# **Redes Wan:**

* **Compuesto por**:
  + Enlaces de comunicaciones.
  + Nodos de red.
  + Equipos terminales.

## **Enlaces de comunicaciones:**

### **Tipos**:

* **Según los puntos que tiene**:
  + Punto a punto.
  + Punto a multipunto.
* **Segun las caracteristicas**:
  + Dedicados
  + Conmutados.

## **Tipos de conmutación:**

| **Característica** | **Circuitos** | **Paquetes - Datagrama** | **Paquetes - Circuitos Virtuales** |
| --- | --- | --- | --- |
| **Conexión** | Física | Sin conexión lógica | Lógica |
| **Transmisión** | Continua | Paquete | |
| **Uso de datos** | Eficiente Voz  Ineficiente Datos | Poco eficiente voz  Eficiente Datos | |
| **Ordenamiento (Ord Transmisión)** | Mantiene | No mantiene | Mantiene |
| **Facturación** | Por tiempo y distancia | Por cantidad de paquetes y tiempo | |
| **Encaminamiento** | Rígido | Ruta menos costosa en delay y saltos | |
| **Ruta** | Dedicada | Sin ruta | Ruta no dedicada |
| **Enrutamiento** | Misma ruta para toda la Tx | Cada paquete tiene la propia | Misma ruta para toda la Tx |
| **Delay** | De establecimiento | De Tx de paquete | De establecimiento y de Tx de paquete |
| **Ancho de Banda** | Fijo | Dinámico | |
| **Congestión** | Bloquea el establecimiento | Aumenta el retardo del paquete | Bloquea el establecimiento y aumenta el retardo del paquete |
| **Mensajes** | No se almacena | Paquete se puede almacenar hasta su envío | Se almacena el paquete obligatoriamente hasta el envío |

## **Tipos de servicios:**

* **Orientado a la conexión:**
  + **Orden**: Mantiene el orden de tráfico.
  + Similar a un tubo.
  + Ej: Sistema telefónico.
* **Sin conexión:**
  + **Orden**: No siempre lo mantiene.
  + **Encaminamiento**: Independiente.
  + Similar a una carta.
  + Ej: Correo postal
* **Circuito virtual:**
  + **Encaminamiento**: Sin decisiones por cada bloque.
  + Establecimiento de ruta extremo a extremo.
* **Datagrama**:
  + **Encaminamiento**: Independiente.
  + Mayor trabajo pero más robusto y con mayor capacidad de adaptación.
  + No determina las rutas de forma anticipada.

# **Red de conmutación de circuitos:**

* Implica la existencia de un canal de comunicaciones dedicado entre dos estaciones.
* **Etapas**:
  + Establecimiento de circuito.
  + Transferencia de datos.
  + Desconexión del circuito.
* **Componentes**:
  + Abonados.
  + Bucle local: Lazo de abonado.
  + Centrales.
  + Líneas principales.

## **Tipos de conmutación por circuitos:**

### **Por división en el espacio:**

* Inicialmente analógicos.
* Las rutas establecidas son físicamente independientes entre sí.

### **Por división en el tiempo:**

* Basado en sistemas digitales y multiplexación por división de tiempo (TDM).
* Canales de menor velocidad son muestreados a mayor velocidad para integrarse a un bus TDM

## **Nuevos conceptos:**

* **Conmutación IP**: Técnica que permite enrutar paquetes de datos más rápido que la tradicional mediante el uso de conmutadores en capa 3.
  + No se necesita un Gateway IP.
* **IP PBX**: Equipo de comunicaciones diseñado para ofrecer VoIP.
* **IP Trunking**: Uso corporativo y a gran escala de VoIP.
  + Para el intercambio de datagramas IP.

## **Protocolo PPP:**

* Punto a Punto.
* Deriva del protocolo HDLC.
* **Capa**: Enlace de datos: 2.
* **Objetivo**: Encapsular datagramas IP cuando se envía a través de una línea serial.
* **Funciones**:
  + Transporte de datos.
  + Asegurar el enlace y recepción ordenada.
    - Utiliza ARQ Sliding Windows.
  + Autenticación.
  + Asignación dinámica de dirección IP.
* **Problemas**:
  + No provee cifrado de datos.

### **Características**:

* Permite la conexión de líneas sincrónicas y asincrónicas.
* Permite asignación dinámica de direcciones IP en ambos extremos de la conexión.
* Permite el transporte de varios protocolos de red.
* Implementa un mecanismo de control de red NCP.
* Se puede usar para crear una VPN cifrada o no cifrada.
  + Si se quiere cifrar, se debe hacer en una capa superior.

### **Etapas**:

* **Establecer conexión**: Se realiza la conexión y se negocian los parámetros relativos al enlace usando LCP.
  + Autenticación y tamaño de datagramas.
* **Autenticación**: No es obligatorio. Se puede realizar a través de:
  + PAP: Password Authentication Protocol.
    - Inseguro debido a que envía usuario y contraseña directamente.
  + CHAP: Challenge Handshake Authentication Protocol.
    - Se envía la contraseña cifrada.
* **Configuración de red**: Se negocian parámetros dependiendo del protocolo de red que utilice.
  + Se pueden usar varios al mismo tiempo pero se deben configurar.
* **Transmisión**: Envío y recepción de la información de red.
  + LCP Comprueba que la línea esté activa durante períodos de inactividad.
* **Terminación**: Se puede finalizar la conexión en cualquier momento y por cualquier motivo.

### **PDU**:

* **Bandera**: B: 8 bits.
* **Dirección**: D: 8 bits: Siempre utiliza el estándar de difusión debido a que el camino ya está asignado.
  + Se puede eliminar.
* **Control**: C: 8 bits: Tipo de trama no numerada.
  + Se puede eliminar.
* **Protocolo**: P: Identificador: 16 bits.
  + Puede asociarse a varios.
* **Información**: 0 a N bits.
* **FCS**: Utiliza CRC: 16 a 32 bits.
* **Bandera de cierre**: 8 bits.

## **SLIP (Solo IP):**

* Serial Line IP.
* Protocolo de proceso de tramas utilizado para envíos IP a través de una línea serial.
* **Objetivo**: Encapsular datagramas IP.
* **Características**:
  + Líneas sincrónicas.
  + Antiguo.

# **WAN X-25:**

* Conjunto de protocolos de la UIT (Unión Internacional de Telecomunicaciones).
* Red de comunicación de paquetes.
* **Capas**: Capa 1, 2 y 3 de OSI.
* Estructura:
  + Terminal de datos:
  + Red X25: Equipos conmutadores de paquetes.
  + Terminal de datos.

## **Características**:

* Es una interfase de usuario y Red: DTE / DCE.
* Asegura una calidad aceptable cuando el medio no es confiable.
  + Existe un problema en los enlaces.
* **Transmisión**: Sincrónica.
* **Control de errores**: ARQ Sliding Windows.
* **Orientado a**: Conexión: Circuitos virtuales.

## **Parámetros de la red:**

* **Costos**: Fijos + Variables.
  + No dependen de la distancia.
* Tamaño de paquete.
* Tamaño de ventana.
* **Throughput**: Cantidad de información.
* Cantidad de canales lógicos.
* **Tipo de canal**:
  + Entrante.
  + Saliente.
  + Bidireccional.
* CUG:
* **SVC o PVC**: Bajo demanda o permanente.
* Selección rápida.
* Cobro revertido.

## **PDU**:

* **Tamaño máximo**: 1080 bits (135 bytes).
* **Nivel Paquete**:
  + Cabeza.
  + Datos.
* **Nivel trama**:
  + Bandera: 8 bits.
  + Dirección: 8 bits.
  + Control: 8 a 16 bits.
  + Información: 0 a N bits.
  + Control de errores: 16 o 32 bits.
  + Bandera: 8 bits.
* **Nivel físico**:
  + Secuencia de bits.

## **Capas**:

### **Capa 1: Físico**:

* Define características mecánicas, eléctricas, funcionales y procedurales para la conexión física entre DTE y DCE.
* **Incluye**:
  + X21: Enlace digital: Señal balanceada.
    - Cada circuito tiene su propio retorno.
  + X21 Bis: Enlace analógico: Señal desbalanceada.
* **Vtx**: Máximo de 64 Kbps.
* **PDU**: Secuencia de bits.

### **Capa 2: Enlace de datos**:

* Define los procedimientos para tener un enlace libre de errores.
* **Protocolo**: HDLC, versión LAP-B.
  + Procedimiento de acceso a enlace.
  + Balanceado.
  + Punto a punto.
  + ABM: Modo balanceado asincrónico.
* **Modo transmisión**: Full Duplex.
* **FCS**: ARQ Sliding Windows:
  + Usa Piggyback.
* PDU: Trama.

#### **HDLC**:

* Protocolo de enlace de la ISO.
* **Orientado**: Al bit.
* **Tipo**: Sincrónico.
* **Tipos de difusión**:
  + **Unicast**: Única para cada cliente.
  + **Multicast**:Enlace multipunto de grupo.
  + **Broadcast**: Enlace multipunto de difusión.
* **FCS**: CRC de 16 bits.
* **Configuraciones**:
  + **Órdenes**: Primaria a secundaria.
  + **Respuestas**: Secundaria a primaria.
  + **Balanceada**: 2 servidores (2 primarias).
  + **No balanceada**: 1 servidor (1 primaria).
* **Modos de operación:**
  + **Respuesta normal (NRM)**: Sin balanceo.
    - Se transmite solo cuando lo indica el servidor (Primaria).
    - Enlace punto a punto o multipunto.
    - Half duplex.
    - No hay cambio de rol.
  + **Respuesta sincrónica (ARM)**: Sin balanceo.
    - Transmite sin permiso del servidor.
    - Enlace punto a punto.
    - Full duplex.
    - No hay cambio de rol.
  + **Balanceado asíncrono (ABM)**: Con balanceo.
    - Cada estación es primaria y secundaria.
    - Enlace punto a punto.
    - Full duplex.

### **Capa 3: Red:**

* Define formato de paquetes, procedimientos para el intercambio y establecimiento o supervisión en la DTE/DCE de circuitos virtuales con los DTE remotos.
* Controla circuitos virtuales y canales lógicos.
  + **Circuitos virtuales**: Asociación lógica de múltiples canales (LC) entre origen y destino.
    - Pueden ser PVC (Permanente) o SVC (Bajo demanda).
  + **Circuitos lógicos**: Multiplexación del enlace en capa 2 en varios canales de capa 3.
    - Se numeran con un ID de LC (LCI).
    - Existen localmente.
* **Modos de operación**: Progreso de envío y recepción.
  + **Por paquete**: Sincronismo punto a punto.
    - DTE.
    - PSDN: Packet Switch Data Network: DCE + DCE
    - DTE.
  + **Caracter**: Sincronismo hasta llegar al PAD, luego es asíncrono en modo caracter:
    - DTE.
    - PSDN: DCE + DCE + PAD.
      * PAD: Package Dissasembler.
    - DTE-C
* **PDU**: Paquete

# **Frame Relay:**

## **Características**:

* **Fast Packet Switching**: La comunicación se produce a nivel de Frame.
  + Capa de enlace de datos (2).
* **PDU**: Frame.
* **Orientado**: Conexión.
  + Circuitos virtuales (PVC).
* **Circuito Virtual (VC)**: Asociación lógica de DLCI.
  + DLCI: Data Link Connection Identifier: Tiene significado local.
* **Tráfico**: Por rafagas.
  + Tipo LAN.
* Se reemplaza LC de X-25 por DLCI.
* Trabaja sobre enlaces de alta calidad.
  + Asociado a la fibra óptica.
  + BER menor a 10 ^ -7.

## **Funciones**:

* Reemplazo de líneas punto a punto.
* Definir la interfaz entre CPE (Equipo de instalación del cliente) y POP (Punto de presencia).
  + CPE: Enrutadores o FRAD (Dispositivos de acceso a FR).
  + POP: Conmutadores rápidos que ofrecen puertos de acceso a la red FR.

## **Estaciones**:

* **Terminales**:
  + Necesitan una mayor inteligencia.
  + Proporcionan:
    - Cobertura de errores.
    - Control de secuencia.
    - Control de flujo
* **Intermedias**:
  + Solo retransmiten.

## **Ventajas**:

* Alta velocidad.
* Baja latencia.
* Uso dinámico del ancho de banda.
  + Solo se ocupa cuando hay información que transmitir.
* Soporte sobre ISDN banda angosta.
  + Intefaz básica.

## **Arquitectura de protocolos:**

* **Usuario**: transferencia de datos a usuarios.
  + Funcionalidad de extremo a extremo.
  + **Capa 1**: L430 / L431.
  + **Capa 2**:
    - Plano de control:
      * Q931 / Q933
      * LAPD: Q921: Control de errores y flujo.
    - Plano de usuario:
      * LAPF Control: Funciones de usuario seleccionables.
      * LAPF Core: Q922
* **Red**: Establecimiento y liberación de conexiones lógicas.
  + Se implementa entre usuario y red.
  + **Capa 1**: L430 / L431
  + **Capa 2**:
    - Plano de control:
      * Q931 / Q933
      * LAPD: Q921
    - Usuario:
      * LAPF Core.

## **Controles**:

### **De errores:**

* Solo detección de errores (FCS) en los extremos.
* La corrección es tarea de capas superiores.
* No se lleva secuenciamiento de cuadros:
  + No se usa campo de control.
  + Es realizado por el LAP-F Control.

### **Prevención de congestión:**

* Mediante FECN y BECN.
  + FECN: Se setea cuando la congestión es en el mismo sentido en el que va el frame.
  + BECN: Se setea cuando la congestión es en sentido contrario en el que va el frame.
  + POP: Setea los bits FECN y BECN.
  + CPE y Admin de red: Detectan los bits.

### **Control de congestión:**

* Mediante datos elegidos para descarte (DE).
  + Hay rechazo de frames.

### **Control de flujo:**

* Realizado por LAP-F Control.

## **Voz sobre FR:**

* La voz es tolerante a perdidas pero no a retardos.
* Prioriza el tráfico y el uso de DLCI para voz.
* Se utilizan FRAD o routers para voz y datos.
* Uso de algoritmos de compresión PCM o ADPCM.
  + 64 - 32 - 16 - 12 - 8 Kbps.

### **Ventajas**:

* Menor costo: Entre 20% y 30% frente a comunicaciones telefonicas convencionales.
* Fragmentación: Menor tamaño de cuadros.
* Menor retardo en la red.
* Aprovecha los silencios.
* Rutas con pocos saltos (Entre 3 y 4).

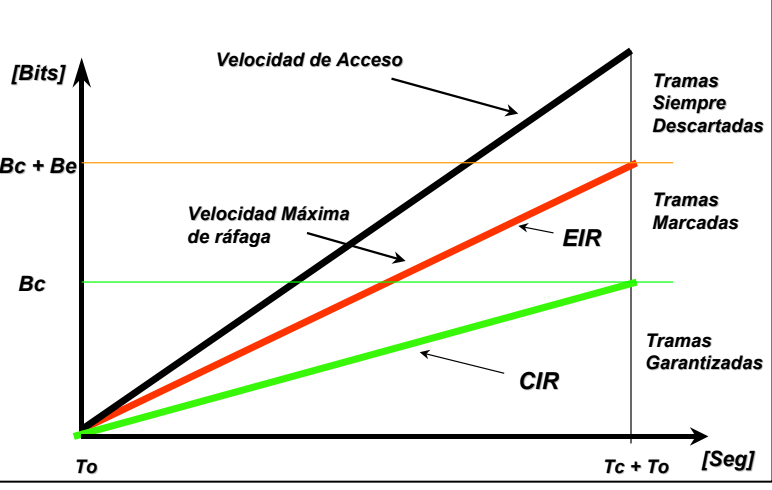
### **Desventajas**:

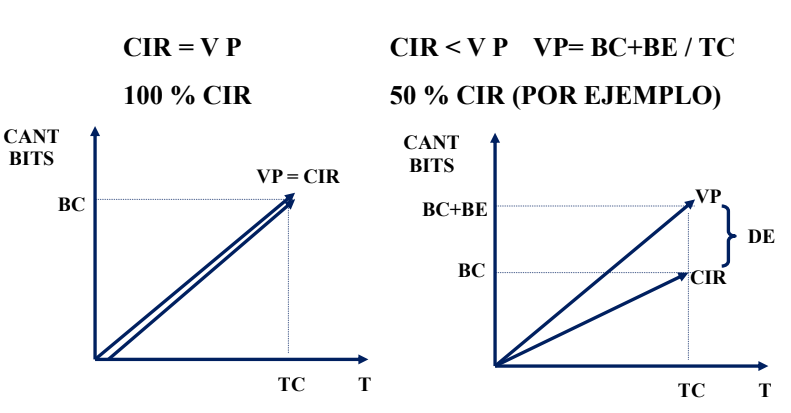
* Menor QoS.
* No acepta retransmisiones por lo que genera interrupciones.

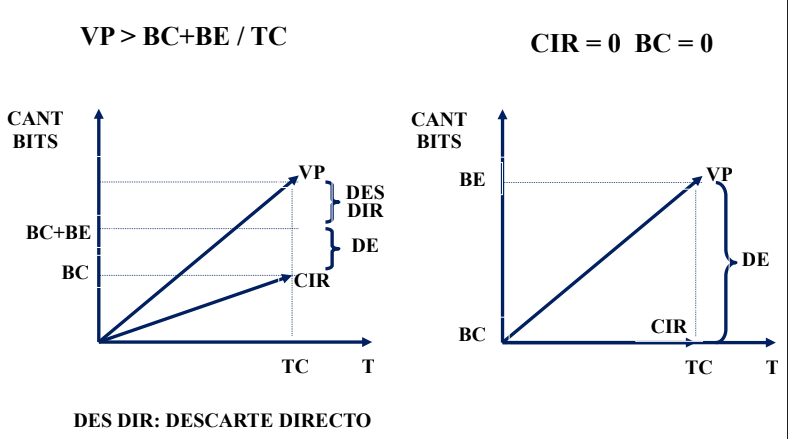
# **Ejercicios Frame Relay:**

## **Definiciones**:

* **Puerto**: Permite el ingreso a la red.
  + POP provee varios.
  + PVC nacen en los puertos.
* **BC** (bits): Tamaño comprometido de ráfaga:
  + Cantidad máxima de bits que se transmiten por un PVC en un intervalo de medicion (TC), en condiciones normales.
* **TC** (segundos): Intervalo de medición.
  + Con y sin actividad.
* **BE** (bits): Tamaño en exceso de ráfaga.
  + Cantidad no comprometida.
* **VP** (bps): Velocidad de puerto: Velocidad máxima de entrada a la red FR.
  + Desde 56 - 64 Kbps a 1,5 - 2 Mbps.
* **CIR** (bps): Velocidad de información comprometida para el PVC en condiciones normales.
  + CIR = BC / TC
* **EIR** (bps): Velocidad de información en exceso.
  + EIR = BE / TC
* **Sobre suscripción**: Asignación dinámica del ancho de banda a los PVC.
  + Multiplexado estadístico.
  + Suma de los CIR de cada PVC > VP







# **Protocolo ATM**

* **Asynchronous Transference Method**: Modo de transferencia asincrónico.
* Es el resultado de nuevas necesidades
  + Cambios en los negocios de las comunicaciones y del trafico

## **Características**:

* **Orientado**: Conexión.
* Montado sobre ISDN Banda Ancha.
  + Basadas en tecnologías SDH.
* **Velocidad**: Binaria de más de 2,4 Gbps.
  + Alta calidad en los vínculos.
* Permite transporte de todo tipo de servicio.
* Utiliza capas de adaptación para integrar servicios.
* Permite conmutación rápida con muy bajo delay.
  + Realizados en capa física (1).
* Reduce funcionalidad en los nodos y delega funciones a los extremos.

## **Asincronismo**:

* Las celdas son transportadas mediante canales **sincrónicos**.
* No se sincroniza respecto a ningún usuario.
* Las posiciones en el flujo se asignan bajo demanda.
  + Tráfico en ráfagas.

## **PDU**:

* Celda o célula.
* **MTU**: 48 bytes.
* Tamaño fijo de 53 bytes.
  + **Encabezado**: 5 bytes.
    - Info de enrutamiento y prioridad.
    - Identificación de celdas de un mismo camino.
  + **Pilot**: Carga: 48 bytes.
    - Transparente de extremo a extremo.
    - Contiene voz, video o datos.
    - Información de mantenimiento.

### **Ventajas**:

* Procesamiento sencillo debido a tamaño fijo.
* Menor retardo y menor buffer debido al pequeño tamaño.

## **Proceso ATM:**

* Flujos digitales entrantes a distintas velocidades:
  + Paquetes de datos.
  + Información a velocidad variable.
  + Información a velocidad constante.
* Módulo ATM.
* Flujo saliente a 155 Mbit/s

## **Trayectos y Canales Virtuales:**

* **Canal Virtual (VC)**: FTE con 1 o más destinos.
  + Similar al circuito virtual de X25 y FR.
  + **VCI**: Identificador: Se puede repetir.
* **Trayecto Virtual (VP)**: VC con los mismos destinos.
  + Agrupa VC en una misma unidad facilitando la gestión y conmutación
  + **VPI**: Identificador: No se puede repetir.

## **Arquitectura ATM:**

### **Planos de operación:**

* **De usuario**: Transferencia de información de usuario y controles asociados.
  + De flujo y errores.
* **De control:** Controles de llamada y de conexión:
* **De gestión**:
  + De plano: Coordinación entre planos y general.
  + De capa: Recursos y parámetros de protocolos.

# **MPLS**:

* **Multi Protocol Label Switching**: Conmutación de etiquetas multiprotocolo.

## **Características**:

* **Basado en etiquetas**: No necesita meterse en los detalles.
  + Solo se analiza la etiqueta.
  + Se abrevia la parte operativa.
* **Conmutación**: De etiquetas.
* **Sustituto de IP sobre ATM** (Combinación de ambas).
* Protocolo para crear túneles.
* Protocolo para acelerar el encaminamiento de los paquetes.
* Funciona sobre cualquier tipo de tecnología de capa 2:
  + PPP, LAN, FR, ATM.
* **Integra capa 2 y 3**:
  + Capa 2: Conmutación rápida.
  + Capa 3: Control de enrutamiento.
* Un conjunto de paquetes se envían por el mismo camino LSP.

## **Problemas que dan origen a MPLS:**

### **QoS**:

* Delay en el procesamiento.
* Delay del enlace.
* El delay no es predecible pero la pérdida de paquetes si lo es.

### **IP Routing:**

* Se repite el cálculo en cada nodo.
  + Se debe realizar todo el análisis de la tabla de ruteo.
* Se realiza por Software.

### **Camino más corto:**

* El camino más corto en internet implica la menor cantidad de saltos.
* **MPLS**: El camino es el más óptimo. el cual implica menor distancia pero no cantidad de saltos.

## **Componentes**:

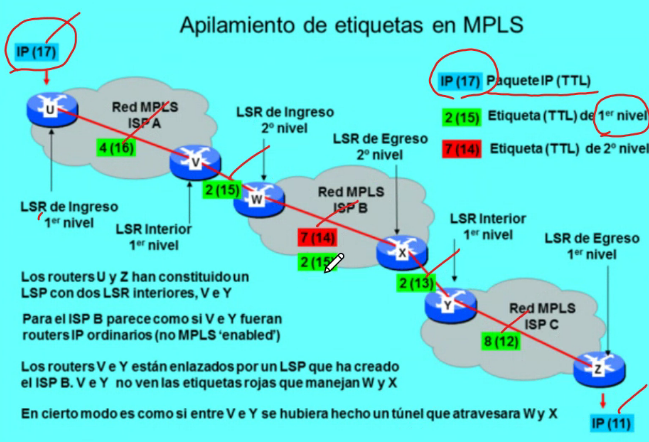
* **LSR**: Label Switching Router: Router de alta velocidad especializado en el envío de paquetes etiquetados por MPLS.
  + Puede enviar paquetes de capa 3 nativos.
  + **Tipos**:
    - Internos: De entrada.
    - Externos: De salida.
  + **Contiene**: LSP + FEC + Etiquetas.
* **Etiqueta**: Identificador cort de longitud fija y con significado local, empleado para identificar un FEC.
  + Jerarquía: Un paquete puede tener una o más etiquetas apiladas.
* **FEC**: Forwarding Equivalence Class: Agrupación de paquetes que comparten los mismos atributos (Dirección, Destino, VPN) y/o requieren el mismo servicio (Multicast, QoS, etc.)
  + Se asigna en el momento en que el paquete entra a la red.
  + Todos los paquetes que forman parte de la clase siguen un mismo LSP.
* **LSP**: Label Switched Path: Ruta a través de uno o más LSR en un nivel de jerarquía que sigue un paquete de FEC en particular.

## **PDU**:

* Datos de Usuario.
* Cabecera IP.
* **Cabecera MPLS**:
  + TTL: Time to Live: 8 bits.
  + S: Stack: 1 bit: Para poder apilar etiquetas de forma jerárquica.
  + EXP: Identificar la Clase de servicio (CoS): 3 bits.
    - Atención especial a los datos.
  + Etiqueta: 20 bits.
* Cabecera Nivel 2.

## **Funcionamiento**:

* Se analiza la cabecera y se asigna la etiqueta.
* Dentro de la nube MPLS se analiza unicamente la etiqueta.
  + Todo el análisis se realiza por HW.
* Se remueve la etiqueta cuando se sale de la nube.



* El TTL del nivel se descuenta dentro del mismo.

## **Control de información:**

* Generación de las tablas de envío que establecen los LSP.
  + Uso de los protocolos de enrutamiento internos IGP.
* Distribución de la información sobre las etiquetas de los LSR:
  + Uso de diversos protocolos con variaciones en el intercambio de etiquetas.

## **Protocolos de intercambios de etiquetas:**

* **LDP**: Label Distribution Protocol: Mapeo de destinos IP en etiquetas.
  + Unicast.
* **RSVP, CR\_LPD**: Constraint Based Routing Label Protocol: Usado para ingeniería de tráfico y reserva de recursos.
* **BGP**: Para etiquetas externas (VPN).

## **Resumen MPLS:**

* Proporciona QoS e ingeniería de tráfico a una red global que soporte todo tipo de tráfico.
* Es una solución con grandes posibilidad de éxito debido a la facilidad en la migración de una red actual a MPLS.
  + El primer paso para que convivan juntos es mediante Software añadido a equipos actuales.
* Facilitar la migración para la próxima generación de la internet óptica.
  + Se acortará la distancia entre el nivel de red IP y la fibra.
* Permitir nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP:
  + Usualmente limitadas a a encaminar por dirección de destino.

# **Seguridad en Redes:**

## **Problemas de seguridad:**

* **Confidencialidad o privacidad**: La información solo puede ser vista por las personas designadas.
* **Autenticidad**: Acceso o visualización a un usuario que no le corresponde.
  + Control de accesos a la red y a la información.
* **Integridad de los datos**: El dato debe llegar sin modificaciones o perdidas a destino.

### **Ataques informáticos:**

* Interceptación.
* Fabricación.
* Modificación.
* Destrucción

## **Potenciales soluciones:**

* **Claves de acceso**: A los recursos o al sistema.
  + EJ: Autenticación doble factor.
* Encriptado de datos.
* Seguridad física en dispositivos.
* Firma digital.
* Firewall.
* Capacitación de usuario y administradores.
* Protocolos de seguridad (IP SEC).
* VPN

## **Analisis de riesgos de seguridad:**

* Riesgos en base al comportamiento humano:
  + Fugas de información: Errores por exceso de confianza.
  + Ataques de virus: Priorizar beneficios sobre los riegsgos.

## **Seguridad por capas OSI:**

* **Capa 1**: Físico:
  + Auditar el canal que se use.
  + Plano de la red.
  + Análisis de la topología
  + Puntos de acceso físico.
  + Potencias y/o frecuencias utilizadas.
* **Capa 2**: Enlace de datos: Ultimo nievl que encapsula a los anteriores.
  + Uso de analizador de protocolos para control de direcciones MAC.
  + Analizar de configuración.
  + Analizar de tráfico y colisiones.
  + Evaluación de accesos WiFi.
* **Capa 3**: Red: El centro de la auditoría seran las rutas y direcciones.
  + Trabajo en el router sobre las contraseñas, configuraciones, protocolos de ruteo, listas de control de acceso, logs.
  + Auditoria en ARP y direccionamiento IP.
    - Estatico o dinamico.
* **Capa 4**: Transporte: Auditar el establecimiento de sesiones y puertos.
  + Operación con conexión (TCP) o sin conexión (UDP).
* **Capa 7**: Aplicación: Se debe auditar:
  + Servidores.
  + Accesos remotos.
  + Firewall y DNS.
  + Correos electrónicos.
  + Logs.

## **Firewall**:

* Sistema que crea una barrera segura entre dos redes (Entre una interna y otra externa).
* Compuestos por Hardware y Software.

### **Beneficios**:

* Concentra la seguridad en un único punto.
* Controla el acceso.
* Regula el uso de la red exterior.
* Registra el empleo de la red interna y externa.
* Protege de ataques externos.
* Limita el tráfico de servicios vulnerables.
* Mejora la privacidad del sistema:
  + Ocultar direcciones IP internas.
  + Bloquear servicios.

### **Tipos**:

* **Nivel de red**: Direcciones IP y números de puerto.
  + EJ: Router.
* **Nivel de aplicación**: No permite tráfico directo entre redes.
  + EJ: Proxy.

### **Decisiones al implementarlo:**

* **Política de seguridad de la organización**:
  + Negación de todos los servicios salvo los autorizados.
  + Permitir libremente el uso de todo excepto lo prohibido.
  + Medir y auditar el uso de la red.
* **Nivel de seguridad deseado**:
  + Analisis de necesidades con niveles de riesgo aceptables.
  + Nivel de seguridad que satisface: Solución de compromiso.
* **Evaluación de costo**:
  + Mejor relación costo - beneficio.

## **Firma digital:**

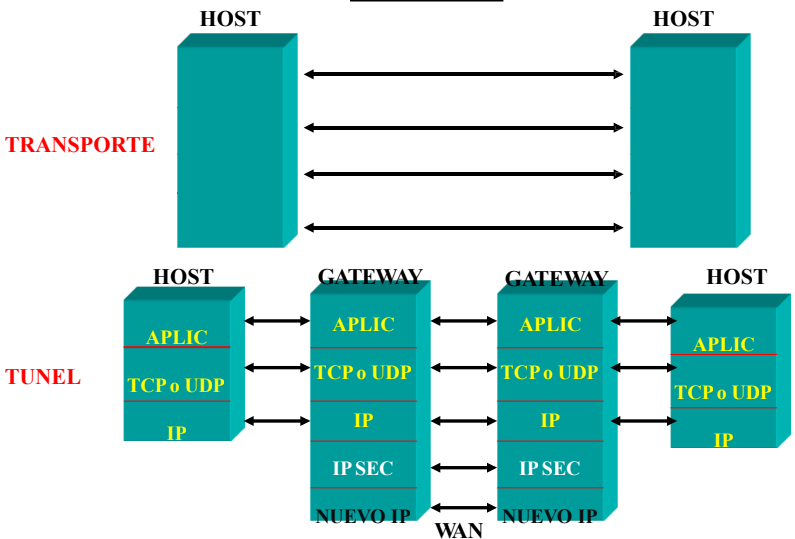
* Técnica de seguridad informática aplicada sobre la información digital que se intercambia en una red.
* **Basado en**:
  + **Criptosistema asimétrico**: Dos claves.
    - Publica y privada.
  + **Función matematica Hash**:
    - Digest: Salida de longitud fija.
  + **Autoridad certificante**: Registra las claves publicas y las distribuye en forma segura.
* **Provee**:
  + Autenticidad.
  + Integridad.
  + No repudio.
* Puede adicionarse el encriptado completado de un mensaje con lo que se provee confidencialidad.

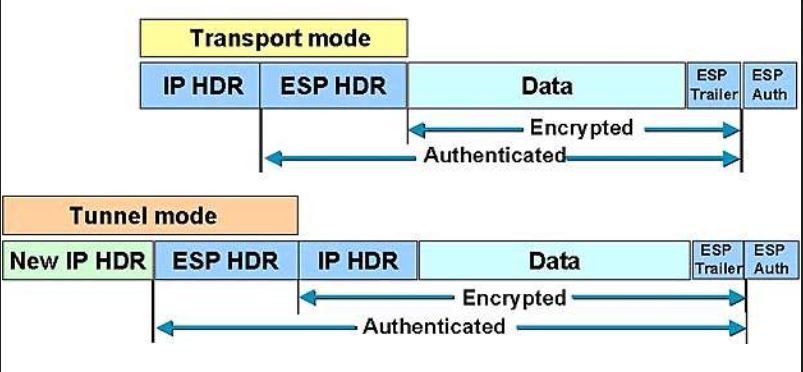
## **IP Security: IP Sec:**

* Conjunto de protocolos de seguridad que permiten agregar encriptado y autenticación a la comunicación.
* **Capa: 3: Red**: Transparente para la aplicación.
* Utilizado frecuentemente en VPN.

### **Modos de operación:**

* **Transporte**: Solo protege la información de transporte (No protege la información de la capa IP).
  + **Funcionamiento**:
    - Host izquierda: Capa aplicación + (TCP o UDP) + IPSEC + IP.
    - Host Derecha: IPSEC + IP.
* **Túnel**: Protege toda la información, por lo que ocupa más información.
  + Funcionamiento:
    - Host Izquierda = Host Derecha: Capa aplicación + (TCP o UDP) + IP.
    - Gateway Izquierda = Gateway Derecha Capa aplicación + (TCP o UDP) + IP + IPSEC + Nuevo IP





## **Seguridad en Wireless:**

* **WPS**: WiFi Protected Setup: Mecanismos para facilitar la conexión de dispositivos a una red inalambrica.
  + Ej: Intercambio por PIN.
* **WEP**: Wired Equivalent Privacy: Ofrece seguridad similar a la red cableada mediante una encriptación
* **WPA**: WiFi Protected Access: Agrega seguridad mediante el uso de claves dinámicas proporcionadas a cada usuario.
* **WPA 2**: Usa algoritmo de encriptación AES.
  + AES: Advanced Encryption Standard.
* **WPA 2 PSK**: Pre Shared Key: Uso doméstico o de oficinas pequeñas.
  + Se comparte la clave.
* **WPA 2 TKIP**: Usa un protocolo de integridad de clave temporal que cambia dinamicamente las claves de un sistema a medida que se utiliza.
* **Otros recursos**:
  + SSID: Nombre de red.
  + MAC Filtering.

## **Comparativa entre WEP - WPA - WPA 2:**

|  | **WEP** | **WPA** | **WPA 2** |
| --- | --- | --- | --- |
| **Encriptación** | RC4 | RC4 | AES |
| **Rotación de claves** | No tiene | Claves de sesión dinámicas | |
| **Distribución de claves** | Asignada manualmente a cada dispositivo | Automática | |
| **Autenticación** | WEP Key | 802.1x, EAP | |