# **Capítulo 1: Introducción**

## **Red**:

* Conjunto de recursos de comunicaciones e informática que forman un sistema para el transporte de información.

### **Clasificación**:

* Según extensión: LAN, WAN, GAN
* Topología: Bus, Anillo, Estrella, Híbrida.

### **LAN vs Wan:**

* **Privacidad**:
  + **LAN**: Completamente privada.
  + **WAN**: Pública. Se comparte infraestructura con otras empresas.
* **Velocidades y errores:**
  + **LAN**: Gbits. Error menor a (10^-9).
  + **WAN**: Mbits. Más errores debido a la distancia y otros factores. Se debe contemplar la ocurrencia de errores y métodos de recuperación.
* **Gestión de enlace:**
  + **LAN**: Lo arreglo yo.
  + **WAN**: Se delega al que gestiona el servicio.
* **Conmutación**:
  + **LAN**: De paquetes.
  + **WAN**: De circuitos. Provee garantía de performance con un alto costo.
* **Protocolos**:
  + **LAN**: El que quieras.
  + **WAN**: Tener en cuenta la detección y corrección de errores.

### **Conmutación de circuitos:**

* Reservar recursos y puertos entre dos abonados. Se cobra por el tiempo bloqueado.

### **Conmutación de paquetes:**

* Configuración de nodos para que un paquete llegue entre abonados. No se reservan completamente los caminos, ya que los utilizan varios.
  + Puede haber sobreventa y congestión.

## **Protocolo de Comunicaciones:**

* Conjunto de reglas y procedimientos que regulan las comunicaciones entre dispositivos.
* Permite intercambiar información entre capas con las mismas funciones.
* Permite interoperabilidad.
* **Protocolo**: Mismo nivel pero distinto sistema.
* **Interfase**: Distinto nivel pero mismo sistema.

### **Funciones**:

* **Control del flujo de datos**: No saturar los canales.
* **Control de actividad**: En el canal de comunicaciones.
* **Control de errores**: Los bloques deben llegar a destino libre de errores, pérdidas, omisiones o duplicaciones.
* **Segmentación y ensamblado**: PDU.
* **Transparencia**: No afectar datos con información de protocolo.
* **Encapsulamiento**: Agregar información de control a los bloques.
* **Sincronismo**: De caracter o bloque.
* **Control de conexión:** Establecer, transferir y liberar.
* **Entrega en orden**: Utilizando numeración secuencial.
* **Direccionamiento**: Niveles, alcance y modos.
* **Multiplexación**: Varias conexiones en un mismo vínculo.
* **Servicios de transmisión**: Prioridad, seguridad, QoS.

### **PDU**:

* Unidad de datos de protocolo.
* **Tamaño pequeño**:
  + Mayor eficiencia en el control de errores.
  + Mayor facilidad de transmisión.
  + Menor cantidad de memoria usada (Buffer).
  + Menor necesidad de interrupciones.
  + Mayor necesidad de información relativa. (-)
  + Mayor tiempo de latencia. (-)
* **Tamaño grande:**
  + Mayor eficiencia de transmisión.

### **Sondeo y selección:**

* Control de las transmisiones en una línea compartida.
* Utilizado en redes jerárquicas.

#### **ARQ**

* Requerimiento automático de repetición.
* Método de control de flujo y errores.
* **Usa**:
  + ACK y NAK.
  + Timeout.
  + Método para detectar errores.
* Tipos:
  + **Stop and Wait**: RQ Inactiva.
    - Vel Trans relacionada con tiempo de propagación.
    - Ineficiente para velocidades altas y grandes distancias.
    - *Half duplex*.
  + **Sliding Windows**: RQ Continua:
    - Ventana: Cant. Paquetes que transmite sin esperar confirmación.
      * Fija o variable.
    - Piggyback: En un paquete transmite información y confirmación de otro paquete.
    - Requiere buffer y Nro. de secuencia.
    - *Full duplex*.

### **Sistema sin sondeo:**

* **X-ON / X-OFF**: Caracteres de control de flujo.
  + Dentro de banda.
  + On: Hay capacidad para recibir.
  + Off: No hay más capacidad.
* **RTS / CTS**: Señales de interfaz digital para control de flujo.
  + Eléctricas.
  + Fuera de banda.
  + Request to Send y Clear to Send.
* **TDMA**: Acceso múltiple por división de tiempo.

## **Modelo OSI:**

* Permite que los dispositivos de distintos fabricantes se puedan comunicar entre sí.
* No propietario.
* Es un modelo de referencia.

### **Características**:

* Capas separadas en funciones distintas.
* Funciones similares dentro de la misma capa.
* Interacción mínima entre capas.
* Protocolo de capa par entre cada emisor - receptor.
* Cada capa agrega un header para que el receptor de la misma capa pueda, utilizando un protocolo en común, obtener el mensaje original con sus datos para el envío.
* **Encapsulamiento**.

### **Capas**:

#### **Física (1)**:

* Bits.
* Define la interfaz física entre dispositivos y reglas para la transmisión.
* Determina el código a usar (Manchester, HBN3).
* Determina el medio de comunicación.
* Determina el significado de los 1 y 0 en los dispositivos, amperaje, voltaje.
* No hay control de errores. (No se puede saber si 1 o 0 esta bien)
* **EJ**: ISDN, LAN.

#### **Enlace (2)**:

* Bits.
* Brindar un enlace seguro y proveer mecanismos para activar, mantener y desactivar el enlace.
* Delimitar tramas. Determinar dónde empieza y termina el mensaje.
  + Eliminar todos los bits auxiliares.
* Garantizar entrega libre de errores utilizando mecanismos de detección y corrección.
  + Recuperar datos perdidos, duplicados o erróneos.
* **EJ**: HDLC, LAP-B.

#### **Red (3)**:

* Encontrarle un camino al mensaje, el cual tiene origen y destino.
* Permite ir más allá de lo conectado en forma adyacente.
* Funciones de conmutación.
  + Encaminamiento
* Gestiona las prioridades.
* Oculta los detalles de la red subyacente a las capas superiores.
* **EJ**: IP, X25.

#### **Transporte (4)**:

* Mecanismos para el intercambio de datos de extremo a extremo.
* Control de errores extremo a extremo.
* Proporciona la calidad de servicio solicitada por la capa Sesión.
* **Orientado a la conexión**: Información libre de errores, ordenado y sin pérdidas ni duplicaciones.
* **EJ**: TCP.

#### **Sesión (5):**

* Detecta si la comunicación sigue activa o si es necesario reiniciarla en caso de caídas.
* Utiliza mecanismos que se suelen implementar en la capa Aplicación.
* **Control de diálogo**: Solicitud de canales simultáneos (Full Duplex) o alternados (Half Duplex).
* **Recuperación**: Procedimientos de puntos de comprobación para recuperación de fallos e interrupción de operaciones.

#### **Presentación (6):**

* Define el formato de los datos que van a intercambiarse.
* Define el formato de compresión para que el receptor pueda descomprimir.
* **Conversión de códigos**: Adaptación de distintos códigos usados en los extremos.
* **Compresión**: De datos.
* **Encriptación**.

#### **Aplicación (7):**

* Proporciona a los programas de aplicación un medio para acceder a OSI.
* Toma los datos de usuario y agrega una cabecera de aplicación.
* Incluye funciones de administración general.
  + Mecanismos para implementar sistemas distribuidos.
* **EJ**: Telnet, FTP.

# **Capítulo 2: Redes LAN**

## **Glosario:**

* **Portadora**: Señal sin información. Reduce la probabilidad de colisión.
* **Hub**: Repetidor multipuerto.
  + Capa física.
* **Colisión**: 2 estaciones sensan un canal desocupado y transmiten en simultáneo.
* **FCS**: Secuencia de control de Trama.
* **CRC**: Código de redundancia cíclica.
  + Utiliza un polinomio generador.
  + No tiene en cuenta el preámbulo.
* **Dominio de colisión:** Área de la red donde se propagan las colisiones por ocupar el medio en forma simultánea.
  + Propagan: Repetidores y Hubs.
  + No propagan: Bridges, Switches y Router.
  + *Cada puerto del Switch es un dominio de colisión, pero los puede filtrar.*
* **Dominio de Broadcast**: Área donde se propagan las tramas de difusión.
  + Router no propaga difusión.
  + Dirección MAC: Solo se puede poner como destino.
* **Tipos de difusión**:
  + Unicast (Unidifusión): 1 a 1. Una interfaz individual.
  + Anycast (Monodifusión): A un conjunto de interfaces individuales priorizando la más cercana según ruteo.
  + Multicast (Multidifusión): 1 a N. Se elige un grupo de destinatarios.
  + Broadcast: A todos los dispositivos de la red.

## **Capas:**

* **Física**: Codificación y decodificación.
  + Preámbulo: Creación y eliminación.
    - Indica el inicio del PDU.
  + Especifica el medio de transmisión y la topología.
* **Enlace**:
  + **MAC**: Media Access Control.
    - Trama: PDU.
      * Armado y desarmado de tramas
    - Detección de errores: CRC.
    - Control de acceso al medio de transmisión.
  + **LLC**: Logical Link Control.
    - Interfaz con capas superiores.
    - Corrección de errores y control de flujo: ARQ.
    - Especifica el destino y origen para protocolos de capa superior.
* **Red**:
  + Encargada de asignar el preámbulo.

### **LLC: Tipos de conexión (Servicios):**

* **Datagrama**: No orientado a conexión. Sin confirmación.
* **Datagrama Confirmado**: Idem pero con confirmación..
* **Modo conexión**: Conexión lógica, control de flujo y errores.

## **Dirección MAC:**

* Grabada en la interfaz de comunicaciones del dispositivo.
  + Dirección física colocada por el fabricante.
  + Identifica univocamente al dispositivo.
* 6 Grupos de dígitos Hexadecimales.
  + 24 bits para el fabricante
  + 24 bits para el dispositivo.

### **Filtrado de MAC:**

* Permitir o denegar el acceso a una red según su dirección MAC.
* **Blacklist o Whitelist**: Deniega o permite todo lo que esté en la lista.
* **Problema**: No es fiable porque se puede emular la dirección MAC.

## **Topologías**:

* **Bus**: Bidireccional.
  + Se escucha todo pero solo se guarda lo que está dirigido a mi.
* **Anillo**: Recorre todo y muere la trama al llegar al destinatario.
* **Estrella**: Dos versiones.
  + Con Hub: Capacidad Total = Vel. Trans
    - Se distribuye entre todos los conectados.
  + Con Switch: Capacidad Total = N \* Vel. Trans
    - Sin colisiones.
  + *Vel Trans. Switch > Vel. Trans Hub.*
* **Modos**:
  + Difusión: Hub.
  + Conmutación: Switch.

## **Protocolos de acceso al medio (MAC):**

### **Contention (Aleatorio):**

* **Aloha**: Detecta colisiones y espera para retransmitir.
  + Tramas de longitud fija.
  + No sensa el canal ocupado.
  + **Ranurado**: Slot de tiempo.
    - Espera a la próxima ranura para poder transmitir.
  + **Puro**: Se transmite si la estación tiene datos.
* **CSM**: Sensa presencia de portadora en el canal.
  + **Round Trip Time**: Tiempo entre estaciones.
  + **Ventana de colisión**: Tiempo entre estaciones más alejadas del mensaje.
  + **Persistente**: Espera un RTT Max para sensar.
  + **No persistente**: Espera un tiempo aleatorio para sensar.
* **CSMA / CD**: Detección y resolución de colisiones.
  + Sensado permanente y aborto de transmisión.
  + Espera un tiempo aleatorio cuando detecta una colisión.
* **CSMA / CA**: Evasión de colisiones.
  + Sensado permanente y uso de técnicas para evasión.

### **Token Passing (Determinístico).**

* Testigo para monopolizar el canal.
  + Se pasa de un terminal a otro según reglas.
* Solo se permite transmisión si se tiene el testigo.
* Se pueden asociar prioridades para transmitir primero algunas tramas.

## **LAN Alta Velocidad:**

* **Interfaz Full Duplex:**
* Transmisión y recepción en simultáneo y son independientes.
* **Ethernet Conmutada**: Utiliza un switch.
  + Cada estación es un dominio de colisión separado, por lo que se elimina CSMA / CD
  + No se necesita competencia para acceder al medio compartido.
  + Se crea una tabla de ruteo.
* **Velocidades**: 100 Mbps, Gigabit o 10 Gigabit.
* **VLAN**: Asociación lógica de las estaciones que la constituyen.
  + Reduce la difusión en la red al aumentar la cantidad de estaciones.
  + Cada VLAN es un dominio de broadcast.
  + **Tag (802.1Q)**: Múltiples redes pueden compartir un mismo enlace.
* **Spanning Tree (802.1D)**:
  + Estándar de Bridges MAC que incluye el protocolo STP.
  + Permite descubrir loops y desactivar vínculos redundantes.
  + Transformar red física de malla en red lógica de árbol sin bucles.

## **Ethernet (802.3)**:

* **Peer to Peer**: Todos los miembros de la red tienen la misma ventaja.
* **Acceso aleatorio**: No se sabe cuando se va a poder transmitir.
* **CSMA / CD**: Acceso múltiple de portadora con detección de colisiones.
  + Método de acceso al medio.
* **Punto a punto / Multipunto**: Especificar origen y destino.
  + Cuando uno transmite las demás escuchan.
  + Son direcciones MAC.
* **Longitud Trama**: Tamaño mínimo de 64 bytes.
  + Máximo de 1518 sin preámbulo ni SFD.
  + *Es la ventana de colisión para que no colisione con otra estación en caso de mandar un mensaje más corto.*
* No tiene confirmación.

### **Trama (PDU)**:

* **Preámbulo** (4): Sincronizar estaciones.
* **SFD** (1): Comienzo trama y fin preámbulo.
* **DA** (6): Destino.
* **SA** (6): Origen.
* **Len / Type** (2): Protocolo de capa superior.
* **Datos** (0 - 1500).
* **Pad** (0 - 46): Relleno para llegar a 64 bytes.
* **FCS** (4): CRC. Control de errores.

### **Tipos**:

* **10 Base 5**: 10 Mbps. 500 m. Coaxil grueso.
* **10 Base 2**: 10 Mbps. 200 m. Coaxil fino.
* **10 Base T**: 10 Mbps. 100 m. UTP.
* **100 Base T**: 100 Mbps. 100 m. UTP.

## **Bridge**:

* Conecta redes LAN que usan la misma capa física y MAC.
* Almacena y realiza control de errores antes de retransmitir tramas MAC.
* **Filtrado de paquetes**: No pasa mensajes de un segmento al otro si no es necesario.
* **Forward**: Envío de paquetes.
* **Dominio**:
  + **Broadcast**: Ambas redes + Bridge.
  + **Colisión**: Cada subred LAN por separado.

## **Switch**:

* Bridge con múltiples puertos.
* Vel Transmisión se aplica a cada puerto de forma independiente.
* **Bridging**: Vincular cada puerto con una dirección MAC.
  + Permite conexión simultánea.
  + Elimina los dominios de colisión.
  + Aprendizaje automático de la ubicación de los hosts.
* **Conmutación**: La estación cree que tiene toda la capacidad del enlace.
* **Problemas**:
  + **Bucles**: Switches conectados entre sí de forma directa o indirecta.
    - Repetición infinita de un broadcast.
  + **Inundación**: Llenar la red de Broadcast.

### **Tipos**:

* **Store and Forward**: Se espera la recepción completa de la trama, se analiza por errores (Calculando el FCS) y se envía.
  + Asegura que no haya errores.
  + Presenta demora.
* **Cut Through**: Lee los primeros 6 bytes (Dirección MAC destino) para decidir y conmutar la trama
  + Reduce la latencia.
  + Puede haber colisiones.
  + No detecta errores
* **Cut Through - Fragment Free**: Lee los primeros 64 bytes y luego retransmite.
  + No hay colisiones.
* **Adaptative Cut Through**: Se elige uno de los dos según necesidad.

# **Capítulo 3: Redes Inalámbricas + Cableado estructurado**

## **Cableado Estructurado:**

* Permite voz y datos dentro del mismo cableado.
* Alta velocidad en transmisión de datos.
* Compatibilidad con tecnologías actuales y futuras.
* Bajo costo de mantenimiento.
* Flexibilidad.
* Fácil supervisión.
* Componentes:
  + Medio de transmisión (FO, Coaxil)
  + Paneles de interconexión.
  + Armario de telecomunicaciones y distribución.
  + Placas y tomas de pared.
  + Puesta a tierra.

### **Problemas en la red:**

* Toda cadena es tan fuerte como su eslabón más débil.
* El cableado maneja todas las transacciones de la red.
* Fuentes de error:
  + Conexiones flojas.
  + Malas terminaciones.
  + Exceso de distancias.
  + Cables doblados.

## **Atenuación**:

* Relación entre la potencia de la señal recibida en el destino y la transmitida en origen.
* **Ideal**: At = 0
* **Peor**: At = - Infinito

## **Diafonía**:

* Consecuencia del acoplamiento inductivo entre los pares de transmisión y recepción de un cable.
  + Parte de la señal de uno aparece en el otro.
* **¿Cómo reducirlo?**: Trenzar los cables lo más cerca de los terminales.
* **Paradiafonía (NEXT)**: Producida en el extremo más próximo al receptor causada por la señal emitida por el mismo.
  + NEXT = 10 \* Log (P2 / P1)
  + Ideal: NEXT = - Infinito.
  + Peor: NEXT = 0

## **Redes Inalámbricas:**

* **Comparativa capas OSI:**
  + Enlace (2): 802.2 + 802.11 MAC
  + Física (1): FH + DS + IR.
* **Bandas no licenciadas**: Pueden ser usadas sin solicitar permiso, aunque deben cumplir ciertos requisitos para no interferir.
  + 2.4 Ghz: Hasta 14 canales pero hay solapamiento.
    - Menor atenuación.
    - Mayor alcance.
    - Menor velocidad.
  + 5.0 Ghz: Todos los canales de 20 Mhz sin solapamiento.
    - Mayor atenuación debido a la mayor frecuencia.
    - Menor alcance.
    - Mayor velocidad.

### **Elementos**:

* Equipos terminales.
* Sistema de distribución: Red LAN cableada.
* **Acces Point**: Donde se conectan los terminales.
  + Permite conectar dispositivos inalámbricos a la red cableada.

### **Usos**:

* **Ampliación de redes**: Empleando puntos de acceso inalámbricos.
* **Interconexión de edificios**: Radioenlaces punto a punto uniendo routers o bridges.
* **Acceso nómade**: Permitir acceso a un dispositivo portátil.
* **Trabajo Ad Hoc**: Peer to Peer. Sin servidor central.

### **Capas**:

* **LLC 802.2**
* **MAC 802.11**
  + **Entrega fiable de datos:** Utilizando un mecanismo:
    - 2 Tramas: Datos + ACK + Timeout.
      * Repite de ser necesario.
    - 4 Tramas: Datos + ACK + RTS / CTS
      * Evita colisiones: Se mantiene en espera.
  + **Control de acceso**: Distribuido o centralizado.
    - DFC: Función de coordinación distribuida.
      * Previene el acceso a la totalidad del tráfico.
      * CSMA / CA: Evita colisiones.
    - PCF: Función de coordinación puntual.
      * Acceso libre de contienda.
      * Asegura el acceso a usuarios.
  + **Seguridad**:
    - Autenticación.
    - Privacidad.
* **IR + SF + SD**

### **Tecnologías**:

#### **De Infrarrojos (IR):**

* Haz dirigido omnidireccional.

#### **Radio por espectro expandido (SS):**

* Permite varios usuarios usando el mismo ancho de banda con pocas interferencias.
* Utilizada en redes WiFi y Bluetooth
* **Seguridad**: Baja detectabilidad y capacidad de encriptación.
* **Desventaja**: Pérdida de eficiencia espectral (Vel. Trans / Ancho Banda)
* **Bandas**: 900 Mhz, 2.4 Ghz y 5.8 Ghz.
* **Técnicas**:
  + Secuencia directa: Expandir la onda ensanchada.
  + Salto de frecuencia.
* **Tecnologías de radio**: MIMO, SIMO, MISO, SISO.

### **Tipos**:

#### **WPAN 802.15 (Bluetooth):**

* Protocolo de bajo costo y poco alcance.
* **Canales**: 23 o 79 según país.
* **Cantidad dispositivos**: 8.
* **Automatización de ID**: PIN.
* **Bluejacking**: Mensaje que introduce un virus en comunicaciones bluetooth.

#### **Wi Max 802.16:**

* Hasta 70 KM.
* No hay colisiones ya que no se trabaja con contienda.
* Punto a multipunto en banda ancha.
* Eficiencia espectral.
* Pueden existir problemas de interoperabilidad entre diferentes proveedores.

#### **WLAN 802.11 (WiFi):**

* Mínima interferencia entre canales y frente a otros dispositivos.
* **Auto - Canal**: Los dispositivos eligen el canal que mejor está funcionando.
* Escaneo y cambio de canal.
* No requiere licencia ya que utiliza las bandas 2.4 y 5.8 Ghz
* **Servicios**: Básicos y extendidos:
  + Asociación o reasociación: Dependiendo si es primera vez o no.
  + Autenticación: También el fin de la misma.
  + Privacidad: Solo visualizan los autorizados.
  + Integración: Puede conectarse a otra LAN.
  + Distribución de mensajes.
* **Canales utilizados**: Solo se pueden utilizar 1 de cada uno de los siguientes rangos de forma simultánea ya que sino se solaparían debido a la pequeña diferencia en frecuencia que hay entre ellos:
  + 1 - 5: 2412 - 2432 Mhz
  + 6 - 10: 2437 - 2457 Mhz
  + 11 - 14: 2462 - 2484 Mhz.

##### **Seguridad**:

* **WPS**: Wifi Protected Setup: Utiliza PIN.
* **WEP**: Wired Equivalent Privacy: Usa encriptación.
* **WPA**: Wifi Protected Access: Uso de claves dinámicas para cada usuario.
* **WPA2**: Utiliza algoritmo de encriptación AES.
  + AES: Advanced Encryption Standard.
* **WPA 2 PSK**: Uso doméstico donde se comparte la clave.
  + PSK: Pre Shared Key.

##### **Trama**:

* **FC (2)**: Control de trama: Indica el tipo:
  + Control: RTS / CTS, ACK.
  + Datos.
  + Gestión: De asociaciones o entre estaciones y APs.
* **D/I (2)**: Duración / Conexión: Tiempo de reserva del canal para identificar una conexión o una transmisión satisfactoria.
* **4 x Address (6)**: Direcciones: Fuente, destino, estación de transmisión y recepción.
* **SC (2)**: Control de secuencia: Fragmentación, ensamblado y N° tramas enviadas.
* **Frame Body (0 - 2312)**: Datos.
* **CRC (4)**: Control de errores.

##### **Evolución**:

* **802.11a:** OFDM + 5 Ghz / 54 Mbps
* **802.11n (WiFi 4)**: Único MIMO + 70m + 2.4 y 5.8 Ghz / 300 a 600 Mbps
* **802.11ac (WiFi 5)**: Multiples MIMO + 30m + 5,8 Ghz / 7 Gbps
* **802.11ax (WiFi 6)**: OFDM + Multiples MIMO + 2.4 y 5.8 Ghz / 10 Gbps

##### **WiFi 6:**

* Posibilita los requerimientos de IoT.
* Mayor eficiencia con alta densidad de usuarios.
* Mayor duración de baterías.
* Evita interferencias de señales vecinas.

## **Problemas en la comunicación por radio:**

### **Estación oculta:**

* Los nodos de una red tienen un alcance limitado, por lo que los miembros de una red pueden no percibirse entre sí al estar en diferentes áreas de alcance.

#### **Solución:**

* Antes de transmitir, la estación A envía RTS.
* Estación B responde con un CTS.
* El terminal C no capta el RTS pero si el CTS.
  + Sabe que no debe transmitir por un tiempo equivalente a 500 bytes.
* Estación A puede enviar su trama sabiendo que no va a colisionar con otros.

### **Terminal expuesta:**

* Una estación quiere transmitir a otro y escucha el canal pero escucha la transmisión de otro equipo, por lo que concluye que no puede enviar aun cuando no le están transmitiendo a su destinatario.

#### **Solución:**

* Los terminales expuestos solo deben escuchar el RTS pero no el CTS
  + Así se les da permiso para enviar paquetes.

# **Capítulo 4: TCP / IP:**

## **Protocolo de internet:**

* **Define**:
  + Ruteo.
  + Conjunto de reglas para la entrega de paquetes no confiables.
* **PDU**: Datagrama.
  + Máximo de 65536 Bytes.

### **Características**:

* **Orientado a la no conexión**: Cada paquete se trata de forma independiente.
  + No hay historia de los paquetes en los routers que fueron tratados ni lo que contenían
* **Entrega no confiable**: Los paquetes pueden ser:
  + **Perdidos**: La capa de red no ofrece confirmación.
  + **Duplicados**: La capa de transporte debe validar y descartar.
  + Desordenados.
  + Demorados.
* **Best - Effort**: Se realiza un intento serio por entregar el paquete.

### **Fragmentación y reensamblado:**

* Si hay un mensaje con tamaño mayor que el máximo permitido no se puede encapsular.
* IP toma el mensaje de la capa de transporte, lo encapsula en un datagrama IP y lo fragmenta para asegurarse que viaje dentro de la trama.
* **MTU**: Tamaño máximo de transferencia.
  + Máximo del campo Datos de la PDU donde se encapsula el datagrama.
* **Router**: Encargado de realizar la fragmentación.
* **Problema**: Tamaño de Datagrama variable + varios MTU.
  + Se divide el datagrama en partes más pequeñas para que entre en un MTU.
* **Desventajas**:
  + Duplica la probabilidad de pérdida de un datagrama.
    - Si se pierde una parte del mensaje, se gastan recursos en transmitir fragmentos parciales y nunca se va a completar.
  + Mayor carga de procesamiento en los routers.
    - Dividir el mensaje, crear nuevas cabeceras, calcular checksums.
  + Excesivas retransmisiones si hay pérdidas de paquetes.
    - Si hay alta tasa de pérdida de paquetes.

### **PDU (Datagrama):**

* **1er**:
  + **Versión (4)**: Indica la versión de IP.
  + **Hlen (4)**: Indica la cantidad de palabras que ocupa la cabecera.
  + **ToS (8)**: Tipo de servicio. Indica la prioridad y urgencia del mensaje.
  + **Longitud total (8)**: Incluye encabezado y datos.
* **2do**:
  + **Identificación (16)**: Para el datagrama y su fragmentación.
  + **Flags (3)**: Controlar la fragmentación
  + **Desplazamiento Fragmentación (13)**.
* **3er**:
  + **TTL (8)**: Segundos de vida del datagrama para que no quede en loop de ruteo.
  + **Protocolo (8)**: Indica el protocolo de capa superior.
  + **Checksum encabezado (16)**: Solo encabezado. No es CRC
* **4to**:
  + **Dirección IP fuente (32)**.
* **5to**:
  + **Dirección IP destino (32)**.
* **6to**:
  + **Opciones (32)**: Pruebas de red o depuración + relleno.
* **7mo**:
  + **Datos**: Longitud variable

### **Direccionamiento**:

* Utiliza 32 bits.
  + 4 bytes separados por puntos.
* Provee una dirección única para cada red.
* Provee una dirección única para cada host dentro de cada red.
* **Difusiones**:
  + Dirigida a una red: Campos de host igual a 1.
  + Limitada en red local: Todos los bits son 1.
  + Identificación de la red: Campos de host igual a 0
  + Identificación del host: Todos los bits son 0.

#### **Clases**:

| **Clase** | **Bits para Host** | **Dirección Desde** | **Dirección Hasta** |
| --- | --- | --- | --- |
| **A** | 24 | 1.0.0.0 | 126.0.0.0 |
| **B** | 16 | 128.1.0.0 | 191.254.0.0 |
| **C** | 24 | 192.0.1.0 | 223.255.254.0 |
| **D** | - | 224.0.0.0 | - |

#### **Máscara**:

* Utilizada para cambiar la interpretación de la dirección IP.
  + Indica cuántos bits se toman del Host para identificar subredes.
  + No viaja en el datagrama IP
* Está compuesta por 4 bytes.
* **Variable**: Si el router lo permite.

#### **Subredes - Subnetting:**

* Utilizada para aprovechar grandes redes
* Se deben determinar la cantidad de subredes y hosts por subred.
* **Se debe definir**:
  + Máscara para la subred.
  + Dirección única para cada subred.
  + Rango de direcciones de host válidas.
  + Dirección de difusión.
* **Características**:
  + Permite que una misma dirección de red identifique varias redes físicas.
  + Algoritmos de ruteo que tengan tablas con máscara de subred.
  + Facilita el proceso de ruteo.
  + Mayor flexibilidad debido a la independencia de cada red física.

## **Protocolos para resolución de direcciones:**

* Todos están en capa Enlace (2)

### **ARP: Resolución de dirección.**

* Permite conocer la dirección MAC de un dispositivo a través de su IP.
* Transmite un Broadcast MAC con la IP destino para que responda con su MAC y se registre en la tabla ARP.

### **RARP: Resolución de dirección inversa.**

* Conocer la IP de un dispositivo a través de su MAC.
* Utiliza un servidor de direcciones.
* Transmite Broadcast MAC para que el destino que coincida con la IP responda con su dirección MAC y se cree una entrada en ARP.

## **Protocolo ICMP: Internet Control Message:**

* Se encapsula sobre IP.
* Utiliza mecanismos para salvar los problemas del protocolo IP:
  + Comunicación de errores a nivel de red.
  + Informa acerca de eventos inesperados.
* Solo informa errores, no especifica soluciones.
* Se empaqueta dentro de un datagrama.

### **Mensajes**:

* **Reporte de error**:
  + Destino inalcanzable: No se puede conmutar o entregar un datagrama por lo que el router envía un mensaje antes de descartarlo.
  + Tiempo de espera agotado: TTL llega a 0 o el host destino dejó de esperar el fragmento.
* **Consulta / Respuesta**:
  + Echo Request / Reply: Saber si la interfaz destino es alcanzable y funciona.

## **Protocolo IGMP: Internet Group Manager:**

* Se encapsula sobre IP.
* Intercambia información entre routers.
* Multidifusión con datagramas IP a un conjunto de máquinas.
* Se propaga en una sola red física o a través de varias redes.

## **Protocolo UDP: User Datagram:**

* Se encapsula sobre IP
* Servicio de datagramas no orientado a la conexión.
* Conmutación de paquetes modo Datagrama.
* **PDU**: Datagrama UDP.
* **Desventaja**: Las aplicaciones deben resolver los problemas del protocolo.
* **Ventaja**: Es más veloz que TCP.
* **Uso**:
  + Procesos simples de Request - Response.
  + Multicast y broadcast.
  + Streaming de audio o video de forma eficiente.

### **Características**:

* No orientado a la conexión: no mantiene estado.
* No confiable: No envía notificaciones en caso de descartar.
* No orden: No tiene un número de secuencia u orden.
* No control de flujo: No tiene un campo ventana.

### **PDU (Datagrama):**

* Puerto origen (16).
* Puerto destino (16)
* Longitud mensaje UDP (16).
* Checksum (16): Solo detección. Opcional
* Datos.

### **QUIC**:

* Variante del protocolo UDP a nivel transporte.
* Equivale a TCP + TLS.

## **Protocolo TCP: Transmission Control:**

* Reside en capa Transporte (4)
  + Se encapsula en IP.
* Conmutación de paquetes modo Circuito Virtual.
* Punto a punto.
* Permite conocer al cliente y el servidor en una comunicación.
* No determina en su PDU la longitud del mensaje porque IP lo fragmenta.
* **PDU**: Segmento.
* **MSS**: Tamaño máximo de segmento.
  + Tamaño máximo del campo de datos.
  + Se declara al establecer la conexión.
  + No se modifica durante el intercambio de segmentos.
  + Se calcula a partir de la MTU de la interfaz.

### **Características**:

* **Orientado a la conexión**: Exclusivo para 2 hosts.
  + El estado lo mantienen ambos extremos de la comunicación.
  + Cada uno lleva la cuenta del progreso de la conexión.
* Entrega ordenada.
* Conexiones full duplex.
* Confirmaciones.
* Timeouts.
* Checksum de mensaje completo (Cabecera + mensaje)
* **Control de flujo**: Mediante Sliding Windows de tamaño variable.
* **Control de congestión**: En sistemas intermedios.

### **Congestión**:

* Más información de lo que la red puede manejar.
  + Se excede la capacidad.
  + Se encolan los mensajes en el buffer o a veces se descartan directo.
* Al descartar un mensaje se requiere una retransmisión.
* **Soluciones**:
  + Uso de algoritmos.
  + **Slow start**: Enviar pequeño e ir aumentando el tamaño conforme la red lo permita.
    - En caso de congestión se reduce el tamaño.
  + **Fast retransmit**: Al recibir un 3er ACK duplicado, se asume que el paquete se perdió y se retransmite el segmento.
  + **Fast recovery**: Evitar volver al Slow Start en caso de perder un segmento.
    - Ayuda con los problemas de Slow Start.

### **PDU (Segmento):**

* **1er**:
  + **Puerto origen (16)**
  + **Puerto destino (16)**
* **2do**:
  + **Nro Secuencia (32)**: Utilizado al enviar varios mensajes.
* **3er**:
  + **Nro Acuse Recibo (32)**: Próximo Nro Secuencia que el emisor de este segmento espera recibir.
* **4to**:
  + **Hlen (4)**: Cantidad de palabras de 32 bits en la cabecera.
  + **Reservado (4)**.
  + **Flags (8)**: Contenido válido + Urgencia + Reiniciar conexión + sin datos.
  + **Tamaño Ventana (16)**: Bytes que el receptor está dispuesto a recibir.
* **5to**:
  + **Checksum (16)**: Detección de errores.
  + **Puntero urgencia (16)**: Apunta al último byte de datos urgentes.
* **6to**:
  + **Opciones (24)**: Opcional. Usualmente indica el MSS.
  + **Relleno (8)**
* **7mo**:
  + **Datos**

### **Establecimiento de una Conexión: 3 Handshake:**

* El cliente se conecta al servidor a través de un mensaje de petición de conexión.
  + Mensaje vacío con flag SYN (Synchronization) activo
* El Servidor envía un mensaje vacío con SYN y ACK confirmando la petición.
  + Envía contenido en Nro secuencia y Nro Acuse Recibo.
* Cliente envía un segmento ACK.
  + Puede o no contener información pero la conexión ya está establecida.

### **Control de flujo:**

* Utiliza ARQ Sliding Windows.
* Separa la confirmación de datos recibidos del permiso para enviar más.
* Cada octeto de datos posee un Número de secuencia.
* **Otorgamiento de créditos**:
  + Un extremo le indica al otro la cantidad de bytes que le permite enviar sin recibir una confirmación.
  + Se comienza con un crédito inicial y con cada confirmación se actualiza el valor de la ventana.

### **Control de errores:**

* En TCP no existe una confirmación de rechazo.
* Se utiliza una confirmación positiva (ACK) y solo se retransmite cuando no llega dentro de un periódo RTO.
  + RTO: Retransmission Time Out.
    - Debe estar en el orden similar al RTT (Tiempo de ida y vuelta de un mensaje)
    - Si es pequeño, se retransmite muchas veces antes de que llegue el ACK.
    - Si es muy grande y hubo error, se tarda mucho en enterar.
* Corrección de errores: ARQ petición de retransmisión.
  + Lo realiza automático el host frente a la ausencia de confirmación.

## **Aplicaciones de Protocolos:**

### **TCP**:

* **Telnet**: Conexión remota a través de Internet con autenticación.
* **FTP**: Protocolo de transferencia de archivos con autenticación.
* **SMTP**: Simple Mail Transfer. Utiliza ASCII.

### **UDP**:

* **TFTP**: Similar a FTP pero más económico y menos sofisticado.
  + Más rápido y sin autenticación.
* **BOOTP**: Especificar aspectos de arranque como dirección IP o servidor.
  + Mejora el RARP.
* **SNMP**: Simple Network Management
  + Administración de red simple.
  + Definir la forma y significado de los mensajes.
  + Definir relaciones administrativas entre routers.

#### **DNS**: Domain Name System

* Pertenece a la capa de Aplicación (7)
* Servicio cliente servidor.
* Base de datos distribuida con un espacio de nombres jerárquico.
* Permite la traducción de un dominio a una dirección IP.
* **Componentes**:
  + **Resolvers**: Clientes que corren en cada dispositivo. Envía pedidos.
  + **Name Servers**: Responden la consulta de los clientes.
* **Espacio de nombres**: Diseño jerárquico, en formato de árbol, que muestra cómo se construyen y delegan los dominios.
* **Niveles**:
  + **Raíz**: No utiliza etiquetas.
  + **Top Level Domain**: Identificados por códigos ISO. (.edu, .org)
  + **Second level**: Pueden contener:
    - Hosts: ftp.microsoft.com
    - Sub dominios: dev.microsoft.com
* **Procedimiento**:
  + El cliente hace una consulta recursiva al servidor de dominio.
  + El Servidor busca en caché una consulta similar y si no encuentra hace una búsqueda iterativa hasta encontrar al dueño.
  + El servidor dueño da la referencia a los DNS donde está el archivo.
  + Se cachea la respuesta en el servidor local y se devuelve al cliente.
* **Tipos de consulta:**
  + **Recursiva**: Se da una respuesta o un error.
  + **Iterativa**: Responde con la mejor respuesta posible.
  + **Inversa**: Se pregunta el nombre del host asociado a una ip.

#### **DHCP: Dynamic Host Configuration**

* Pertenece a la capa de Aplicación (7)
* Centraliza y administra la asignación de direcciones IP.
  + Mantiene un registro de la IP asignada a cada cliente.
* Se encapsula un mensaje en un protocolo de capa Transporte (4) dentro de un datagrama IP cuyo origen y destino se desconoce.
* **Tipos de asignación**:
  + Estática.
  + Dinámica

##### **Asignación dinámica:**

* No necesita llevar registro de direcciones asignadas.
  + No se necesita al administrador de red ya que es automático.
* Facilita la modificación del espacio de direcciones de red.
* Uso eficiente de un espacio de direcciones reducido.
* Elimina los errores manuales de la configuración de IP o máscara.
* Permite asignar a cada host todos los parámetros de configuración.

### **ICMP**:

* **Ping**: Envía solicitud de Echo y captura la respuesta.

## **Ruteo**:

* Ocurre en la capa Red (3)
  + Cumple con el encaminamiento y direccionamiento.
* **¿Como se realiza un salto?**: El router hace:
  + Determinar el mejor camino a destino.
  + Conmutar el datagrama: Encapsular en protocolo capa 2.
* **Tabla de ruteo:**
  + Almacena la información de la topología y la información que tiene el host de la red.
  + **Columnas**:
    - Red destino
    - Mascara
    - Gateway (próximo salto)
    - Interfaz (Por donde debe ir)
    - Métrica (Cuanto menor sea, más recomendable es ir por ahí)
* **Tipos**:
  + **Estático**: Solo funciona cuando hay un solo camino para llegar.
    - Al definir un camino prioritario, sólo va a intentar ir por ese.
  + **Dinámico**: Utilizado cuando se tienen varias rutas posibles.
    - Intercambio automático de dirección sin intervención.
* **Cálculo del mejor camino**:
  + **Vector distancia**: Menor cantidad de saltos.
  + **Estado del enlace**: Distancias + Delay + Capacidad + Confiabilidad.
  + **Vector camino**. No estima distancia ni costo.

### **Protocolos**:

* **Interiores (IRP)**: Distribuye información dentro de un AS.
  + Más detalle en la información.
* **Exteriores (ERP)**: Distribuye información entre diferentes AS.
  + Más simple y menos detallado.

#### **BGP**:

* Exterior (ERP).
* Border Gateway Protocol.
* Intercambio de información de ruteo entre AS.

#### **OSPF**:

* Open Shortest Path First.
* Interior (IRP)
* Calcula una ruta a través de redes suponiendo el menor costo que defina el usuario.
  + Delay o Velocidad de Transmisión.
* Cada Router debe armar un grafo completo de toda la red.

### **Características**:

* **Flexibilidad**: Configurable, adaptable a cambios.
* **Óptimo**: Mejor camino posible dentro de una topología.
* **Rápida convergencia**: Reconfiguración frente a falla de un enlace.
* Robusto.
* Simple.

## **Voice over IP (VoIP):**

* Es distinto a la telefonía IP.
* **Parámetros**: Codecs + Delay + Calidad
* **Cliente**: Usuario Skype.
* **Servidor**: Conmutador IP | IP PBX.
* **IP Trunking**: Dispositivo corporativo para intercambiar datagramas IP.
* **Gateway**: Puente de comunicación que provee interfaces con telefonía tradicional.
* **Puertos**:
  + FXS: Debe conectarse al teléfono (Abono).
  + FXO: Se debe conectar con la central telefónica.

## **IPv6**:

* **Campo de dirección**: Pasa de 32 a 128 bits.
  + Espacio de direcciones ampliado.
  + Evita el uso de máscara de IP (NAT).
* Formato de encabezado flexible
* Mecanismo de opciones mejorado.
* Permite características adicionales.
* Provee una funcionalidad para asignación de recursos.

### **Direcciones**:

* Se asignan a interfaces individuales de nodos.
* Permite agrupar por jerarquía de red, proveedores, proximidad, institución, etc.
* Tablas de ruteo más pequeñas.
* Consultas más rápidas.
* **Formato**: Notación hexadecimal. 16 bytes con 2 números hexa cada uno.

# **Capítulo 5: Redes WAN:**

## **Tipos de conmutación**:

| **Característica** | **Circuitos** | **Paquetes - Datagrama** | **Paquetes - Circuitos Virtuales** |
| --- | --- | --- | --- |
| **Tipo Conexión** | Física | Sin Lógica | Con Lógica |
| **Transmisión** | Continua | Paquete | Paquete |
| **Eficiencia Uso** | Voz | Datos | Datos |
| **Ordenamiento** | Orden de Trans | No Orden Trans. | No Orden Trans. |
| **Facturación** | Tiempo y Distancia | Cant Paquetes y Tiempo | Cant. Paquetes y Tiempo |
| **Ruta** | Rígida - Dedicada | Menos Saltos y Delay - Sin Ruta | Menos Saltos y Delay - Ruta no Dedicada |
| **Enrutamiento** | Misma para la Tx | Cada Paquete tiene propia | Misma para la Tx |
| **Delay** | Al establecer | De Tx de Paquete | Ambos |
| **Ancho de Banda** | Fijo | Dinámico | Dinámico |
| **Congestión** | Bloquea establecer | Aumenta Delay Paquete | Ambos |
| **Mensajes** | No almacena | Almacena hasta envío (Opcional) | Almacena hasta envío |

## **Tipos de servicios:**

* **Orientados a la conexión**: Mantiene orden del tráfico.
  + Similar a un tubo.
* **Sin conexión**: Encaminamiento independiente.
  + Puede o no mantener el orden.
  + Similar a una carta.
* **Circuito Virtual**: No decide encantamiento por cada bloque.
  + Establece una ruta de extremo a extremo.
* **Datagrama**: Encaminamiento independiente.
  + No determina rutas de forma anticipada.
  + Más robusto y más adaptable.
  + Implica un mayor trabajo.

## **Redes de Conmutación de circuitos:**

* Debe haber un canal de comunicaciones dedicado entre dos estaciones.
* **Pasos**:
  + Establecer circuito.
  + Transferir datos.
  + Desconectar el circuito.
* **Componentes**:
  + Abonados.
  + Lazo de abonado.
  + Centrales.
  + Líneas principales.
* **Conmutación IP**: Permite enrutar paquetes de datos más rápido que la forma tradicional mediante el uso de conmutadores en capa Red (3).
  + No se necesita un Gateway IP.

### **Tipos de conmutación:**

* **Por división en el espacio**: Las rutas establecidas son físicamente independientes entre sí.
  + Originalmente analógicos.
  + Puede ser de 1 o 3 etapas.
* **Por división en el tiempo**: Basado en multiplexación por división de tiempo (TDM).
  + Sistemas digitales.
  + Los canales de menor velocidad son muestreados a mayor velocidad para integrarse a un bus TDM.

### **Protocolo PPP:**

* Punto a punto.
* Capa de Enlace (2)
* Encapsula datagramas IP cuando se envía a través de un Serial.
* Utiliza ARQ Sliding Windows.
* **Funciones**:
  + Transportar datos.
  + Asegurar el enlace y la recepción ordenada.
  + Autenticación.
* **Ventajas**:
  + Permite líneas sincrónicas y asincrónicas.
  + Asignación dinámica de direcciones IP.
  + Transporte de diversos protocolos de red.
  + Permite la creación de VPN cifradas y no cifradas.
* **Desventaja**: No provee cifrado de datos.
* **Etapas**:
  + Establecimiento de conexión: Negociar parámetros.
  + Autenticación: Es opcional a través de:
    - *PAP*: Inseguro porque se envía la información directo.
    - *CHAP*: Se envía la contraseña cifrada.
  + Configuración de red: Negociar parámetros según protocolo de red.
  + Transmisión: Envío y recepción de información.
  + Terminación: En cualquier momento y por cualquier motivo.

### **Protocolo SLIP:**

* Serial Line IP.
* Procesamiento de tramas en envíos IP a través de un Serial.
* Encapsular datagramas IP.

# **Capítulo 6: WAN X25**

## **Características**:

* Red de conmutación de paquetes.
* **Transmisión**: Sincrónica.
* **Control de errores**: ARQ Sliding Windows.
* **Orientado a la conexión**: Circuitos virtuales.
* **Ventajas**:
  + Asegura una calidad aceptable cuando el medio no es confiable.
* **Componentes**:
  + Terminal de datos.
  + Red X25: Equipos conmutadores de paquetes.
* **PAD**: Ensamblador de paquetes.

## **Parámetros de la Red:**

* Costos fijos y variables.
* Tamaño de paquete o ventana.
* Cantidad de información.
* Cantidad de LC.
* **Tipo de canal**: Entrante + Saliente + Bidireccional.
* **Tipo de Circuito Virtual**: Conmutado (SVC) o Permanente (PVC)

## **Capas**:

* **Física** (1): Define características para la conexión física entre DTE y DCE.
  + X21: Enlace digital. Señal balanceada.
  + X21 bis: Enlace analógico.
* **Enlace** (2): Define procedimientos para un enlace libre de errores.
  + Transmisión full duplex.
  + ARQ Sliding Windows con Piggyback
* **Red** (3): Define formato de paquetes, procedimiento de intercambio para DTE/DCE de VC con los DTE remotos.
  + Circuitos Lógicos (LC): Multiplexar enlace de nivel 2 en canales nivel 3.
  + Circuitos Virtuales (VC): Asociación lógica de múltiples LC entre origen y destino.
  + Modos de operación: Proceso de envío y recepción.
    - *Por paquete*: Sincronismo punto a punto
    - *Caracter*: Sincronismo hasta el PAD y luego asíncrono modo caracter.

### **HDLC: High Level Digital Link Control.**

* Protocolo de capa de Enlace (2)
* Orientado a la conexión.
* Orientado al bit.
* Sincrónico.
* Permite una transmisión transparente, independiente del código.
* Solo se utiliza en entornos punto a punto.
* **Control de errores**: CRC 16
* **Estaciones**:
  + Primarias: Controlan el enlace de datos.
    - Transmiten ordenes y reciben respuestas a secundarias.
  + Secundarias: Responden ordenes.
  + Combinadas: Actúan como primaria y secundaria.
* Configuraciones:
  + No equilibrada: Una terminal primaria y varias secundarias.
  + Equilibrada: Todos son combinados.

#### **Inserción de ceros:**

* Garantizar que no va a existir, dentro del campo de datos, una secuencia que trunque el mensaje erróneamente creyendo que llegó a su fin.
* Luego de leer la secuencia “11111” se inserta un cero sin importar lo que venga después.
* El receptor se encarga de remover ese cero cuando reciba la secuencia.

## **PDU**:

* **Máximo**: 135 bytes
* **Capa Red** (3): Paquete
  + GFI (4): Secuencia de numeración de paquetes.
  + LCI (12): Nro. grupo LC.
  + TPI (8): Tipo de paquete.
  + ADD (16): Plan de numeración.
  + FAC: Cobro revertido
  + Datos de usuario (16 - 128 - 1024): Identifica protocolo superior. Opcional.
* **Capa Enlace** (2): Trama.
  + Flag (8)
  + Address (8)
  + Control (8 - 16)
  + Información (0 a N)
  + Control de errores (16 - 32)
  + Flag (8)
* **Capa Físico** (1): Secuencia de bits.

# **Capítulo 7: Frame Relay:**

## **Características**:

* Protocolo de capa de Enlace (2).
* Orientado a la conexión.
* Basado en Circuitos Virtuales (VC) de tipo permanente (PVC)
* Trabajo sobre enlaces de alta calidad.
  + BER menor a 10 ^ -7
* **Circuitos Virtuales Permanentes (PVC):** Permite multiplexar comunicaciones, utilizando el mismo acceso físico para compartir paquetes por TDM.
* **Derivado de HDLC**:
  + Más liviano y sin ventanas.
  + No provee control de flujo ni errores.
  + No provee calidad de servicio ni recuperación frente a errores.
* **Define interfaz**: Entre:
  + CPE: Enrutadores o FRAD (Dispositivos de acceso a FR)
  + POP: Conmutadores rápidos con puertos de acceso para FR.
* **Topologías**:
  + Estrella: Utilizado cuando el flujo va hacia el nodo central.
  + Malla: Interconexión general entre varias sucursales.
* **Planos**:
  + De control: Establecimiento y liberación de conexiones lógicas.
  + De usuario: Responsable de la transferencia de los datos de usuario entre los suscriptores.

## **Control de errores:**

* Detección de errores en los extremos.
* No utiliza secuenciamiento de frames.
* **LAP - F**: Encargado del control de errores y flujo.
  + Versión mejorada de LAPD

## **Congestión**:

* Solo realiza notificación de congestión.
* Utiliza 2 bits en la cabecera para notificar congestión:
  + FECN: Hacia adelante.
  + BECN: Hacia atrás.

## **Gestión del tráfico:**

* **TC (Segundos)**: Intervalo de medición.
  + Durante el cual se mide la tasa de transmisión.
* **BC (bits)**: Tamaño de la ráfaga comprometida.
  + Cantidad máxima de bits que la red garantiza entregar durante un TC bajo condiciones normales.
* **CIR (bps)**: Tasa de información comprometida.
  + Lo mínimo que se tolera cuando la red está muy congestionada.
  + *CIR = BC / TC*
* **BE (bits)**: Tamaño en exceso de ráfaga.
  + Cantidad máxima de bits por encima del CIR que la red intentará entregar durante un TC.
* **EIR (bps):** Velocidad de información en exceso.
  + EIR = BE / TC
* **Access Rate**: Velocidad de transmisión del medio físico.
  + Es lo máximo que se puede utilizar.
* **Aclaraciones**:
  + Todo lo que esté por debajo del valor de BC está garantizado.
  + Lo que sea mayor que BC pero menor que (BC + BE) está comprometido.
  + Todo lo que esté por encima de (BC + BE) se descarta siempre.

# **Capítulo 8: ATM**

## **Características**:

* **Modo de transferencia asincrónico**:
  + Las celdas se transportan mediante canales sincrónicos.
  + No se sincroniza respecto de ningún usuario.
  + Tráfico en rafagas: Asignación de la posición en el flujo bajo demanda.
* **Transmisión transparente**: Cualquier secuencia arbitraria independiente del código.
* **PDU Pequeña**:
  + Tamaño fijo: Sencillo procesamiento.
  + Menor delay y buffer necesario.:
* Orientado a la conexión.
* Permite multiplexación de conexiones lógicas.
* Realiza conmutación en capa Física (1) con muy bajo delay.

## **Capas**:

* **Nivel 1**:
  + **Subcapa física**:
    - Convergencia de Tx: Independizar la velocidad del flujo de celdas de la interfaz física.
      * Generación y verificación del HEC (CRC)
      * Sincronización de celdas.
      * Conversión de celdas ATM en bits.
    - Medio físico: Controlar las funciones que dependen del medio.
      * Cables, conectores.
  + **ATM**: Multiplexación
    - Armado y delimitación de celdas.
    - Agrega y remueve el encabezado.
    - Control de congestión y ruteo.
* **Nivel 2**: No cumple la totalidad de la capa que pretende OSI.
  + **AAL:**
    - Convergencia: Independizar protocolos superiores.
      * Identificar los mensajes.
    - Segmentación y Reensamblado: De información en capas superiores.
      * Manejar cuadros de longitud mayor que las celdas.
      * Adaptar información a 48 bytes.

## **PDU (Celda).**

* Tamaño fijo de 53 bytes.
* **VPI + VCI**: Identifican la conmutación lógica con niveles de jerarquía.
  + Ambos tienen significado local.
* **MTU**: 48 bytes.
* **Encabezado**: 5 bytes.
  + VPI: 12 bits: ID Virtual Path. Ruteo dentro de red.
    - No se puede repetir.
  + VCI: 16 bits: ID Virtual Channel. Ruteo extremo a extremo.
    - Se puede repetir
  + CLP: 1 bit: Indica prioridad de celda.
    - 0 (Prioridad alta), 1 (Puede descartar)
  + HEC: 8 bits: Control de errores de cabecera mediante función polinómica.
    - Puede corregir 1 bit erroneo. Si hay más se descarta.
  + Información de enrutamiento y prioridad.
  + Identificación de celdas de un mismo camino.
* **Carga**: 48 bytes.
  + Transparente de extremo a extremo.
  + Información de mantenimiento.

## **Interfaces**:

* El control de flujo se realiza en el punto de ingreso a la red.
  + Una vez dentro, solo se transporta lo acordado a menos que haya congestión.
* **NNI**: Network to Network: Entre nodos de una red.
  + Tráfico interno.
* **UNI**: User to Network.
  + Punto de ingreso a la red.

## **Conmutación:**

* **VP Switch**: Solo conmuta los VPI (Caminos).
  + Conmuta todos los canales dentro de ese camino.
  + Se encuentran dentro del core de la red.
* **VC Switch**: Conmuta los canales que estan en distintos caminos para poder alcanzar los distintos destinos.
  + VCI de entrada y salida son modificados.

## **Clases de servicios:**

* **Tiempo real (RT)**:
  + Constante (CBR): Durante la conexión. Retardo máximo estable.
  + Variable (VBR): Restricción al retardo y a su variación.
* **No tiempo real (NRT)**:
  + Variable (VBR): Requisitos críticos en respuestas.
  + Disponible (ABR): Reserva con conocimiento de AB necesario.
    - Transmisión por rafagas.
  + No especificada (UBR): Aprovecha capacidad sin usar.
    - Best effort.
  + De tramas garantizadas (GFR): Servicio a subredes IP.
* **Calidad de servicio (Garantizado → Best Effort)**:
  + CBR → RT - VBR → NRT - VBR → ABR → UBR
* **Complejidad de implementación (Mínima a máxima)**.
  + UBR → CBR → NRT - VBR → RT - VBR → ABR

## **Atributos de tráfico:**

* Son indicados por el usuario.
* En el caso de que el usuario se pase, se marca como descartable la celda.
* **Peak Cell Rate (PCR)**: Velocidad máxima de transmisión.
  + Longitud de rafaga.
* **Sustainable Cell Rate (SCR)**: Limite al promedio de la tasa de transmisión.
  + Tasa sostenida para bits variables.
* **Maximum Burst Size (MBS)**: Cantidad máxima de celdas enviadas de forma continua a velocidad PCR.
* **Minimum Cell Rate (MCR)**: Tasa mínima requerida para la red.

## **Parámetros Quality of Service (QOS):**

* El usuario indica que calidad espera de la red.
* **Peak 2 Peak Cell Delay Variation**: Variación máxima soportada de retardo entre celdas.
* **Maximum Cell Transfer Delay**: Tiempo entre la transmisión del último bit en la UNI y recepción del primer bit de la UNI destino.
* **Cell Loss Ratio**: Tasa de pérdida máxima soportada en la conexión.

# **Capítulo 9: MPLS**

## **Características**:

* Multi Protocol Label Switching.
* Se encuentra entre la capa de Enlace (2) y capa de Red (3)
* Orientado a la conexión.
* **Basado en etiquetas**: Identifican las redes destino.
  + Evita meterse en los detalles del mensaje.
* **Ventajas**:
  + Ruteo de IP unicast y anycast.
  + Calidad de servicio que no se suele utilizar en IP.
  + Reducción de la tarea de conmutación core.
  + Procesamiento a partir de un match exacto de un String de longitud fija.
  + Permite transportar distintos protocolos de capa Red (3)

## **Problemas que originan MPLS:**

* **QoS**: Delay en:
  + Procesamiento.
  + Enlace.
  + No es predecible.
* **IP Routing**: Repetición del cálculo en cada nodo.
  + Se vuelve complejo el uso de tablas cuando la red crece.
* **Camino más corto**: Búsqueda del camino con menor cantidad de saltos.

## **Componentes**:

* **LSR**: Label Switching Router.
  + Entienden IP y MPLS.
  + **Tipos**:
    - Edge (Entrada / Salida): Toman un paquete, lo analizan y le asignan la etiqueta para que ingrese a la red.
      * Cuando sale de la red, le quitan la etiqueta y entregan el paquete original.
    - Core (Internos): Solo conoce MPLS
      * Más eficiente que un router común.
* **Etiqueta**: Identificador de 4 bytes que define el destino y el servicio de un paquete.
  + Identifica un FEC
  + **Significado local**: Cada LSR mapea una etiqueta a un FEC.
    - La asociación se intercambia entre los LSR.
* **FEC**: Clase equivalente de envío: Grupo de paquetes tratados de la misma forma sobre un mismo camino.
  + Identifica un red destino.
  + Permite, dentro de una misma red, tener 2 flujos distintos.
  + Se asigna en el momento en el que un paquete entra a la red.
* **LSP**: Intercambio de rutas por etiqueta: Ruta a través de uno o más LSR en un nivel de jerarquía que sigue un paquete de FEC.

## **Arquitectura de un Router:**

* **Plano de control**: Procesos que corren en el router con una función administrativa o de control.
  + Intercambio de información de ruteo y etiquetas con otros equipos.
* **Plano de datos**: Parte del router que se encarga de la conmutación del tráfico.
  + Identificar el mejor camino dentro de la tabla de ruteo.

## **PDU**:

* Datos de usuario.
* Cabecera IP.
* **Cabecera MPLS**:
  + TTL (8): Misma función que en IP.
  + Stack (1): Apilar etiquetas con jerarquía.
  + Exp (3): Identificar clase de servicio.
  + Etiqueta (20).
* Cabecera nivel 2.

# **Capítulo 10: Seguridad:**

## **Criptografía**:

* Ciencia de lectura y escritura de mensajes codificados.
* Es una pieza fundamental en los mecanismos de:
  + **Autenticación**: Establecer la identidad del transmisor y receptor de información.
  + **Integridad**: Asegurarse que los datos no fueron alterados.
  + **Confidencialidad**: Asegurar que nadie, salvo los involucrados, son capaces de interpretar los datos transmitidos.

## **Ataques informáticos:**

* **Tipos**:
  + Interceptación.
  + Fabricación.
  + Modificación.
  + Destrucción.
* **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.

## **Encriptación**:

* Mecanismo criptográfico que consiste en un algoritmo que usa un valor (clave) para encriptar el mensaje.
  + La longitud de la clave es importante para la fortaleza del mecanismo.
* **Simétrica**: Única clave en común y el mismo algoritmo para encriptar o desencriptar.
  + **Ventajas**:
    - Simple y eficiente en términos de cómputo
  + **Desventajas**:
    - Se dificulta la distribución de claves a muchos participantes.

### **Asimétrica**:

* Clave pública. Los extremos pueden o no usar el mismo algoritmo.
* **Garantiza**:
  + Confidencialidad: Solo el receptor puede leerlo.
  + Integridad: No se modifican los datos salvo con la llave privada del receptor.
  + Autenticación.
  + No repudio
* **Pasos**:
  + Dos personas intercambian las claves públicas.
  + Cada uno encripta con clave privada propia y clave pública del receptor.
* **Función de Hash:** Toma una entrada de longitud arbitraria y genera una de longitud fija.
  + Consistencia: Misma entrada generar la misma salida.
  + Aleatoriedad: Impedir adivinar el mensaje original.
  + Unicidad: Casi imposible encontrar 2 mensaje con la misma salida.
  + One way: Para una salida no se puede deshacer la operación y obtener el original.

## **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.

## **Firewall**:

* Sistema que actúa como barrera segura entre dos redes.
* Está compuesto por HW y SW.
* **Ventajas**:
  + Concentración de la seguridad en un único unto.
  + Regular el uso de la red exterior.
  + Limitar el tráfico de servicios vulnerables.
  + Mejorar la privacidad del sistema.
* **Tipos**:
  + A nivel de red: Direcciones IP y Nro. de puerto.
  + A nivel de aplicación: No permitir tráfico directo entre redes.
* **Decisiones al implementarlo**:
  + Política de seguridad de la organización: Whitelist o Blacklist.
  + Nivel de seguridad deseado:
    - Analisis de necesidades con riesgo aceptable.
    - Nivel de seguridad que satisfaga.
  + Evaluación de costos: Mejor relación costo - beneficio.

## **Firma digital:**

* Técnica de seguridad informática aplicada sobre la información digital que se intercambia en la red.
* **Garantiza**: Autenticidad, integridad y no repudio.
  + Puede garantizar confidencialidad si se adiciona a un mensaje encriptado completamente.
* **Basado en**:
  + Criptosistema asimétrico: Clave pública y clave privada.
  + Función Hash: Salida de longitud fija.
  + Autoridad certificante: Registro y distribución de claves públicas.

## **TLS (Transport Layer Security):**

* Protocolo para proteger tráfico web entre servidor HTTP y un browser.
* Usa encriptación asimétrica (Establecer conexión) y simétrica (todo lo demás)
* El cliente envía una propuesta de encriptación cuando recibe el certificado del servidor.

### **Certificados**:

* El servidor los presenta a los clientes.
* Garantiza que el servidor es quien dice ser según la url.
* Entidad certificante: Encargados de generar certificados con un tiempo de duración establecida

## **IP Security (IP Sec):**

* Conjunto de protocolos de seguridad que permiten agregar encriptado y autenticación en la comunicación.
* Reside en Capa Red (3) y es transparente para las aplicaciones.
* **Modos**:
  + Transporte: Solo protege la información de transporte.
    - No protege información de IP.
  + Túnel: Protege toda la información.
    - Tiene un costo superior.
* **Protocolos**:
  + AH (Auth. Header): Garantiza autenticidad e integridad.
    - No realiza encriptación
  + ESP (Encrypted Security Payload): Garantiza autenticidad, integridad y privacidad.