:
 - Con licencia
 - Sin licencia

Bluetooth . IEEE 802.15 . WPAN

Clase	Potencia máxima permitida	Alcance	Versión	Velocidad de Transmisión
1	100 mW	100 m	1.2	1 Mbps
2	2,5 mW	5 a 10 m	2.0 +EDR	3 Mbps
3	1 mW	1 m	3.0 +HS	24 Mbps
4	0,5 mW	0,5 m	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	-	-	-		70 m	30 m	-
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.

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

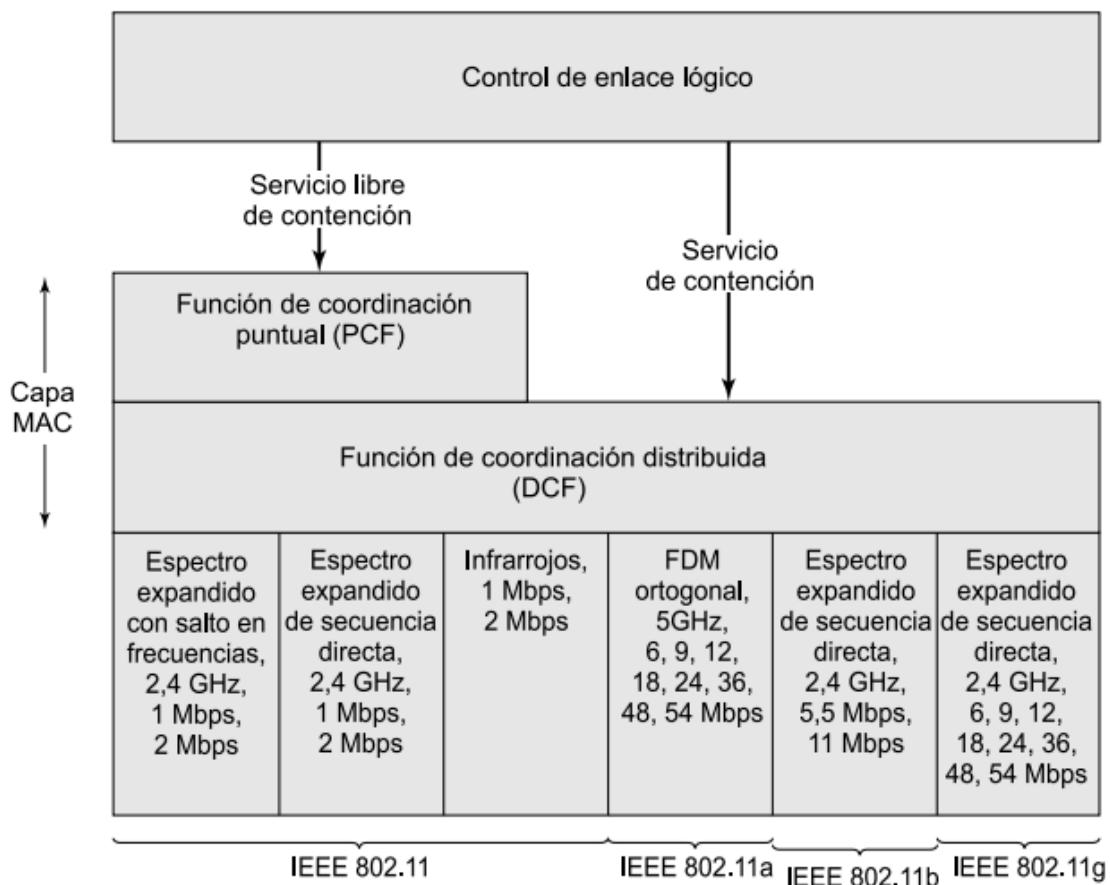


Figura 17.5. Arquitectura de protocolos IEEE 802.11.

Modelo de Capas

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

Estructura

Posee una estructura celular donde cada celda (llamada BSS) contiene:

- Distribution System (DS) : generalmente la red LAN cableada
- Access Point (AP) : estación base a la cual se conectan los terminales remotos
- Terminales

Subcapa MAC 802.11 - Funciones

Tiene tres funciones: entrega fiable de datos, control de acceso y seguridad.

Entrega Fiable de Datos

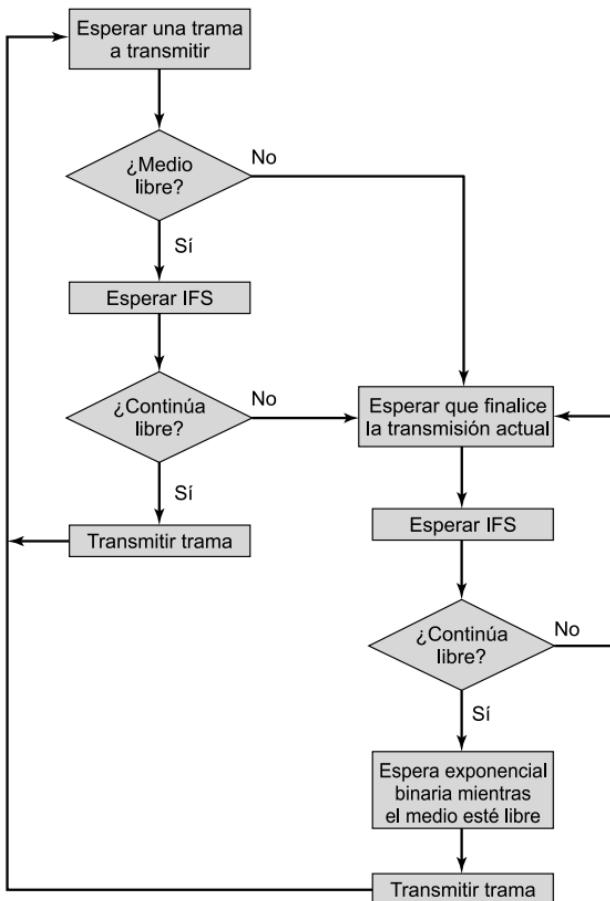
- Por un tema de eficiencia, se maneja el problema de los errores en esta capa. Para eso se define un **protocolo de intercambio de tramas**
- Mecanismo de 2 tramas. Cuando una estación recibe una trama de datos, devuelve un ACK a la estación de origen. Este intercambio es tratado como una unidad atómica, sin ser interrumpido por una transmisión procedente de cualquier otra estación. Si la fuente no recibe la confirmación en un intervalo corto de tiempo, la fuente retransmite la trama.
- Mecanismo de 4 tramas. La fuente emite una trama de **solicitud para enviar (RTS)** hacia el destino. La estación destino responde con una **trama de permiso para enviar (CTS)**. Tras recibir la CTS, la fuente emite la trama de datos y el destino responde con una **confirmación (ACK)**.
 - RTS alerta a todas las estaciones que se encuentran dentro del rango de recepción de la fuente de que una transmisión está en curso. El resto de estaciones se abstiene de transmitir con objeto de evitar que se produzca una colisión entre dos tramas transmitidas al mismo tiempo.
 - CTS alerta a todas las estaciones que están en el rango de recepción del destino de que se va a producir un intercambio.

Control de Acceso

- Protocolos de acceso distribuido.

- La decisión para transmitir se distribuye sobre todos los nodos usando un mecanismo de detección de portadora.
 - Redes *ad-hoc* de estaciones paritarias.
 - Redes LAN inalámbricas que trabajan con tráfico a ráfagas.
- Protocolos de acceso centralizado
 - Implican una regulación de la transmisión por una autoridad central de toma de decisiones.
 - Para configuraciones en las que una serie de estaciones inalámbricas se encuentran interconectadas entre sí y con algún tipo de estación base que actúa como pasarela hacia una LAN troncal cableada.
 - Útil cuando parte de los datos tiene algún requisito de tiempo real o alta prioridad.
- Algoritmo DFWMAC
 - Proporciona un mecanismo de control de acceso distribuido sobre el que se ubica un control centralizado opcional.
- Función de coordinación distribuida (DCF)
 - Utiliza un algoritmo de contención para proporcionar acceso a la totalidad del tráfico. El tráfico asíncrono ordinario hace uso directamente de la DCF.
- Función de coordinación puntual (PCF)
 - Algoritmo MAC centralizado usado para ofrecer un servicio libre de contención.
 - La PCF se ubica justo por encima de la DCF y utiliza las características de ésta para asegurar el acceso a sus usuarios.

CSMA/CA



- Una estación que desee enviar una trama empieza con un retroceso aleatorio.
- La estación espera hasta que el canal está inactivo, para lo cual detecta que no hay señal durante un periodo corto (DIFS) y realiza un conteo descendente de las ranuras inactivas, haciendo pausa cuando se envían tramas
- Cuando el contador llega a 0, envía la trama.
- Si la trama logra pasar, el destino envía de inmediato una confirmación de recepción corta.
- La falta de una confirmación de recepción se interpreta como si hubiera ocurrido un error. En ese caso, el emisor duplica el periodo de retroceso e intenta de nuevo, continuando con el retroceso exponencial (algoritmo exponencial binario) hasta que la trama se transmite con éxito o se llegue al número máximo de retransmisiones.

Vector de Asignación de Red (NAV)

Para reducir las ambigüedades con respecto a qué estación va a transmitir, el 802.11 define la detección del canal como un proceso física y virtual.

- **Detección física:** solo se verifica el medio para ver si hay una señal válida.

- **Detección virtual:** cada estación mantiene un registro lógico del momento en que se usa el canal rastreando el **NAV**.

Cada trama lleva un campo NAV que indica cuánto tiempo tardará en completarse la secuencia a la que pertenece esa trama. Las otras estaciones que escuchen la trama saben que el canal estará ocupado durante el período indicado por el NAV, sin importar si pueden detectar o no una señal física.

Función de coordinación distribuida

Se usa CSMA/CA refinado mediante un mecanismo basado en distintos IFS (ordenados por tamaño/prioridad)

- **SIFS (Short IFS).** La estación que use un SIFS tiene la prioridad más alta. Enviar el siguiente fragmento después de esperar sólo un tiempo SIFS es lo que evita que otra estación irrumpa con una trama a mitad del intercambio. Se usa en:
 - **ACK.** Una estación que recibe una trama exclusiva responde con una trama ACK tras esperar un SIFS. La fuente recibe el ACK, espera un SIFS y envía la siguiente trama. La fuente mantiene el control hasta que se envíen todos los fragmentos.
 - **CTS/RTS.**
 - **Poll response.**
- **PIFS (Point coordination function IFS).** Lo usa el controlador central en el esquema PCF cuando emite sondeo.
- **DIFS (Distributed coordination function IFS).** Se usa como un retardo mínimo para las tramas asíncronas que compiten por el acceso al medio.

Función de Coordinación Puntual

Consiste en un sondeo realizado por un elemento central de sondeos (coordinador puntual). El coordinador hace uso de un PIFS cuando emite un sondeo. Dado que un PIFS es más pequeño que un DIFS, el coordinador puntual puede adueñarse del medio y bloquear todo el tráfico asíncrono mientras emite un sondeo y recibe las respuestas.

Se usa un intervalo **supertrama** para evitar bloquear todo el tráfico al emitir sondeos. El coordinador puntual emite sondeos a todas las estaciones configuradas para el sondeo usando un esquema de turno rotatorio. Después, el coordinador espera un tiempo igual a lo que reste de la supertrama, permitiendo así la existencia de un período de contención para el acceso asíncrono.

Subcapa MAC 802.11 - Trama

2 oct	2 oct	6 oct	6 oct	6 oct	2 oct	6 oct	0 a 2.312 oct	4 oct
FC	D/I	Dir. Destino	Dir. Origen	Dir. Receptor	SC	Dir. Transmisor	PAYLOAD	CRC

FC = Control de Trama

D/I = ID de duración/conexión

SC = Control de secuencia

- **Control de trama**

- Indica el tipo de trama (control, gestión o datos) y proporciona información de control. La información de control contiene información de control y relativa a la privacidad.

- **ID de duración/conexión**

- Indica el tiempo (en microsegundos) que el canal será reservado para una transmisión satisfactoria de una trama MAC.

- **Direcciones**

- **Control de secuencia**

- Subcampo **número de fragmento** (4 bits). Fragmentación y reensamblado.
 - Subcampo **número de secuencia** (12 bits). Numeración de las tramas enviadas entre un transmisor dado y un receptor.

- **Payload**

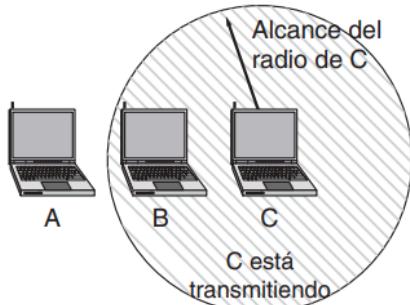
- **CRC**

Tipos de Trama

- **Control** (sondeo de ahorro de energía, RTS, CTS, ACK, fin período libre contienda CF, CF-ACK).
- **Datos** (Datos, +ACK-CF+CF-POLL, etc).
- **Gestión** (entre estaciones y puntos de acceso, gestión de asociaciones).

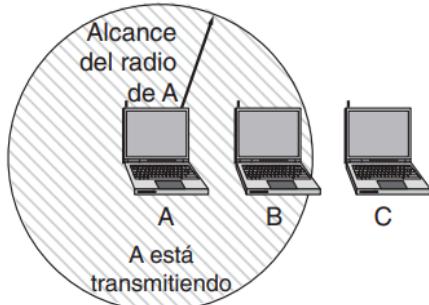
Problemas en la comunicación por radio

A desea enviar a B
pero no puede escuchar
que B está ocupada



(a)

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



(b)

a. Terminal oculta

- Una estación no puede detectar a un competidor potencial por el medio debido a que dicho competidor está demasiado lejos.
- **Solución:** mecanismo RTS/CTS que usa el NAV.
 - A desea enviar datos a B. A envía un RTS a B. B responde con CTS para indicar que el canal está libre. A recibe la CTS y envía su trama e inicia un temporizador ACK. B recibe la trama de datos y responde con un ACK para completar el intercambio. Si el temporizador de A expira antes de que la ACK vuelve, se considera una colisión y se realiza todo el protocolo de nuevo.
 - C no recibe el RTS, pero sí el CTS. Actualiza su NAV y se queda esperando.

b. Terminal expuesta

- Una estación se encuentra dentro del rango de otra y no puede realizar una transmisión porque detecta que el canal está ocupado.

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	2 a 5 km	5 a 10 km	2 a 5 km	Hasta 50 km
Frecuencia de operación	10 a 66 GHz	< 11 GHz	< 6 GHz	-
Velocidad de Transmisión	32 a 134 Mbps	75 Mbps	15 Mbps	300 Mbps

U5. Protocolos de Interconexión TCP/IP

Definiciones

- **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

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

Protocolo de Internet (IP)

- Define la unidad básica para la transferencia de datos, selección de rutas (ruteo) y conjunto de reglas para la entrega de paquetes no confiable.
- Toma los datos del nivel superior (TCP o UDP) y los inserta en la internet como **datagramas**. Los datagramas son independientes, no hay relación entre ellos, y viajan por distintas redes (Ethernet, FDDI, Frame Relay, X.25, etc).
- Usa ICMP para reportar errores.
- Se basa en servicio NO orientado a la conexión y NO confiable (sin validación). No se garantiza que el datagrama llegue a destino.
- Es un servicio de entrega con **Best Effort**.

Datagramas

Se estructura en palabras de 32 bits (4 B). 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		<i>1^{ra} palabra</i>					
	Identificación 16 bits		Banderas 3 bits	Desplazamiento de Fragmento 13 bits		<i>2^{da} palabra</i>					
	Tiempo de Vida 8 bits	Protocolo 8 bits	Suma de Verificación del HEADER 16 bits			<i>3^{ra} palabra</i>					
	Dirección IP del Origen 32 bits					<i>4^{ta} palabra</i>					
	Dirección IP del Destino 32 bits					<i>5^{ta} palabra</i>					
	Opciones + Relleno Longitud variable					<i>6^{ta} palabra</i> ...					
MTU 65.515 B máximo	PAYLOAD Longitud variable					<i>...</i> <i>Última palabra</i>					

1º Palabra. Funciones de aspectos operativos y de formato

- **Versión** del protocolo
- **Longitud del Header (IHL - Internet Header Length)**: longitud de la cabecera expresada en palabras de 32 bits. El valor mínimo es de 5 (20 octetos).
- **Tipo de servicio**: especifica los parámetros de fiabilidad, prioridad, retardo y rendimiento.
 - Primeros 6 bits: servicios diferenciados (DS)
 - Últimos 6 bits: campo de notificación explícita de congestión (ECN).
- **Longitud Total** del datagrama

2º Palabra. Fragmentación

- **Identificación**: junto a la dirección origen y destino y el protocolo de usuario identifica de forma única un datagrama.
- **Banderas o indicadores**.
 - Primer bit (More Fragments - MF). Se usa para la fragmentación y reensamblado.
 - Segundo bit (Don't Fragment - DF). Prohibe la fragmentación cuando es 1. En ese caso, si el datagrama excede el MTU, se descarta y se genera un mensaje ICMP.
 - Tercer bit. No es usado.

- **Desplazamiento de Fragmento:** indica el lugar donde se sitúa el fragmento dentro del datagrama original, medido en unidades de 64 bits.

3° Palabra. Temas operativos

- **Tiempo de vida:** especifica cuánto tiempo [segundos] se le permite a un datagrama permanecer en la red. Cada dispositivo de encaminamiento que procesa el datagrama debe decrementar este campo al menos en una unidad, de forma que el tiempo de vida es de alguna forma similar a una cuenta de saltos.
- **Protocolo:** identifica el protocolo de la capa superior.
- **CRC:** detección de errores en el Header.

4° Palabra

- **Dirección IP Origen**

5° Palabra

- **Dirección IP Destino**

6° 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.

Números de protocolos

Protocolo	HEX
ICMP	0x01
IGMP	0x02
IP	0x04
TCP	0x06
EGP	0x08
IGP	0x09
UDP	0x11
IPv6	0x29
EIGRP	0x58
OSPF	0x59

Direcciones

En IPv4, las direcciones son de 32 bits. Cada host y router de Internet tiene una dirección IP. La dirección no se refiere a un host, sino a una interfaz de red. Si un host está en dos redes, debe tener dos direcciones IP. Los enrutadores tienen varias interfaces, entonces tienen varias direcciones IP. La dirección IP de cada red debe ser única; la de cada host, única dentro de una misma red.

Formato

Las direcciones son jerárquicas. Cada dirección está compuesta por una porción de red de longitud variable en los bits superiores, y de una porción de host en los bits inferiores. Dentro de una misma red, la porción de red tiene el mismo valor para todos los hosts (**prefijo**).

Se escriben en *notación punto decimal*. Cada byte se escribe en decimal (de 0 a 255).

Ejemplo:

10000000 11010000 00000010 10010111 = 80 D0 02 97 = 128.208.2.151

El **prefijo** se escribe después de la dirección IP. Ejemplo: si para 128.208.2.151 el prefijo contiene 2^8 direcciones, la porción de red es de 24 bits, se escribe 128.208.0.0/**24**

Difusión

- **Difusión Dirigida**
 - Broadcast limitado a la red.
 - Todos los bits del campo de host son 1s.
- **Difusión Limitada**
 - Limitada a la red local.
 - Todos los bits son 1s.
- **Multidifusión**
 - Se hace con clase D

Direcciones especiales

Dirección	Descripción
Todo 0s	Identificador del host en red local.
Todos los bits de host 0s	Identificador de una red
Todos los bits de host 1s	Dirección de broadcast
127.0.0.1	Se refiere al mismo dispositivo.
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)
10.0.0.0 hasta 10.255.255.255	Direcciones IP privadas
169.254.0.0 hasta 169.254.255.255	
172.16.0.0 hasta 172.31.255.255	
192.168.0.0 hasta 192.168.255.255	

Clases

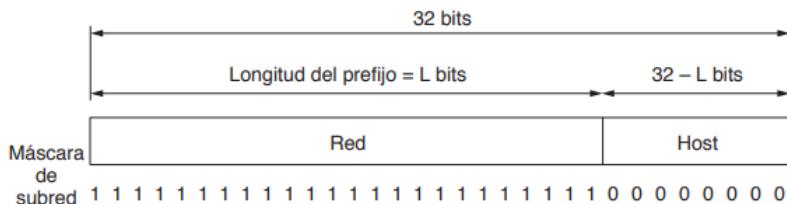
Hay cinco clases de redes que se pueden asociar a las siguientes condiciones:

- Clase A
 - 0XXXXXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX.
 - Primer octeto: 1 hasta 127
 - Pocas redes, cada una con muchos computadores.
- Clase B
 - 10XXXXXXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX.
 - Primer octeto: 128 hasta 191
 - Número medio de redes, cada una con un número medio de computadores.
- Clase C
 - 110XXXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX
 - Primer octeto: 192 hasta 223
 - Muchas redes, cada una con pocos computadores.
- Clase D
 - 1110XXXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX
 - Primer octeto: 224 hasta 239
 - Multidifusión
- Clase E
 - 11110XXX.XXXXXXXXXX.XXXXXXXXXX.XXXXXXXXXX
 - Primer octeto: 240 hasta 247
 - Uso futuro

Clase	# Redes	# Hosts	Rango
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

Subredes y máscaras de subred

Solucionan el problema del crecimiento de una red. Se divide el bloque de direcciones en varias partes para uso interno en forma de múltiples redes (**subredes**), pero para el exterior se considera una red única. A cada LAN se le asigna un número de subred. Se “ceden” bits del host.



La longitud del prefijo corresponde a una máscara binaria de 1s en la porción de red (**máscara de red**). Los 1s corresponden a la parte de **red** y **subred**.

Ejemplo. Se tiene un prefijo /16 (Clase B). Hay 3 LANs (Departamento de Sistemas, Química e Industrial). Se definen 3 subredes. La mitad del bloque (/17) se asigna a Sistemas, una cuarta parte a Química (/18) y una octava parte (/19) a Industrial. El octavo restante queda sin usar.

Sistemas:	10000000	11010000	1 xxxxxxxx	xxxxxxxx	128.208.128.0/17
Química:	10000000	11010000	00 xxxxxxxx	xxxxxxxx	128.208.0.0/18
Industrial:	10000000	11010000	011 xxxxx	xxxxxxxx	128.208.96.0/19
A Internet:	10000000	11010000	xxxxxxxx	xxxxxxxx	128.208.0.0/16

Cuando llega un paquete, el router analiza su dirección de destino y verifica a qué subred pertenece. Se aplica un AND a la dirección de destino con la máscara para cada subred y verifica que el resultado sea el prefijo correspondiente. El objetivo de la máscara de subred es borrar la parte del host y dejar el número de red y subred.

Para el ejemplo anterior, si llega 128.208.2.151, se verifica:

128.208.2.151 AND 255.255.128.0 = 128.208.0.0 (Coincide con Química).

(a) Representaciones punto decimal y binaria de las direcciones IP y las máscaras de subred

	Representación binaria	Punto decimal
Dirección IP	11000000.11100100.00010001.00111001	192.228.17.57
Máscara de subred	11111111.11111111.11111111.11100000	255.255.255.224
Operación AND bit-a-bit de la dirección y la máscara (número de red/subred resultante)	11000000.11100100.00010001.00100000	192.228.17.32
Número de subred	11000000.11100100.00010001.001	1
Número de computador	00000000.00000000.00000000.00011001	25

(b) Máscaras de subred por defecto

	Representación binaria	Punto decimal
Máscara de clase A por defecto	11111111.00000000.00000000.00000000	255.0.0.0
Ejemplo de máscara de clase A	11111111.11000000.00000000.00000000	255.192.0.0
Máscara de clase B por defecto	11111111.11111111.00000000.00000000	255.255.0.0
Ejemplo de máscara de clase B	11111111.11111111.11110000.00000000	255.255.248.0
Máscara de clase C por defecto	11111111.11111111.11111111.00000000	255.255.255.0
Ejemplo de máscara de clase C	11111111.11111111.11111111.11111100	255.255.255.252

Hay dos direcciones reservadas:

- La dirección más baja es la *Network Identifier* (el id de la subred). Todos los bits del host son 0s.
- La dirección más alta es la dirección de broadcast. Todos los bits del host son 1s.

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.

Si la dirección de red default es la misma para un grupo de subredes, se pueden *sumarizar* en una misma dirección:

192.168.0.0/26, 192.168.0.64/26, 192.168.0.128/26, and 192.168.0.192/26.

Tienen la misma dirección de red (192.168.0). Se pueden sumarizar en la red 192.168.0.0/24

Se necesita un bloque de direcciones mayor o igual a la suma de los bloques de las subredes. En el ejemplo anterior la suma da 256 y la superred tiene un bloque de 256.

Direccionamiento IP Sin Clase (CIDR)

Se asignan bloques de direcciones sin pertenecer a ninguna clase. Uso de máscara en notación CIDR. Se determinan la primera dirección, la longitud y el broadcast del bloque. La dirección IP se escribe seguida de "/" junto con la longitud de prefijo.

Direccionamiento Privado

Se reserva un bloque clase a, clase b y c para uso privado y se pueden comunicar todos los dispositivos en la red LAN.

10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Variable Length Subnet Mask (VLSM)

FLSM usa la misma máscara de subred para todas las subredes. VLSM Permite un uso más eficiente asignando distintas máscaras a las interfaces de un router. Se extiende el uso de FLSM. Se subnetea la red usando FLSM. Después se usa FLSM otra vez para cada subred. Se repite el proceso hasta que cumplamos con el requerimiento.

Requerimiento = Hosts + 2 (red y broadcast)

Ejemplo:

Segmento	Requerimiento	Bloque	Hosts válidos	CIDR
LAN 1	29	32	30	/27
LAN 2	21	32	30	/27
LAN 3	12	16	14	/28
LAN 4	8	16	14	/28

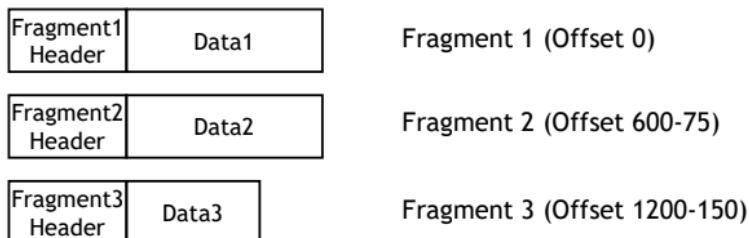
Segment	CIDR	Subnet Mask	Network Address	Broadcast Address	Valid host addresses
LAN Segment 1	/27	255.255.255.224	192.168.1.0	192.168.1.31	192.168.1.1 to 192.168.1.30
LAN Segment 2	/27	255.255.255.224	192.168.1.32	192.168.1.63	192.168.1.33 to 192.168.1.62
LAN Segment 3	/28	255.255.255.240	192.168.1.64	192.168.1.79	192.168.1.65 to 192.168.1.78
LAN Segment 4	/28	255.255.255.240	192.168.1.80	192.168.1.95	192.168.1.81 to 192.168.1.94

Fragmentación y Reensamblado

Si se tiene un mensaje mayor que el MTU, IP oculta los detalles de la tecnología subyacente. Divide los datagramas en fragmentos. Los fragmentos deben ser ensamblados en Destino.

El tamaño de fragmento se elige múltiplo de 8 bytes más próximo al MTU del trayecto. Cada fragmento se convierte en un datagrama independiente. Tiene el mismo identificador, Dirección Origen y Destino que el datagrama original.

Datagram Header	Data1 600 bytes	Data2 600 bytes	Data3 280 bytes
-----------------	--------------------	--------------------	--------------------



Desventajas

- Duplica la probabilidad de pérdida de un datagrama.
- Genera mayor carga de procesamiento en los routers.
- No compatible con el balanceo de carga (server farm).

IPv6

La necesidad de un incremento en la cantidad de direcciones llevó a la nueva versión de IP. La dirección es de 128 bits. No es compatible con IPv4, pero sí con otros

protocolos auxiliares (TCP, UDP, ICMP, IGMP, OSPF, BGP y DNS). La unidad de datos es "paquetes" en lugar de "datagrama".

Mejoras respecto a IPv4

- Espacio de direcciones ampliado.
 - 2^{128} direcciones posibles
- Mecanismo de opciones mejorado.
 - Las opciones de IPv6 se encuentran en cabeceras opcionales separadas situadas entre la cabecera IPv6 y la cabecera de la capa de transporte.
 - La mayoría de estas cabecerasopcionales no se examinan ni procesan por ningún dispositivo de encaminamiento en la trayectoria del paquete, simplificando y acelerando el procesamiento que realiza un router sobre los paquetes.
- Autoconfiguración de direcciones.
 - Asignación dinámica de direcciones.
- Aumento de la flexibilidad en el direccionamiento.
 - Incluye *anycast*: un paquete se entrega sólo a un nodo seleccionado de entre un conjunto de nodos.
 - Las direcciones más grandes permiten agrupar las direcciones por jerarquías de red, por proveedores de acceso, por proximidad geográfica, etc. Esas agrupaciones conducen a tablas de enrutamiento más chicas y a consultas más rápidas.
- Funcionalidad para la asignación de recursos.
 - Habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el que el emisor solicita un tratamiento especial. Facilita el tratamiento del tráfico especializado como el de vídeo en tiempo real.

Estructura de un paquete IPv6

40 B	Variable	Variable	8 B	Variable	Opcional, Variable 20 B	Variable
Header IPv6	Hop-by-hop Options	Routing	Fragment	Destination Options	Header TCP	Data
Header obligatorio	Headers opcionales				PAYLOAD	

Estructura Cabecera IPv6

Header obligatorio 40 B	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	
	Dir. IPv6 Origen 128 bits = 16 B				
	Dir IPv6 Destino 128 bits = 16 B				

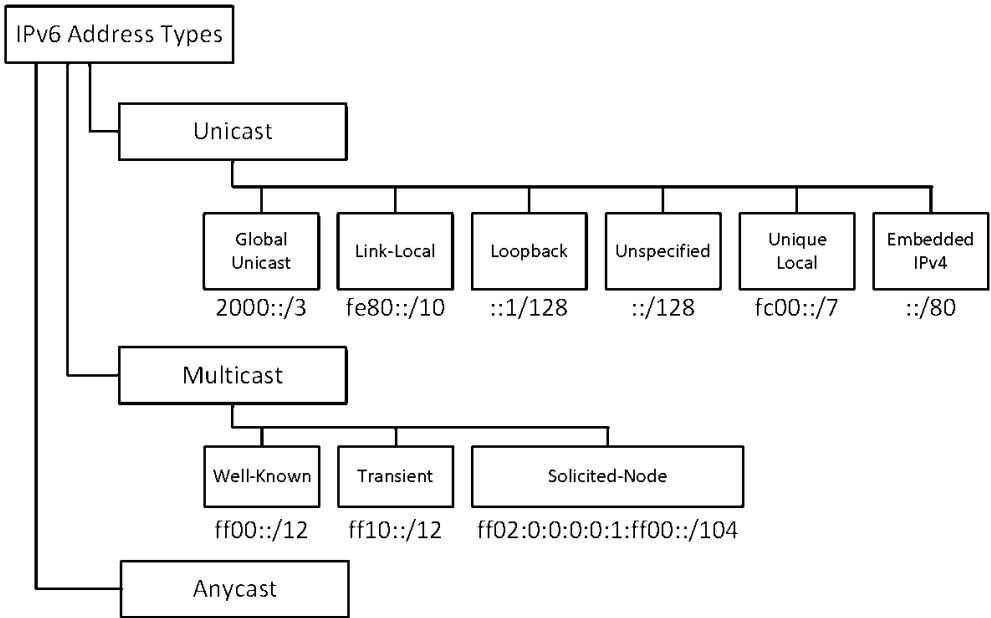
- **Versión (6)**
- **Clase de tráfico:** identifica y distingue entre clases o prioridades de paquete.
- **Etiqueta de flujo:** etiqueta paquetes con tratamiento especial de encaminamiento/ruteo.
- **Longitud del PAYLOAD:** medida en octetos de las cabeceras de extensión + PDU de transporte
- **Cabecera siguiente:** cada HEADER tiene un campo que apunta al siguiente HEADER. Puede ser de extensión o de TCP/UDP.
- **Límite de saltos:** similar a "tiempo de vida".
- **Dirección origen**
- **Dirección destino**

Direcciones

Las direcciones se asignan a interfaces individuales en los nodos, no a los nodos. Un nodo, en IPv6, es cualquier dispositivo que implemente IPv6 (conmutadores o routers). Una única interfaz puede tener múltiples direcciones únicas. Cualquiera de las direcciones asociadas a las interfaces de los nodos se puede utilizar para identificar de forma única al nodo.

Hay tres tipos de direcciones:

- **Unicast.** Un identificador para una interfaz individual. Un paquete enviado a una dirección de este tipo se entrega a la interfaz identificada por esa dirección.
- **Anycast.** Un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección anycast se entrega a una de las interfaces identificadas por esa dirección (la más cercana).
- **Multicast.** Un identificador para un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast se entrega a todas las interfaces identificadas por esa dirección.



Los 128 bits (16 B) se escriben como ocho grupos de cuatro dígitos hexadecimales, separando los grupos por dos puntos:

8000:0000:0000:0000:0123:4567:89AB:CDEF

Optimizaciones:

- Se pueden omitir los ceros a la izquierda de un grupo.
 - Ej: 0123 se escribe 123
- Se pueden reemplazar uno o más grupos de 16 ceros con dos puntos (:).
 - Ej: 8000::123:4567:89AB:CDEF
- Las direcciones IPv4 se pueden escribir como un par de signos de dos puntos y un número decimal anterior separado por puntos.
 - ::192.31.20.46

Direcciones Unicast

Loopback. Los hosts utilizan la dirección de loopback para enviarse paquetes a sí mismos, y esta dirección no se puede asignar a una interfaz física. Está formada por todos ceros, excepto el último bit, representado como **::1/128** o, simplemente, **::1** en el formato comprimido.

Default route. Compuesta solo por ceros representada como **::/128** o **:::**. Es el peor match en la tabla de ruteo, va al default gateway.

Prefijos

Se usa la representación CIDR: Dirección / longitud del prefijo.

2001:db8:2a0:2f3b::/64 es un prefijo de red.

2001:db8:3f::/48 es un prefijo de ruta sumarizada.

Si una dirección es /64, representa un red porque los otros 64 son el identificador de interfaz. No es necesario expresar el prefijo.

Si una dirección es /48, es una ruta sumarizada o un rango de direcciones que sumariza una porción del espacio de direcciones v6.

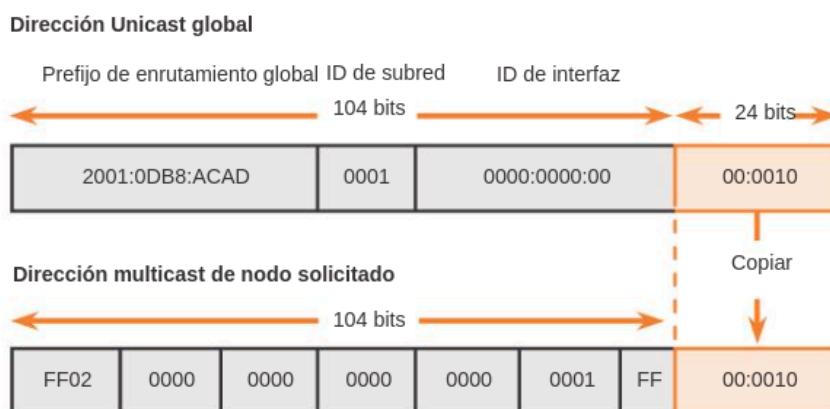
Unicast Address Format

En IPV6 la IP no identifica un host sino que identifica a una interfaz en un host.

48 bits	16 bits	64 bits
Global Routing Prefix	Subnet ID	Interface ID

Broadcast en IPv6

En IPv6 no hay dirección de broadcast. Esa funcionalidad se realiza con direcciones multicast especiales. Las direcciones que empiezan con ff00::/12 son direcciones bien conocidas. Por ejemplo: FF02::1 (todos los nodos IPv6) y FF02::2 (todos los routers).



Dirección IPv6 unicast global: 2001:0DB8:ACAD:0001:0000:0000:0000:0010

Dirección IPv6 multicast de nodo solicitado: FF02::0:FF00:0010

Se puede usar una dirección multicast de nodo solicitado para reducir el número de dispositivos que deben procesar tráfico. Una dirección multicast de nodo solicitado es

una dirección que coincide solo con los últimos 24 bits de la dirección IPv6 unicast global de un dispositivo. Los únicos dispositivos que deben procesar estos paquetes son aquellos que tienen estos mismos 24 bits en la porción menos significativa

Protocolos de control en Internet

ARP . Protocolo de Resolución de Dirección

Las NIC (Tarjetas de Interfaz de Red) de la capa de enlace de datos no entienden las direcciones de IP. ARP permite conocer la dirección MAC por medio de su dirección IP. Pertenece a una capa intermedia entre la 2 y 3: "interfaz de red". Todo dispositivo conectado a una red necesita una tabla ARP que relaciona la dirección IP con la dirección MAC. La tabla reside en memoria (la tabla se vacía cuando se apaga el dispositivo). Los pasos son:

1. El emisor revisa la tabla para ver si se encuentra la IP del destino. Si está, envía el mensaje; si no, paso 2.
2. El emisor envía un *broadcast* MAC con la dirección IP del destino.
3. El destino con esa IP responde con su dirección MAC.
4. El emisor recibe la respuesta y la registra en la tabla ARP.

RARP . Protocolo de Resolución de Dirección Inversa

Permite que una máquina conozca su dirección IP mediante su dirección MAC. Transmite un *broadcast* MAC de solicitud para que el servicer RARP responda la dirección IP correspondiente a la dirección MAC de la máquina solicitante.

DHCP . Protocolo de Configuración Dinámica de Host

Cada red debe tener un servidor DHCP responsable de la configuración. Al iniciar una computadora, esta no cuenta con una IP. La computadora difunde una solicitud de una dirección IP en su red. La computadora usa un paquete DHCP DISCOVER que debe llegar al servidor DHCP. Cuando el servidor recibe la solicitud, asigna una dirección IP libre y la envía al host en un paquete DHCP OFFER. El servidor identifica a un host mediante su rección Ethernet (se transporta en el paquete DHCP DISCOVER).

Problema: determinar cuánto tiempo se debe asignar una dirección IP

Solución: **arrendamiento**. La asignación de direcciones IP es por un período de tiempo fijo. Justo antes de que expire el arrendamiento, el host debe pedir una renovación al DHCP. Si no se hace la solicitud o si se rechaza, tal vez el host ya no pueda usar esa dirección.

Es usado ampliamente por los ISPs y reemplazó a los protocolos anteriores (BOOTP y RARP).

ICMP . Protocolo de Mensajes de Control en Internet

ICMP proporciona un medio para transferir mensajes desde los dispositivos de encaminamiento y otros computadores a un computador. Proporciona feedback sobre problemas del entorno de la comunicación:

El mensaje ICMP se envía en respuesta a un datagrama, bien por un router en el camino del datagrama o por el computador destino deseado.

ICMP es un usuario de IP. Cuando se construye un mensaje ICMP, se pasa a IP para que lo encapsule con una cabecera IP y transmita el datagrama resultante. Ya que IP no garantiza la entrega, no se puede considerar fiable.

Tipo de mensaje.	Descripción.
<i>Destination unreachable</i>	El router no puede localizar el destino. En algunas redes, el router puede detectar si un computador es inalcanzable. El mismo computador de destino puede devolver este mensaje si algún punto de acceso de un nivel superior no es alcanzable. Un paquete con el bit DF no puede entregarse porque hay una red de paquetes pequeños que se interpone.
<i>Time exceeded</i>	Se descartó un paquete porque su TTL ha llegado a cero.
<i>Parameter problem</i>	Valor inválido en el header.
<i>Source quench</i>	Se usaba para el control de flujo
<i>Redirect</i>	El router detecta que el paquete está mal enrutado. El router avisa al host emisor que se actualice con una mejor ruta.
<i>Echo and echo reply</i>	Se usan para ver si un destino es alcanzable y está vivo. El destino debería responder <i>ECHO REPLAY</i> luego de recibir un <i>ECHO</i> . Se usan en la herramienta ping .
<i>Timestamp request/replay</i>	Similares a <i>echo</i> . El tiempo de llegada y de salida de la respuesta se registran.
<i>Router advertisement/solicitation</i>	Permiten que los hosts encuentren routers cercanos.

IGMP . Protocolo de Administración de Grupo en Internet

Las estaciones y routers usan IGMP para intercambiar información sobre la pertenencia a los grupos de multidifusión de una LAN. Sus funciones principales:

- El envío de mensajes desde las estaciones a los encaminadores para suscribirse y para abandonar grupos de multidifusión definidos por una dirección de multidifusión dada.
- La comprobación periódica de los routers sobre qué grupos de multidifusión interesan a qué estaciones.

La versión actual es la IGMPv3. Las dos primeras versiones tenían el modelo de operación:

- Los receptores deben suscribirse a los grupos de multidifusión.
- Las fuentes no tienen que suscribirse a los grupos de multidifusión.
- Cualquier estación puede enviar tráfico a cualquier grupo de multidifusión.

La v3 agrega:

- Permite a las estaciones especificar la lista de equipos desde los que quieren recibir tráfico. El tráfico proveniente de otras estaciones es bloqueado en los encaminadores
- Permite a las estaciones bloquear los paquetes que provengan de fuentes que envíen tráfico no deseado.

Los mensajes de IGMP se transmiten en datagramas IP. Hay dos mensajes: "consulta de pertenencia a grupo" e "informe de pertenencia a grupo". Una computadora usa IGMP para darse a conocer como un miembro del grupo con una dirección de multidifusión concreta a todos los computadores de la LAN y a todos los dispositivos de encaminamiento de la LAN.

Para unirse a un grupo, una estación envía un mensaje IGMP de informe de pertenencia a grupo, en el que el campo de dirección de grupo sea la dirección de multidifusión del grupo. Este mensaje se envía en un datagrama IP con la misma dirección de multidifusión destino. Todas las estaciones que sean en ese momento miembros de este grupo de multidifusión reciben el mensaje y descubren así la existencia del nuevo miembro del grupo.

El router envía periódicamente mensajes de consulta general para mantener la lista de las direcciones de grupo activas actualizada, enviados en datagramas IP con la dirección de multidifusión (224.0.0.1). La estación que quiera permanecer en el grupo deberá responder el mensaje.

Cuando una estación deja un grupo, envía un mensaje de abandono de grupo a la dirección estática de multidifusión de todos los routers.

DNS . Sistema de Nombre de Dominio

Provee un esquema jerárquico de nombres basado en dominios y un sistema de base de datos distribuido para implementar este esquema de nombres. DNS se usa para asociar los nombres de host con las direcciones IP. El sistema es cliente-servidor:

- **DNS Resolver.** Envía el pedido de resolución entre la aplicación y el servidor de nombres.
- **Name Server.** Reciben el pedido y resuelven el nombre de Host a una dirección IP.

Espacio de Nombres

Diseño jerárquico en formato de árbol, que muestra cómo se construyen y delegan los dominios.

- **Root Level Domain.** Lo más alto de la jerarquía. No usa etiquetas, pero puede identificarse con el “.”.
- **Top-Level Domain.** .com; .edu; .mil, etc.
- **Second-Level Domains.** Pueden contener Hosts u otros dominios llamados sub-dominios. Por ejemplo: dev.microsoft.com
- **Host Names.** Se agregan al comienzo del nombre de dominio. Generalmente se los identifica con el “Fully Qualified Domain Name” (FQDN).

Roles de los servidores

- **Primary Name Server.** Los archivos de información de la zona se almacenan localmente
- **Secondary Name Server.** Obtiene la información de zona del Master Name Server
- **Master Name Server.** Fuente de información para un Secondary Server. Pueden ser Primary o Secondary Servers.
- **Caching Only.** No almacena información de zona.

Resolución de Nombres

- **Consulta Recursiva.** El servidor de nombres consultado está obligado a responder con los datos o con un error.
- **Consulta Iterativa.** El servidor consultado responde con su mejor respuesta. Puede ser el nombre resuelto o una referencia a otro servidor de nombres, que pueda ser capaz de responder la consulta.
- **Consulta Inversa.** El *resolver* solicita el nombre de Host asociado a una IP dada.

Caching & TTL

Los DNS Servers cachean las consultas iterativas. Cada entrada en caché tiene asociado un TTL. Cuando expira, la entrada se borra. El TTL remanente es enviado al *resolver* cuando se responde una consulta recursiva.

Procedimiento

1. El cliente hace una consulta recursiva al DNS Server
2. El servidor busca en caché una consulta similar y si no encuentra hace una búsqueda iterativa hasta encontrar al dueño.
3. El servidor dueño da la referencia a los DNS donde está el archivo.
4. Se cachea la respuesta en el servidor local y se devuelve al cliente.

Los mensajes de solicitud y respuesta se envían como paquetes UDP. Armado con la dirección IP, el programa puede entonces establecer una conexión TCP con el host o enviar paquetes UDP.

Resource Records

- **Host Record** : asocia estáticamente un nombre de Host con una dirección IP.
Comprende la mayor parte del archivo y lista todos los Hosts dentro de la zona
`www IN A 200.69.225.145`
- **MX Mail Exchange** : asocia un dominio de email con la dirección de los servidores de correo
`@ IN MX [10] mailhost`
`@ IN MX [20] mail1.infovia.com.ar`
- **CNAME Canonical Name** : permiten asociar más de un nombre de Host a una única dirección IP (alias)
`ftp CNAME Rhino`

VoIP y ToIP

- **Voz sobre IP (VoIP)**
 - La voz se digitaliza para que viaje en el datagrama IP.
 - La telefonía VoIP (digital; no es la voz natural) tiene menor calidad que la telefonía convencional (analógica; es la voz natural).
- **Telefonía IP (ToIP)**
 - 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).

U5B . Protocolos de Transporte (TCP/UDP)

UDP . Protocolo de Datagrama de Usuario

Es un protocolo de la capa de transporte. Proporciona un servicio no orientado a la conexión. Es un servicio no fiable, pero eso permite reducir la sobrecarga del protocolo. Se sitúa encima de IP y le incorpora la capacidad de un direccionamiento de puerto. Solamente envía paquetes entre aplicaciones, y deja que las aplicaciones construyan sus propios protocolos en la parte superior según sea necesario.

UDP transmite **segmentos** que consisten en un encabezado de 8 bytes seguidos de la carga útil. Los **puertos** identifican los puntos terminales dentro de las máquinas de origen y destino.

Datagrama

Puerto Origen 16 bits	Puerto Destino 16 bits
Longitud 16 bits	CheckSum 16 bits
Payload	

- **Puerto Origen:** se usa cuando hay que enviar una respuesta al origen.
- **Puerto Destino**
- **Longitud:** incluye el encabezado de 8 bytes y los datos. La longitud mínima es de 8 bytes, para cubrir el encabezado. La longitud máxima es de 65.515 bytes (menor al número que cabe en 16 bits debido al límite de tamaño en los paquetes IP).
- **CheckSum:** se realiza una suma de verificación para el encabezado, los datos y un pseudoencabezado IP. Si no se usa, se pone en 0.

PseudoHeader

Dirección Origen 32 bits		
Dirección Destino 32 bits		
0 0 0 0 0 0 0 8 bits	Protocolo = 17 8 bits	Longitud 16 bits

Es útil incluir el pseudoencabezado en el cálculo de la suma de verificación de UDP para detectar paquetes mal entregados, pero al incluirlo también se viola la jerarquía de

protocolos debido a que las direcciones IP en él pertenecen a la capa IP, no a la capa UDP.

Contiene las direcciones IPv4 de origen y destino, el número de protocolo y la cuenta de bytes para el segmento UDP (incluyendo el encabezado).

TPC . Protocolo de Control de Transmisión

TCP se diseñó para proporcionar una comunicación fiable entre pares de procesos (usuarios TCP) a través de redes e interconexiones fiables y no fiables. Proporciona dos servicios útiles para etiquetar los datos, forzado y urgente.

- **Flujo de datos forzado.** TCP decide cuándo se han acumulado suficiente datos para formar un segmento para su transmisión. El usuario puede requerir que TCP transmita todos los datos pendientes incluyendo una etiqueta con un indicador de forzado.
- **Señalización de datos urgentes.** Proporciona un medio para informar al usuario TCP destino que en el flujo de datos que recibe existen datos significativos o «urgentes».

Segmento TCP

Puerto Origen 16 bits		Puerto Destino 16 bits			
Número de Secuencia 32 bits					
Número de Confirmación de Recepción 32 bits					
Longitud de encabezado 4 bits	Reserva 4 bits	Banderas 8 bits	Tamaño de Ventana 16 bits		
CheckSum 16 bits		Puntero de Urgencia 16 bits			
Opciones + Relleno 0 a 320 bits, variables					
PAYLOAD N bits					

- **Puerto Origen**
- **Puerto Destino**
- **Número de secuencia (SN).** Número de secuencia del primer octeto de datos en este segmento. Si SYN está activado, se trata del número de secuencia inicial (ISN) y el primer octeto de datos es el ISN +1.

- **Número de confirmación (AN).** Número de secuencia del siguiente octeto que la entidad TCP espera recibir.
- **Longitud de la cabecera.**
- **Reservado**
- **Indicadores o banderas**
 - CWR y ECE: se usan para indicar congestión cuando se usa ECN.
 - URG: 1 si está en uso el *apuntador urgente*.
 - ACK: 1 si el *número de confirmación de recepción* es válido.
 - PSH: 1 si los datos se deben transmitir de inmediato.
 - RST: se usa para restablecer de manera repentina una conexión que se ha confundido debido a una falla de host o alguna otra razón; y para rechazar un segmento no válido o un intento de abrir una conexión.
 - SYN: se usa para establecer conexiones.
 - $SYN = 1 \text{ y } ACK = 0 \Rightarrow CONNECTION\ REQUEST$
 - $SYN = 1 \text{ y } ACK = 1 \Rightarrow CONNECTION\ ACCEPTED$
 - FIN: se usa para liberar una conexión y especifica que el emisor no tiene más datos que transmitir.
- **Tamaño de Ventana.** El control de flujo en TCP se maneja mediante una ventana deslizante de tamaño variable. Indica la cantidad de bytes que se pueden enviar, empezando por el byte cuya recepción se ha confirmado (Número de confirmación). Un 0 significa que se han recibido los bytes hasta $Número\ de\ confirmación - 1$, inclusive, pero que el receptor no ha tenido la oportunidad de consumir los datos y ya no desea más datos por el momento.
- **CheckSum.** Se realiza sobre el encabezado, los datos y un pseudoencabezado (igual a UDP, pero con protocolo = 6).
- **Puntero de urgencia.** Cuando se suma al número de secuencia del segmento, contiene el número de secuencia del último octeto de la secuencia de datos urgentes. Esto permite al receptor conocer la cantidad de datos urgentes que llegan.
- **Opciones.** Características adicionales. Las opciones son de longitud variable, llenan un múltiplo de 32 bits mediante la técnica de relleno con ceros y se pueden extender hasta 40 bytes para dar cabida al encabezado TCP más largo que se pueda especificar. Algunas opciones se transmiten cuando se establece una conexión para negociar o informar al otro extremo sobre las capacidades disponibles. Las más usadas son:
 - **Maximum Segment Size (MSS)**
 - **Timestamp**
 - **Escala de ventana**
 - **Confirmación de Recepción Selectiva (SACK)**

Options

MSS. Es declarada al establecimiento de la conexión, (segmentos SYN) No puede modificarse durante el intercambio de segmentos. Determina el tamaño máximo del segmento de datos que es capaz de aceptar. Deber ser: MTU de la interfaz - 40 B.

Timestamp. El origen pone el stamp y el destino responde con un stamp al confirmar (ACK). Permite calcular de manera más precisa el RTT por cada segmento. Sin esta opción, el RTT se calcula por cada venta (ineficiente para ventanas grandes).

Escala de ventana. Permite al emisor y al receptor negociar un factor de escala de ventana al inicio de una conexión.

SACK. Permite a un receptor indicar al emisor los rangos de números de secuencia que ha recibido. Complementa el Número de confirmación de recepción y se utiliza después de haber perdido un paquete y de la llegada de los datos subsiguientes (o duplicados).

Mecanismos TCP

Establecimiento de la conexión

Usa un diálogo en tres pasos (Three-way Handshake). Cuando el indicador SYN está activado, el segmento es esencialmente una solicitud de conexión. Para iniciar una conexión:

1. Una entidad envía un SYN, SN=X, donde X es el número de secuencia inicial.
2. El receptor responde con SYN, SN=Y, AN=X+1 mediante la activación de los indicadores SYN y ACK. Esto indica que el receptor está esperando recibir un segmento que comience con el octeto de datos X+1, confirmando el SYN que ocupaba SN=X.
3. El que inicia la conexión responde con AN=Y+1.

Una conexión está únicamente determinada por los sockets (estación, puerto) origen y destino. Así, en cualquier instante de tiempo, sólo puede haber una única conexión TCP entre un único par de puertos. Sin embargo, un puerto dado puede admitir múltiples conexiones, cada una con un puerto diferente.

Transferencia de datos

Los datos se transmiten en segmentos sobre una conexión de transporte, pero la transferencia de datos se ve desde un punto de vista lógico como un flujo de octetos. Cada segmento contiene el número de secuencia del primer octeto del campo de datos. El control de flujo se hace usando **asignación de créditos**, donde un crédito es un número de octetos en lugar de segmentos.

Los datos se almacenan temporalmente en la transmisión y en la recepción. TCP aplica su propio criterio para decidir cuándo armar y enviar el segmento. El indicador PUSH se usa para obligar a que los datos acumulados sean enviados.

El usuario puede indicar que un bloque es urgente mediante el puntero de urgente. El receptor es alertado de que está recibiendo datos urgentes.

Si durante el intercambio de datos llega un segmento que aparentemente no va dirigido a la conexión actual, se envía un segmento con el valor del indicador RST activado.

Cierre de la conexión

Cada usuario TCP debe emitir una primitiva *Close*. Se setea el bit FIN en el último segmento que envía. Si un usuario emite un *Abort*, se produce un cierre abrupto. Se descartan todos los datos del buffer y se envía un RST al otro extremo.

Control de errores

En TCP no existe una confirmación de rechazo (REJ o SREJ). TCP se basa en la confirmación positiva de la recepción y retransmite cuando la confirmación no llega dentro del RTO.

RTO (Temporizador de retransmisión). Cuando se envía un segmento, se inicia un temporizador de retransmisiones. Si la confirmación de recepción del segmento llega antes de que expire el temporizador, éste se detiene. Por otro lado, si el temporizador termina antes de que llegue la confirmación de recepción, se retransmite el segmento

Control de flujo

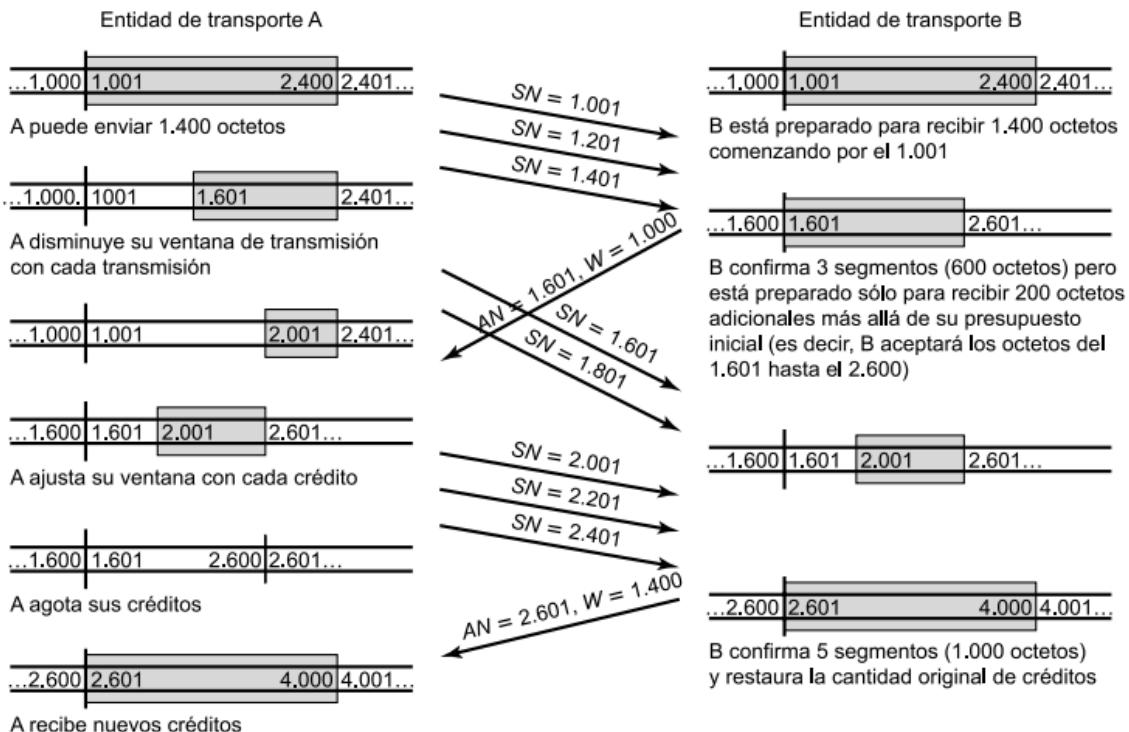
Usa un **esquema de otorgamiento de créditos**. Es similar a ventana deslizante, pero separa la confirmación de datos recibidos del permiso para enviar más . Cada octeto de datos se considera que tiene un número de secuencia único.

Además de los datos, cada segmento incluye tres campos relacionados al control de flujo:

1. Número de secuencia (SN)
2. Número de confirmación (AN)
3. Ventana (W)

Al enviarse un segmento, se incluye el número de secuencia del primer octeto del campo de datos del segmento. El segmento recibido se confirma con un segmento de retorno que incluye ($AN = i$, $W = j$):

- Todos los octetos con números de secuencia lleguen hasta $SN = i$ se confirman. El siguiente octeto esperado tiene número de secuencia i .
- Se da permiso para enviar una ventana adicional de $W = j$ octetos de datos. Es decir, los j octetos correspondientes a los números de secuencia desde i hasta $i + j - 1$.



Control de Congestión

Congestión es la condición de retraso severo causada por una sobrecarga de segmentos en uno o más puntos de conmutación. Se produce un colapso de la red.

Consecuencias:

- Aumento de retrasos.
- Descarte de segmentos por superar la capacidad de almacenamiento del router.
- Retransmisión de datagramas por exceso de time-out.

Las técnicas para evitar la congestión pueden agruparse en:

- **Gestión de temporizadores de retransmisión.** Al cambiar las condiciones de red, un temporizador de retransmisión estático puede expirar demasiado rápido o demasiado tarde. Las implementaciones TCP intentan estimar el retardo de ida y vuelta actual mediante la observación del patrón del retardo de segmentos más recientes, para establecer el temporizador a un valor un poco mayor que el

retardo de ida y vuelta estimado. Técnica estándar de TCP: algoritmo de Jacobson

- **Gestión de la venta.** El tamaño de ventana puede influir en que TCP pueda ser utilizado eficientemente sin causar congestión. Dos técnicas: el arranque lento y el ajuste dinámico.

Arranque lento

Cuanto mayor es la ventana de emisión de TCP, más segmentos puede enviar la fuente TCP antes de que deba esperar una confirmación. Esto crea un problema cuando se establece por primera vez una conexión, ya que la entidad es libre de vaciar la ventana de datos completa en la red.

Estrategia: el emisor envía con una ventana relativamente grande, pero no con su máximo tamaño, esperando aproximarse al tamaño máximo que sería proporcionado por la conexión finalmente. Para evitar que el emisor inunde la interconexión con muchos segmentos, la ventana se expande de manera gradual hasta que se reciban las confirmaciones.

$$awnd = \text{MIN}(\text{crédito}, cwnd)$$

awnd = **ventana permitida** [segmentos]. Cantidad de segmentos que se pueden enviar sin recibir confirmaciones adicionales

cwnd = **ventana de congestión** [segmentos]. Se usa durante el inicio para reducir el flujo durante los períodos de congestión. Empieza en 1 cuando se abre una conexión. Al recibirse una confirmación, $\text{cwnd}++$, hasta algún valor máximo.

crédito = cantidad de créditos concedidos y no utilizados en la confirmación más reciente [segmentos]. Cuando se recibe una confirmación,
crédito = *ventana/tamaño de segmento*.

cwnd crece de manera exponencial. Después del primer ACK, *cwnd* = 2 (se envían dos segmentos). Con la confirmación de esos dos, TCP desplaza la ventana 1 segmento e incrementa *cwnd* en una por cada ACK que llega. TCP puede enviar cuatro segmentos. Cuando se confirmen esos cuatro segmentos, se puede enviar ocho ...

Retransmisión rápida

Cuando la fuente recibe un ACK duplicado, significa:

- El segmento fue demorado, pero finalmente llegará.
- El segmento se perdió (tiene que retransmitirse).

En lugar de esperar a que caduque el RTO, si se reciben 3 ACK duplicados, se retransmite el segmento perdido.

Recuperación rápida

Esta variante permite al transmisor evitar volver al Slow-Start en caso de perderse un segmento. Cuando se recibe el 3º ACK duplicado, se setea $cwnd = cwnd/2$

Ajuste dinámico

Cuando se pierde un segmento (expira un temporizador), es señal de que se está produciendo una congestión. Lo prudente sería inicializar $cwnd$ en 1 y comenzar el procedimiento de arranque lento de nuevo. El arranque lento puede ser demasiado agresivo y empeorar la congestión. Alternativa: usar arranque lento para comenzar, seguido de un crecimiento lineal de $cwnd$.

Comparativa de Control de Errores (IP-UDP-TCP)

Protocolo	IP	UDP	TCP
Detección de Errores	Checksum en el header	Checksum en el datagrama UDP y en el pseudoheader del datagrama IP	Checksum en el segmento TCP y en el pseudoheader del datagrama IP
Corrección de Errores	No.	No. No corrige ni recupera	Sí (ARQ). En el segmento TCP y en el pseudoheader del datagrama IP

UDP vs TCP

	UDP	TCP
Nombre PDU	Datagrama UDP	Segmento TCP
Tipo de Servicios	Sin conexión Los datagramas UDP viajan por caminos distintos	Con 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	No se establece.	Sí se establece.

Sesión entre Hosts		
Comunicaciones admitidas	Punto-a-punto. Punto-a-multipunto	Solamente punto-a-punto (usa ARQ)
Controles de flujo y congestión	No hace control de flujo	Control de flujo → extremo a extremo, (mediante sliding windows). El problema puede aparecer en los extremos. Control de congestión → en sistemas intermedios. El problema puede aparecer en la nube.
Corrección y detección de errores	Las aplicaciones que corren sobre UDP requieren corrección/detección de errores.	Las aplicaciones que corren sobre TCP no requieren corrección/detección de errores.
Uso de Ip	Usan IP como Capa 3	
Capa de residencia	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
Casos de uso	Procesos simples de petición/respuesta (aplicaciones no críticas, sin necesidad de control de flujo/errores) Multicast y Broadcast Streaming de audio y video.	Se usa en la comunicación cotidiana (HTTP, SMTP, SSH, FTP, etc.).

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 dirige las conexiones.

Protocolo de aplicación	FTP	TELNET	SMTP	DNS	TFTP	SMNP	
Número de Puertos	21	23	25	53	69	161	
Protocolos de Transporte	TCP			UDP			

U5.C - Routing/Routing Protocols

El proceso de ruteo ocurre en la capa 3 (Capa de Red) del modelo OSI. Un router, para enviar los datagramas al siguiente "Hop", realiza dos funciones básicas:

- **Determinar el mejor camino a destino.** Consiste en revisar todos los caminos disponibles a la red destino y elegir el camino óptimo. La información de topología de red utilizada para determinar la ruta óptima es almacenada en **tablas de ruteo**.
- **Comutar el datagrama.** Consiste en cambiar la dirección destino física de la trama, por la del próximo salto.

Objetivos

- **Flexible.** Rápida adaptación a los cambios en la topología de la red. Cuando una red deja de estar disponible, el protocolo debe detectarlo y determinar el próximo camino hacia esa red. Cuando la red vuelve a estar disponible, debe actualizar su tabla para reflejar el cambio.
- **Óptimo.** Habilidad para elegir la mejor ruta. Depende de la *métrica* que usa para calificar sus rutas (número de saltos, combinación de saltos, retardo de la red, etc).
- **Rápida Convergencia.** La Convergencia ocurre cuando todos los routers dentro de una red poseen tablas de ruteo consistentes. Cuando ocurre un evento, todos los routers deben recalcular las rutas óptimas. En ese momento existen inconsistencias en las tablas de ruteo y pueden producirse "routing loops".
- **Robusto.** Poder mantener el correcto funcionamiento en condiciones inusuales o impredecibles.
- **Simple.** Habilidad de operar eficientemente. Un protocolo debe operar con el mínimo overhead.

Sistemas Autónomos

- Se compone de un conjunto de routers y redes gestionadas por una única organización.
- Consiste en un grupo de dispositivos de encaminamiento que intercambian información a través de un protocolo de encaminamiento común.
- Está conectado (grafo). Existe un camino entre cualquier par de nodos.

Tabla de ruteo

Se almacena la información de topología, la información que tiene el host acerca de la red. Las columnas son:

- **Destination network.** Red destino o prefijo.
- **Netmask.** Máscara o longitud de prefijo.
- **Gateway.** Próximo salto. Para llegar al destino debo enviar el datagrama al vecino gateway. Si el gateway es "On-link", ejecuto ARP porque cualquier destino que está en ese network
- **Interface.** El host debe saber por cuál interfaz debe conectarse/alcanzar un determinado destino.
- **Metric.** Si tengo dos entradas idénticas, gana la que tiene menos metric.

Clasificación

- **Estáticos/Dinámicos.**
- **Single-Path/Multipath.**
- **Flat/Hierarchical**
- **Interior/Exterior.**
- **Según Estrategia**
 - Distance Vector.
 - Link State
 - Path Vector

Estáticos/Dinámicos

Ruteo estático. Las decisiones no se basan en mediciones o estimaciones del tráfico y la topología actual. La decisión se calcula por adelantado. Es útil cuando la elección es clara. No responde a las fallas.

Ruteo dinámico. Las decisiones cambian para reflejar los cambios de topología y los cambios en el tráfico.

Interior/Exterior

Interior Router Protocol. Distribuye la información entre los dispositivos dentro de un AS. El protocolo que se emplea dentro de un SA no necesita ser implementado fuera del sistema.

Exterior Router Protocol. Se utiliza para pasar información entre diferentes AS. Necesita pasar menos información que un IRP: solo se necesita información para

determinar el AS objetivo y calcular la ruta para entrar en ese sistema. El ERP no necesita conocer los detalles de la ruta seguida en el AS destino.

Plano/Jerárquico

Plano. El mismo proceso va a correr en todos los routers, y todos intercambian información entre sí. Es una dificultad a la escalabilidad.

Jerárquico. Permite hacer áreas entre una cantidad de routers, estas áreas se conectan, hay procesos de ruteo reducidos, y entre áreas se pasan información consolidada. No todos hablan con todos, se puede escalar.

Estrategias de ruteo

Distance Vector.

Cada router tiene una tabla que proporciona la mejor distancia conocida a cada destino y el enlace que se puede usar para llegar ahí. Las tablas se actualizan intercambiando información con los vecinos. Eventualmente, todos los routers conocen el mejor enlace para alcanzar cada destino. La tabla de ruteo está indexada por cada router de la red. La entrada tiene dos partes:

1. Línea preferida de salida a usar para ese destino.
2. Estimación del tiempo o distancia a ese destino.

Link State.

Cada router debe:

1. Descubrir a sus vecinos y conocer sus direcciones de red.
2. Establecer la métrica de distancia o de costo para cada uno de sus vecinos.
3. Construir un paquete que indique todo lo que acaba de aprender.
4. Enviar este paquete a todos los demás enrutadores y recibir paquetes de ellos.
5. Calcular la ruta más corta a todos los demás enrutadores.

Con esto se distribuye la topología completa a todos los routers. Luego se puede ejecutar el algoritmo en cada router para encontrar el camino más corto.

Path Vector

No hay métricas. Solo se proporciona información acerca de qué redes pueden ser alcanzadas por un router determinado y los AS que se deben atravesar para llegar. Las diferencias con el vector de distancia:

- No incluye una estimación de distancia o costo.

- Cada bloque de información de ruteo enumera todos los AS visitados para alcanzar mediante esta ruta la red destino.

Enumerar todas las AS que debe atravesar un datagrama si sigue una ruta, permite al router llevar a cabo políticas de ruteo, es decir, puede decidir evitar un camino determinado para evitar transitar por un AS concreto.

Protocolos

RIP

Tiene tres timers:

- Cada 30 segundos envía la tabla de ruteo completa a sus vecinos.
- Si una ruta no es actualizada en 3 minutos, su métrica se setea a infinito y se informa a los vecinos.
- El borrado de una ruta de la tabla de ruteo demora 2 minutos

Una entrada en la tabla de un router es válida siempre y cuando el router envíe updates periódicamente.

Inicialización. Envía un request a todos los vecinos (broadcast) solicitando sus tablas de ruteo completas. No realiza Neighbor Discovery. Envía broadcasts y no recibe confirmación.

Confiabilidad. Se basa en la retransmisión periódica de toda la información.

Subnets. Solo en la versión 2. Incluye información de subred en la tabla de ruteo y la informa en las actualizaciones a sus vecinos.

Seguridad. Password opcional de 16 bytes (cleartext). Evita la existencia de black-holes (routers que informan todas las redes con métrica 0).

OSPF

Cada router que corre OSPF arma un grafo completo de toda la red, establece relaciones entre los vecinos. Converge más rápido que RIP porque no tiene timers. Intercambia menos información que RIP porque no envía cada 30 segundos nada.

Balanceo de carga. Cuando existen dos rutas con la misma métrica, puede enviar tráfico por ambas rutas.

Confiabilidad. Realiza flooding, con confirmación de los vecinos. Checksum de los mensajes.

Flooding. Se notifica a todos a la vez cuando hay cambio de topología. Eso es posible porque se tiene el grafo completo.

Subnets. Diseñado para trabajar con VLSM y CIDR

Seguridad. Contraseña simple cleartext. MD5 - preshared key.

Todos son dinámicos y de interior.

	RIP	OSPF	IGRP	EIGRP
Estrategia	Distance Vector	Link State	Distance Vector	Distance Vector
Métrica	Saltos (15 como máximo)	Ancho de banda y delay	Ancho de banda, carga, delay, MTU y fiabilidad	Ancho de banda, carga, delay, fiabilidad
Algoritmo de mejor camino	Distance Vector	SPF	Distance Vector	Diffusing update
Flat/Hierarchical	Flat	Hierarchical	Flat	Flat

U6 - Redes WAN

Una **red de área amplia** cubre una extensa área geográfica, requieren atravesar rutas de acceso público y utilizan circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Una WAN consiste en una serie de dispositivos de conmutación interconectados. Una transmisión se encaminará a través de estos nodos internos hasta alcanzar el destino. A los nodos no les interesa el contenido de los datos, su función es proporcionar el servicio de conmutación.

Redes conmutadas

Los tipos de conmutación se clasifican según la forma en que se conmutan los nodos:

- **Conmutación de circuitos.**
- **Conmutación de paquetes.**
 - Datagramas
 - Circuitos virtuales

Red de conmutación de circuitos

Implican la existencia de un canal de comunicaciones dedicado entre dos estaciones (secuencia de enlaces conectados entre nodos). En cada enlace físico se dedica un canal lógico para cada conexión establecida.

Puede ser ineficiente porque la capacidad del canal se dedica permanentemente a la conexión mientras dure aunque no se transfieran datos.

Su ventaja es la transparencia: una vez establecido el circuito, este parece una conexión directa entre las dos estaciones, sin necesitar la inclusión de lógica de red especial en las estaciones.

Fases

1. **Establecimiento del circuito.** Se necesita establecer un circuito extremo a extremo antes de transmitir.
2. **Transferencia de datos.**
3. **Desconexión del circuito.**

Componentes

- **Abonados.** Dispositivos que se conectan a la red.

- **Línea de abonado/bucle de abonado/bucle local.** Enlace entre el abonado y la red
- **Centrales.** Centros de conmutación de la red.
 - **Centrales finales.** Centros de conmutación a los que se conectan directamente los abonados.
- **Líneas troncales.** Enlaces entre centrales.

Conmutación de circuitos

Se establece un camino dedicado (secuencia conectada de enlaces físicos) a través de los nodos de la red. En cada enlace, se dedica un canal lógico a cada conexión. Los datos generados por la estación fuente se transmiten por el camino dedicado tan rápido como se pueda. En cada nodo, los datos de entrada se encaminan o conmutan por el canal apropiado de salida sin retardos. Ejemplo: red de telefonía.

Por división en el espacio

Las rutas de señal que se establecen son físicamente independientes entre sí. Cada conexión necesita del establecimiento de un camino físico a través del conmutador que se dedique únicamente a la transferencia de señales entre los dos extremos. Se desarrolló para entornos analógicos y se desplazó al contexto digital.

El bloque básico es una matriz de conexiones metálicas (o puntos de cruce) o puertas semiconductoras que una unidad de control puede habilitar o deshabilitar. Cada estación se conecta a la matriz a través de una línea de entrada y otra de salida. La conexión entre dos líneas cualquiera es posible habilitando el punto de cruce correspondiente.

Por división en el tiempo

Se basa en sistemas digitales y multiplexación por división de tiempo (TDM). Involucra a la fragmentación de una cadena de bits de menor velocidad en segmentos que compartirán una secuencia de velocidad superior con otras cadenas de bits. Los fragmentos individuales, o ranuras, se gestionan por parte de la lógica de control con el fin de encaminar los datos desde la entrada hacia la salida.

Conmutación de paquetes

No es necesario hacer una asignación a priori de recursos en el camino. Los datos se envían en pequeñas unidades (**paquetes**). Cada paquete se pasa de nodo en nodo siguiendo algún camino. En cada nodo, el paquete se almacena durante un breve

intervalo y después se transmite al siguiente nodo. Los paquetes contienen una parte de los datos de usuario + información de control.

Ventajas

- Más eficiente. Un único enlace entre dos nodos se puede compartir dinámicamente en el tiempo entre varios paquetes. Los paquetes forman una cola y se transmiten sobre el enlace tan rápidamente como es posible.
- Realiza una conversión en la velocidad de los datos. Dos estaciones de diferente velocidad pueden intercambiar paquetes, ya que cada una se conecta a su nodo con una velocidad particular.
- Cuando aumenta el tráfico, la red rechaza la aceptación de solicitudes de conexión adicionales mientras no disminuya la carga de la red.
- Se puede hacer uso de prioridades; de la cola transmite los más prioritarios primero.

Datagramas

Cada paquete (**datagrama**) se trata de forma independiente. Cada nodo elige el siguiente nodo en la ruta del paquete de acuerdo con información recibida de los nodos vecinos acerca del tráfico, fallo en las líneas, etc. No todos los paquetes seguirán la misma ruta. Los paquetes pueden perderse en el camino, pero es responsabilidad del destino detectar la pérdida y actuar.

Circuitos virtuales

Se establece una ruta previa al envío de los paquetes. Todos los paquetes intercambiados entre dos partes siguen ese camino a través de la red. Se llama **circuito virtual** porque el camino es fijo mientras dura la conexión lógica (similar a conmutación de circuitos). Además de los datos, cada paquete contiene un identificador de circuito virtual. Cada nodo de la ruta sabe hacia dónde dirigir los paquetes, sin necesitar decidir el encaminamiento.. Cada estación puede tener más de un circuito virtual hacia otras estaciones.

Característica principal. La ruta entre las estaciones se establece antes de la transferencia de los datos. El nodo no necesita tomar decisiones de encaminamiento para cada paquete, sino que ésta se toma una sola vez para todos los paquetes que usan dicho circuito virtual.

Desventajas frente a Datagramas

- En Datagramas no existe la fase de establecimiento de llamada. Si una estación desea enviar sólo uno o pocos paquetes, el envío resultará más rápido.

- Es menos flexible. Si hay congestión, es más difícil solucionarla porque las rutas ya están definidas.
- Es menos seguro. Si un nodo falla, se pierden todos los circuitos virtuales que pasan por ese nodo.

Tipos de conmutación . Cuadro comparativo

Conmutación de circuitos	Conmutación de Paquetes (Circuitos Virtuales)	Conmutación de Paquetes (Datagrama)
Con conexión física.	Con conexión virtual.	Sin conexión virtual.
Ruta dedicada	Ruta no dedicada	No hay ruta
La ruta se establece para toda la transición		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.	

PPP . Point to Point Protocol

Protocolo para enmarcar el protocolo IP cuando se envía mediante una línea serial.

Internet necesita enlaces de punto a punto. PPP (Capa de enlace de datos) se utiliza para enviar paquetes a través de esos enlaces. Para transportar los paquetes se necesita cierto mecanismo de entramado para diferenciar los paquetes ocasionales del flujo de bits continuo en el que se transportan. PPP se ejecuta en enrutadores IP para proveer ese mecanismo.

Funciones

- **Transporte de datos.** Asegura el enlace y recepción ordenada. Emplea ARQ Ventana Deslizante.
- **Autenticación**
- **Asignación dinámica de IP.**

Características

PPP provee tres características principales:

- Un método de entramado que define sin ambigüedades el final de una trama y el inicio de la siguiente. El formato de trama también maneja la detección de errores.
- Un protocolo de control de enlace para activar líneas, probarlas, negociar opciones y desactivarlas en forma ordenada cuando ya no son necesarias. Este protocolo se llama **LCP** (Protocolo de Control de Enlace).
- Un mecanismo para negociar opciones de capa de red con independencia del protocolo de red que se vaya a utilizar. El método elegido debe tener un **NCP** (Protocolo de Control de Red) distinto para cada capa de red soportada.

PDU

1 B	1 B	1 B	1 a 2 B	Variable B	2 a 4 B	1 B
Bandera 01111110	Dirección 11111111	Control 00000011	Protocolo	Payload	CRC	Bandera 01111110

El formato es parecido al de **HDLC**. Las diferencias son:

- PPP está orientado a bytes, no a bits. PPP usa el relleno de bytes en las líneas y todas las tramas tienen un número entero de bytes.
- HDLC provee una transmisión confiable con una ventana deslizante, confirmaciones de recepción y expiración de temporizadores. PPP usa un "modo

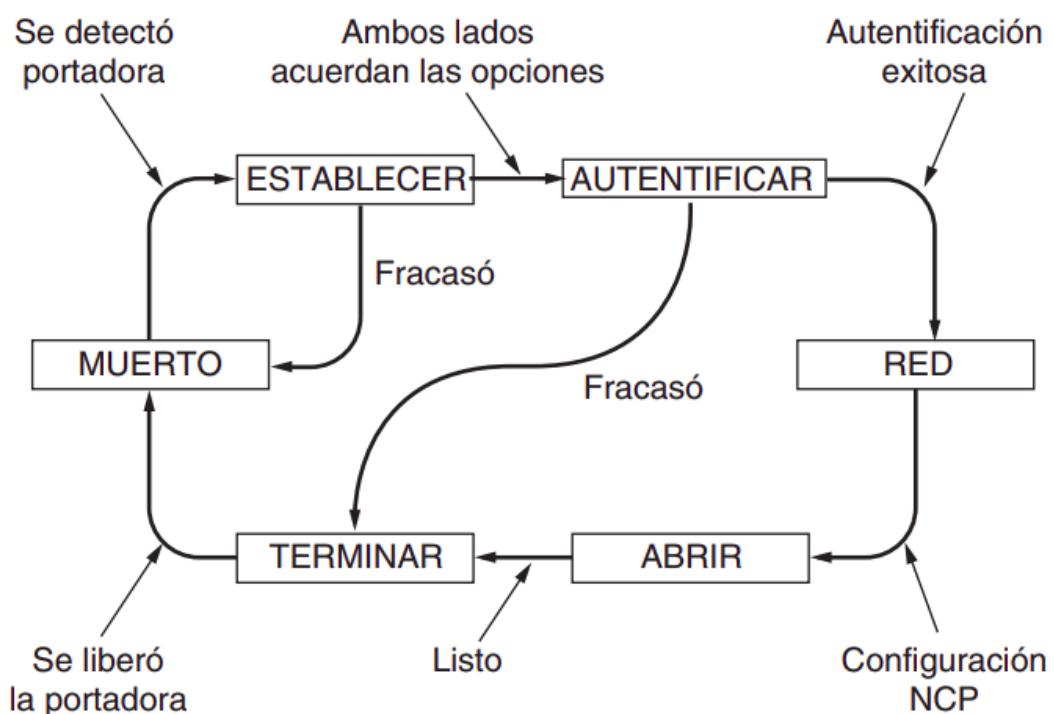
no numerado" para proveer un servicio sin conexión ni confirmación de recepción.

Campos

- **Bandera.** Byte bandera de HDLC 0x7E
- **Dirección.** El valor 1111111 indica que todas las estaciones deben aceptar la trama.
- **Control.** El valor 00000011 indica una trama no numerada
- **Protocolo.** Identificador de protocolo. Puede asociarse a varios.
- **CRC** de 16 o 32 bits.

Funcionamiento

El enlace inicia en estado MUERTO.



Fases

1. **Establecimiento de conexión.** Una computadora contacta con la otra y negocian los parámetros relativos al enlace usando el protocolo LCP. Este protocolo es una parte fundamental de PPP y por ello están definidos en el mismo RFC. Usando LCP se negocia el método de autenticación a utilizar, el tamaño de los datagramas, números claves para usar durante la autenticación,...

2. **Autenticación.** No es obligatorio. Existen dos protocolos de autenticación. El más básico e inseguro es PAP, aunque no se recomienda dado que manda el nombre de usuario y la contraseña en claro. Un método más avanzado y preferido por muchos ISPs es CHAP, en el cual la contraseña se manda cifrada.
3. **Configuración de red.** Se negocian parámetros dependientes del protocolo de red que se esté usando. PPP puede llevar muchos protocolos de red al mismo tiempo y es necesario configurar individualmente cada uno de estos protocolos. Para configurar un protocolo de red se usa el protocolo NCP correspondiente. Por ejemplo, si la red es IP, se usa el protocolo IPCP para asignar la dirección IP del cliente y sus servidores DNS.
4. **Transmisión.** Se manda y recibe la información de red. LCP se encarga de comprobar que la línea está activa durante periodos de inactividad. Obsérvese que PPP no proporciona cifrado de datos.
5. **Terminación.** La conexión puede ser finalizada en cualquier momento y por cualquier motivo.

Comparación con SLIP

SLIP: protocolo de proceso de tramas usado antaño para envíos IP a través de una línea serial.

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.

U7.A - Protocolo X.25

X.25 es un estándar de ITU-T que especifica una interfaz entre una estación y una red de conmutación de paquetes. X.25 es un protocolo (de WAN) de conmutación de paquete. Se especifica en 3 niveles:

- Capa física (N1).
- Capa de enlace (N2).
- Capa o nivel de paquete (N3).

Características

- 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 comutadores 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.

Empaqueamiento

Niveles

Paquete	Cabeza	Datos	
Trama	Bandera	Dirección	
Físico	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.
Conecotor utilizado	DB-15 (15 pines).	DB-25 (25 pines)

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 (Paquete)

- Gestiona circuitos virtuales y maneja la commutación 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].
 - **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.

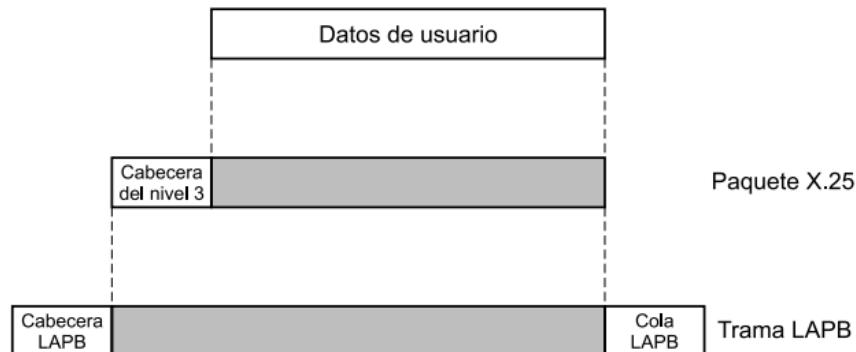


Figura 10.17. Datos de usuario e información de control del protocolo X.25.

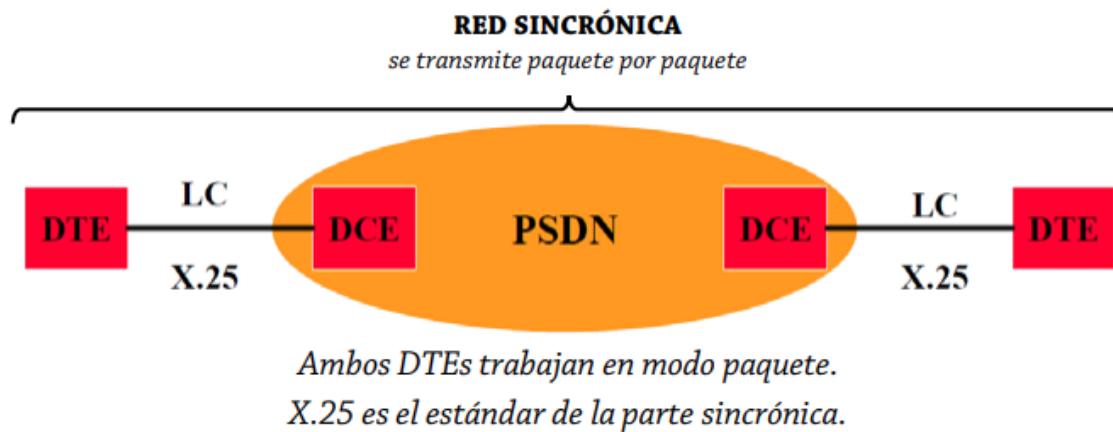
Parámetros de red a considerar – Facilidades

- 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).

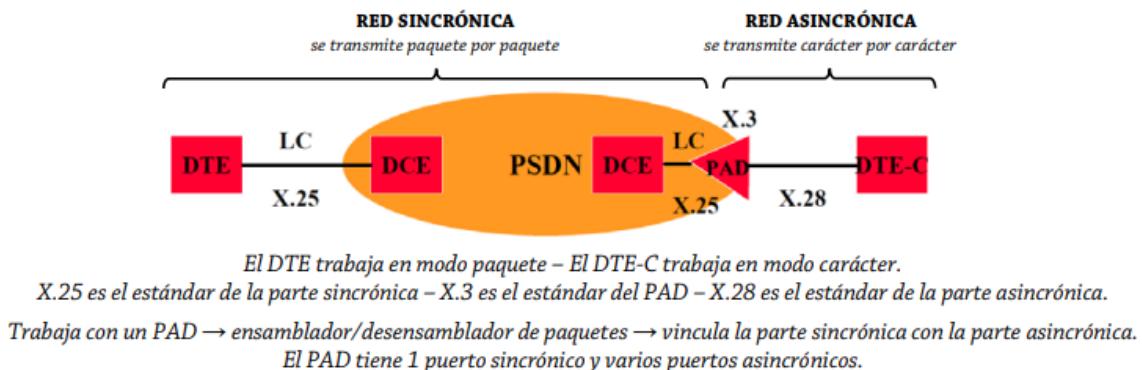
- $V_{TX} > V_{realTX}$
- Cantidad de LCs y tipo de LCs (entrante, saliente o bidireccional).
- Grupo cerrado de usuarios.
- Si se va a trabajar con PVC o SCV.
- Si se va a trabajar con selección rápida → “marcación rápida” en el teléfono.
- Cobro revertido → no se le cobra al transmisor sino al receptor.

Modos de Operación

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



- Carácter → modo sincrónico/asincrónico.



U7.B - Protocolo HDLC

Características

- Protocolo orientado al bit.
- Permite una transmisión “Transparente” (Independiente del código).
- Tramas delimitadas por “flags”.
- Formato único de trama.
- Confirmación por ventana deslizante.

Estaciones

- **Estación primaria (EP).** Responsable de controlar el funcionamiento del enlace.
Trama Generada = Órden.
- **Estación secundaria (ES).** Funciona bajo el control de la estación primaria.
Trama Generada = Respuesta. La primaria establece un enlace lógico independiente con cada una de las secundarias presentes en la línea.
- **Estación combinada (EC).** Puede generar órdenes y respuestas.

Configuraciones

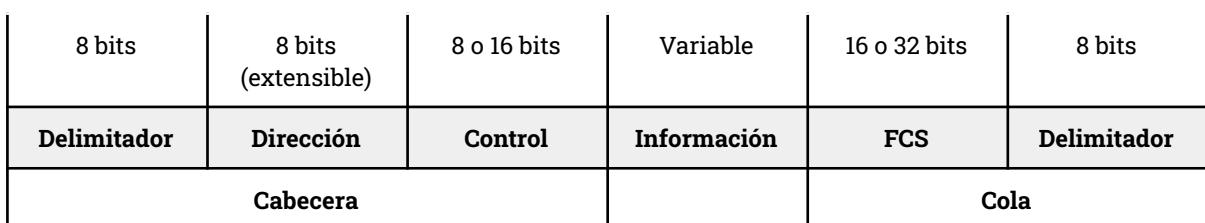
- **Configuración no balanceada.** Una estación primaria y una o más secundarias.
Permite *full-duplex* y *half-duplex*.
- **Configuración balanceada.** Dos estaciones combinadas. Permite *full-duplex* y *half-duplex*.

Modos de transferencia de datos

- **Modo respuesta normal (NRM).** Se usa en la configuración no balanceada. La EP puede iniciar la transferencia de datos hacia la ES, pero la ES solo puede transmitir datos en base a respuestas a las órdenes emitidas por la EP. Se usa cuando varias terminales están conectadas a una computadora central que sondea cada una de las entradas.
- **Modo balanceado asíncrono (ABM).** Se usa en la configuración balanceada. Cualquier EC puede iniciar la transmisión sin necesidad de recibir permiso por parte de la otra EC. Es el más usado porque no necesita realizar sondeos.
- **Modo de respuesta asíncrono (ARM).** Se usa en la configuración no balanceada. La ES puede iniciar la transmisión sin tener permiso explícito de la primaria. La EP sigue teniendo la responsabilidad del funcionamiento de la línea, incluyendo la iniciación, la recuperación de errores y la desconexión lógica.

	NRM	ARM	ABM
Configuración	No balanceada	No balanceada	C/estación puede comportarse como primaria y secundaria
Tipo de Enlace	Punto-a-Punto. Punto-a-Multipunto.	Punto-a-Punto.	Punto-a-Punto.
Tipo de Comunicación	Half-Duplex.	Full-Duplex.	Full-Duplex.

Estructura de la trama



Campos de delimitación

Los dos delimitadores corresponden a 01111110. Los receptores buscan detectar la secuencia de delimitación para sincronizarse con el comienzo de la trama, y detectar el final. Para evitar que esa combinación de bits aparezca en otro lugar dentro de la trama, se realiza una *inserción de bits*:

1. El emisor cada vez que aparece 11111, inserta un 0 extra.
2. Si el receptor encuentra 11111, el sexto bit se analiza:
 - Si es un 0, se elimina.
 - Si es un 1 y el séptimo un 0, la combinación se considera un delimitador.
 - Si el sexto y séptimo son 1s, el emisor indicó el cierre.

Ejemplo:

Mensaje original	11111111111011111101111110
Después de la inserción	11111 0 11111011011111 0 1011111 0 10

Cuando se usa un solo delimitador para el final y el comienzo, un error en un bit causaría que dos tramas se fundan en una; que la trama se parte en dos

Campo de dirección

Identifica a la estación secundaria que ha transmitido o va a recibir la trama. No se utiliza en enlaces punto a punto. Puede ser de grupo y difusión.

Campo de control

Acá se implementan todos los mecanismos de control de flujo y control de enlace. Hay tres tipos de tramas:

- **Tramas de información (I).** Transportan los datos generados por el usuario. Se incluye información para el control ARQ de errores y de flujo.
- **Tramas de supervisión (S).** Aceptación de tramas; solicitud de transmisión de tramas; suspensión temporal de la transmisión.
- **Tramas no numeradas (U).** Proporcionan funciones complementarias para controlar el enlace (conexión/desconexión del enlace; control del enlace).



Bit P/F (Poll/Final)

- La EP utiliza el bit P (Poll) para solicitar una respuesta de estado a la estación secundaria
- La ES responde al bit P con una trama de información o de supervisión y el bit F.
- El bit F indica también final de la transmisión de la ES, en NRM.

Campo de información

Solo está presente en las tramas-I y en algunas tramas-U.

Campo FCS (control de errores)

La secuencia de comprobación de trama es un código para la detección de errores calculado a partir de los bits de la trama (excluyendo los delimitadores). Se usa CRC de 16 y 32.

Funcionamiento

Inicio

Cualquier extremo puede solicitar el inicio.

- Se avisa al otro extremo sobre la solicitud de iniciación.
- Se especifica qué modo se está solicitando.
- Se indica si se van a utilizar números de secuencia de 3 o 7 bits.

Si el extremo acepta la solicitud, envía un **UA**, caso contrario un **DM**.

Transferencia de Datos

Cuando se acepta la iniciación, los extremos pueden empezar a enviar datos usando tramas-I (empezando por el número de secuencia 0). Los campos N(S) y N(R) contienen los números de secuencia con los que se hace el control de flujo y de errores. La secuencia se numera con módulo 8 o 128 usando el campo N(S). N(R) se usa para confirmar las tramas-I recibidas.

Las tramas-S también se usan para el control de flujo y errores.

- **Trama RR.** Confirma la última trama-I recibida indicando la siguiente trama-I que se espera recibir. Se usa cuando no hay tráfico en sentido contrario en el que se puedan incluir las confirmaciones.
- **RNR.** Confirma una trama-I y solicita la suspensión de la transmisión.
- **REJ.** Inicia el procedimiento ARQ con vuelta atrás N. Se indica que la última trama-I recibida se rechazó y se solicita la retransmisión de todas las tramas-I con números posteriores a N(R).
- **SREJ.** Solicita la retransmisión de una única trama.

Desconexión

Cualquiera de los dos extremos puede iniciar la desconexión. Se envía la trama DISC. El receptor puede responder con UA e informando a su capa 3 sobre la finalización de la conexión.

Derivados del HDLC

LAP-B (Link Access Procedure - Balanced)

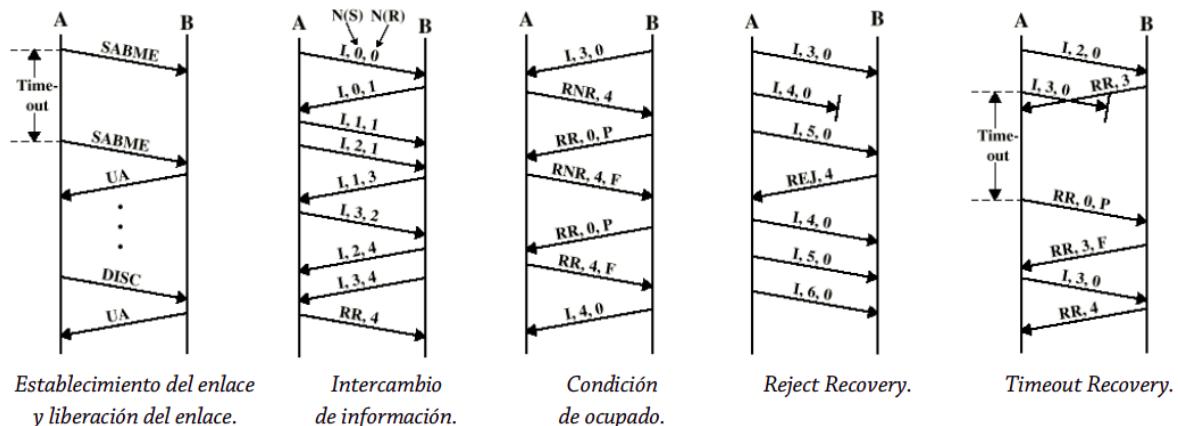
- Definido por la UIT-T como parte de la norma X.25
- Subconjunto de HDLC

- Proporciona solo el modo ABM.
- Diseñado para enlaces punto a punto entre el sistema usuario (DTE) y el nodo de una red de conmutación de paquetes (DCE)
- Formato de trama idéntico al HDLC

LAP-D (Link Access Procedure – D Channel)

- Definido por la UIT-T como parte de las recomendaciones para ISDN.
- Proporciona el procedimiento para el control del enlace de datos sobre el canal D.
- Proporciona solo el modo ABM.
- Utiliza números de secuencia de 7 bits.
- Campo de dirección de 16 bits.

Ejemplo



U.7C - Protocolo Frame Relay

- Protocolo de Capa 2 en el modelo OSI.
- Nacido para ser utilizado sobre el canal D en redes ISDN (LAP-D).
- Derivado del HDLC.
- Orientado a la conexión.
- No provee calidad de servicio ni recuperación de errores.
- Utiliza “circuitos virtuales” para interconectar sitios remotos. Generalmente permanentes (PVCs).
- Implementado sobre velocidades de $n \times 64$ hasta 34Mbps.
- 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

Fundamentos

X.25 es muy costoso porque el protocolo intercambia tramas de datos y de confirmación en cada salto a través de la red; y cada nodo intermedio debe mantener tablas de estado para cada circuito virtual. El costo solo se justifica si la probabilidad de error es alta, cosa que no se da en los sistemas modernos.

Diferencias con X.25

- La señalización de control de llamadas se transmite a través de una conexión lógica distinta de la de los datos de usuario. De este modo, los nodos intermedios no necesitan mantener tablas de estado ni procesar mensajes relacionados con el control de llamadas individuales.
- La multiplexación y conmutación de conexiones lógicas tienen lugar en la capa 2 en lugar de en la capa 3; se elimina una capa completa de procesamiento.
- No existe control de flujo ni de errores a nivel de líneas individuales (salto a salto). Si se lleva a cabo este control, será extremo a extremo y responsabilidad de capas superiores.

Se envía una trama de datos hasta el destino, y se devuelve al origen una trama de confirmación generada por una capa superior.

Desventajas frente a X.25

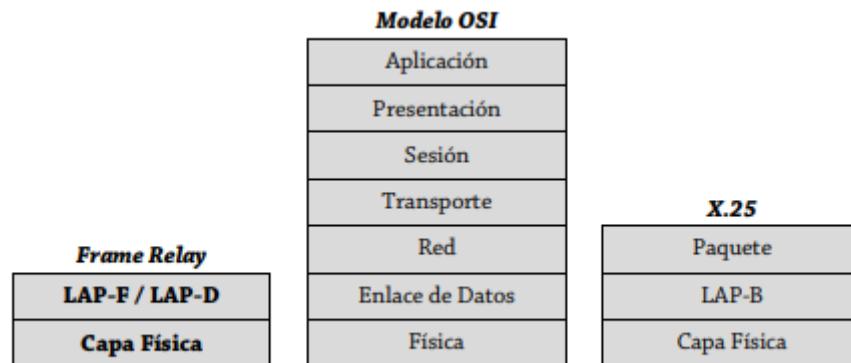
- Se pierde la posibilidad de llevar a cabo un control de flujo y de errores en cada enlace.

- En X.25 Existen varios circuitos virtuales a través de un mismo enlace físico. El protocolo LAPB permite una transmisión fiable a nivel de enlace desde el origen hacia la red de commutación de paquetes, y después hacia el destino. Frame Relay no provee ese control a nivel de enlace.

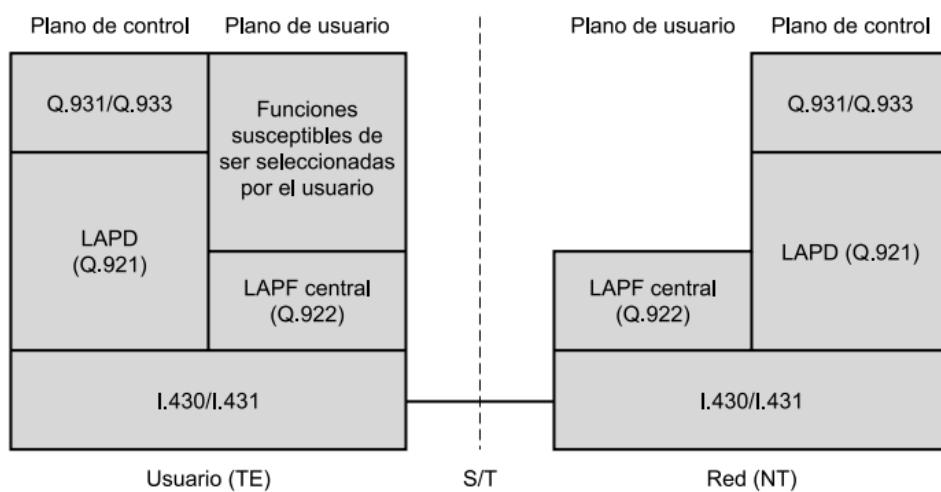
Ventajas frente a X.25

- Menor retardo y mayor rendimiento.

Modelo



Arquitectura



Plano de control

Relacionado con el establecimiento y liberación de conexiones lógicas. Se implementan entre el usuario y la red.

En la capa de enlace se usa el protocolo **LAPD (Q.921)** para proporcionar un servicio de control del enlace de datos fiable, con control de errores y de flujo, entre el usuario (TE) y la red (NT) sobre el canal D.

Plano de usuario

Responsable de la transferencia de los datos de usuario entre abonados. Proveen funcionalidad extremo a extremo.

LAPF (Q.922) es el protocolo del plano de usuario para la transferencia real de información entre usuarios finales. Solo se usan las funciones básicas:

- Delimitación de tramas, alineamiento y transparencia.
- Multiplexación/demultiplexación de tramas utilizando el campo de dirección.
- Inspección de las tramas para asegurar que éstas constan de un número entero de octetos, antes de llevar a cabo la inserción de bits cero o tras una extracción de bits cero.
- Inspección de la trama para comprobar que no es demasiado larga ni demasiado corta
- Detección de errores de transmisión.
- Funciones de control de congestión

Excepto la última, todas las funciones están en LAPD.

LAPF constituye una subcapa de la capa de enlace de datos. Proporciona el servicio de transferencia de tramas del enlace de datos entre abonados sin control de flujo ni de errores. El usuario puede seleccionar funciones adicionales. Una red ofrece *Frame relay* como un servicio orientado a conexión de la capa de enlace:

- Se preserva el orden de la transferencia de tramas entre el origen y el destino.
- Existe una probabilidad pequeña de pérdida de tramas.

Transferencia de Datos de Usuario

Trama

Indicador	Dirección	Información	FCS	Indicador
<---1--->	<---2-4 --->	<-----Variable ----->	<---2--->	<---1--->

Es el formato para el protocolo LAPF de funcionalidad mínima (**LAPF Central**). Es similar al de LAPD y LAPB (sin el campo de control):

- Existe un único tipo de trama, usada para el transporte de datos de usuario, y no existen tramas de control.
- No es posible llevar a cabo control de flujo ni de errores, dado que no existen números de secuencia.

LAPF completo (**LAPF de control**) se usa para realizar funciones por encima de las funciones centrales de LAPF. La trama tiene campo de control.

Campos

- **Indicador** y **FCS** funcionan como HDLC.
- **Información**. Contiene datos de capas superiores.
- **Dirección**.

Campo dirección

8	7	6	5	4	3	2	1
Parte superior DLCI				C/R	EA 0		
Parte inferior DLCI	FECN	BECN	DE	EA 1			

(b) Campo de dirección - 2 octetos (por defecto)

8	7	6	5	4	3	2	1
Parte superior DLCI				C/R	EA 0		
DLCI	FECN	BECN	DE	EA 0			
DLCI						EA 0	
Parte inferior DLCI o control DL central				D/C	EA 1		

(d) Campo de dirección - 4 octetos

8	7	6	5	4	3	2	1
Parte superior DLCI				C/R	EA 0		
DLCI	FECN	BECN	DE	EA 0			
Parte inferior DLCI o control DL central				D/C	EA 1		

(c) Campo de dirección - 3 octetos

EA	Bit de ampliación del campo de dirección
C/R	Bit de orden/respuesta
FECN	Notificación explícita de congestión hacia adelante
BECN	Notificación explícita de congestión hacia atrás
DLCI	Identificador de conexión del enlace de datos
D/C	Indicador DLCI o de control DL central
DE	Conveniencia de rechazo

- **DLCI**. Identificador de conexión del enlace de datos. Misma función que el número de circuito virtual en X.25 (permitir la multiplexación de varias conexiones lógicas a través de un único canal). Tiene sentido local.
- **C/R**. Comando/respuesta (uso por la aplicación).
- **EA0/EA1**. Bit de extensión del campo de dirección (ubicado 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 frame se descartará.
- DE = 0 → el frame no está elegido para descarte, no se descartará.

Prevención y Control de Congestión

- Prevención de Congestión
 - Mediante FECN y BECN.
 - Avisa a los extremos que va a experimentar congestión y que deben bajar la tasa de transmisión e ingresar menos tráfico a la red.
 - Cuando la congestión es en el mismo sentido que va el frame, se setea el FECN. Indica que la trama, sobre su conexión lógica, ha encontrado recursos congestionados.
Cuando la congestión es en el sentido opuesto en que va el frame, se setea el BECN. Indica que las tramas que transmite el usuario a través de esta conexión lógica pueden encontrar recursos congestionados.
 - 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 Errores 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 frames, que sí lo hace LAP-F Control.
- Control de Flujo
 - Hecha por el LAP-F Control.
 - Se produce en los extremos de la comunicación.

Control de Congestión/Tráfico

El control de congestión es responsabilidad conjunta de la red y de los usuarios finales.

Técnica	Tipo	Función	Elemento Clave
Control de rechazo	Estrategia de rechazo	Proporciona ayuda a la red sobre las tramas a rechazar	bit DE
Notificación explícita de congestión hacia atrás	Prevención de congestión	Proporciona ayuda a los sistemas finales acerca de la congestión en la red	bit BECN o mensaje CLLM
Notificación explícita de congestión hacia delante	Prevención de congestión	Proporciona ayuda a los sistemas finales acerca de la congestión en la red	bit FECN
Notificación implícita de congestión	Recuperación de congestión	Un sistema final infiere la existencia de congestión a partir de la pérdida de tramas	Números de secuencia en las PDU de capas superiores

Las técnicas de control de congestión:

- **Estrategia de rechazo.** La red rechaza las tramas. Debería ser equitativo para todos los usuarios.
- **Prevención de congestión.** Busca minimizar el efecto de congestión
- **Recuperación de congestión.** Busca prevenir el colapso de la red ante la ocurrencia de congestión severa. Empieza cuando la red empieza a perder tramas. La pérdida se indica con algún software de capas superiores.

Gestión de la tasa de tráfico

Los gestores de trama disponen de una cantidad finita de memoria para colocar las tramas en las colas. La forma más sencilla es rechazar arbitrariamente. Para mejorar la reserva de los recursos, se incluye la **CIR** (Committed Information Rate). Es una velocidad en bps que acuerda la red para dar soporte a una conexión. Si un dato se transmite a una velocidad mayor al CIR, puede ser rechazado cuando se produce una congestión.

La suma de las CIR no debería superar la capacidad del nodo.

Si un usuario envía datos a una velocidad menor al CIR, el gestor de tramas entrante no altera el bit DE. Si la velocidad excede la CIR, el gestor de tramas entrantes activa el bit DE en las tramas en exceso y las transmite. También se define una **velocidad de**

máxima de manera que cualquier trama por encima del máximo es descartada cuando llega al gestor de trama.

Además de la CIR, el gestor de tramas mide el tráfico sobre cada conexión lógica durante un intervalo de tiempo dado y después toma la decisión en base a la cantidad de datos recibidos durante el intervalo. **Parámetros:**

- **Tamaño de ráfaga contratado (B_c)**. Máxima cantidad de datos que la red acuerda transmitir, en condiciones normales, en un intervalo de medida T. Los datos pueden ser o no contiguos (en una o varias tramas).
- **Tamaño de ráfaga en exceso (B_e)**. Máxima cantidad de datos en exceso de B_c que intentará transmitir la red, en condiciones normales, en un intervalo de medida T. Son las tramas marcadas (pueden o no ser transmitidas).
- **Velocidad de información en exceso (EIR) [bps]**.
- **Velocidad de Acceso (AR) [bps]**. Es la velocidad del puerto. La velocidad máxima de entrada a la red. Rango entre 64 Kbps y 2 Mbps.

$$CIR = \frac{B_c}{T}$$

$$EIR = \frac{B_e}{T}$$

$$v_{puerto} = \frac{B_c + B_e}{T} = CIR + EIR$$

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

CAR (Committed Access Rate). Es la garantía mínima ofrecida por el servicio. Se asegura que esa capacidad va a estar disponible siempre, aun en caso de congestión.

CIR (Committed Information Rate). Es una velocidad en bps que acuerda la red para dar soporte a una conexión. Si un dato se transmite a una velocidad mayor al CIR, puede ser rechazado cuando se produce una congestión.

SLA (Service Level Agreement). Es un contrato entre un proveedor de servicios y un cliente que define los niveles de servicio garantizados (acá se contempla el CIR y el CAR)

Ejemplo: En una red FR con una tasa de acceso de 2Mbps se transmiten en un proceso de streaming 244 tramas con DE:0, 122 con DE:1 y se descartan 122. Si cada trama es de 4 Kbit y t=1s. Indique los valores de CIR, Be y Bc.

$$B_c = 224 \text{ tramas} \times 4 \frac{\text{Kbit}}{\text{trama}} = 896 \text{ Kbit} \quad B_e = 122 \text{ tramas} \times 4 \frac{\text{Kbit}}{\text{trama}} = 448 \text{ Kbit}$$

$$CIR = \frac{B_c}{T} = 896 \text{ Kbps}$$

Ejemplo 2: En un enlace WAN entre dos redes que utiliza FR, con E1 de ancho de banda, un CIR del 50%, EIR de 512 kbps y t=1 seg, con un tráfico promedio de 1000 kbps, con tramas de 5000 bytes. Al agregar un nuevo nodo de 08 a 12.30 el tráfico genera picos de 2000 kbps. Dado que se utiliza una aplicación donde no se deben perder tramas, ¿se debería negociar un nuevo enlace?

$$AB[E1] = V_p = 2048 \text{ Kbps}; \quad CIR = 0,5V_p = 1024 \text{ Kbps};$$

$$B_c = CIR \times T = 1024 \text{ Kb} = 25 \text{ tramas} \quad B_e = EIR \times T = 512 \text{ Kb} = 12 \text{ tramas};$$

$$\text{Durante el pico } 2000 \text{ Kbps}/T = 2000 \text{ Kb} = 50 \text{ tramas} \Rightarrow Des = 50 - (12 + 25) = 13$$

U8 - Protocolo ATM

- 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* de tamaño fijo (53 B).
- Es 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.

Arquitectura de Protocolos

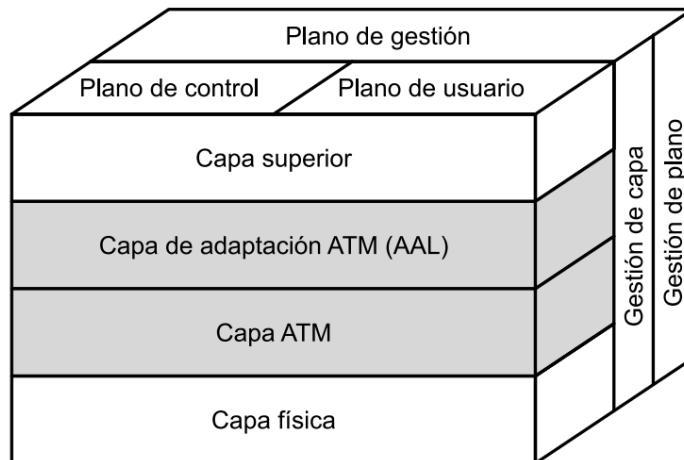


Figura 11.1. Arquitectura de protocolos ATM.

Capas

- **Capa física**
 - **Convergencia de Transmisión**
 - **Medio Físico**
- **Capa ATM.** Común a todos los servicios. Proporciona capacidad de transferencia de paquetes.

- **Capa de adaptación ATM (AAL).** Depende del servicio. Convierte la información de las capas superiores en celdas ATM. Extrae la información de las celdas y las transmite a las capas superiores.
 - **Convergencia**
 - **Segmentación y Reensamblado**

Modelo OSI	Capas ATM	Subcapas ATM	Acciones
Capa 2	Altas	Convergencia	Homogeniza las diferencias que recibe de las capas superiores. Identifica mensajes. Recupera señal de reloj.
	AAL	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 comutación. 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

Planos

- **Plano superior.** Permite la transferencia de información de usuario así como de controles asociados (control de flujo y de errores).
- **Plano de control.** Realiza funciones de control de llamada y de control de conexión.
- **Plano de gestión.**
 - **Gestión de plano.** Funciones de gestión relacionadas con un sistema como un todo. Coordinación entre todos los planos
 - **Gestión de capa.** Gestión relativa a los recursos y a los parámetros residentes en las entidades de protocolo.

Celda



Al ser pequeñas y de tamaño fijo:

- Se reduce el retardo.
- La conmutación es más sencilla.
- La implementación hardware es más sencilla.

La cabecera depende de la interfaz:

- **Interfaz usuario-red (UNI).**
- **Interfaz red-red (NNI).**

Header

UNI (interfaz usuario-red)	NNI (interfaz red-red)									
4 b 8 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).**
- **VPI (Identificador de camino virtual).** Se usa para el ruteo dentro de la red.
- **VCI (Identificador de canal virtual).** Se usa para el ruteo desde y hacia el usuario final.
- **PT (Tipo de carga útil).**
 - 1° bit = 0 \Rightarrow User Cell
 - 1° bit = 1 \Rightarrow OAM Cell
 - 2° bit = 1 \Rightarrow Indica congestión de red. La red setea en 1 si el user excede alguno de los parámetros de tráfico acordados. Similar a DE en Frame relay
 - 3° bit = 1 \Rightarrow Identifica extremo a extremo.
- **CLP (Prioridad de pérdida de celdas).** Se usa para ayudar a la red ante la aparición de congestión.
 - $CLP = 0 \Rightarrow$ celda de prioridad alta (no se debe descartar).
 - $CLP = 1 \Rightarrow$ la celda se puede descartar.
- **HEC (Control de errores de cabecera).** Permite detectar errores en la cabecera y corregir hasta 1 error.

Caminos y Canales Virtuales - Conexiones Lógicas ATM

Conexión de canal virtual (VCC)

- Similar a un circuito virtual en X.25.
- Unidad básica de conmutación en una red ATM.
- *Full-duplex* y de velocidad variable.

- Identificador: VCI (se puede repetir)

Conexión de camino virtual (VPC)

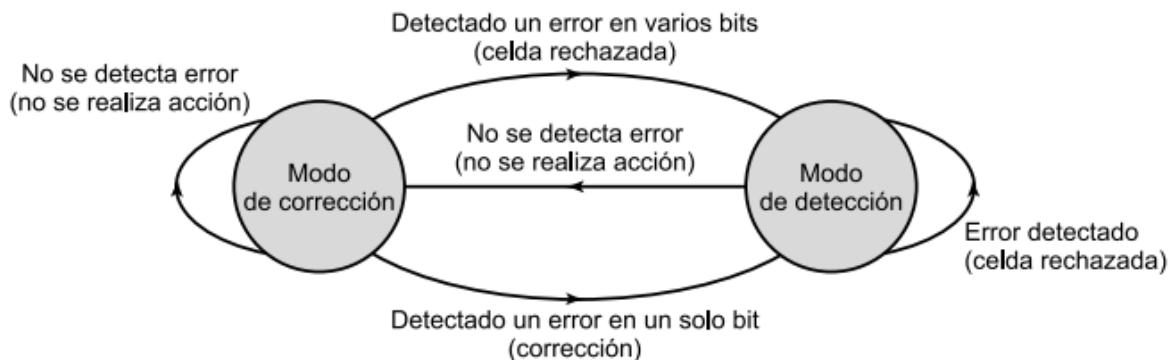
- Agrupamiento de VCC con los mismos extremos. Todas las celdas transmitidas a través de todas las VCC de una misma VPC se comutan conjuntamente.
- Identificador: VPI (no se puede repetir).

Las VCC pueden hacerse entre:

- **Usuario-Usuario.** Transportan los datos de usuario de extremo a extremo
- **Usuario-Red.** Señalización de control desde el usuario hacia la red.
- **Red-Red.** Gestión del tráfico de red y ruteo.

Control de Errores de Cabecera (HEC)

HEC se calcula en base a los restantes 32 bits de la cabecera. Se usa el polinomio $X^8 + X^2 + X + 1$. Hay suficiente redundancia para la detección y, en algunos casos, corrección de errores.



Clases de Servicio

Servicio	Velocidad	Acrónimo	Ejemplos (de aplicaciones)
En tiempo real	Constante	CBR	Requieren velocidad constante fija durante toda la conexión y un retardo de transmisión máximo estable. Audio y vídeo sin comprimir
	Variable	rt-VBR	Sensibles al tiempo (con restricciones respecto al retardo y variación del mismo). Una fuente rt-VBR funciona a ráfagas. Más flexible (multiplexación estadística). Vídeo con compresión.
En no tiempo real	Variable	nrt-VBR	Requisitos críticos en respuestas. Correo electrónico multimedia.

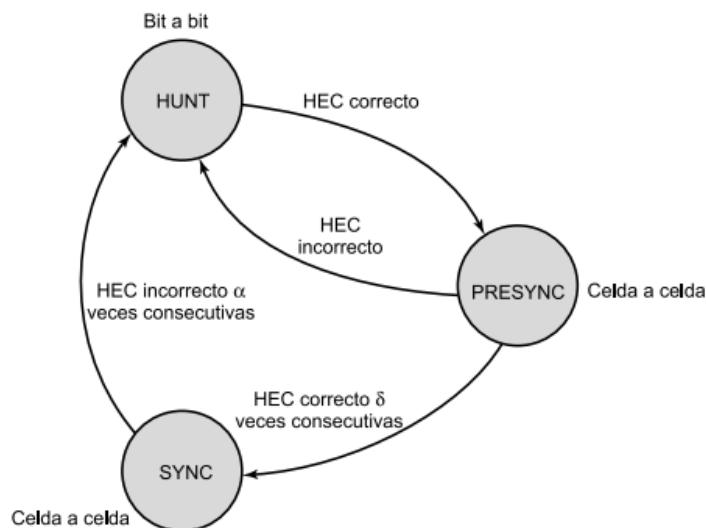
	Disponible	ABR	Reserva con conocimiento de AB necesario. Interconexión de LANs. Transmisión por ráfagas.
	No especificada	UBR	Aprovecha la capacidad sin usar. FTP en segundo plano. IP (best effort).
	Tramas Garantizadas	GFR	Servicio a subredes troncales IP.

Capa física

Funciones:

- Delimitación de celdas
- Monitoreo de errores
- Inserción de celdas vacías (idle)
- Mantenimiento del sincronismo

El sincronismo y la delimitación de celdas se obtienen mediante el HEC:



1. En el estado **HUNT** se ejecuta un algoritmo de delimitación de celdas bit a bit para determinar el cumplimiento de la regla de codificación HEC. Si hay coincidencia, pasa el método al estado **PRESYNC**.
2. En el estado **PRESYNC** se supone una estructura de celda. El algoritmo de delimitación de celdas se lleva a cabo celda a celda hasta que la regla de codificación se confirme α veces consecutivas.
3. En el estado **SYNC** se usa el HEC para la detección y corrección de errores. La delimitación de la celda se supone perdida si la regla de codificación HEC resulta incorrecta δ veces consecutivas.

Los valores α y δ son parámetros de diseño. Valores altos de δ causan grandes retardos en la sincronización, pero mayor robustez frente a falsas delimitaciones. Valores grandes de α incrementan los retardos en la detección de detección de desalineamientos, aunque también aumentan la robustez frente a falsos desalineamientos.

La ventaja de usar el esquema de transmisión basado en celdas es la sencillez de la interfaz que resulta cuando tanto las funciones en modo de transferencia como las de en modo de transmisión se basan en una estructura común.

Capa de adaptación (AAL)

El uso de ATM hace necesaria la existencia de una capa de adaptación para dar soporte a protocolos de transferencia de información que no estén basados en ATM. Las funciones de la capa son:

- Manejo de los errores en la transmisión
- Segmentación y reensamblado
- Manejo de las celdas perdidas o mal insertadas
- Control de flujo

Está organizada en dos subcapas lógicas:

- **Convergencia (CS).** Funciones necesarias para dar soporte a aplicaciones específicas que hacen uso de AAL. Cada usuario AAL se conecta a la capa AAL mediante un SAP. La capa depende del servicio.
- **Segmentación y ensamblado (SAR).** Empaquetar la información recibida desde la subcapa CS en celdas para su transmisión y desempaquetar la información en el otro extremo. Empaquetar las cabeceras y colas SAR y añade información de la subcapa CS en bloques de 48 octetos.

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.

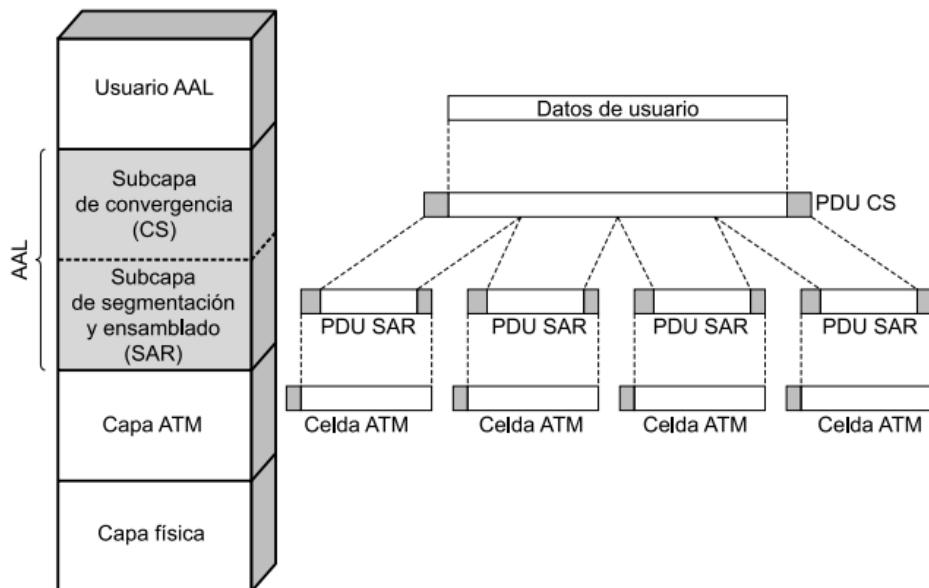


Figura 11.13. Protocolos y PDU AAL.

Atributos de tráfico

Los indica el usuario. Describen el tráfico acordado. Si el usuario excede el acuerdo, la celda se marca como descartable.

1. **Peak cell rate (PCR).** Velocidad máxima de transmisión. Es obligatorio para servicios CBR y VBR.
2. **Sustainable Cell Rate (SCR).** Límite al promedio de la tasa de transmisión. Requerido para VBR
3. **Maximum Burst Size (MBS).** Cantidad máxima de celdas enviadas continuamente a velocidad PCR. Tamaño máximo de la ráfaga. Requerido para VBR.
4. **Minimum cell rate (MCR).** Utilizado en ABR.

Parámetros de QoS

El usuario indica qué calidad espera de la red.

1. **Peak-to-peak cell delay variation (jitter).**
2. **Maximum Cell Transfer Delay.** Retardo máximo que tolera la conexión extremo a extremo. Es el tiempo que tarda un bit que ingresa en una interfaz en salir por otra
3. **Cell Loss Ratio.**

Call Admission Control - CAC

Cuando un usuario solicita una nueva VCC debe especificar los servicios requeridos en ambas direcciones para esa conexión: **categoría del servicio; descriptor del tráfico e indicar la calidad de servicio que espera de la red.**

User parameter control - UPC

Control realizado por la red en el primer punto de acceso al VCC (una vez que acepte lo requerido por el usuario va a controlar que se ejecute lo acordado). Controla que el usuario cumpla con los valores contratados de:

- PCR (Tasa pico)
- SCR (Tasa sostenida)

Si se excede marca las celdas como excedidas (prioridad de la celda)

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.

Comparación entre protocolos

	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 corri- gen. 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 corri- gen. Detecta en el HEADER sola- mente.
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.
Commutación	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.

U9 - Protocolo MPLS

- Tecnología que busca simplificar o mejorar la eficiencia de las redes.
- Puede considerarse como un protocolo para acelerar el encaminamiento de los paquetes y/o 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 previas (IP sobre ATM y conmutación IP)
- Funciona sobre cualquier tecnología de Capa 2.
- 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

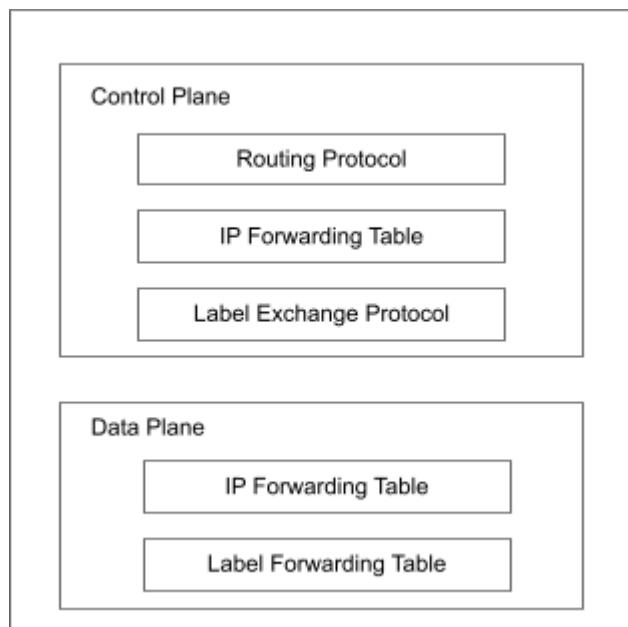
Arquitectura

Plano de control

- Es el plano administrativo.
- Es en donde corren todas las aplicaciones que hacen a la eficiencia en la operación del dispositivo.
- Son todas las funciones de cálculo (se elige cuál es la mejor forma de llegar al destino, es decir, se encarga del ruteo).

Plano de datos

- Acá ocurre la conmutación de datos.
- Debe ser lo más rápido posible.
- La tabla de ruteo (IP Forwarding Table) y de conmutación de etiquetas (Label Forwarding Table) existe en este plano.



Componentes

- **LSR (Label Switching Router).**
- **LER (Label Edge Router).**
- **LSP (Label Switched Path).** Ruta a través de uno o más LSRs en un nivel de jerarquía que sigue un paquete de un FEC en particular.
- **Etiqueta.**
- **FEC (Forwarding Equivalence Class).**

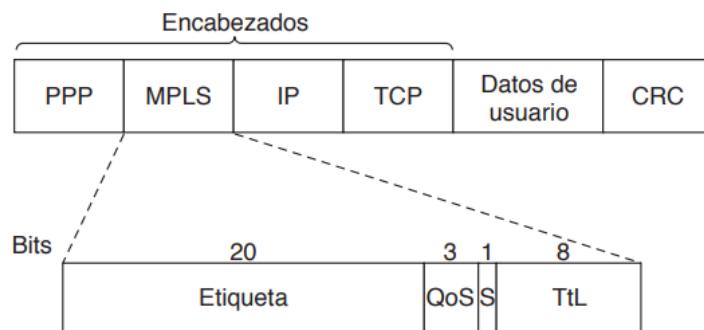
LSR

Es un router que soporta MPLS: es capaz de entender las etiquetas MPLS y de recibir y transmitir paquetes etiquetados. Puede ser:

- **Ingress LSRs.** Reciben un paquete que no está etiquetado y le insertan una etiqueta.
- **Egress LSRs.** Reciben un paquete etiquetado, remueven la etiqueta (label) y lo envían en un enlace de datos.
- **Intermediate LSRs.** Reciben un paquete etiquetado, realizan una operación sobre el, switchean el paquete y lo envían por el enlace de datos correcto.

Los primeros dos se denominan *edge* o **LER**. Los intermedios se denominan *provider*. Los edge tienen que aprender acerca de las redes IPs y hacer el mapeo entre una red y una etiqueta.

Formato de la etiqueta



- **Etiqueta.** Contiene el índice.
- **QoS.** Indica la clase de servicio.
- **S.** Indica el apilamiento de múltiples etiquetas.

- **TTL.** Indica cuantas veces se puede reenviar el paquete. Se decrementa en cada router. Si llega a 0, se descarta el paquete. Sirve para evitar los ciclos infinitos en caso de inestabilidad del enrutamiento.

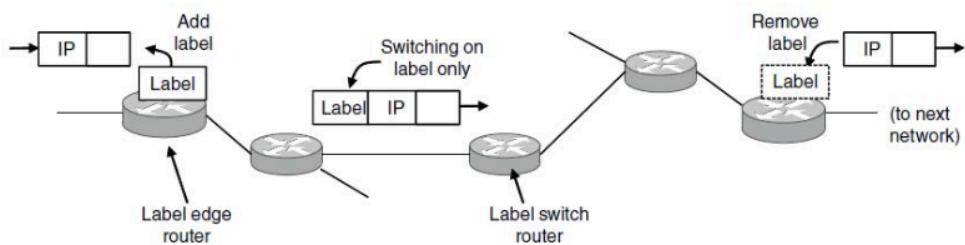
Forwarding Equivalence Class (FEC)

Una FEC es un grupo de paquetes tratados de la misma manera, sobre un mismo camino.

Es común que los routers agrupen varios flujos que terminan en un enrutador o LAN en particular y que usen una sola etiqueta para eso. Los flujos que se agrupan bajo una sola etiqueta pertenecen a la misma **FEC**. Esa clase cubre hacia dónde van los paquetes y también su clase de servicio, ya que todos los paquetes se tratan de la misma forma para fines de reenvío.

Funcionamiento

MPLS agrega una etiqueta en frente de cada paquete. El reenvío se basa en la etiqueta, no en la dirección de destino. La etiqueta se convierte en un índice de una tabla interna, permitiendo un reenvío mucho más rápido.



1. Cuando un paquete IP llega al extremo de la red MPLS, el LER inspecciona la dirección IP de destino y origen, y el tipo de servicio para determinar la FEC. Si la FEC existe, ya tiene una etiqueta asignada. Si es nueva, se tiene que asignar una nueva etiqueta. Se define el LPS.
2. Cuando un paquete llega a un LSR, la etiqueta se utiliza como un índice en una tabla para determinar la línea de salida y la nueva etiqueta a utilizar. La etiqueta solo tiene importancia local.
3. En el otro extremo, la etiqueta se elimina para revelar el paquete IP a la siguiente red.

Se usan distintos protocolos para el intercambio de etiquetas (**LDP**, **RSVP**, **BGP**).

Establecimiento de las tablas

La información de reenvío se establece mediante protocolos que son una combinación de protocolos de routing y de establecimiento de conexión (**OSPF, ISIS, RIP**). Están separados del reenvío de etiquetas, permitiendo múltiples protocolos.

1. Cuando se enciende un router, éste revisa cuáles son las rutas para las que será el destino final (qué prefijos pertenecen a sus interfaces).
2. Crea una o más FECs para estas rutas, asigna una etiqueta para cada una de ellas y pasa las etiquetas a sus vecinos.
3. Los vecinos introducen las etiquetas en sus tablas de reenvío y envían nuevas etiquetas a sus vecinos, hasta que todos los routers hayan adquirido la ruta.

Pila de etiquetas

MPLS puede operar a múltiples niveles al mismo tiempo agregando más de una etiqueta al frente de un paquete.

Caso: Muchos paquetes con distintas etiquetas que deben seguir una ruta común hacia cierto destino.

Solución: Se establece una sola ruta. Cuando los paquetes etiquetados llegan al inicio de la ruta, se agrega otra etiqueta al frente (**pila de etiquetas**). La etiqueta más externa guía a los paquetes a lo largo de la ruta. La etiqueta se elimina al final y las etiquetas restantes (si hay) se usan para reenviar el paquete. El bit S permite al router determinar si quedan etiquetas adicionales. S=1 para la etiqueta inferior. S=0 para las demás.

Problemas que resuelve - Beneficios

- **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.
- MPLS reduce la tarea de commutación en el “*core*”
 - El core es el núcleo de la red por donde pasa todo el tráfico.
 - En la arquitectura tradicional de capas en donde tengo una red de acceso, una de distribución y un “*core*”, el tráfico pasa por esas capas, llega al core, es commutado y va a hacia la periferia de nuevo (el destino).
- Puede transportar otros protocolos (multiprotocolo), no solo IP.

U10 - Seguridad

Conceptos

- **Privacidad.** Solo entidades autorizadas pueden tener acceso a la información.
- **Integridad.** Los datos sólo deben ser modificados por partes autorizadas.
- **Disponibilidad.** Los datos deben estar disponibles para las partes autorizadas.
- **Autenticidad.** Se requiere verificar la identidad de un usuario.

Ataques

- **Ataque pasivo.** Se busca averiguar o hacer uso de información del sistema, pero sin afectar a los recursos del mismo. Es difícil de detectar.
 - **Divulgación del contenido de un mensaje.**
 - **Ánalysis de tráfico.**
- **Ataque activo.** Se busca alterar los recursos del sistema o influir en su funcionamiento. Es difícil de impedir. El objetivo es detectarlos y recuperarse de cualquier interrupción.
 - **Enmascaramiento.** Una entidad pretende ser otra.
 - **Retransmisión.** Captura pasiva de datos y retransmisión posterior para producir un efecto no autorizado.
 - **Modificación de mensajes.**
 - **Denegación de servicio.** Impide o inhibe el normal uso o gestión de servicios de comunicación.

Potenciales soluciones

- Claves de acceso: Al sistema o recursos.
- Encriptado de datos.
- Seguridad física de dispositivos.
- Firma digital.
- Firewall
- Protocolos de seguridad.
- VPN.
- Capacitación a usuarios.

Seguridad en OSI

- **Físico (1):**
 - Análisis de la topología.
 - Auditoría del canal que se utiliza.
 - Potencias y/o frecuencias usadas.
- **Enlace (2):**

- Analizar protocolos para control de direcciones MAC.
- Analizador de configuración, tráfico y colisiones.
- Evaluar acceso WiFi.
- **Red (3):**
 - Auditoría de ARP y direccionamiento IP (Estático o dinámico)
 - Contraseñas, configuraciones, protocolos de ruteo, logs.
- **Transporte (4):** Operación con conexión (TCP) o sin conexión (UDP).
- **Aplicación (7):** Auditoría de:
 - Servidores.
 - Accesos remotos.
 - Firewall y DNS.

Encriptación

Encriptación Simétrica

Se utiliza una clave única. Sus componentes:

- **Texto nativo.** Mensaje original.
- **Algoritmo de cifrado.** Realiza las sustituciones y transformaciones sobre el texto nativo.
- **Clave secreta.** Las sustituciones y transformaciones dependen de la clave.
- **Texto cifrado.** El mensaje alterado. Dos claves diferentes producen dos textos cifrados diferentes.
- **Algoritmo de descifrado.** Es el algoritmo de cifrado aplicado a la inversa.

Los requisitos para el uso seguro del cifrado simétrico:

- Se necesita un algoritmo de cifrado robusto. El oponente debe ser incapaz de descifrar el texto o descubrir la clave incluso si él o ella poseyera varios textos cifrados junto a sus correspondientes textos nativos.
- El emisor y el receptor tienen que haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto.

Encriptación Asimétrica (Clave Pública)

La criptografía de **clave pública** es asimétrica porque usa dos claves diferentes.

Componentes:

- **Texto nativo.**
- **Algoritmo de cifrado.**
- **Clave pública y privada.** Si una se usa para el cifrado, la otra se usa para el descifrado. Las transformaciones dependen de la clave pública o privada que se suministre como entrada.

- **Texto cifrado.**
- **Algoritmo de descifrado.** Recibe el texto cifrado y la clave, produciendo el texto nativo.

La clave pública se hace pública para que la usen los otros; la privada es conocida solamente por el dueño. Todo algoritmo se basa en una clave para el cifrado y otra diferente para el descifrado.

Características de los algoritmos

- No es factible, por limitaciones computacionales, determinar la clave de descifrado si sólo se conoce el algoritmo criptográfico y la clave de cifrado.
- Para la mayoría de los esquemas de clave pública, cualquiera de las dos claves relacionadas puede utilizarse para el cifrado, utilizando la otra para el descifrado.

Los pasos son:

- Cada usuario genera un par de claves que van a ser utilizadas para el cifrado y el descifrado de los mensajes.
- Cada usuario publica una de las dos claves de cifrado en un registro público. Ésta es la clave pública. La clave compañera se mantiene privada. Cada usuario mantiene una colección de claves públicas de otros usuarios.
- Si Robert desea enviar un mensaje privado a Alice, él cifra el mensaje usando la clave pública de Alice.
- Cuando Alice recibe el mensaje, lo descifra usando su clave privada.

Firma digital

Robert quiere enviarle un mensaje a Alice, teniendo la certeza de que el mensaje proviene efectivamente de él. Robert usa su propia clave privada para cifrar el mensaje. Cuando Alice recibe el texto cifrado, prueba descifrarlo con la clave pública de Roberto, demostrando que el mensaje fue cifrado por Robert. El mensaje sirve como **firma digital**. El mensaje está **autenticado** en términos de origen e integridad de los datos ya que es imposible alterar el mensaje sin acceder a la clave privada de Robert.

Una forma eficiente consiste en cifrar un pequeño bloque de bits que sea función del documento. Ese bloque es el **código de autenticación**. No debe ser posible modificar el documento sin cambiar el código de autenticación. Si el código de autenticación se cifra con la clave privada del emisor, sirve como una firma que verifica el origen, contenido y la secuencia.

Provee:

- Autenticidad
- Integridad
- No repudio

La firma digital no ofrece privacidad: el mensaje está seguro frente a alteraciones, pero no lo está de ser leído por otros.

IPSec

IPSec proporciona la capacidad de asegurar las comunicaciones que se efectúen a través de una red. Ejemplos:

- Conectividad segura entre sucursales a través de Internet.
- Acceso remoto seguro a través de Internet.
- Establecimiento de conectividad intranet y extranet con socios.
- Mejora de la seguridad en el comercio electrónico.

IPSec puede cifrar/autenticar todo el tráfico a nivel IP. Todas las aplicaciones distribuidas pueden hacerse seguras.

IPSec proporciona tres servicios:

- **Authentication Header (AH)**. Solo autenticación.
- **Encapsulating Security Payload (ESP)**. Autenticación y cifrado.
- **Intercambio de claves**. Esquema manual o automático.

Para VPN privadas se usa ESP:

- Usuarios no autorizados no deben entrar en la red privada virtual
- Si hay observadores en Internet, no deben poder leer los mensajes enviados por la red privada virtual.

Security Association (SA)

Una SA es una relación en un solo sentido entre un emisor y un receptor que proporciona servicios de seguridad al tráfico que transporta. Los servicios de seguridad se proporcionan a una SA para que utilice AH o ESP, pero no ambos.

Una SA se identifica por:

- **Índice de parámetros de seguridad (SPI)**. Cadena de bits asignada a esta SA y con significado local solamente. El SPI se transporta en las cabeceras AH y ESP para que el receptor seleccione la SA donde procesará un paquete recibido.
- **Dirección IP destino**.
- **Identificador del protocolo de seguridad**. Distingue entre una SA de AH o ESP.

Una implementación de IPSec incluye una base de datos de asociaciones de seguridad que define los parámetros asociados con cada SA. Una SA se define por:

- **Contador del número de secuencia.**
- **Desbordamiento del contador de secuencia**
- **Ventana contra retransmisiones.**
- **Información de AH.**
- **Información de ESP.**
- **Tiempo de validez de la asociación de seguridad**
- **Modo del protocolo IPSec.**
- **MTU de la ruta.**

Modos

Túnel

Todo el paquete IP se encapsula en el cuerpo de un paquete IP nuevo con un encabezado IP totalmente nuevo. Es útil cuando termina en una ubicación que no sea el destino final. El final del túnel puede ser un firewall. Ese es el caso de las VPNs.

También es útil cuando se agrega un conjunto de conexiones TCP y se maneja como un solo flujo cifrado, porque así se evita que un intruso vea quién está enviando cuántos paquetes a quién.

La desventaja es que agrega un header más, lo que incrementa el tamaño del paquete en forma considerable.

Transporte

El encabezado IPsec se inserta justo después del encabezado IP. El campo Protocolo del encabezado IP se modifica para indicar que sigue un encabezado IPsec después del encabezado IP normal (antes del encabezado TCP). El encabezado IPsec contiene información de seguridad, principalmente el identificador SA, un nuevo número de secuencia y tal vez una verificación de integridad del campo de carga

Protocolos

Auth Header (AH)

Proporciona la verificación de integridad y seguridad antirrepetición, pero no la confidencialidad (no hay encriptación). En IPv6 es un encabezado de extensión y se trata como tal.

Header IP	AH	Header TCP	Payload + relleno
-----------	----	------------	-------------------

8 bits	8 bits	16 bits
Siguiente encabezado	Longitud de la carga útil	
Índice de parámetros de seguridad (SPI)		
Número de secuencia		
Datos de autenticación (Variable)		

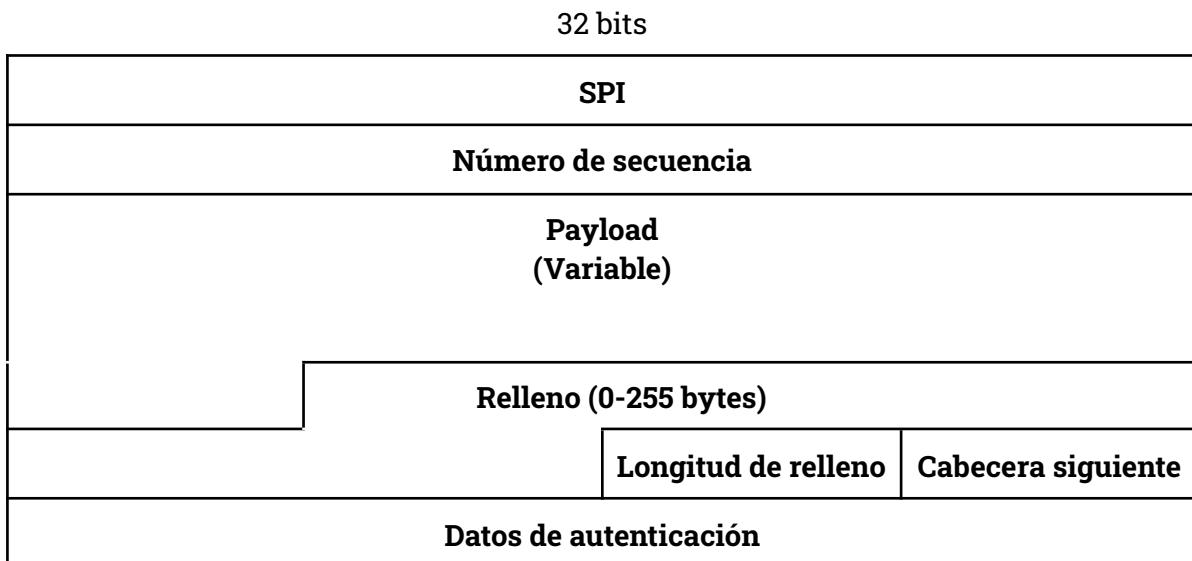
- **Siguiente encabezado.** Almacena el valor que tenía el campo Protocolo de IP antes de reemplazarlo con 51 para indicar que sigue un encabezado AH.
- **Longitud de carga útil.** Número de palabras de 32 bits en el encabezado AH menos 2.
- **Índice de parámetros de seguridad.** Identifica una SA
- **Número de secuencia.** Se usa para enumerar todos los paquetes enviados en una SA. Cada paquete recibe un número único, incluso las retransmisiones. Sirve para detectar ataques de repetición. Si se agotan los números, se tiene que establecer una nueva SA.
- **Datos de autenticación.** Contiene la firma digital de la carga útil. IPsec se basa en la criptografía de clave simétrica y el emisor negocia con el receptor una clave compartida antes de establecer una SA, dicha clave compartida se utiliza en el cálculo de la firma.

El contenido en **datos de autenticación** se calcula sobre:

- Los campos inmutables de la cabecera IP o que tienen un valor predecible de AH SA cuando llegue al extremo. Por ejemplo, longitud de la cabecera de Internet y la dirección origen.
- La cabecera AH que no sea el campo de datos de autenticación. El campo de datos de autenticación se establece a cero para propósitos de cálculo tanto en el origen como en el destino.
- Todos los datos del protocolo de la capa superior, que se supone que son inmutables durante el camino.

Encrypted Security Payload (ESP)

Proporciona servicios de privacidad, incluyendo privacidad del contenido de los mensajes y una limitada privacidad del flujo de tráfico. También puede proporcionar un servicio de autenticación.



- **SPI**
- **Número de secuencia**
- **Payload**. Segmento de la capa superior protegido mediante cifrado.
- **Relleno**.
- **Longitud de relleno**
- **Cabecera siguiente**. Identifica el tipo de datos contenidos en el campo de datos de carga útil mediante la identificación de la primera cabecera en esa carga útil.
- **Datos de autenticación**. Contiene el valor de comprobación de integridad calculado sobre el paquete ESP menos el campo de datos de autenticación.

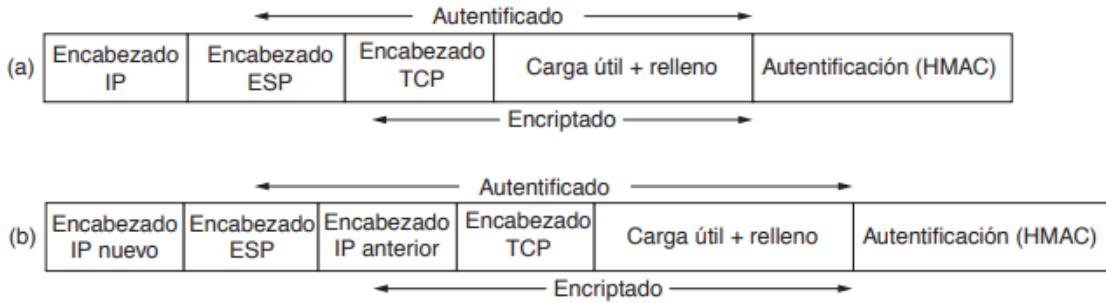


Figura 8-28. (a) ESP en modo de transporte. (b) ESP en modo de túnel.

Firewall

Un **firewall** actúa como un filtro de paquetes. Inspecciona todos y cada uno de los paquetes entrantes y salientes. Los paquetes que cumplen cierto criterio descrito en reglas formuladas por el administrador de la red se reenvían en forma normal. Los que fallan la prueba simplemente se descartan.

Los criterios se proporcionan como reglas o tablas que listan los orígenes y destinos aceptables y bloqueados; y las reglas predeterminadas acerca de lo que se debe hacer con los paquetes que entran y salen a otras máquinas. Los criterios, a nivel de red, usan la dirección IP y número de puerto.

La **DMZ** es parte de la red que está fuera de la zona de seguridad

Pueden ser:

- **Con estado.** Asocian paquetes a las conexiones y usan campos del encabezado TCP/IP para mantener un registro de las conexiones.
- **Con puertas de enlace a nivel de aplicación.** El interior de los paquetes, todavía más allá del encabezado TCP, para ver lo que está haciendo la aplicación.

Ventajas:

- Concentración de la seguridad en un único punto.
- Regular el uso de la red exterior.
- Limitar el tráfico de servicios vulnerables.
- Mejorar la privacidad del sistema.

Certificados

El problema de usar claves simétricas es cómo distribuir las claves de forma segura. El problema desaparece cuando se usa el cifrado de clave pública. Si Robert quiere enviarle un mensaje a Alice:

1. Prepara el mensaje.
2. Cifra el mensaje utilizando cifrado simétrico con una clave simétrica de sesión de un solo uso.
3. Cifra la clave de sesión utilizando la clave pública de Alice
4. Adjunta la clave de sesión cifrada al mensaje y lo envía a Alicia.

Solamente Alice puede descifrar la clave de sesión. Esto genera otro problema: alguien podría haber difundido una clave pública para hacerse pasar por Alice. La solución es el uso de **certificados**.

Un **certificado de clave pública** consta de una clave pública más un identificador de usuario del propietario de la clave. Todo eso está firmado por una tercera parte de confianza, que generalmente es una CA (Certificate Authority). Un usuario puede presentar su clave pública a la autoridad de un modo seguro y obtener un certificado. El usuario puede entonces publicar el certificado. Cualquiera que necesite la clave pública de este usuario puede obtener el certificado y verificar que es válido mediante la firma adjunta en que se confía.

La **cadena de seguridad (chain of trust)** es:

Certificado que ve el usuario → Certificado intermedio → Certificado Root CA

Para instalar un certificado:

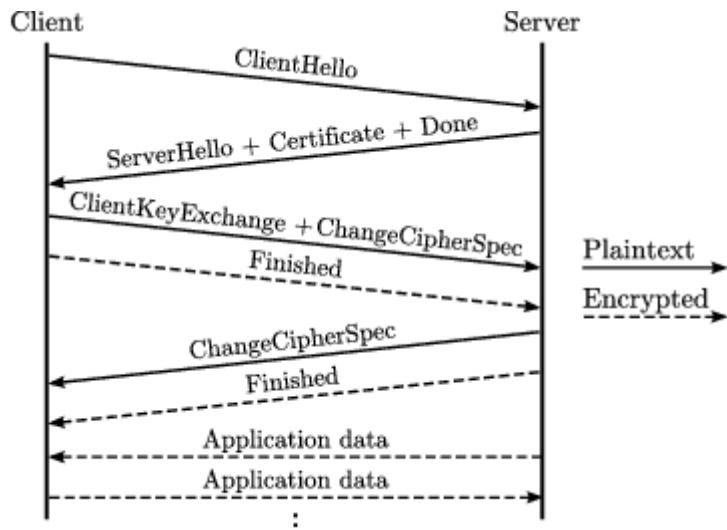
- Generar un CSR (certificate signing request).
- Cargo los valores que quiera que tengan.
- Se genera la clave privada que me guardo.
- Ese pedido lo envío a una entidad certificante para comprarlo.

Transport Layer Security (TLS)

Es la evolución de SSL (Secure Socket Layer). Es un protocolo usado ampliamente para proteger el tráfico web entre un servidor HTTP y un browser. Usa encriptación asimétrica (establecimiento de la conexión) y simétrica (resto de la comunicación).

Funcionamiento

El *sender* hace una propuesta de encripción luego que el servidor le envíe su certificado, el servidor aceptará o pedirá cambiar y se establece la conexión.



Cipher Suite es una lista de algoritmos criptográficos ordenados por orden de preferencia. El servidor elegirá el mayor que pueda soportar. Contiene:

- *Key exchange algorithm.* Cómo se intercambiarán las claves simétricas.
 - *Authentication algorithm.* Cómo se autenticará.
 - *Bulk encryption algorithm.* Algoritmo de clave simétrica a utilizar.
 - *Message Authentication Code (MAC).* Método para chequear integridad.