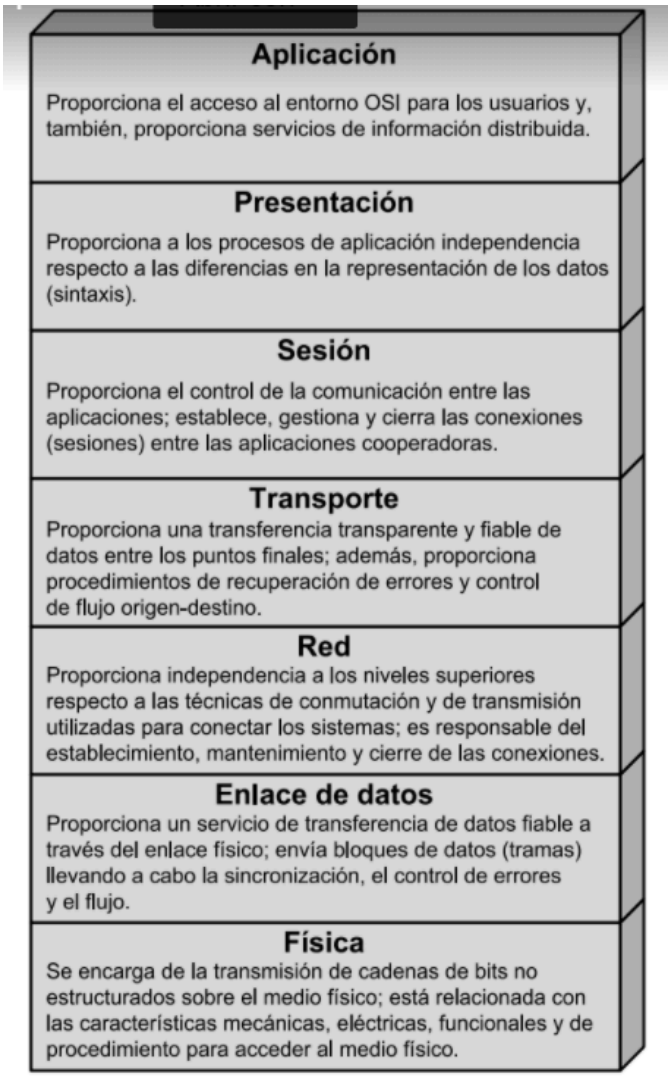
Modelo OSI

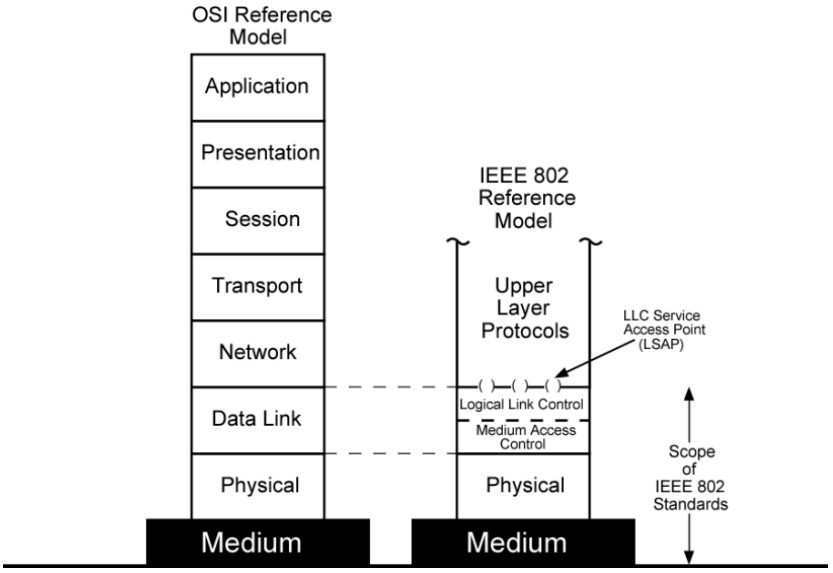


Redes de área local (LAN)

Utiliza el modelo de referencia IEEE 802.
Usa protocolos sincrónicos orientados al bit o al carácter.

Capa 1 y 2 de OSI. La capa de enlace del modelo OSI se divide en dos subcapas: LLC y MAC.

IEEE 802 v OSI



Capa física:

- Codificación / decodificación
- Generación / eliminación del encabezamiento: lo que se le agrega al encabezado del bloque de datos, para mantener el sincronismo de bloque.
- Transmite y recibe bits
- Determina al medio de transmisión y a la topología.
- Permiten modos de operación half-duplex
- Operan sobre líneas dedicadas o conmutadas

Subcapa MAC (Control de acceso al medio):

- Servicios:
  - En transmisión, ensamblado de datos en tramas con campos de dirección y de detección de errores.
  - En recepción, desensamblado de tramas, reconocimiento de dirección y detección de errores.
  - Control de acceso al medio de transmisión LAN.
- Ensamblado (tx) y desensamblado (rx) de tramas.
- Permite que los usuarios compartan el único medio disponible
- Control de acceso al medio de transmisión/flujo:
  - El transmisor arma tramas con datos y campos para direccionamiento y detección de errores -> El receptor desarma las tramas, reconoce direcciones y detecta errores
  - El manejo del acceso al medio de transmisión no existe en la capa 2 del modelo tradicional
  - Para la misma LLC, hay varias opciones MAC
  - Métodos de acceso:

- Rotación circular (Round robin): Bueno si hay muchas estaciones que deben transmitir mucho tiempo
- Reserva: El tiempo se divide en ranuras, bueno para tráfico continuo
- Contención/Contienda: Todas las estaciones que deseen hablar pelean por el canal. Simple para implementar, bueno para trafico en rafagas, colapsa con carga alta.

Detección de errores: mediante CRC

Control de enlace de datos

HDLC

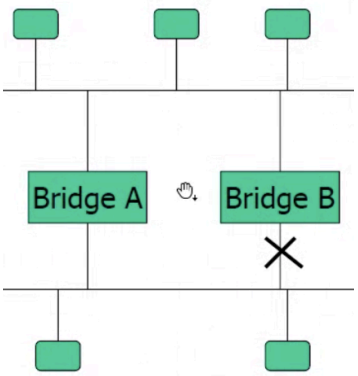
Acceso al medio

- **CSMA 1-Persistente con espera exponencial binaria**
  - Todas las estaciones conocen inmediatamente que comenzó una transmisión. Primero escuchan para ver si el medio está disponible (carrier sense), y en este caso comienza a transmitir. Esperan un tiempo razonable y envían ACK • Si no reciben ACK retransmiten
  - 1 Persistente: Evita dejar el canal libre. Si el medio está ocupado, espera que se libere y entonces transmite inmediatamente. Si dos o más estaciones esperan, seguramente habrá colisión. Por lo que hace un algoritmo para volver a transmitir. Lo utiliza IEEE 802.3 y ethernet
    Las estaciones están escuchando todo el tiempo.
    1. La capa MAC de una estación recibe la indicación de un protocolo superior de transmitir un mensaje.
    2. Se consulta a la capa física si el medio está libre (en ethernet: uno persistente).
    3. Cuando está libre, empieza la transmisión: envía los bits al medio.
    4. Escucha lo que se está transmitiendo para chequear si hubieron colisiones.
       a. No hubo colisión: finaliza, vuelve a escuchar.
       b. Hubo colisión:
          i. Se hace una señal de jamming
          ii. Se incrementa un contador de colisiones (n).
          iii. Se genera aleatoriamente una N ($0 <= N <= 2^n - 1$).
          iv. Se espera N intervalos de tiempo (la ventana de colisión, 51.2ms) antes de volver a intentarlo ⇒ cuanto más colisiones haya, más se va a esperar y menos posibilidades habrá de que vuelvan a colisionar.
- **CSMA/CD**
  Lo utilizan las tecnologías half-duplex.
  Evita que las colisiones ocupen el medio. La estación sensa el medio para ver si está ocupado y puede detectar colisiones.

1. Si el medio está libre, transmite
2. Si está ocupado, espera se libere, y transmite
3. Si detecta colisión, la refuerza con interferencia y para
4. Espera un tiempo aleatorio y vuelve al paso 1

Bridging

Se parte el segmento y se crean 2 dominios de colisión separados. Va aprendiendo que MAC están de cada lado del bridge dividiendo el tráfico. Están en el mismo dominio de broadcast; filtra tramas que no tienen que pasar a cierto lado; permite que el tráfico local quede local, mejora la performance; las estaciones no se enteran de la existencia del bridge.
Bridging Loop & STP: teniendo dos bridges en la red ⇒ el problema es que escuchan y reciben lo mismo ⇒ en caso de haber un broadcast va a quedar un loop infinito (tormenta de broadcast, bridging loop) ⇒ inutiliza la red ⇒



802.1D-Spanning tree(IEEE802.1D):

Los bridges se conocen y evalúan si hay un loop, por lo que si lo hay, anulan lógicamente el loop.

Cada switch envía un BPDU cada 2 segundos. Cada switch tiene un Bridge Id (Bridge priority + MAC address). La prioridad menor se designa root. Cuando cambia el estado de un port, se envían notificaciones de cambio de topología (TCN) y comienza nuevamente el cálculo del árbol.

Blocking ➔ listening ➔ learning ➔ forwarding.

VLANs (Virtual LANs)

Organización lógica de los puertos creadas dentro del mismo switch (que debe soportar VLAN); divide dominios de broadcast; aisla las redes

802.1Q / trunking:

Permite crear VLANs en switches separados. Teniendo dos switches separados (que deben soportar el protocolo), crea un tubo (enlace troncal) conectado a un puerto físico de cada switch por el cual pasa tráfico de todas las VLANs;

Subcapa LLC

- Se encarga de transmitir los PDUs entre dos estaciones
- Interfaz con las capas superiores y control de errores y de flujo
- Especifica los mecanismos para direccionar estaciones a través del medio y para controlar el intercambio de datos entre dos usuarios.
- Debe soportar el acceso múltiple en un medio compartido: Multiplexado usando puntos de acceso al servicio LLC (LSAP)

Control de flujo

ARQ con parada y espera y ventana deslizante.
Indica cuándo transmitir y cuándo no, mediante las señales ACK y NAK.

- Una vez se envía un paquete no se envía el siguiente paquete hasta que no se recibe el correspondiente ACK (confirmación de la recepción) y en caso de recibir un NACK (rechazo de la recepción) se reenvía el paquete anterior

Control de errores

ARQ con parada y espera, vuelta atrás N y rechazo selectivo.

- Control de flujo:Detección: para saber si el mensaje llegó bien.
- Corrección: se queda con el correcto.

Protocolos

Ethernet / 802.3

Protocolo de acceso al medio.
Especifica el medio físico y el protocolo MAC para las redes cableadas.
Peer to peer (el control está completamente descentralizado)y half-duplex. Punto a multipunto. No existe la confirmación, se asume exitosa.

Acceso al medio

CSMA/CD : Lo utiliza para controlar el acceso al medio. Tiene la posibilidad de sensar constantemente el medio

Detección de errores

Mediante el campo FCS detecta errores en la transmisión: CRC de toda la trama

Redes LAN inalámbricas (Wireless LAN)

- > flexibilidad y movilidad, < seguridad
- Toda comunicación se hace a través del access point. Comunicación inalámbrica por radio frecuencia a través del access point que tiene una antena.
- Dos bandas de uso no licenciado: 2.4 y 5.8 que se usan para redes wireless, bluetooth, etc.

Control de acceso al medio: CSMA/CA

- El acceso al medio CSMA/CD no sirve en este caso, ya que podría pasar que las estaciones no se puedan escuchar entre ellas
- Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos. El access point devuelve el CTS
- DCF - función de coordinación distribuida:

- ➢ Transmite solo si el medio está libre por un intervalo de tiempo determinado (DIFS) → transmite un RTS → el access point recibe el RTS y responde un CTS → se envían los datos → el access point devuelve un ACK. El access point envía un NAV que marca la cantidad de tiempo que se le brinda para transmitir los datos. No se tiene certeza de en qué momento voy a poder transmitir; es totalmente aleatorio. Después de mandar los datos hay otro espacio (SIFS) hasta el ACK, y un DIFS + ventana hasta los siguientes datos.
- ➢ Ventana de contienda o contención o competencia (contentwindow): cuando las estaciones se aseguran de que el medio está libre, esperan un periodo de tiempo aleatorio antes de empezar con el envío. Se duplica con cada colisión. Se corresponde con el Binary Exponential Backoff (BEB) del protocolo CSMA/CD.

❖ **PCF:** Acceso múltiple coordinado. Sustituye o complementa DCF. Las terminales se asocian al access point; El access point pregunta uno por uno si tiene que transmitir y si tiene, transmite el mensaje + ACK y el access point le confirma al mismo tiempo que le pregunta al siguiente. Entre cada intervalo hay una distancia SIFS. Arranca enviando una trama Beacon y finaliza enviando una trama Beacon CF-End.

Seguridad

❖ Seguridad:
- ➢ Deshabilitar beacon: Broadcast que manda el equipo transmitiendo el SSID. Al desabilitarlo, solamente se podrán conectar quienes conozcan el SSID. Se oculta pero igualmente las tramas de datos que se propagan incluyen el SSID entonces se podría interceptar capturando la trama en el espectro.
- ➢ Filtrado de MAC: Decirle al equipo que mac puede o no puede comunicarse
- ➢ Autenticación: WPA2 (personal o empresarial). Hay una clave compartida entre el access point y los clientes. Para la autenticación y la encriptación

Subcapa MAC 802.11

❖ Especifica el medio físico y el protocolo MAC para las redes inalámbricas

Control de acceso - CSMA/CA

(Explicado arriba)
Puede ser protocolo de acceso distribuido o centralizado.
- ➢ Función de coordinación distribuida (DCF): Entran todos, pero previene colisiones. Utiliza CSMA/CA.
- ➢ Función de coordinación puntual (control centralizado opcional) (PCF): todos pueden acceder, pero en forma coordinada.

Detección de errores

Mediante CRC

Fragmentación, reensamblado

Tiene el campo SC (sequence control) de dos bits

Puente entre cableado e inalámbrico

Portal: Cuando el acces point está conectado por un cable a la red cableada. Integración lógica entre LANs cableadas y 802.11. Puente entre cableado e inalámbrico.

En las redes Wi-Fi, El modo **Bridge** permite a dos o más access point comunicarse entre ellos con el propósito de unir muchas LANs.

Arquitectura TCP/IP

Capas:

1. Interfaz (no se especifica ni la capa física ni la de enlace)
2. Internet (IP + ARP + RARP + ...)
3. Transporte (TCP -confiable- o UPD -no confiable-)
4. Aplicación:
    - Capa 5, 6 y 7 del OSI. Cada protocolo tiene algo.
    - Una capa que es la que maneja la interfaz con el usuario (con el browser)
    - Una capa tiene las primitivas para el manejo de protocolos

El protocolo IP (internet) cumple con la mayoría de las funciones de la capa de red. El protocolo TCP (transporte) cumple con la mayoría de las funciones de la capa de transporte y con algunas de la capa de sesión. El resto de las capas se agrupan en la aplicación.
IP es orientado a la no conexión y no es confiable.

IP

Es un servicio connectionless por lo que: no es confiable, los paquetes son tratados independientemente y tiene una entrega best-effort.

Datagrama IP: siempre tiene 32 bits de datos por la cantidad de palabras dado por el HLEN.

Fragmentación y reensamblado

- IP divide los datagramas en fragmentos y los fragmentos deben ser reensamblados en destino. Esto se hace para evitar que haya problemas si un datagrama supera el MTU de un router.
- MTU (maximum transfer unit): límite máximo para la cantidad de datos que se pueden transmitir por trama.
- Si el MSS es mayor que el MTU hay fragmentación
- Campos de trama que utiliza
    - Identificación (todos los fragmentados tienen el mismo ID)
    - Desplazamiento de fragmento: Dice en qué posición del datagrama arranca el paquete enviado. Lo dice de a múltiplos de 8, por lo que si el offset fuera 600 se expresaría como 75 (75 * 8 = 600).
    - FLAGS: va a tener 3 bits (1 sin uso, 1 que dice “no fragmentar” y 1 que dice “más fragmentos”).

- La fragmentación es no deseable ya que: IP no garantiza la entrega ⇒ es doblemente (si se parte en dos) probable que el paquete se pierda; hay mayor carga de procesamiento en los routers (aunque tampoco es tan grave). Hoy en día es poco común la fragmentación.
- Para que no haya fragmentación la MTU tiene que ser de datos enviados + 20 bytes

Direccionamiento y encaminamiento

- Permite identificar a los miembros de la red y mostrar por qué camino ir.
- Utiliza campo TTL: tiempo de vida del datagrama; ya que no es orientado a la conexión, es posible que el host destino no se pueda alcanzar por lo que el paquete se podría quedar dando vueltas; Disminuye en 1 cada vez que pasa por un router.

Direcciones

- Todos los hosts de la misma red tienen una parte que tienen en común (identificador de red) y una parte única (identificador de host).
- La máscara de subred define cuántos bytes tiene cada identificador.
- Identifican a un puerto en una red. Si un host se mueve a otra red, debería cambiar su dirección.
- Se usan en la capa 3.

Subredes

Para el mejor aprovechamiento de las grandes redes, estas se pueden subdividir en redes más pequeñas. Se toma algún bit del espacio de host para identificar a más subredes (redes). Trabaja sí o sí con clases.

- Ayuda al direccionamiento jerárquico: el datagrama mira primero la red, después la subred, y por último el host.
    - **VLSM** (Máscara variable): cuando la máscara varía en las subredes según la cantidad de host que necesita usar.

Superred/CIDR: Uso más eficiente de las cada vez más escasas direcciones IPv4. Permite agrupar varias redes en una única superred. Para esto se altera la máscara de red. Disminuye drásticamente el tamaño de las tablas de enrutamiento. A los vecinos se les tienen que dar redes contiguas para que las pueda agrupar. Un dominio al que se le ha asignado un rango de direcciones tiene la autoridad exclusiva de la agregación de sus direcciones, y debería agregar todo lo que sea posible siempre y cuando no introduzca ambigüedades.

Encapsulamiento

Parámetros que utiliza:

- El tamaño del encabezado/longitud (dependiendo el protocolo puede ser fijo o variable) para conocer dónde comienza y termina el header y datos
- Protocolo: Determina a quien tiene que entregarle la respuesta

Detección de errores

Checksum del encabezado: verifica que no hubo errores en la cabecera; IP no da servicio de garantía de errores en los datos; si da incorrecto se descarta el datagrama.

Protocolo IP v4

- Dirección única en internet de 4 bytes.
    - Se compone de identificador de clase, número de red, número de host.
- **Difusión IP**:
    - Dirigida (broadcast):A todas las estaciones de la red destino.
    - Limitada: A todas las estaciones de la red origen.
    - Multidifusión.
- Direcciones reservadas:
    - 127.0.0.1: dirección de loopback, retroalimentación. En realidad todo 127.x.x.x.
    - 255.x.x.x: es para difusión limitada.
    - 224.x.x.x y 247.x.x.x
- NAT: dispositivo que permite traducir las direcciones privadas ↔ públicas.
    - Dinámico: Asigna direcciones en forma dinámica.
    - Estático: Estáticamente configurada.
- Servidor de DHCP: Protocolo de configuración dinámica de host. Asigna direcciones IP en forma dinámica. Corre sobre UDP.

Direcciones IP con clase

La IANA creo clases para asignar dependiendo de lo que se necesite. Cada una tiene un identificador de clase al principio.

Clase	Identificador binario	Desde	Hasta	Bits de Red	Bits de Host
A	Primer bit 0	0.X	126.X	1er octeto	Últimos 3 octetos
B	10.X	128.X	191.X	2 primeros octetos	Dos últimos octetos
C	110.X	192.X	223.X	3 Primeros octetos	Último octeto
D	1110.X	224.X	239.X	Para multicast	
E	1111.X	240.X	247.X	Para usos posteriores	

Regla del primer octeto: se mira el primer octeto y en base al número que tiene ya se sabe la clase.

VPN

Permite pasar con cierto grado de seguridad y menor riesgo el tráfico que va de una red LAN hacia otra pasando por una red pública.

- ❖ Se obtiene tráfico dedicado, los proveedores intermedios reservan ancho de banda para que no se pierdan esos paquetes.
    - ➢ Se hace de diferentes maneras siempre encriptando de la capa n hacia arriba:

- En capa 5/4 (de aplicación: Cuando salgo por encima de la red. Cifrados de túneles para sesiones. Lo hace SSL: Capa 4 y TLS: Entre capa 4 y 5
- En la capa 4 IPSec lo hace en modo transporte: Bloquea todo el tráfico que no sea de la vpn. La computadora queda solo para uso de cosas que vayan por la VPN. Utiliza AH (autentication header) que da autenticación e integridad.
- En la capa 3:
    - Implementación por hardware: El túnel se establece por hardware. Cifrado a nivel físico. Agrega seguridad personalizada. Tiene latencia porque agrega procesamiento previo, pero agrega mayor seguridad. Utilizado en cancillería, ejército.
    - Implementación por software: Se hace un túnel IPSec que se usa como un enlace dedicado: El tráfico va cifrado y ningún router intermedio puede examinar los datos del paquete IP. Los extremos con contraseñas y criptografía pueden examinarlo.
        - Protocolo: ESP da autenticación integridad y confidencialidad
        - Utilizan ACL en las entradas.
        - Puede ser red/host a red/host.
- En capa 2 lo hace con los protocolos que permiten que no haya decisiones de enrutamiento en el medio del túnel.
    - PPTP: Point to point tunnel protocol. Túnel cifrado que usa el propietario. Utilizan un complemento del header PPP acompañado con un protocolo GRE y dentro de eso va el datagrama IP. Permiten múltiples accesos remotos.
    - L2TP: Layer 2 tunnel protocol. Estandarización de PPTP y L2F. No depende de IP. Es multiprotocolo. Auténtica los enlaces, lo controla y se le puede agregar IPSec para el cifrado de los paquetes que van dentro.

- Disminuyen el costo de las conexiones WAN
- Permiten el acceso remoto: Para teletrabajo por ej.
- DH: Diffie-Hellman : Tamaño de la clave que puedo usar: DH1 (768 bits), DH2(1024 bits), DH5(1536 bits)

Protocolos IP

ICMP: Protocolo de mensajes de control de internet

- Parte de la capa IP.
- Verifica e informa sobre eventos de control en la red IP.
- Trabaja con el protocolo PING en la capa de aplicación.

IGMP: Protocolo de administración de grupo en internet

- Es un protocolo de multidifusión a grupos que utiliza datagramas para llevar a cabo la comunicación. Intercambio entre routers.
- Parte de la capa IP.

UDP: Protocolo de datagrama de usuario

- Como es en modo datagrama sé que trabaja sin conexión.
- Está en la capa de transporte; usa IP para el nivel 3.
- PDU se denomina **Datagrama UDP**
- Los programas que corren sobre UDP deben garantizar la confiabilidad necesaria.
- La ventaja que tiene es que es muy rápido (más que TCP). Inunda la red, no importa tanto si se pierde.
- No utiliza ACK
- Formato de datagrama UDP
  - También se divide en palabras.
  - Primera palabra: 16 bits para puerto de origen + 16 para puerto destino.
  - Segunda palabra: longitud de mensaje + suma de verificación.
  - Datos

No hay segmentación

A diferencia de TCP que utiliza segmentación UDP manda un datagrama completo y deja que IP lo fragmente si es necesario.

Detección de errores

Utiliza **detección** a través de un **Checksum** del datagrama UDP + direcciones IP + código de protocolo.
Transmisiones no confiables, sin validaciones; puede haber pérdidas; etc. Tiene varios problemas, pero los resuelven las capas superiores.

No hay control de flujo

No implementa

Conmutación

De paquetes.

Tamaño cabecera

8 Bytes.

TCP: Protocolo de control de transmisión

- Transferencia confiable de extremo a extremo.
- Es el más utilizado en internet, en ambiente LAN no es el más recomendado.
- Brinda confiabilidad.
- Permite comunicación peer to peer con el otro extremo.
- Está en la capa de transporte; usa IP para el nivel 3.
- Utiliza puertos para identificar la aplicación: Interfaz de socket: Permite a una aplicación cliente saber a qué aplicación pedirle el servicio (que sea su servidor):
  - Socket basado en service access point: Puerto
  - Socket basado en dirección lógica: IP

- ❖ Orientado a la conexión.
- ❖ PDU se denomina **Segmento TCP.**
- ❖ Modos de enlace/conexión:
  - ➢ Pasivo abierto: Un servidor espera pedidos
  - ➢ Activo abierto: Un cliente inicia pedido
- ❖ Encabezado mínimo 5 palabras de 32 bits.
- ❖ Tiene el MSS: Maximum segment size. Es la máxima longitud de tamaño de un segmento de datos que puede entregar a la capa inferior.
- ❖ Campos utilizados para sliding windows
  - ➢ Número de secuencia : Permite manejar varias sesiones. Para ordenarlo en el receptor.
  - ➢ Acknowledgement number: Número de acuse de recibo. Indica los octetos que puede recibir. Contiene el valor del siguiente número de secuencia que el emisor del segmento espera recibir.
  - ➢ Window: indica el número máximo de bytes pendientes de asentimiento.
- ❖ Items pasados a IP: Precedencia, retardo normal/bajo, flujo normal/alto, confiabilidad normal/alta, seguridad

Control de errores

- Detecta errores mediante el checksum del segmento TCP y direcciones IP.
- Corrige errores. Usa ACK y NAK en ARQ sliding windows.

Tiene número de secuencia para descartar paquetes duplicados e identificar los faltantes.

Entrega ordenada

El orden se logra debido de que a cada paquete se le asigna un número de secuencia consecutivo único, y el receptor usa los números para colocar los paquetes recibidos en el orden correcto.

Control de flujo

Mediante la ventana deslizante. Regula cuando hay retardo dentro de la red y cuando el receptor está desbordado.
Limita lógicamente el número de secuencia, sino podría ser infinito.

1. Al momento de la conexión se establece una reserva de bytes y se acuerda con el receptor cuantos bytes le puede mandar sin saturarlo.
2. Esa ventana deslizante va renegociandose según los retardos de la red.
3. Cuando todos los bytes fueron enviados
   a. Si no se recibieron los acuses de recibo por cada segmento enviado en la ventana el transmisor para de transmitir.
   b. El receptor envía un ACK indicando a que byte se refiere la confirmación y el siguiente segmento esperado. A nivel de cantidad de bytes esperados lo regula el transmisor.

El encabezado TCP utiliza un campo de 16 bits para informar al remitente del tamaño de la ventana del receptor. La ventana más grande que se puede utilizar es 2^16 = 64 kilobytes

Control de congestión

Congestionamiento: Retraso causado por una sobrecarga de datagramas en uno o más puntos de conmutación. La congestión se da en los saltos de red, no en el receptor como control de flujo.
Consecuencias: aumento de retrasos, descarte de datagramas, retransmisión de datagramas. Para evitarlo se pueden usar algoritmos:

- Disminución multiplicativa: Utilizando la ventana de congestión reduce la cantidad de segmentos exponencialmente que se están transmitiendo
- Arranque lento: Si estás en una etapa de crecimiento del tráfico, hacerlo crecer más lento.
- Jacobson/Karel: Se reduce la ventana a la mitad hasta un valor mínimo.

Retransmisiones: En los enlaces hay un retardo variable. Se mide el RTT (round trip time) del enlace para ajustar la espera. Se usa un promedio ponderado entre el valor medido anteriormente y el nuevo (smoothing). Cuando da un valor inferior entre el envío y la confirmación a la anterior detecta una congestión.

Segmentación

Tiene segmentación y reensamble

Multiplexación de puertos

Realiza multiplexado y demultiplexado de puertos:

- Ascendente: Un proceso de un nivel inferior le brinda servicios a varios procesos del nivel superior
- Descendente: Inverso ascendente. Esta técnica puede ser utilizada para proporcionar fiabilidad, rendimiento o eficiencia.

Conmutación

De circuitos. Utiliza circuitos virtuales. Hay una reducción del riesgo respecto al desorden. Pero como corre sobre IP no hay garantía de que no haya pérdida o desorden. IP no se entera del camino virtual.

Tamaño cabecera

20 Bytes.

Aplicaciones

- DNS (UDP): sistema de nombre de dominio. Traduce la dirección IP a un dominio pronunciable. Puede trabajar tanto en UDP como en TCP usando el mismo número de puerto. Tiene una estructura de árbol jerárquico. Entre los servidores usa TCP.
- PING: ICMP.
- SNMP (UDP): administración de red para automatizar intercambio de información.
- Logueo remoto:

- ➢ TELNET (TCP): protocolo que se utiliza para conexiones remotas. Permite manejar un dispositivo a distancia. Tiene autenticación. No es seguro, no se recomienda.
- ➢ SSH: Evolución de TELNET. Ambos son protocolos de nivel Aplicación, por lo que tanto cliente como servidor deben estar configurados en la capa 3 (IP).

❖ Transferencia de archivos:
- ➢ FTP (TCP): protocolo de transferencia de archivos con autenticación. Usa comunicaciones fuera de banda. TFTP (UDP): como FTP pero sin autenticación.
- ➢ SSL-FTP: Transferencias confidenciales
- ➢ SFTP: Transferencias con tunel SSH
- ➢ SCP: Transferencia con tunel
- ➢ TFPT(UDP): Trivial FTP. Más reducido que FTP, pensado para LAN, copia archivos enteros. Ambos extremos necesitan ACK o sino piden retransmisión generando duplicación de paquetes.
- ➢ NFS (UDP/TCP): Network file system. Sirve para administrar archivos, no para copiar. Opera en forma transparente (como si el remoto fuera local)
- ➢ RPC: Remote procedure call. Implementa NFS. Permite representar ítems de datos de computadoras heterogéneas

❖ Correo electrónico: La interfaz del usuario se ocupa de actualizar el correo. La transferencia de mensajes la maneja por separado.
- ➢ SMTP (TCP): Transmisión de correo saliente. Especifica formato de mensajes. Usa ASCII.
- ➢ POP3 y IMAP (TCP): transferencia de correo entrante. MIME es la variante segura.

❖ Web: La URI agrega información del contenido de la página.
- ➢ HTTPS/Navegación web (TCP): Un servidor proxy maneja la caché.

❖ Asignación de direcciones IP: En el ambiente LAN.
- ➢ ARP: Protocolo de resolución de dirección. Permite conocer la dirección MAC de la IP destino.
- ➢ RARP: Protocolo de resolución de dirección inversa. Permite que una máquina conozca su dirección IP mediante su dirección MAC.
  El mensaje ARP / RARP va en el encabezado de la trama.
- ➢ BOOTP (UDP): es una mejora del RARP. Asigna direcciones IP.
- ➢ DHCP (UDP): También asigna direcciones IP dinámicas en la misma red, es el más nuevo. Más nuevo que BOOTP. Eficiencia en seguridad y administración de IPs. En IPV6 embebe la dirección mac para lograr compatibilidad.

❖ Aplicaciones de voz y video
- ➢ Voz sobre IP: Paquetizar voz y, mediante varios protocolos, enviarla. Por ej en el meet escuchas voz sobre IP.
  - ■ VoIP ≠ telefonía sobre IP(UDP). El primero incluye al segundo. Las llamadas telefónicas pueden tener red IP y que pasen por servidores/switchs etc. El gateway está embebido en una central telefónica.
  - ■ FXS abonado; FXO central. EIM: Red y red de ambos lados. Utilizados para identificar a un puerto.

        - Protocolo H.323: Maneja la señalización de cómo se interpretan los paquetes de datos sobre Voz sobre IP en relación a la voz utilizando un gateway hacia la red.
    - ➢ Otros: SIP (UDP), SDP, Qos, RSVP

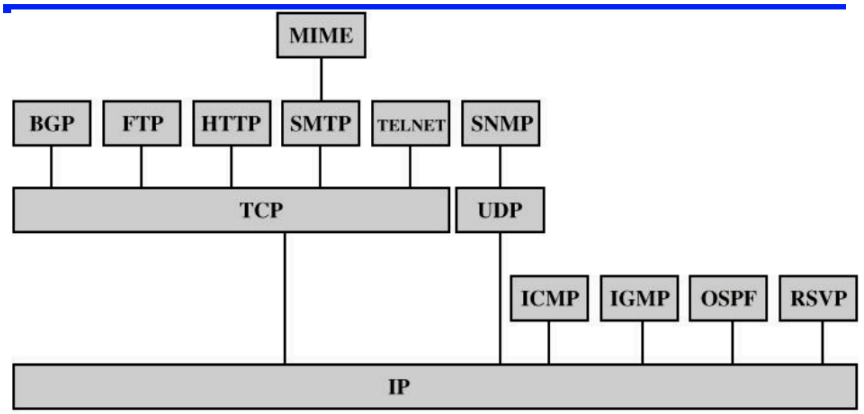
3 elementos para analizar estos servicios:

- Que estadística tiene respecto a errores: Si puede sufrir pérdida de datos.
- Ancho de banda: Capacidad del canal. Lo que es elástico es el uso del canal. Hasta donde lo usa.
- Sensible al retardo: Si le afecta o no el retardo.

Características de servicios

APLICACIÓN	PERDIDA DE DATOS	ANCHO DE BANDA	SENSIBLE AL RETARDO
Transf.archivos	No tolerable	Elástico	No
Correo	No tolerable	Elástico	No
Navegación web	No tolerable	Elástico	No
Telefonía	Tolerable	<1Mbps	<300 ms
Música	Tolerable	<1Mbps	segundos
Juegos	Tolerable	<10kbps	cientos de ms
Mensajes	No tolerable	Elástico	depende

Protocolos TCP/IP



BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

Protocol Family Enca

Layer 7 Application

Provides standard services to applications and end-user interfaces.

Layer 6 Presentation

Performs data format conversion. Provides compression, encoding, and encryption of data.

Layer 5 Session

Establishes sessions between services. Synchronizes and performs translations for naming services

Layer 4 Transport

Manages connections and provides reliable packet delivery. Operates in units of messages.

Layer 3 Network

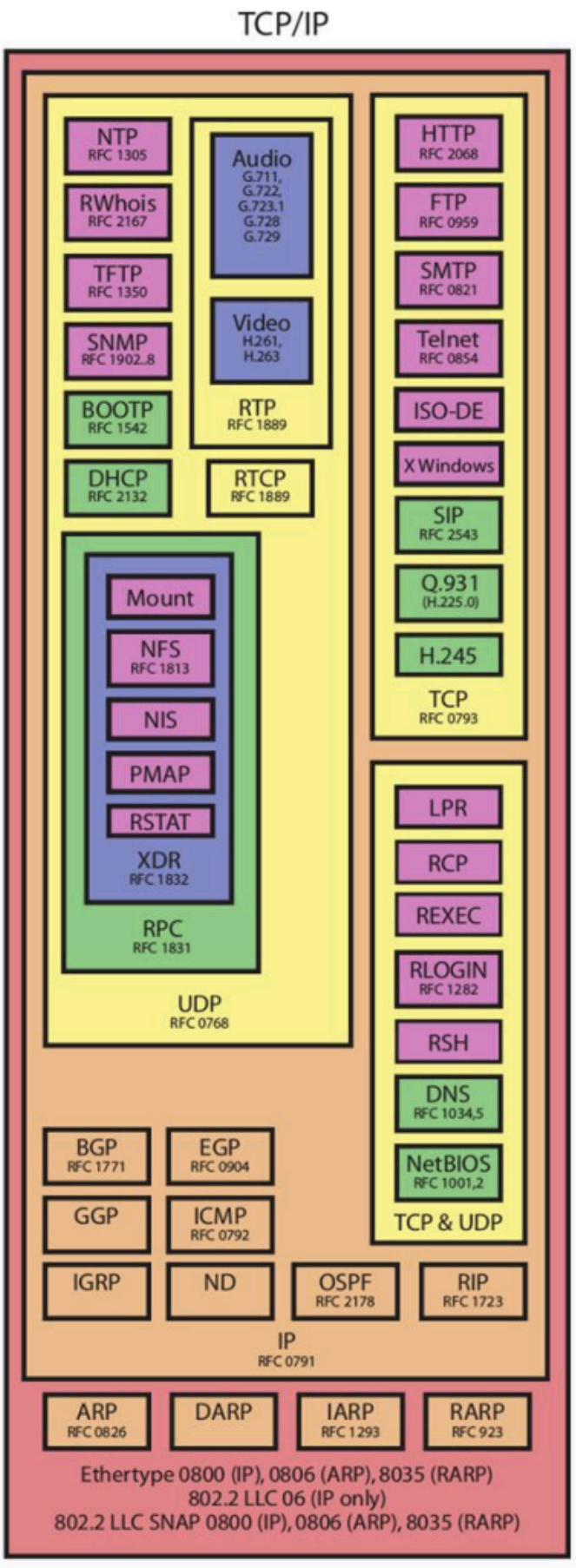
Addresses and routes datagrams. Performs fragmentation and reassembly (IP). Operates in units of packets.

Layer 2 Logical Link

Provides hardware addressing and error detection/correction. Operates in units of frames.

Layer 1 Physical

Defines connection, electrical, and wiring specifications. Operates in units of bits.



Router

Si recibe una dirección dentro de sus redes el ruteo es directo (entrega directa). Cuando le llega una dirección que no forma parte de su red tiene asignada a qué dirección mandarle para que redireccione.

Tabla de enrutamiento: Tabla que está en la RAM del router armada para saber por donde mandar los paquetes.

Estrategias de ruteo

- Vector distancia: Buscan el camino más corto basándose en las tablas de enrutamiento que le mandan sus vecinos. Puede recibir información errónea. No necesita un gran procesador, consume mayor ancho de banda. Es fácil de configurar.
- Estado de enlace: Tienen una base de datos de todos los enlaces que hay en ese sistema autónomo. Por medio de broadcasts cada router mide la menor distancia a cada red. Con todos los que comparte información se tiene que lograr una convergencia. Consume menos ancho de banda. Necesitan un procesador interesante. Pueden rearmar rutas. Es mejor, necesito router con mayor capacidad de RAM y procesador. Para averiguar la ruta conveniente se fijan en varios criterios: retardo, ancho de banda, cuánto demoró la rta, si hubo pérdida de datos, costo, estabilidad, tolerancia a fallos, etc. Quizás hace más saltos pero es más rápido.
    - Por ej: OSPF: Hace la difusión a los routers vecinos.

Solución a los bucles de enrutamiento:

- Cantidad máxima de saltos: Por ej RIP tiene máximo de 15 saltos. Cuando llega al salto 16 descarta la trama
- Horizonte dividido: El vecino manda la tabla de enrutamiento pero no se puede compartir. No se puede compartir una tabla que te compartieron a otra.
- Actualización Inversa
- Actualización desencadenada

IP V6

- Razones para el cambio:
    - Se agotan las direcciones IP:
        - El direccionamiento de dos niveles (red y computadora) desperdicia espacio
        - La dirección de red se usa aún si no se conecta a Internet
        - El crecimiento de las redes y de Internet
        - El uso extendido de TCP/IP
    - Hay una sola dirección por computadora
- Mejoras: 128 bits para dirección; formato de encabezado más flexible; mecanismo de opciones mejorado; funcionalidad para asignación de recursos.
- Fragmenta en los extremos (en vez de en la nube) para bajar los tiempos de latencia (o retardo).

- Opera en modo datagrama (sin conexión)
- PDU se llama paquete que tiene cabecera de longitud fija, de 40 octetos. Mejora el procesamiento.
- Encabezado (40 bytes) + 4 palabras de origen y destino
- Cabecera:
    - Hay 8 bits para servicios diferenciados y notificar congestión.
    - Etiqueta de flujo para identificar los paquetes según el tratamiento que hay que darle (MPLS surge en v4 para darle esta funcionalidad de etiquetas).
    - Longitud de carga (más allá de los 40 bytes).
    - Cabecera siguiente.

Direcciones IPv6

- Se asignan a interfaces individuales de nodos.
- Eficiencia mejorada en el encaminamiento: se combina dirección larga y múltiple por interfaz.
- Como las clases desperdiciaban varias combinaciones, en IPv6 solamente se usa CIDR (/27), sin clases.
- Se usa notación hexadecimal con dos puntos para facilitar el manejo. Son 16 Bytes.
- Tipos de direcciones:
    - Unicast: unidifusión, apuntan a una sola interfaz.
    - Anycast: monodifusión, la dirección IP identifica a un conjunto de interfaces, pero le entrega a la más cercana, según el protocolo de enrutamiento.
    - Multicast: multidifusión, el paquete se entrega a todas las interfaces incluídas. Diferencia con broadcast: el broadcast apunta a todas las de la red, el multicast solo a las que tiene incluídas. Clase D.

Redes WAN

- Vinculan redes LAN ubicadas en edificios mediante enlaces punto a punto
- Mientras las LAN pertenecen a los usuarios, los enlaces WAN pertenecen a los proveedores de servicios
- A diferencia de en una LAN, en la WAN hay interoperabilidad entre distintas tecnologías, cada router puede tener una tecnología distinta.
- Se compone de
    - Red de transporte (backbone)
        - Principales conexiones troncales de Internet
        - Problemas:
            - Problemas de congestión y cómo se controlan
            - Necesidad de priorizar tráfico
            - Mejorar rendimientos
        - Tres tipos de routers unidos por enlaces:
            - Servidores de acceso remoto (RAS) en los POP con muchos puertos de baja velocidad.
            - Router troncales o de backbone con pocos puertos de alta velocidad vinculados a Internet o a otros proveedores.
            - Concentradores que unen varios POP hacia los router troncales, con características intermedias

- ➢ Redes de acceso
  - Incluye el equipamiento del cliente y los enlaces hasta el punto de presencia (POP) más cercano de la red del proveedor
  - Se conectan a la red backbone
  - Pueden ser cableadas o no cableadas.

Conmutación de circuitos

Se genera un vínculo físico en el conmutador y se viaja mediante un enlace a otro conmutador donde se establece un vínculo físico y se viaja por otro enlace, etc. Hay una reserva de recursos para la comunicación entre A y B, o sea que nadie puede usar ningún tramo de ese camino. Los paquetes llegan en orden. Uso eficiente para voz e ineficiente para datos. Transmisión continua. Tiene un ancho de banda fijo. La congestión bloquea el establecimiento. Elige el encaminamiento más rígido. Tiene retardo de establecimiento de conexión.

Conmutación de paquetes

Transmisión en paquetes. Uso eficiente para datos y menos para voz. Menos costoso. AB dinámico (ventaja). En el órgano de conmutación hay paquetes de múltiples comunicaciones, no es dedicado. No hay monopolio de recursos. Si hay mucha gente usando se puede congestionar. Elige la ruta menos costosa en retardos y cantidad de saltos.
Modos de operación puede ser:

- ❖ Circuitos virtuales: con conexión (virtual); se establece un camino para esa conexión y todos los paquetes viajan por el mismo, uno atrás del otro. Pueden haber varios circuitos de enlaces viajando por el mismo camino. Los paquetes llegan en orden. La congestión bloquea el establecimiento y aumenta el retardo. Tiene retardo de establecimiento de conexión y de transmisión de paquete. Ej: **TCP**
- ❖ Datagrama: sin conexión; cada datagrama puede tomar diferentes caminos. No mantiene el orden de los datos. La congestión aumenta el retardo de paquetes. Tiene retardo de transmisión de paquete. Ej: **UDP, IP**

Tipos de enlace

Dedicados

El medio puede estar compartido pero la capa de enlace establece una comunicación lógica punto a punto. No garantizan el ancho de banda.

Protocolo PPP

Utilizado para conectarse al ISP, y mediante él se accede a Internet. **Se establece un enlace dedicado** con el ISP.

- ❖ Funciona sobre el enlace: Capa 2. Define a la subred de acceso.
- ❖ Ofrece autenticación a diferencia de HDLC.
- ❖ Se usa para armar redes privadas virtuales (túneles)
- ❖ Emplea ARQ ventana deslizante.

- En la capa de enlace se puede usar TCP de manera de mandar datagramas con enlaces dedicados (puede tener cable compartido).
- Provee servicios de:
  - Configuración de enlace: En la capa física se utilizan enlaces de tipo SDH, E1/T1, modems dedicados.
  - Autenticación
  - Transporte de datos, asegura el enlace y recepción ordenada
  - Multiplexación de protocolos de red (IPX, IP): Hoy no se usa ya que IP está arriba y lo hace.
  - Testeo de calidad de enlace: Velocidad, rendimiento, confiabilidad.
  - Asignación dinámica de direcciones IP
- Fases de la operación
  - Enlace muerto. La capa física no está lista, Detecta la presencia del dispositivo y/o portadora. La levanto diciendo qué protocolo usar
  - Establecimiento del enlace: Orientado a la conexion- Se intercambian tramas LCP para configurar el enlace: MRU (unidad máxima de recepción), etc.
  - Validación: - Autenticación: Proceso PAP o CHAP - LCP
  - Red: El protocolo NCP configura el protocolo de red.
  - Intercambio de datos: Se intercambian paquetes de datos y LCP(control de enlace) y NCP(control de red)
  - Terminación de enlace
- Tiene dos protocolos:
  - *LCP - Control de enlace - (Link Control Protocol).*

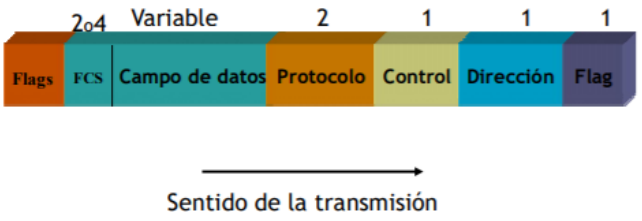
    El control se hace fuera de banda (por un lado van datos y por otro control).
    - Se realiza la autenticación. No se pasa a la etapa NCP sin haberla completado:
      - PAP: Poco seguro, envia clave junto con la identificación de la estación del cliente.
      - CHAP: Tiene intercambio de claves a través de hash.

    Detección de errores: Mediante CRC

  - *NCP - Manejo de red: (Network control protocol)*

    Funcionamiento de PPP con NCP: establecimiento ⇒ autenticación (si falla termina) ⇒ red ----NCP----> se activa la red ⇒ termina.

Trama de capa de enlace



Protocolo HDLC (High-Level Data Link Control)

Enlace dedicado. Control dentro de banda, hay un solo protocolo y diferentes tipos de tramas. No tiene autenticación.

- Funciona sobre el enlace de datos: Capa 2
- Establece enlaces dedicados punto a punto y punto a multipunto.
- Sincrónico, orientado al bit, con ARQ ventana deslizante + CRC - 16.
- A **diferencia de PPP**, no tiene autenticación (tendré que hacer algun tunel IP)
- Estaciones
  - Primaria: Controla la operación/funcionamiento del enlace. Las tramas generadas por esta estación se llaman órdenes. Proveedor da servicio a múltiples estaciones. Mantiene enlaces separados por cada estación secundaria: Hace division lógico
  - Secundaria: Sus tramas son respuestas a los comandos de la primaria. El control del enlace lo hace la primaria.
  - Combinada: Maneja comandos y respuestas
- Configuraciones
  - Balanceado: Dos estaciones combinadas. Permite que las dos estaciones trabajen como maestro/esclavo o primaria/secundaria simultáneamente, el enlace se ajusta a lo que el transmisor y receptor necesitan.
  - Desbalanceado: Una estación primaria y una o más secundarias. Pregunta si están todos listos para transmitir.
- Distintos modos de gestionar el enlace según lo que corre arriba/ modos de operacion
  - NRM: Modo de respuesta normal. Configuración **desbalanceada**. enlace punto a punto o punto a multipunto; half dúplex. Es el único que **permite multipunto**.
  - ABM: Modo **balanceado** asíncrono. Cualquier estación puede transmitir sin tener que pedir permiso a otro punto del enlace. **Full- duplex**, resulta **más eficiente**, al no realizar sondeos.
  - ARM: Modo de respuesta asíncrona. Configuración desbalanceada. El control del enlace lo hace la primaria pero da control a secundaria para transmitir sin permiso. Cada estación se comporta como primaria y secundaria; enlace punto a punto; Full - dúplex. Las estaciones pueden estar transfiriendo al mismo tiempo. Es poco usado.
- Delimitación: línea inactiva (01111111); bandera (01111110) - sincronismo de bloque.
- Transparencia: procedimiento por el cual se evita que se confunda información de datos con información del protocolo. Se resuelve mediante inserción (en el transmisor) y eliminación (en el receptor) de bit 0 en secuencia similar a la bandera. Si 11111, se inserta un 0 en el transmisor; si 111110, se elimina 0 en el receptor. Bit stuffing.
- **Control de errores, control de enlace** (dentro de banda): Dependiendo el campo control: Los primeros bits identifican el tipo de trama.
  - Trama I (información) => 0: datos
  - Trama S (supervisión) => 10: es una trama de supervisión (controla errores por **ARQ, parada y espera**).
  - Trama U (no numerada) => 11: controla el enlace, estado caidas

        - Bit de poll/final: Su uso depende del contexto
- **Detección de errores**: Campo FCS

Conmutados

Tienen el protocolo de enlace en el nivel de la subred de acceso (protocolo de capa 2) y otro protocolo para la subred backbone (encaminando en circuitos o paquetes el movimiento de las PDUs a través de la subred backbone). x.25 y Frame Relay

Protocolo x.25

Define una interfaz entre DTE y DCE. Opera en capas 1, 2 y 3 del modelo Osi. Orientado a la conexión (**circuitos virtuales**). Red de **conmutación de paquetes**, transmisión sincrónica. Enlaces poco confiables.

- Mucho overhead debido a encabezados de capa 2 y 3, múltiples controles entre nodo y nodo tanto en subred de acceso como en red backbone

Control en capa 2 y 3 se hace dentro de banda
Capas:
X.25 en capa 2, Enlace: Protocolo

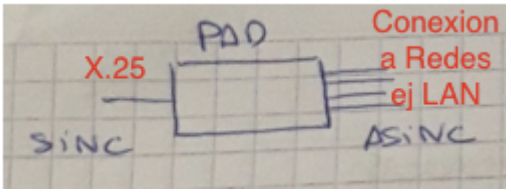
LAP-B hijo de HDLC

- Hace la **conmutación de circuitos**: decidir el enlace y decidir el camino lógico. Establece y gestiona el circuito.
- Servicios que otorga:
    - Circuito virtual externo: Conexión lógica entre DCE-DTE. Cada circuito virtual externo se corresponde con uno interno y viceversa. Administran acceso entre origen y destino a cada canal lógico. Conexión local.
    - Circuito virtual interno: Conexión lógica de una ruta específica planeada a través de la red x.25 (entre cada conmutador). De un DCE a otro.
      Los circuitos virtuales o o canal lógico se forma entre los dos pares DCE - DTE de cada extremo.
      Control de flujo: Con ARQ ventana deslizante; confirma mediante piggyback.
    - **Control de errores**: Mediante checksum
- Permite una transmisión full dúplex;
- Circuito virtual:
    - Permanente-> PVC: establezco conexión y la mantengo, es la que mas se usa
    - Conmutado-> SVC: Bajo demanda.

x.25 en capa 3

- Multiplexa hasta 4096 caminos lógicos en un camino físico.
- Dentro del circuito establecido por la capa 2, se mira el destino y se enruta hacia el destino.
- Define cómo se mueve entre router y router.

- El encabezado agrega información de **control**, provee números de secuencia para **controles de flujo y errores**, identifica circuito virtual. **Cada nodo** hace este control. Más lento. **Hay doble control, en capa 2 y 3.**
- Se puede operar en:
  - Modo paquete: sincrónico total, toda la red, incluida la nube. Canales lógicos. x.25.
  - Modo caracter: requiere un dispositivo PAD (ensamblador/desensamblador de paquetes). Hasta el PAD es sincrónico, después hay n canales asincronos.



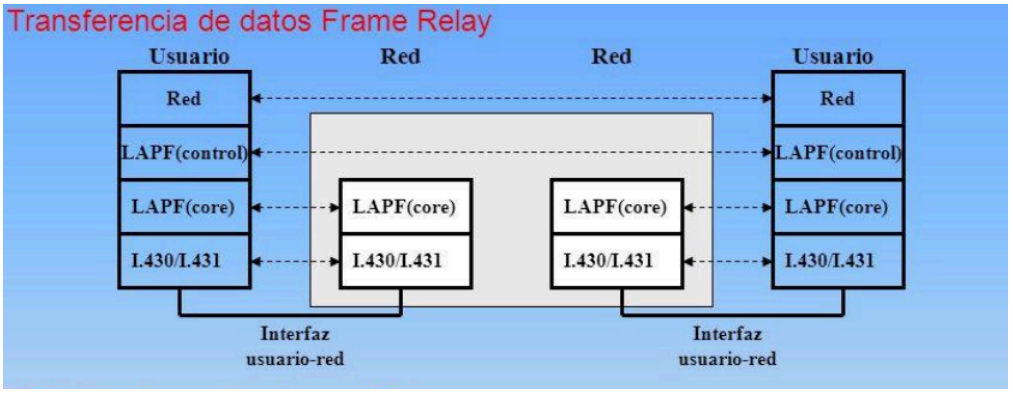
Protocolo Frame relay

- Es una técnica de conmutación rápida de paquetes (como X.25).
- Luego de X.25, viene a mejorar el rendimiento quitando la capa 3 y esa lógica alivianandola y la coloca identificando de manera local los controladores de cada circuito virtual.
- La nube de FR es compartida por varios dispositivos, es una red pública.
- En la nube hay el menor procesamiento posible: el **control de errores** más robusto, de flujo y de secuencia se hace en los extremos ⇒ > velocidad; < latencia.
- El ancho de banda se asigna dinámicamente, según necesidad.
- Se utilizan circuitos virtuales PVC, pero en capa o nivel 2, X.25 lo hacía en capa o nivel 3.
- A los canales se los denomina DLCI: se agrupan y constituyen los circuitos virtuales.
- Define la interfaz entre CPE (FRAD) y POP. Entre POPs existe DLCI al igual que entre CPE y POP.
- En nivel 2 están LAPD y LAPF, con el primero realizando control fuera de banda
- FRAD (Frame relay access device): Dispositivo de acceso a la red Frame Relay. La diferencia con PAD es que ambos lados son sincrónicos en FRAD.
- **Arquitectura:**

Existen dos planos de operación en Frame Relay

- Plano de control:
  - Se implementa entre usuario y red.
  - Lleva la información necesaria para el buen funcionamiento de la red
  - Establecimiento y libera de las conexiones lógicas.
  - *Protocolo: **LAPD**:*
    - **Control de errores** (CRC) **y flujo** en temas propios del funcionamiento de la red, entre usuario y red y en cada salto de la red (entre POPs)
    - Control de enlace
- Plano de usuario:
  - Lleva a cabo la transferencia de datos de usuario
  - Actúa de extremo a extremo (entre usuarios)
  - DLCI: Identificador de conexión del enlace de datos

        - Hay hasta 1024 combinaciones posibles.
        - Representa el numero del camino virtual correspondiente a una conexión en particular.
    - ➢ Lo que hacía X.25 a nivel 3 acá lo hace **multiplexando** dentro de enlaces lógicos (DLCI) con un identificador para multiplexar tramas de múltiples terminales. Se mandan datos de distintos usuarios en el mismo camino lógico.
    - ➢ *Protocolo: **LAPF**:*
        - LAPF control: **control de flujo**.
        - LAPF core
            - **Congestión en la nube:** Prevención de congestión mediante FECN (congestión hacia delante) y BECN (congestión hacia atrás). Control de congestión mediante descarte (bit DE)**.**
            - **Detección de errores** mediante CRC. La corrección la hacen los extremos.



- ❖ *Diferencias con X.25*
    - ➢ Multiplexacion y conmutacion en capa 2 (elimina procesamiento de una capa), da mayor performance
    - ➢ Se abaratan los costos con CIR
    - ➢ No hay control de flujo ni de errores salto a salto mejorando rendimiento/velocidad de transmisión, en redes confiables no es necesario, este control lo hacen las capas superiores.
    - ➢ No hay calidad de servicio (QoS), lo hacen capas superiores. Por ej TCP/IP lo utilizaba.
    - ➢ Mejora rendimiento, pasa de 64Kbps a 2Mbps, retardo en envio de tramas es mucho menor
    - ➢ Mientras que en X.25 si el error es mayor a 10^-4 no lo soporta, frame relay soporta hasta errores de 10^-7
    - ➢ Cada usuario envía tramas de datos de fuentes destino y espera ACK de capas superiores
    - ➢ Usa control fuera de banda
    - ➢ Trafico en ragafas: Optimiza el ancho de banda en un 35%. Más redituable a pesar del descarte.
    - ➢ Tiene circuitos virtuales permanentes

Protocolo ATM (Modo de Transferencia Asincrónico)

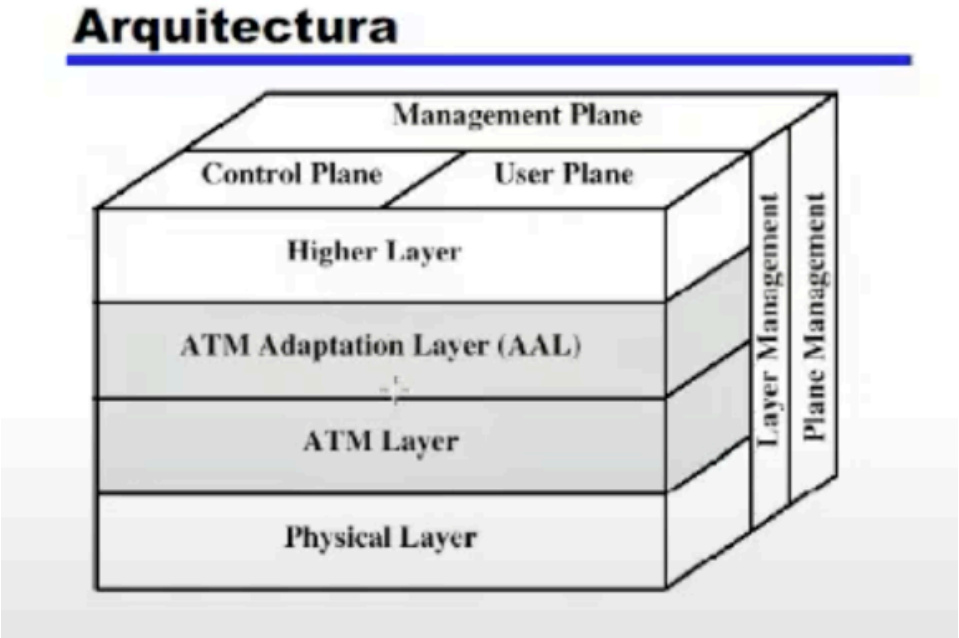
- Surge para mejorar las Qos (quality of service). Evolución de Frame relay.
- Red de conmutación de paquetes en fragmentos fijos
- Optimiza y gestiona fuera de banda.
- Crea una arquitectura de dos dimensiones, capas y planos.
- Permite velocidades de 25 Mbps a 622 Mbps
- Comunicación full duplex.
- Tiene un header muy elemental pero muy robusto. Es muy eficiente porque los bytes del header son utilizados dependiendo cual es la capa o plano que lo necesita
- Tiene mínimo control de error y flujo, debido a que las redes físicas fueron más confiables (fibra)
- La PDU se llama celda o célula, se transporta sobre canales sincrónicos y tiene un tamaño pequeño y fijo ⇒ < retardo; < memoria; > fragmento.
- Permite transportar todo tipo de servicio. Usa capas de adaptación para integrar sus servicios. Conmutación rápida con muy bajos retardos. Normalizado por la UIT.

¿Por qué es asincrónico? las celdas se transportan sobre canales sincrónicos, pero ningún usuario tiene reservado en forma fija un espacio en el flujo de las celdas, se asignan dinámicamente por demanda.

Caminos y canales virtuales

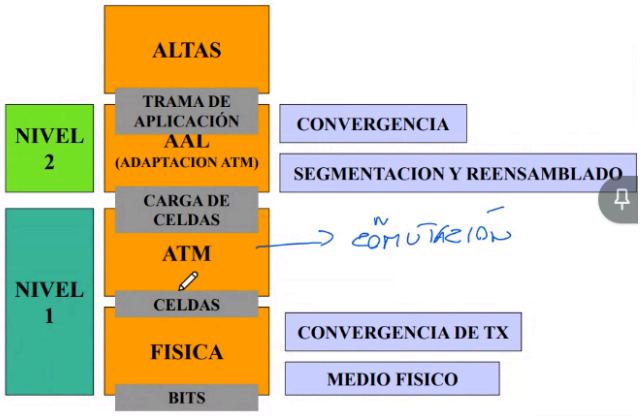
- **VC (Canal virtual)**: tiene uno o más destinos; es similar al circuito virtual de x.25 y FR. El VCI (identificador) se puede repetir. Vincula usuario con usuario. Unidad basica de conmutación.
- **VP (Camino virtual):** se agrupan los VC con los mismos destinos en una unidad ⇒ facilita gestión y conmutación. El VPI no se puede repetir. Vinculan router origen con router destino. Extremo a extremo
- La combinación de estos permiten mejorar y distinguirla de las anteriores:
  - Arquitectura simplificada a través de los caminos virtuales (toda la lógica de separar en planos y capas permite que se organice de manera simple, si todos los canales virtuales van al mismo destino, están en un camino virtual único, cada nodo ATM tiene menos procesamiento)
  - Mayor calidad de servicio: Se separa tipo de dato a enviar en caminos virtuales. Reduce costos, los canales van cambiando según las necesidades del usuario. El plano de gestión maneja esto.
  - Integridad de secuencia de llamada: Permite establecer el acceso a la red y mejorar su integridad en términos lógicos.
  - Posibilidad de monitorear el tráfico y medirlo
  - Restricciones: No se pueden agruparse en canales virtuales cruzados

Arquitectura



Tres planos

- Control: Es fuera de banda.
  - Busca buen funcionamiento de la red
  - Genera y maneja las peticiones de señalización.
  - Se encarga de de los controles de llamada y conexión.
- Usuario: Transfiere información del usuario
- Gestión: Funciones de administración de la capa y funciones de administración del plano. Se establecen buffers, parámetros, etc.



- *Tres capas*
  - De adaptación de ATM o AAL: Se arma la carga de la celda. Hace de middleware entre ATM y todo lo que venga de arriba, lo organiza para que queden en celdas ATM de 53 bytes.
    - Servicios que ofrece:
      - **Manejo de errores** de transmisión
      - **Segmenta** y rearma: Para organizar porciones de 48 bytes (+ 5 de header). Le agrega SAR para poder volver a ensamblar en destino

- Maneja celdas perdidas y mal insertadas
- **Control de flujo** de los enlaces y temporización pudiendo descartar tramas
- **Multiplexación**
- Inducción y extracción del header.
- Convergencia de tx: independiza la velocidad del flujo de celdas de la interfaz física.

■ Arriba puede ir IP, Frame Relay, etc.

➢ De ATM: Coloca el header en la celda. **Conmutación**. Utiliza una **clase de servicio** según lo que tenga que hacer.

➢ Física.

Clases/categorias de servicios de ATM

❖ De tiempo real: trabajar con información sensible a los retardos
  ➢ CBR**:** velocidad constante, ej: videollamada, circuito E1, audio y video sin comprimir
  ➢ rt-VBR**:** velocidad variable, ej: envío de video, compresión.

❖ De tiempo no real: no es tan grave si hay delay.
  ➢ nrt-VBR: velocidad variable, ej: mail, multimedia.
  ➢ ABR: velocidad a disposición, varía según la necesidad, ej:tráfico de ráfagas interconexiones de LAN.
  ➢ UBR: velocidad no especificada. Aprovecha la capacidad que está sin usar. Best effort. Ej: FTP en segundo plano, IP (best effort)
  ➢ GFR: de tramas garantizadas, ej: Servicio a conexiones troncales IP

Interfaces

❖ UNI (interfaz usuario - red): como es de usuario a usuario tiene los bits de control de flujo.
❖ NNI (interfaz red - red): tiene más bits de VPI ⇒ mayor capacidad para gestionar trayectos virtuales.
❖ Según cuál se use va a haber una diferencia en el encabezado de la celda.

Diferencias ATM y Frame relay

❖ ATM manda un tamaño de datos fijos (48 bytes) + 5 de header, PDUs de 53 bytes, permitiendo que no se saturen los conmutadores intermedios.
❖ ATM optimiza los circuitos agrupando múltiples circuitos virtuales que van a un mismo destino en caminos virtuales. Optimiza la sobrecarga de información en la subred backbone.

Diferencia con IP

Los paquetes son de longitud fija a diferencia de IP y Frame relay

Comparación entre protocolos:

Comparación

x.25 < FR < ATM

Decidir camino a tomar en la red backbone:

- ❖ IP no tiene un camino preestablecido y puede cambiar dependiendo la tabla de enrutamiento del momento
- ❖ X.25 (en capa 2), frame relay una vez que se establece el camino no cambia.
- ❖ ATM decide hacia donde manda la celda ATM en base al identificador del camino. El circuito virtual no va a cambiar (usuario A se comunica con servidor Z), puede cambiar el camino virtual. Va cambiando en cada salto, si llega a un salto y encuentra varios circuitos hacia el mismo lado va a ponerle el mismo camino.

Comparación entre sistemas

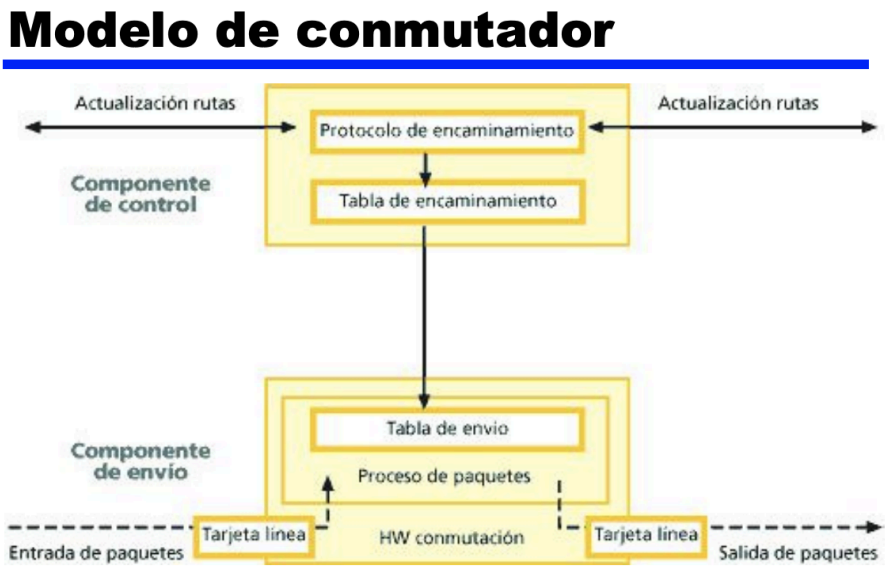
	TDM	X.25	FRAME RELAY	ATM
Facilidades	Muy pocas	Muchas	Pocas	Pocas
Velocidad	Alta	Media	Alta	Muy Alta
Retardo	Muy bajo	Alto	Bajo	Muy bajo
Throughput	Alto	Bajo	Alto	Muy alto
Coste CPE	Bajo	Bajo	Bajo	Alto
Overhead	Bajo	Bajo	Bajo	Alto
Puerto Comp.	No	Sí	Sí	Sí
Tipo tráfico	Cualquiera	Datos	Datos/voz	Multimedia

- Facilidades: Servicios que da en concepto de dificultad
- Velocidad
- Retardo: Complejidad en la subred backbone por tener que encaminar o dado por perdidas o sobrecarga.
- Throughput/rendimiento/performance: En ATM debido al control fuera de banda, achico header y campo de datos.
- Coste CPE
- Overhead: En ATM se debe a los planos y capas, pero hace un rendimiento muy alto ya que son muy pequeñas

MPLS (Multi Protocol Label Switching)

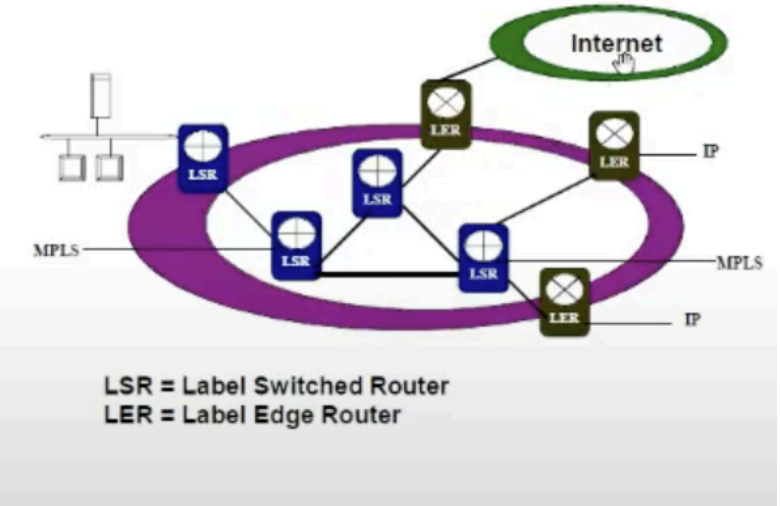
Permite manejar de manera más eficiente tráficos de distinta naturaleza. El enrutamiento IP está dentro de los datos de MPLS.
Se considera como: un sustituto de IP sobre ATM, un protocolo para hacer túneles, una técnica para acelerar el encaminamiento de paquetes. Integra los niveles 2 y 3.
Busca resolver los problemas de routeo y camino más corto.

- Conmuta etiquetas para múltiples protocolos. Soporta FR, ATM, SDH, etc.
- Cabecera genérica: datos usuario + cabecera IP + cabecera MPLS + cabecera nivel 2
- Funciona sobre cualquier tecnología de nivel 2 (PPP, LAN, FR, ATM, etc).
- Integra los niveles 2 y 3 del modelo OSI, el nivel 3 por IP que le provee un buen control de enrutamiento y el nivel 2 por ATM que provee conmutación rápida.
- Etiqueta: identificador corto de longitud fija, con significado local. Identifican un FEC. Los paquetes pueden tener más de una etiqueta.
- **FEC** - Forwarding equivalence class:
  - agrupación de paquetes que comparten los mismos atributos y/o requieren el mismo servicio.
  - Conjunto de paquetes que comparten tramos pero tienen distintos destinos.
  - Según la FEC, se tienen diferentes caminos (**LSP** - camino de conmutación de etiquetas)
  - La FEC se asigna al entrar a la red MPLS. **En cada router se decide si hay que actualizar la FEC**, los paquetes que van por una ruta puede ser que tengan que salir de ella.
  - En cada router solo se analiza la etiqueta y **se procesa por hardware**, más eficiente
  - Un paquete puede llevar varias etiquetas en una pila LIFO para atender varios caminos virtuales



- **PHB** - Per hop behaviour: Cambia el comportamiento de la red MPLS en cada salto, ya que la calidad de servicio requerido hace que se modifique los caminos en cada salto.
- Diferencia con circuitos virtuales: En los circuitos virtuales la ruta se arma en los extremos y en la red backbone no se va cambiando, acá se va optimizando todo el tiempo.
- Clases de servicio: Dependen del tipo de tráfico que se necesite, clasifica el flujo de tráfico a partir de lo que dice la capa 3. No es lo mismo que QoS o ToS.
- Routers:
  - Hay dos tipos:
    - De borde: Convergen con el mundo IP (LER)

        - Analizan el encabezamiento IP para decidir la ruta (LSP -> todo el camino completo)
        - Agrega y quita etiquetas a los paquetes
    - De backbone: En un mundo MPLS puro están los LSR.
        - Encaminan el paquete según la LSP: Puede ser que un nodo tenga reserva de recursos o distinta priorización o restricción de rutas.
        - Hacen ruteo según OSPF



➢ Almacenan una LIB (Label Information Base) y las tablas de encaminamiento pasadas por OSPF.

- **Túneles**: Mejoran la topología de manera lógica, si se cae un enlace físico el camino lógico puede seguir estando. La ingeniería de software es quien se encarga de esto.
- Control de información: generación de tablas de envío que establecen los LSPs.

Ingenieria de trafico

- Inteligencia que se le puede poner a las redes para el manejo de ruteo. Decidir más allá de lo que diga la tabla de ruteo.
- Optimiza la operación de la red en capa 3
- Fija objetivos para mejorar el tráfico o reducir los recursos
- La existencia de congestión indica que los recursos son escasos o las rutas mal elegidas
- Se debe monitorear la red, fijar políticas y tomar acciones mediante comandos
- Se mide la proporción de recursos libres en cada nodo

En MPLS

- Controla bien la carga de los enlaces
- Automáticamente se recupera de fallas y optimiza la operación
- Trabaja con MPLS CoS: Para dar soporte a diferentes clases de servicios.
- Integra control de capa 2 con ruteo de capa 3: permite que se controle como si fuera de capa 2 pero con la lógica de ruteo (mejor camino) de capa 3
- Beneficios de capa 2 y de IP en un solo equipo

VPN en MPLS

- ❖ Busca establecer canales lógicos, punto a punto, de manera que el ISP ofrezca en la red backbone caminos garantizados.
- ❖ La información de ruteo se distribuye sólo a los routers que pertenecen a la VPN
- ❖ Permite transitividad, A se conecta con B, y B con D, a puede llegar por VPN a D
- ❖ Permite que el ruteo sea más simple y conectar intranet contra intranet sobre internet
- ❖ Da seguridad
- ❖ En los bordes se establecen los túneles, en todos los routers intermedios viajan como túneles, las etiquetas MPLS se intercambian en un subgrupo de LSR (bordes). La ingenieria de trafico se restringe a los LER y los CPE (equipos del cliente)

MPLS y ATM

- ❖ Pueden coexistir. Tienen funcionalidades distintas, ATM se puede ocupar desde el usuario al ingreso a la red, y MPLS funciona desde los bordes de la red hasta ingresarlos en la red MPLS.
- ❖ ATM incorpora
  - ➢ Interfaces entre usuario, red y red privada
  - ➢ Troncales de voz
  - ➢ Emulación de circuitos
  - ➢ Hace capa de adaptación
- ❖ MPLS incorpora
  - ➢ VPN
  - ➢ Clase de servicio: CoS, prioridades para los paquetes
  - ➢ Ingenieria de trafico

Problemas que resuelve de IP

- ❖ Permite redes con distintas tecnologia
- ❖ Optimiza el enrutamiento
- ❖ Da QoS distinta a cada aplicacion de los usuarios.
- ❖ La ingenieria de trafico mira mas alla de la mejor ruta (IP solo miraba el destino y elige el mas optimo, manda todos por ahi).

- IP: Cada equipo conmuta paquetes en base a la dirección IP, manda por una ruta todos los paquetes que van al mismo **destino**
- MPLS: manda por mismos tramos paquetes que pueden o no ir al mismo destino, pero comparten algun/os tramos con la misma necesidad de calidad de servicio. Cuando dejan de hacerlo se separan.

Contratación de servicios

QoS: Lo decide el usuario. Para garantizar QoS los proveedores ofrecen ToS.
Parámetros de QoS: Retardo, variación del retardo y confiabilidad (reliability)
Calidad de servicio requerido según el tipo de tráfico

	RETARDO	VARIACIÓN DEL RETARDO	RELIABILITY
CORREO	BAJO	BAJO	ALTO
TRANSFERENCIA DE ARCHIVOS	BAJO	BAJO	ALTO
BASE DE DATOS	BAJO / MEDIO	BAJO	ALTO
VIDEOS (MPEG)	ALTO	MEDIO	BAJO
TELEFONÍA	ALTO	ALTO	BAJO
VIDEOCONFERENCIA	ALTO	ALTO	BAJO

CoS: Lo decide el usuario. El proveedor dispone distintas clases de servicio.
Tipos de servicio ToS: Como los protocolos dan el servicio al protocolo superior. Vienen definidos en algunos protocolos para organizar el procesamiento en los conmutadores.

Seguridad en redes

- Ataques: interceptación; fabricación; modificación; destrucción.
- Riesgos:
  - error humano; fugas de información; exceso de confianza
  - priorizar beneficios sobre los riesgos ⇒ ataques.
- Hay diferentes acciones para tomar según cada capa del modelo OSI:
  - Capa 1: auditar el canal; análisis de topolofía; AP; potencias y frecuencias.
  - Capa 2:
  - Capa 3: manejo de routers; logs; ARP y direccionamiento IP.
  - Capa 4: auditar establecimiento de sesiones; operaciones con conexión (TCP) y sin (UDP).
  - Capa 5: control de sesiones
  - Capa 6: criptografía.

Criptografía

Algoritmo que altera el mensaje en función de una clave; más grande la clave ⇒ menor posibilidad de romper por fuerza bruta
Autenticación: establece la identidad. El mensaje debe provenir de quien dice que proviene
Integridad: asegura que los datos no fueron alterados.
Confidencialidad: asegura que nadie puede interpretar los datos, más allá del transmisor y del receptor
Vinculación o No repudio: asegura que quien envió el mensaje es quien dice ser y no puede negarlo.
Tipos de encripción:

- **Simétrica / clave secreta:** única clave común, mismo algoritmo para encriptar y desencriptar. Se usa en gral para encriptar el contenido de mensajes. Ej: DES, 3DES, AES
- **Asimétrica / clave pública:** 2 claves; los extremos pueden usar algoritmos distintos para encriptar y desencriptar; cada extremo tiene una clave pública y una privada; se usa para garantizar integridad, confidencialidad, no repudio y autenticación

- **Para garantizar confidencialidad:** A y B crean sus claves y las intercambian → cuando A quiere mandarle un mensaje a B, encripta el mensaje con la clave pública de B y B la desencripta con su clave privada.
- **Para garantizar la autenticación y el no repudio:** doble encripción; A encripta el mensaje con su clave privada y con la clave pública de B.
- **Para garantizar la integridad**: se usan las funciones de hash.

Firma digital: se encripta un digesto para confirmar identidad y garantizar integridad. Se basa en criptosistema asimétrico (clave pública y privada); utiliza hash; interviene una autoridad certificante. **Provee autenticidad, integridad y no repudio, confidencialidad** (si se encripta). Puede llegar a tener encriptado. No ofrece privacidad, el mensaje que se envía está seguro frente a alteraciones, pero no lo está de ser leído por otros.

- ❖ Funcionamiento: usuario A envía un mensaje a B. Se firma con la clave privada de A y en B se certifica que la clave pública de A coincida.

Métodos de autenticación de peers de VPN: Firmas RSA y PSK

Acciones que se pueden tomar para dar seguridad a una red

Requerir claves de acceso a la red; encriptado de datos; seguridad física de dispositivos; firma digital; firewall; capacitación de usuaries y administradores; protocolos de seguridad (como IPsec); VPN.

Firewall: sistema que crea una barrera segura entre dos redes. Se compone de hw y sw.

- ❖ Beneficios: concentra seguridad en un único punto; controla acceso; regula el uso de la red exterior; protege de ataques internos; mejora la privacidad del sistema; etc.
- ❖ Hay que buscar el punto justo para no limitar de más y perder funcionalidades.
- ❖ Hay que complementarlo con otras acciones. Está a nivel de red (ej: router) y a nivel de aplicación (ej: servidor proxy).

IPSEC

Es un conjunto de protocolos de seguridad que permiten agregar encriptado y autenticación a las comunicaciones. Es de capa 3. Uso frecuente en VPN (fortinet). Dos modos:

- ❖ Transporte: va sobre IP, protege a la capa de transporte. Se implementa en los extremos. Es más rápido, pero menos seguro. Al encabezado común se le agrega un encabezado de IPSEC (se llama ESP).
- ❖ Túnel: se protege al protocolo IP de origen y de destino. Se implementa en la nube (gateway). Precisa de otra capa de IP para la nube. Más lento. Se le agrega también el ESP y la nueva IP.

El cifrado se utiliza en los siguientes niveles: PPTP y L2TP -> nivel 2. IPSec -> Nivel 3. MPLS: Modifica la criptografía de la red. SSL: Nivel de sesión. TLS: Nivel intermedio entre capa 4 y 5.

Seguridad en WIFI: siempre conviene usar WPA2 PSK para uso doméstico.

- WEP es más viejo, ya no se usa.
- Otros recursos: nombre de la red (SSID) y filtrado de direcciones MAC.