# **Capítulo 1: Introducción**

### **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.

## **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.
* **Colisión**: 2 estaciones sensan un canal desocupado y transmiten en simultáneo.
* **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.
    - Especifica el destino y origen para protocolos de capa superior.
* **Red**:
  + Encargada de asignar el preámbulo.

## **Segmentación**:

* **Ventajas**:
  + Aislar el tráfico entre los segmentos.
  + Aumentar el ancho de banda al crear dominios de colisión más pequeños
  + Mejorar la seguridad.
* **Desventajas**:
  + Menor performance ya que se agregan más equipos a la red.
* **¿Como hacerlo?**: Usando un Router, un Bridge o un 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.
  + Sostiene la transmisión para que las demas estaciones sepan que hubo una colisión.
  + Espera un tiempo aleatorio cuando detecta una colisión.
* **CSMA / CA**: Evasión de colisiones.
  + Sensado permanente y uso de técnicas para evasión.
  + Usa RTS / CTS para reservar el medio.
  + El receptor verifica el FCS y devuelve un ACK.
  + Solo transmite si el medio está libre por un tiempo determinado.

### **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.

## **VLAN**:

* Asociación lógica de las estaciones que la forman.
* Cada VLAN es un dominio de broadcast.
* **TAG (802.1Q)**: Múltiples redes pueden compartir el mismo enlace.

## **Ethernet (802.3)**:

* Sin confirmación.
* **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.*

### **Trama 802.3 Vs. Ethernet**

* **802.3**: Preámbulo (7B) + SFD (1B) + MAC (2B o 6B) + Long. Trama (2B)
* **Ethernet**: Preámbulo (8B) + MAC (6B) + Type (2B)

## **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.
* **Spanning Tree (802.1D)**:
  + Descubrir loops y desactivar vínculos redundantes.
  + Red física de malla → Red lógica de árbol sin bucles.

### **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**

## **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:**

* **CSMA / CA.**
* **Elementos:**
  + Access Point: Conectar dispositivos inalambricos a red cableada.
  + Terminales.
  + Sistema de distribución: Lan cableada.
* **Normas**:
  + 802.11a: 54 Mbps. 5Ghz
  + 802.11ac: Hasta 3 Gbps. 2,4 y 5 Ghz.
* **Problemas**:
  + Nodo oculto: Una estación cree que el canal está libre pero en realidad está ocupado por un nodo al que no escucha.
    - A → RTS. B→ CTS. C → Capta CTS. A → Envía.

### **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: Distribuida. Todos lo hacen por su cuenta.
      * Competencia para transmitir.
      * *NAV*: Indica que el medio está libre → transmito
      * *RTS / CTS*: CSMA / CA
    - PFC: Centralizado: Que no sea 100% aleatorio.
      * Acotar la incertidumbre para transmitir.
      * El AP se encarga de asignar turnos para transmitir a los equipos.
      * Mientras está en PFC, los equipos no escuchan para transmitir.
        + Cuando se conectan dicen si quieren suscribirse a la lista.
        + Va preguntando a cada uno si quieren transmitir.
      * Al final regresa a DFC.
  + **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.

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

* Mínima interferencia entre canales y frente a otros dispositivos.
* Escaneo y cambio de canal.
* No requiere licencia ya que utiliza las bandas 2.4 y 5.8 Ghz
* **Acceso al medio**: CSMA / CA.
* **Auto - Canal**: Los dispositivos eligen el canal que mejor está funcionando.
* **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.
* **Campos:**
  + Dirección 1: Destino de la trama.
  + Dirección 2: Origen de la trama.
  + Dirección 3: Filtrado por AP y Sistemas de distribución.
  + Dirección 4: Opcional.
  + Duración: Campo de la cabecera que indica el valor del NAV.
    - Tiempo restante para transmitir

#### **WiFi 6:**

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

# **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.

### **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**:
  + A:
  + B: 128 a 191
  + C: 192 a 223
  + D: 224.0.0.0 en adelante.
    - Reservadas para multidifusión.
    - No se usa para conectar hosts.

#### **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.
    - Network Unreachable: No sabe como llegar a la red.
    - Host Unreachable: Llegó a la red pero el host no contesta.
    - Fragmentation Needed: El bit DF = 1 pero se necesita fragmentar.
  + 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.
* **Traceroute**: Sirve para conocer la ruta que va a realizar un paquete.
  + Se envía un mensaje a cada nodo del camino con la idea de que se agote en el (Utilizando el TTL.
  + Al agotarse, se descarta y, mediante ICMP, se envía un mensaje del tipo “Tiempo de espera agotado” con la información del nodo.
    - IP, delay, problemas.

## **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.

## **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.
* **Multiplexación**: Información proveniente de diferentes fuentes puedan compartir la misma línea en simultaneo.
  + Usa los campos Puerto origen y destino.
* **MSS**: Tamaño máximo de segmento.
  + Tamaño máximo del campo de datos.
  + Se declara al establecer la conexión en el campo opciones.
  + No se modifica durante el intercambio de segmentos.
  + Se calcula a partir de la MTU de la interfaz.
* **Opciones**: Permite realizar optimizaciones en las transmisiones.
  + MSS
  + Window Scaling.
  + Selective ACK
* **Puntero urgente**: Campo que permite indicar donde termina la secuencia de datos urgentes.

### **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.
* **Control de flujo**: Mediante Sliding Windows de tamaño variable.
* **Control de congestión**: En sistemas intermedios.
* Entrega ordenada.
* Conexiones full duplex.
* Confirmaciones.
* Timeouts.
* Checksum de mensaje completo (Cabecera + mensaje)

### **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.

### **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.

### **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
  + Nro. Secuencia = X
  + Nro. Acuse recibo = null
* El Servidor envía un mensaje vacío con SYN y ACK confirmando la petición.
  + Nro. Secuencia = Y
  + Nro Acuse recibo = X +1
* Cliente envía un segmento ACK.
  + Puede o no contener información pero la conexión ya está establecida.
  + Nro Secuencia = X + 1
  + Nro Acuse Recibo = Y + 1

### **Cierre de conexión:**

* Cliente envía FIN.
* Servidor responde ACK
* Cliente espera que el servidor envíe FIN.
* Cliente responde con ACK.

## **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
  + 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.
* **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.

## **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.
* **Default gateway**: Camino por defecto para conectarse a otras redes.
* **Default route**: Para paquetes sin información de próximo salto.
  + Hace uso del default gateway
* **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.

### **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.

### **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.

## **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.
* **Broadcast**: No implementa.
  + Utiliza multicast para enviar un paquete a todas las interfaces de un grupo.

### **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.
* 320 bits.
* **Formato**: Notación hexadecimal. 16 bytes con 2 números hexa cada uno.
  + ID Ruteo: 6B.
  + ID Subred: 2B.
  + ID Interfaz: 8B.

### **Trama**:

* Versión 4 bits.
* ToS: 8 bits
* Etiqueta Flujo: 20 bits
* Longitud total: 16 bits
* Protocolo: 8 bits
* TTL: 8 bits
* IP Origen: 128 bits
* IP Destino: 128 bits

# **Capítulo 5: Redes WAN:**

## **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.

### **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.

# **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.

## **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 flujo**: ARQ Sliding Windows.
* **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.

#### **Trama**:

* Flags: 8 bits.
* FCS: 16 o 32 bits.
* Datos: Variable.
* Control: 8 o 16 bits.
  + Mecanismos de control de flujo y enlace.
* Dirección: 8 bits.
  + ID Secundaria que transmitió o va a recibir la trama.

#### **Tipos de trama:**

* **De información**: Transportar información y realizar control de flujo y errores cuando se usa piggyback.
* **De supervisión**: Control de flujo y errores cuando no se requiere piggyback.
* **No numeradas**: Funciones para control de enlace.

#### **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.

# **Capítulo 7: Frame Relay:**

## **Características**:

* Protocolo de capa de Enlace (2).
* Orientado a la conexión.
* Trabajo sobre enlaces de alta calidad.
  + BER menor a 10 ^ -7
* Permite multiplexar.
* **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 flujo:**

* Mediante datos elegidos para descarte (DE = 1)

## **Trama**:

* Flag: 8 bits.
* Dirección: Mínimo 16 bits.
  + DLCI: 10 bits. Canal.
  + EA: 1 bit. Fin de cabecera.
  + C/R: 1 bit.
  + DE: 1 bit.
  + FECN: 1 bit.
  + BECN: 1 bit.
* Datos: Máximo 4096 B.
* FCS: CRC - 16
* Flag: 8 bits.

## **Control de errores:**

* Detección de errores en los extremos.
  + CRC - 16
  + Capas superiores se ocupan de la corrección.
* No utiliza secuenciamiento de frames.
* **LAP - D**: Control enlace de datos para canales que transportan información de control y señalización.
* **LAPF Core**: Encargado del control de errores y flujo.
  + Versión mejorada de LAPD

## **Definiciones**:

* **Puerto**: Permite el ingreso a la red.
* **Velocidad Puerto (bps)**: Velocidad máxima de entrada a la red.
* **TC (seg)**: Intervalo de medición.
* **BC (bits)**: Tamaño comprometido de rafaga.
* **BE (bits)**: Tamaño en exceso de rafaga.
* **CIR (bps)**: Velocidad Información comprometida.
* **EIR (bps)**: Velocidad información en exceso.

## **Congestión**:

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

# **Capítulo 8: ATM**

## **Características**:

* Orientado a la conexión.
* Mínimo control de errores.
* Permite multiplexación de conexiones lógicas.
* Realiza conmutación en capa Física (1) con muy bajo delay.
* **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.
* **MTU**: 48 Bytes.
* **PDU:** Celda**:** Tamaño fijo (53 Bytes)
  + Sencillo procesamiento.
  + Menor delay y buffer necesario.
  + **VPI + VCI**: Identifican la conmutación lógica.
    - Significado local.
* **Interfaces**:
  + **NNI**: Network 2 Network: Interno
  + **UNI**: User 2 Network: Ingreso a la red.

## **Trama**:

* **Cabecera**: 5 Bytes.
  + GFC: 4 bits. Solo UNI.
  + VPI: 8 o 12 bits (UNI o NNI)
  + VCI: 16 bits.
  + Payload Type: 3 bits.
  + CLP: 1 bit: Prioridad.
  + HEC: 8 bits: Control de errores de cabecera.
    - Solo corrige 1 bit erroneo. Si hay más descarta.
* **Datos**: 48 Bytes.

## **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.

## **Planos de operación:**

* **De usuario**: Transferencia de info de usuarios y controles de flujo y errores.
* **De control:** Controles de llamada y de conexión.
* **De gestión**:
  + De plano: Coordinación entre planos y como un todo
  + De capa: Recursos y parámetros de protocolos.

## **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.

# **Capítulo 9: MPLS**

## **Características**:

* Multi Protocol Label Switching.
* Se encuentra entre la capa de Enlace (2) y capa de Red (3)
* Conmutación Datagrama.
* Orientado a la conexión.
* **Funciones**:
  + Control de tráfico (Seguridad)
  + Control de AB
* **Basado en etiquetas**: Identifican las redes destino.
  + Evita meterse en los detalles del mensaje.
* **Ventajas**:
  + Ruteo de IP unicast y anycast.
  + Calidad de servicio adaptable.
  + 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.

## **Trama**:

* Label: 20 bits. Identifica el FEC.
* EXP: 3 bits: Calidad de servicio.
* Stack: 1 bit: Indica si hay etiquetas anidadas.
* TTL: 8 bits: Mismo uso que en IP.

## **Componentes**:

* **LSR**: Label Switching Router.
  + Solo conoce MPLS
  + Más eficiente que un router común.
  + **Label Distribution Protocol**: Para intercambiar información de etiquetas entre los distintos LSR.
* **LER:** Label Edge Router:
  + 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.
* **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: Concatenación de Ler (ingreso) + N \* LSR + Ler (Egreso)

## **Planos:**

* **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.
* **De datos**: Parte del router que se encarga de la conmutación del tráfico.
  + Identificar el mejor camino dentro de la tabla de ruteo.

# **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.

## **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: Las partes involucradas participaron y no lo pueden negar.
* **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.

## **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.
* **Desventajas**:
  + Una firma se vincula con un único documento.
  + Requiere de una autoridad certificante.
* **Basado en**:
  + Criptosistema asimétrico: Clave pública y clave privada.
  + Función Hash: Salida de longitud fija.
  + Autoridad certificante: Registro y distribución de claves públicas.

## **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.