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.

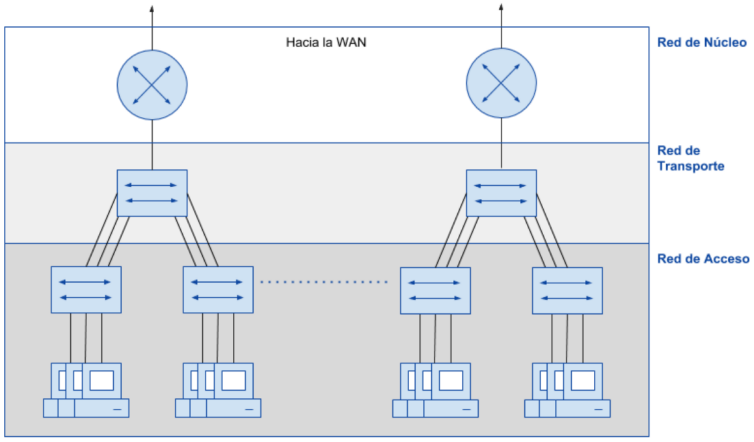
REDES WAN

La red de acceso para ingresar desde una LAN a la red WAN puede ser de dos formas:

1. Cableada: red telefónica conmutada, ADSL, cable-módem
2. Inalámbrica: GPRS, WIFI y para acceso corporativo (empresa, facultad) enlace dedicado o WI-MAX

SS7 es el sistema que usa la vieja red telefónica (red del teléfono domiciliario). También está X25 (ya no se utiliza) y Frame Relay (que hay algunos acceso que lo tienen)

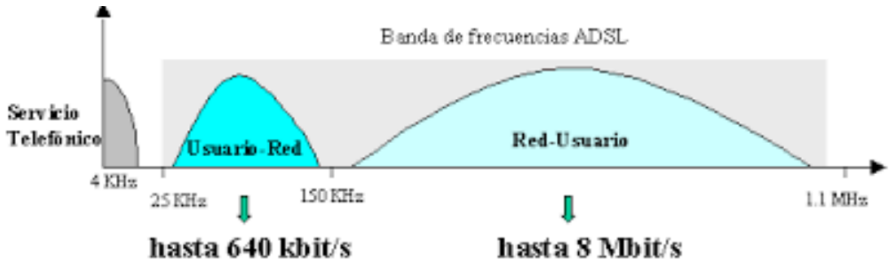
Desde la Red de acceso (LAN + Router) pasa por la Red de Transporte y va hacia la Red Núcleo de WAN



Hay 3 tipos de routers unidos por los enlaces.

1- Servidores de acceso remoto /RAS: en los POP. Tienen muchos puertos de baja velocidad (desde red de acceso a transporte)
2- Troncales o de Backbone: Tienen pocos puertos de alta velocidad (capa transporte). Se comunica con otros ISP.
3- Concentradores: unen varios POP hacia los troncales con características intermedias

El acceso residencial por ADSL ya no se utiliza porque las telco ya llegan con fibra o con cobre a las casas. El ADSL permitió mantener la comunicación telefónica mientras uno tenía el acceso a datos. ADSL amplió la frecuencia Red-Usuario



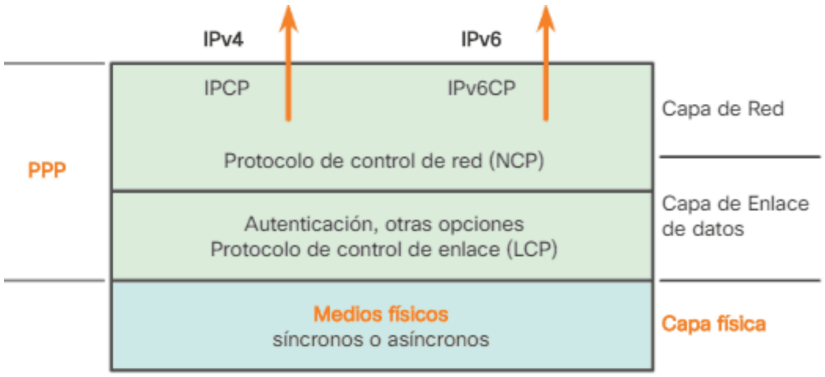
Ahora la red de transporte va a internet por un lado y por el otro a la red de acceso de los usuarios.

Protocolo PPP □ Point to Point Protocol. RFC 1661 (año 1994).

Fue generado por la necesidad de transmitir datagramas IP a través de vínculos punto a punto.

Servicios que brinda PPP:

- Permite configurar enlaces
- Multiplexar protocolos de red (IPx-no se utiliza-, IP)
- Testear la calidad del enlace
- Asignación dinámica de direcciones IP



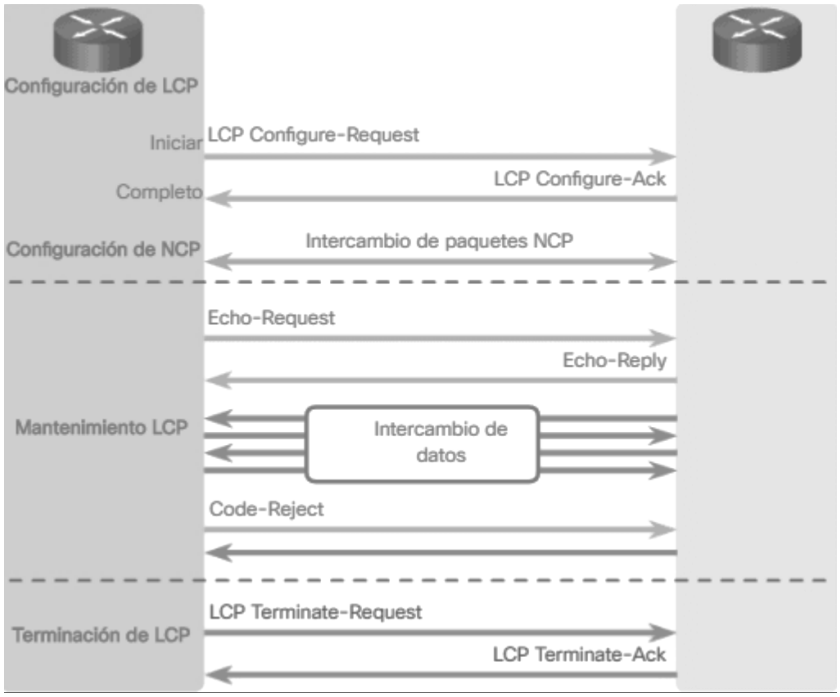
LCP, NCP forma parte de la familia de HDLC

Capa física

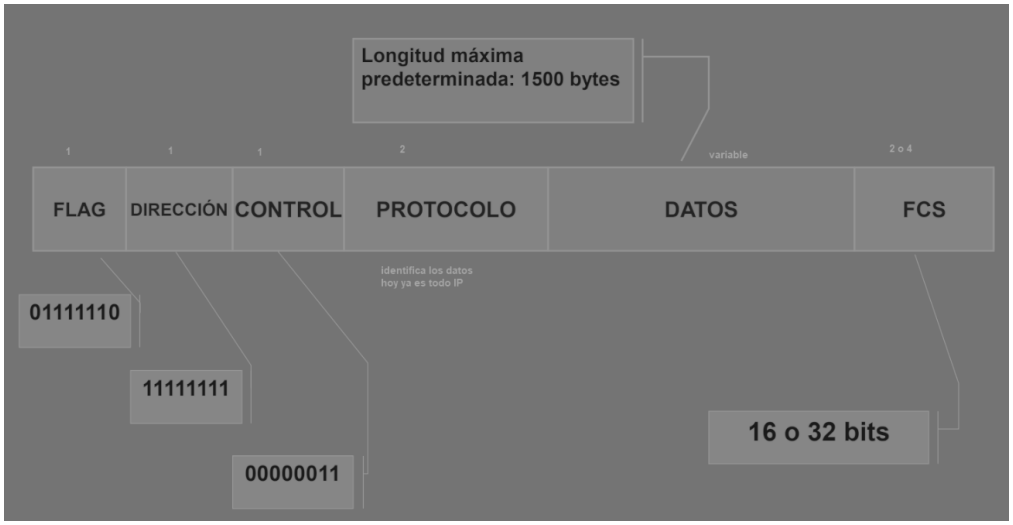
Hay enlaces seriales de distintos tipos:

- enlaces ethernet
- enlaces SDH
- enlaces con módem sincrónicos o asincrónicos
- enlace de la red digital de servicios integrados (RDSI)

LCP: configuración, mantenimiento y terminación



Trama de la capa de enlace



Conexión por enlace telefónico – PASOS

1.Fase de establecimiento del enlace (LCP)

2.Fase opcional de autenticación

3.Fase de protocolo de capa de red

4.Fase de terminación del enlace

Autenticación en PPP

PAP: Password autentication protocol poco seguro dado que envía la clave en claro sin encriptar de forma conjunta con la identificación de la estación-cliente. Durante el establecimiento de la sesión del LCP se negocia el uso de este protocolo en caso de que se requiera. Sólo se realiza cuando se inicia el enlace. No hay protección ante ataques de prueba y error.

CHAP: Challenge autentication protocol Envía un mensaje en claro que luego el cliente cifra con su clave y le devuelve cifrado al servidor. El servidor realiza el cifrado del mensaje y controla que ambos textos cifrados coincidan y durante el período de actividad de este enlace se envían frecuentes verificaciones de autenticación.

El proceso de autenticación se efectúa mediante el establecimiento del enlace (LCP). No se pasa a NCP hasta tanto no se completa la autenticación del LCP.

Ventajas de PPP sobre HDLC

- Más confiable
- Puede trabajar con distintos enlaces (E1, módems)
- Normalizado por RFC
- Mayor seguridad
- Permite compresión de datos

Frame Relay

- Significa “Rtx de cuadro”. Es una técnica de fast packet switching.
- Opera en la capa 2 del modelo OSI.
- Trabaja sobre enlaces de alta calidad. Asociado a la fibra óptica.
- Fundamentalmente se usa para reemplazar líneas punto a punto (dedicadas).
- Las estaciones terminales dan: cobertura de errores, control de secuencia y de flujo. Necesitan una mayor inteligencia. Las intermedias retransmiten.
- Servicio: se basa en una red de conmutación de paquetes compuesta por conmutadores y concentradores enlazados mediante líneas bidireccionales de media o alta velocidad.
- El control de errores se hace en la capa 2.
- Describe un estándar optimizado para el transporte de protocolos orientados a datos, en unidades discretas de información (paquetes genéricos).
- Multiplexa datos estadísticamente, con lo cual comparte el AB y se obtiene eficiencia.
- Elimina mucho el procesamiento de protocolo desempeñado por la red, reduciendo de este modo la latencia de tx.
- Interfaces:
    - UNI: interfaz entre usuario y red FR.
    - NNI: interfaz entre red FR y otra red FR.

Características

- Alta velocidad y baja latencia.
    - Latencia: es la suma de retardos temporales dentro de una red (tiempo que tardo en cruzar la red). Factores que influyen en la latencia: tamaño de los paquetes transmitidos, tamaño de los buffers dentro de los equipos de conectividad.
- Basado en VC (circuitos virtuales) de nivel 2 de tipo permanente (PVC).
- Se identifica por DLCI (Data Link Connection Identifier).
- El VC es una asociación lógica de DLCIs.
- El DLCI tiene significado local.
- La conmutación se produce a nivel de frame.
- Uso dinámico del AB: se ocupa cuando hay info para transmitir.
- Orientado a tráfico por ráfagas (tipo LAN).
- Define la interfaz entre CPE (equipo en la instalación del cliente) y POP (Point Of Presence).
    - CPE son routers o FRAD (dispositivo de acceso a FR).
    - POP son switches rápidos que ofrecen puertos de acceso a la red FR.

- Nivel 2: LAPD y LAPF (subconjunto del LAPD) ambos son versión del HDLC.
    - LAP: Link Access Protocol. D=Data, F=Frame.
- PDU: cuadro.

Ubicación respecto al modelo OSI

OSI	X.25	Frame Relay
Aplicación		
Presentación		
Sesión		
Transporte	Un poquito de Paquete	
Red	Paquete	
Enlace de datos	LAPB	LAPF / LAPD
Físico	Capa física	Capa física

Las capas 1 y 2 soportan al Frame Relay.

Arquitectura de FR

- La de usuario difiere de la de red en que la primera incluye funciones seleccionables por el terminal del usuario.
- En los sistemas finales y sistemas intermedios se tienen dos arquitecturas distintas y separadas:
    - Plano de operación de control: establecimiento y liberación de conexiones lógicas. Nivel 2: LAPD, Nivel 3: Q.933.
    - Plano de operación de usuario: transferencia de datos de usuarios. Nivel 2: LAPF.
- LAPD: Protocolo de control de enlace de datos para los canales tipo D que son usados para transportar info de control y señalización y que nunca se separan de los canales B que transportan datos de usuario.

Cuadro FR (LAPF) – Trama

- F (Flag): se usa para separar tramas. Cuando no hay tramas para tx, se generan flags continuamente.
- Add: direcciones (address). Puede ser de 2, 3 o 4 octetos.
    - F (FECN): notificación de congestión explícita hacia adelante (en el sentido de la tx). Bit fijado por el nodo de red (FR switch) que experimenta congestión.
    - B (BECN): notificación de congestión explícita hacia atrás (en el sentido contrario a la tx). Bit fijado por el nodo de red que experimenta la congestión.

- DE: elección para descarte.
    - Fijado por el DTE (access device FRAD, router, etc.) o los nodos de red (FR switches).
    - Puede ser modificado por los nodos de red en el evento que el usuario ha excedido el CIR y la red experimenta congestión.
    - Las tramas que tienen este bit igual a 1 son susceptibles de descarte en situaciones de congestión.
- EA: extensión de campo de dirección. Se permiten más de 2 octetos en el campo de control, entonces 0=”detrás siguen más octetos”, 1=”último octeto del campo de control”.
- C/R: comando – respuesta. No es un bit utilizado por la red.

<u>Control de errores y de flujo en FR</u>

- Control de errores: solo detección de errores (FCS) en los extremos. Capas superiores se ocupan de la corrección. No se lleva secuenciamiento de cuadros (no se usa campo de control).
- Control de congestión: mediante FECN y BECN. FECN se setea cuando la congestión es en el mismo sentido en que va el cuadro. BECN, cuando es en el sentido contrario. Los POP setean estos bits y los CPE junto con el administrador de la red, los detectan.
- Control de flujo: mediante datos elegidos para descarte (DE).

<u>Definiciones</u>

- Puerto: permite el ingreso a la red. Los POP proveen varios. Los PVC nacen en los puertos.
- BC [bits]: tamaño comprometido de ráfaga. Cantidad máx de bits que se transmiten por un PVC en un intervalo de medición (TC).
- TC [segundos]: intervalo de medición (con y sin actividad).
- BE [bits]: tamaño en exceso de ráfaga. Cantidad no comprometida (marcar con DE).
- Vel. Puerto (VP) [bps]: velocidad máxima de entrada a la red FR. Rango 56-64 Kbps / 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.
- Las tramas entre VP y EIR siempre se descartan. Las que están entre EIR y CIR son marcadas con DE (descarte ante congestión) y las que están por debajo de CIR son garantizadas.

Sobresuscripción: asignación dinámica del AB a los PVCs (multiplexado estadístico). Es que la suma de los CIR de cada PVC supere la VP.

Voz sobre FR

- Tolerante a pérdidas, no a retardos.
- Menor QoS, menor costo (20 a 30% menos) frente a comunicaciones telefónicas convencionales.
- No acepta rtx, eso genera interrupciones.
- Aprovechar silencios (cuando no se manda nada aprovecha para bufferear).
- Uso de algoritmos de compresión (PCM, ADPCM) 64, 32, 16, 12, 8 kbps.
- Priorizar tráfico y uso de DLCI para voz.
- Menor tamaño de los cuadros (fragmentación).
- Rutas con pocos saltos (3 o 4). Menor retardo en la red.
- FRADs o routers para voz y datos.

Protocolo ATM

Modo de Transferencia Asincrónico

- Resultado de nuevas necesidades (trafico), cambios del negocio de las telecom y del tráfico. Distintos tamaños de trama en los protocolos entonces el router no puede predecir nada.
- Protocolo de capa 2.
- Montado sobre redes ISDN Banda Ancha basadas en tecnología SDH.
- Permiten velocidades binarias de más de 2,4 Gbps por la alta calidad de los vínculos. Más de 15 TB por segundo.
- La PDU es la celda o célula, son de tamaño fijo y pequeñas (53 b = 5 header + 48 de info).
- Permiten transportar todo tipo de servicio (voz, video, datos, combinaciones).
- Usa capas de adaptación (AAL) para integrar servicios.
- Permite conmutación rápida (SWITCH) con muy bajos retardos.
- Reducción de funcionalidades en los nodos y delegación de funciones a los extremos.
- Protocolo orientado a la conexión.
- Normalizado por la UIT y por el Forum ATM.
- Cuando no hay nada transmitiendo, transmite celdas vacías.
- Entran flujos digitales a distintas velocidades en el módulo ATM y sale un flujo a una velocidad.

- Características:
    - Utiliza celdas (tamaño fijo)
    - Servicio orientado a conexión
    - Soporta multitud de facilidades de control
    - Tecnología WAN utilizada también en LAN, a diferencia de X.25 o FR.

Celda ATM

- Tamaño fijo: procesamiento sencillo.
- Tamaño pequeño: menor retardo, memorias más pequeñas.
    - Encabezamiento: información de enrutamiento y prioridad. Identificación de celdas de un mismo camino.
    - Carga: video, voz o datos (transparente de extremo a extremo).

Operación y Mantenimiento (OyM): va en la carga.

Sincronismo

- Lo que tiene de **sincrónico** ATM es que las celdas se transportan sobre canales sincrónicos.
- **Asincrónico** por:
    - No están sincronizadas con respecto a ningún usuario.
    - Las posiciones en el flujo se asignan por demanda (tráfico por ráfagas).

Caminos y canales virtuales

- VC (Canal Virtual): fuente con uno o más destino similar al camino de X.25 y Frame Relay.
- VP (Camino Virtual): VC con los mismos destinos. Agrupa VC en una misma unidad facilitando la gestión y la conmutación.
- Identificadores: los VPI no se pueden repetir. Los VCI se pueden repetir pero no dentro de un mismo VP.

Arquitectura ATM pura

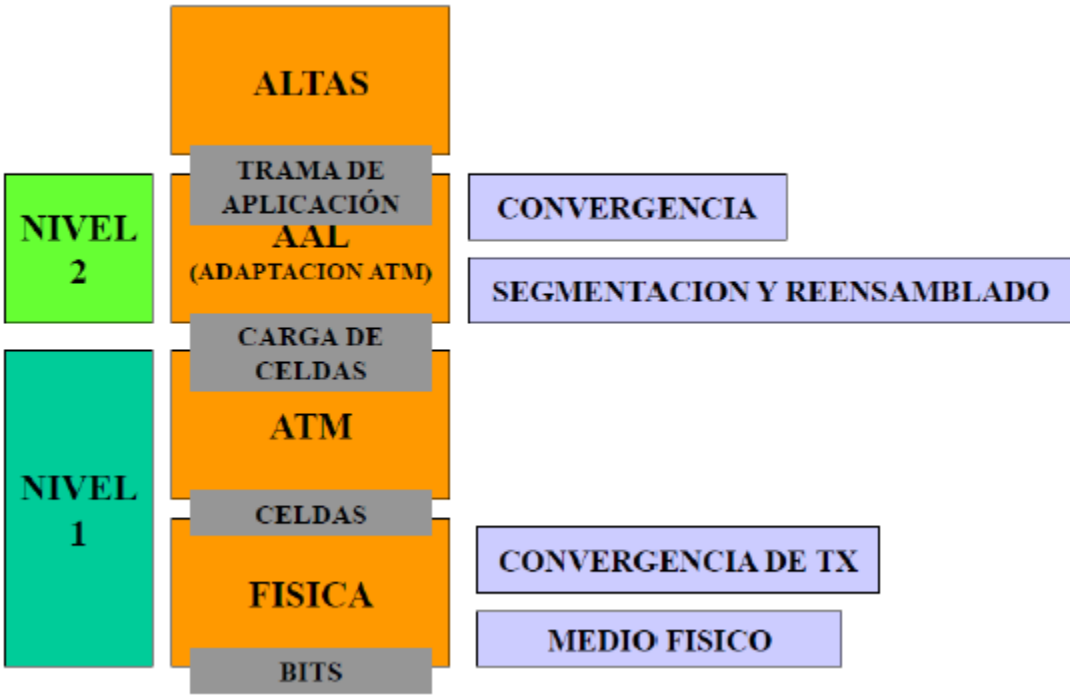
- El conmutador se conecta a las estaciones igual que un conmutador Ethernet.
- Cada estación utiliza un Identificador de Camino Virtual (VPI) y un Identificador de Circuito o Canal Virtual (VCI).
- El sistema necesita construirse desde la base, las redes LAN existentes no pueden adaptarse en una ATM pura.

Arquitectura de protocolos ATM

Planos de operación:

- De usuario: transferencia de info usuario y controles asociados (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.

Capas y subcapas de ATM



Funciones:

- Convergencia: independiza la pila de protocolos que está debajo de ella, de las capas superiores. Identifica los mensajes, recupera la señal de clock.
- Segmentación y reensamblaje: segmentar la información de las capas superiores. Permite manejar cuadros de mayor longitud que las celdas. Adapta la info a los 48 bytes, acorde a la clase de servicio que se trate. Reensamblado.
- ATM: multiplexión. Armado de celdas. Introducción y extracción del header. Control de congestiones y ruteos (flujo) en UNI.
- Convergencia de tx: independiza la velocidad del flujo de celdas de la interfaz física. Todos los distintos tipos de datos van por el mismo canal.

- Medio físico: controla las funciones que dependen del medio físico, tipos de cable, conectores, etc. Funciones de bit. Basada en SDH (jerarquia digital sincrónica)

Clases de servicios ATM (del más caro al más barato)

Servicio	Velocidad	Acrónimo	Ejemplo
De tiempo real	Constante	CBR	Circuito E1
	Variable	Rt-VBR	Videoconferencia
De tiempo no real	Variable	Nrt-VBR	Correo electrónico Multimedia
	Disponible	ABR	Consultas web Tx ráfagas con conocimiento de AB
	No especificada	UBR	FTP 2do plano IP (best effort)

Lo que más ofrecen las empresas de telecomunicaciones son UBR (no se comprometen a nada)1

Capas AAL según requerimientos de servicios

Requerimiento	Clase A	Clase B	Clase C	Clase D
Tiempo entre fuente y destino	Requerido (sensible a demoras) Rt		No requerido (no sensible a demoras) Nrt	
Bit rate	Constante CBR	Variable rt-VBR	nrt-VBR	
Modo de conexión	Orientado a la conexión			No orientado a la conexión

- AAL 1: audio y video sin compresión.
- AAL 2: video comprimido.
- AAL 3 / AAL 4: datos en general.
- AAL 5: servicio con menor overhead y mejor detección de errores (emulación LAN, FR, ATM, IP sobre ATM).

Encabezamiento de celda

- UNI: interfase red-usuario.
- NNI: interfase red-red.
- GFC: control de flujo genérico.
- PT: tipo de carga útil (de usuario o de gestión de red/mantenimiento).

- CLP: prioridad de pérdida de celda (0=alta, 1=puede descartar la red).
- HEC: control de errores de cabecera (detección y a veces corrección error simple).

Mapeo de celdas ATM: forma en que las celdas son introducidas en contenedores normalizados:

- SDH
- PDH
- Estructura de celdas

Comparación de tecnologías

	X.25	**Frame relay**	**ATM**
Niveles de protocolos	1, 2, 3 OSI	1, 2 OSI	Medio físico, ATM, AAL
Vel bin máx	64 kbps	2 Mbps o más	622 Mbps y más
Control de errores	Detección y corrección salto por salto LAP-B (HDLC)	Nodos intermedios rtx. Extremos detectan. Capas superiores corrigen. LAP-F y LAP-D (HDLC)	Solo de extremo a extremo hay control de header de celda (detecta y puede corregir a veces). Capas superiores corrigen.
Soporte comunicación	Red analógica y digital Baja calidad	ISDN Mejor calidad	B-ISDN Alta calidad
PDU	Trama y paquete	Cuadro	Celda o célula
Longitud de la PDU	Grande y variable (16/1024 B paq)	Grande y variable (1600/4096 B)	Pequeña y fija (53 B)
Tipo de tráfico más adecuado	File transfer, batch, correo electrónico	Ráfagas (LAN), voz	Info en tiempo real, voz, video, videoconf
Tipo de servicio	A la conexión	A la conexión	A la conexión
Conmutación	Por software (mayor procesamiento)	Por software (menor procesamiento)	Por hardware (menor retardo)
Multiplexación e identificadores	LC (canal lógico) VC (circuito virtual) LCI	VC DLCI	VP (camino virtual) VC VPI y VCI
Eficiencia	Asignación fija	Asignación por demanda	Asignación por demanda

MTU (Unidad de Transferencia Máxima de una red)

Tamaño máximo del campo de datos de la PDU de una red.

- Ethernet: 1500 B
- FDDI: 4770 B
- Token bus: 8182 B
- Token ring: 65535 B
- X.25: 128 B (N3)
- Frame Relay: 4090 B
- ATM: 48 B

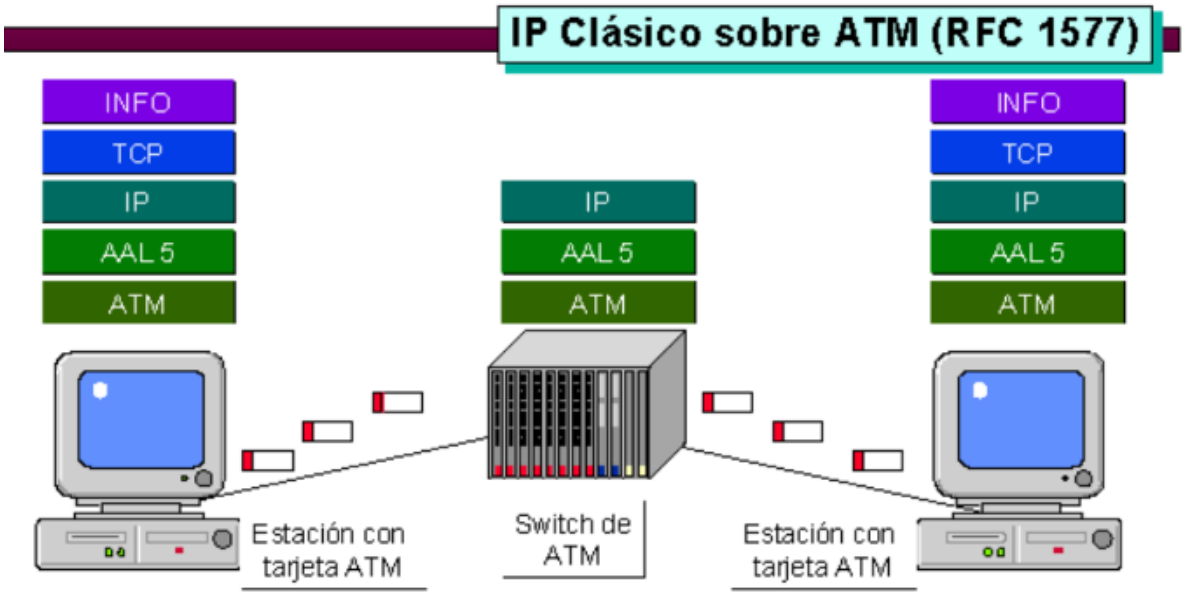
LAN sobre ATM

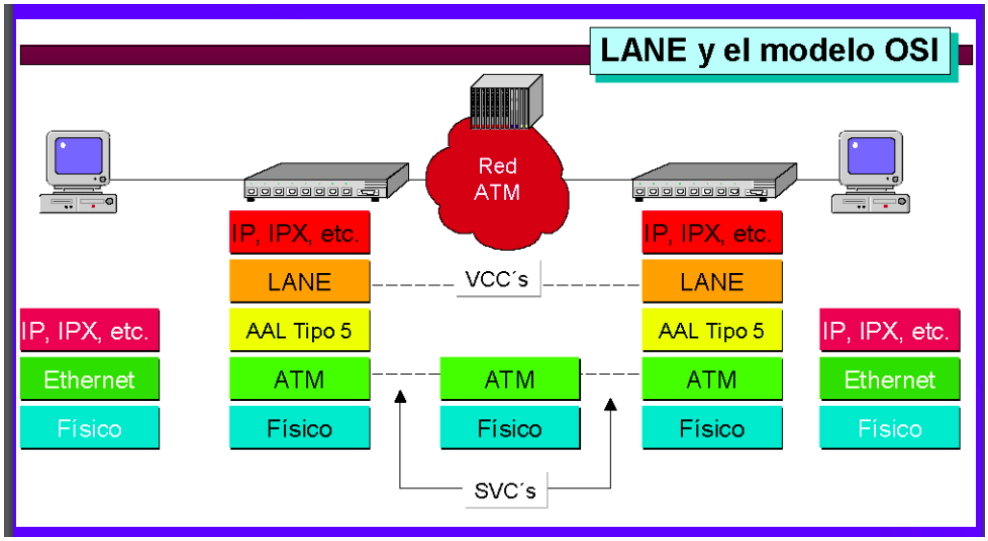
- LANE define cómo deben interactuar redes LAN a través de ATM.
- Permite que aplicaciones diseñadas para operar en una red LAN permanezcan sin cambios cuando se introduce ATM en la red.

Elementos de una LAN Emulada

- Se compone de un grupo de clientes y un grupo de servidores.
- Una PC puede ser parte de diferentes ELANs.
- En una red ATM puede haber varias ELANs. Cada ELAN es como una LAN virtual en la red ATM porque hay independencia lógica.
- El tráfico sólo se distribuye entre sus miembros. Para hablar entre ELANs se requiere de un ruteador por ejemplo.

IP clásico sobre ATM: una red ATM se comporta como una LAN pero se efectúan los direccionamientos de acuerdo a direcciones IP.





Seguridad en redes

- La seguridad en redes debería brindar:
  - Confidencialidad o privacidad.
  - Autenticidad.
  - Integridad de los datos.
- Ataques informáticos:
  - Interceptación (man in the middle).
  - Fabricación (de ataque).
  - Modificación (de mensajes, etc).
  - Destrucción (ataques que rompen todo).

Algunos métodos

- Claves de acceso: al sistema o los recursos
- Encriptado de datos
- Seguridad física de dispositivos
- Firma digital (inequívoco, es fidedigna)
- Firewall
- Capacitación de usuarios y administradores
- Protocolos de seguridad (ej: IPSec).
- Red privada virtual (VPN)

Criterios para evaluar los sistemas de computadoras

El Departamento de Defensa de EEUU plantea una clasificación de los sistemas según niveles para evaluar la confiabilidad y seguridad:

Niveles: imponen límites y condiciones que debe reunir un sistema para alcanzar un esquema de seguridad respecto de SW y HW. Son 4 niveles:

- Nivel D: protección mínima.
    - Sistemas que no tienen clasificación de seguridad.
    - No requiere protección.
- Nivel C: protección discrecional.
    - Sistemas con cierta protección.
    - Incluye: capacidad de auditoría + responsabilización de sujetos y sus acciones.
- Nivel C1: protección de seguridad discrecional.
    - Separación entre usuarios y datos.
    - Registro de usuarios mediante nombre y clave de acceso.
    - Cuenta de administrador de sistema sin restricciones.
- Nivel C2: protección de acceso controlado (ej: Unix, Windows NT).
    - Refuerza restricciones de usuarios.
    - Responsabiliza a los usuarios por sus acciones mediante login, auditoría y aislación de recursos.
    - Especifica niveles de acceso, permisos de lectura, escritura o ambos.
- Nivel B: protección de mandatario.
    - Mayor importancia en preservar la integridad de la información sensible.
    - Usa reglas para el control de acceso del administrador.
- Nivel B1: protección de seguridad clasificada.
    - Requiere lo incluido en C2.
    - Establece políticas de seguridad en función de la clasificación de seguridad que se asigne a los datos (reservado, confidencial, secreto, ultrasecreto).
    - Trabaja sobre el control de acceso a “objetos”. Los cambios solo pueden ser realizados por su dueño.

    - Se aplica sobre info que debe ser exportada y se desea mantener los derechos del autor.
- Nivel B2: protección de estructura.
    - Identificación de objeto según la protección necesaria.
    - Establece pautas de comunicación entre un objeto de nivel más elevado de seguridad con uno de menor nivel.
    - Incremento de controles y mecanismos de autenticación.
- Nivel B3: dominios de seguridad.
    - Empleo de hardware de seguridad.
    - Alta resistencia al acceso no autorizado.
    - Establecimiento de rutas seguras en la comunicación.
- Nivel A: protección verificada.
    - También llamado “Nivel de diseño verificado”.
    - Abarca verificaciones en el diseño, desarrollo e implementación de HW y SW.
    - Prevé la administración y gestión de la seguridad del sistema.

Firewall

- Es un sistema que crea una barrera segura entre dos redes. Se compone de HW y SW.
- Es un componente de la seguridad de una red. Hay que complementarlo con otras acciones.
- Muchas veces está bueno filtrar por MAC ya que es muy difícil de emular.

Beneficios de un firewall

- Concentra seguridad en un único punto.
- Controla acceso.
- Regula el uso de la red exterior.
- Registra el empleo de la red interna y la externa.
- Protege de ataques externos.
- Limita el tráfico de servicios vulnerables.
- Mejora la privacidad del sistema (ej: ocultar direcciones IP internas o bloquear servicios).

Decisiones al implementar un firewall

1- Política de seguridad de la organización:

    - Negación de todos los servicios, excepto algunos autorizados.
    - Permitir libre uso de todo, excepto lo expresamente prohibido.
    - Medir y auditar el uso de la red.
2- Nivel de seguridad deseado:
    - Análisis de necesidades con niveles de riesgo aceptables.
    - Nivel de seguridad que satisface. Solución de compromiso.
3- Evaluación de costos:
    - Mejor relación costo-beneficio.

Tipos de firewall

- Nivel de red: direcciones IP y números de puerto. Ej: router.
- Nivel de aplicación: no permiten tráfico directo entre las redes. Ej: servidor proxy.

Firma digital

- Es la técnica de seguridad informática aplicada sobre la información digital que se intercambia en una red, basada en:
    - Criptosistema asimétrico: clave pública, clave privada.
    - Función matemática (HASH), salida long fija (DIGEST).
    - Autoridad certificante: registra las claves públicas y las distribuye en forma segura.
- Provee autenticidad, integridad y no repudio (no se puede decir “yo no fui”).
- Puede adicionarse el encriptado completo de un mensaje con lo que se provee confidencialidad (privacidad).

IP Security (IPSec)

- Es un conjunto de protocolos de seguridad que permiten agregar encriptado y autenticación a la comunicación.
- Es de capa 3 resultando totalmente transparente para las aplicaciones.
- Uso frecuente en VPN.
- Modos de aplicación:
    - Transporte: va de host a host directo.
    - Túnel: de un host perteneciente a una LAN, sale por una Gateway a otra Gateway y de ahí de nuevo a otro host de esa otra LAN.

A PARTIR DE ACA NO VA MAS NADA

DLCI (Data Link Connection Identifier)

- Identificador de conexión de enlace de datos.
- Permite definir hasta 2014 circuitos virtuales.
- La función de multiplexación se realiza en el nivel 2 y con el DLCI se identifica al canal lógico al que pertenece cada trama.
- Los números de canal lógico se asignan bajo contrato.
- Originalmente era el DLCI 1023. El anexo D lo compatibilizó con las funciones de señalización en RDSI, pasando a adoptar el DLCI 0. Esta es la versión más utilizada.

LMI (Interfaz de Gestión Local)

Define un protocolo de polling entre el FRAD y la red para el intercambio de informaciones sobre el estado de la interface y de los PVCs, tales como:

    - Notificación de un nuevo PVC.
    - Detección del cancelamiento de un PVC.
    - Notificación de la disponibilidad de un PVC.
    - Verificación de la integridad del enlace (UNI).
- Maneja que esté funcionando todo bien y, si no, manda la alerta.
- Es un protocolo asimétrico: el FRAD emite un polling periódico (STATUS ENQUIRY) hacia la red, la cual contesta (con un STATUS).
- El periodo de polling es de 10 seg, negociables entre 5 y 30 seg.
- El polling tiene la finalidad básica de verificar si la interfaz de acceso está activa y operando correctamente.
- Este polling periódico permite detectar errores, tales como errores del canal de señalización o problemas internos de la red.
- Cada cierto número de pollings para detección de actividad, el FRAD pide el estado de todos los PVCs definidos en la interface de acceso. Gralmente es cada 6 pollings.
- Los mensajes de estado completo incluyen informaciones sobre todos los PVCs configurados en el canal portador, incluso la historia reciente y disponibilidad de los PVCs.

Protocolo HDLC (High-level Data Link Control)

- Sincrónico, orientado al bit (cambiando un solo bit modifico muchas cosas).
- Con arquitectura de ventana deslizante.

Formato de la trama

- Máx tamaño 1080 bits (135 bytes).
- B: bandera. 8 bits.
- D: dirección. 8 bits.
- C: control. 8 o 16 bits.

- Tres tipos de trama: información (pura), supervisión y no numerada.

Configuraciones

- Órdenes (estación primaria a secundaria), respuestas (estación secundaria a primaria).
- Balanceada (2P), no balanceada (1P).

Modos de operación

- Respuesta normal (NRM): no bal, se tx solo cuando lo indica la primaria, enlace punto a punto o multipunto, half dúplex.
- Respuesta asíncrona (ARM): no bal, se tx sin permiso de la primaria, enlace punto a punto y dúplex.
- Balanceado asíncrono (ABM): cada estación es primaria y secundaria, enlace punto a punto dúplex.

Tipos de tramas

- No numeradas (U): establecimiento y desconexión. No llevan número de secuencia.
- De información (I): tiene número de secuencia.
- De supervisión (S): control de errores y de flujo. Tiene número de secuencia.

Delimitación

- Línea inactiva: 01111111
- Bandera: 01111110

Transparencia

- Inserción/eliminación de bit 0 en secuencia similar a la bandera.
- Bit stuffing: sirve para delimitar la trama. Si 11111, se inserta un 0 en el tx. Si 111110, se elimina el 0 en el rx.

FCS: CRC-16.

Direcciones

- Única para cada secundaria.
- De grupo (enlace multipunto).
- De difusión (enlace multipunto).

Bit P/F (Pool/Final)

- De escrutinio/final.
- Si envía un 1 en la orden, indica que rx debe confirmar.
- Si envía 1 en la rta, indica que rx está confirmando.

MPLS (MultiProtocol Label Switching)

- MPLS es una tecnología de conmutación de paquetes basada en etiquetas que tuvo su origen en la combinación de IP y ATM en una única tecnología (tag switching).
- Es la integración de los niveles 3 y 2 del modelo OSI, o sea un protocolo “ruteable” (IP) y uno de “enlace” (ATM).
- Los routers del backbone de la red IP-MPLS no necesitan examinar la cabecera IP para tomar una decisión respecto al reenvío del paquete, sino que lo hacen a través de la etiqueta que lleva incorporado el paquete IP.
- La asignación de etiquetas a los paquetes IP se realiza de acuerdo con una gran variedad de criterios (interfaz/subinterfaz de acceso, dirección IP, puerto y protocolo).
- Switch L2L3: switch con router adentro (IP dentro de ATM).

Servicios en ATM

<table>
<tr><th></th><th>Clase A</th><th>Clase B</th><th>Clase C</th><th>Clase D</th></tr>
<tr><td>Características</td><td>Bit rate constante</td><td>Bit rate variable</td><td>Orientado a la conexión</td><td>Orientado a la no conexión</td></tr>
<tr><td>Sincronización entre fuente y destino</td><td colspan="2">Requerida</td><td colspan="2">No requerida</td></tr>
<tr><td>Bit rate</td><td>Constante</td><td colspan="3">Variable</td></tr>
<tr><td>Tipo de conexión</td><td colspan="3">Orientado a la conexión</td><td>Orientado a la no conexión</td></tr>
<tr><td>Capa de adaptación</td><td>AAL 1</td><td>AAL 2</td><td>AAL 5</td><td>AAL 3/4</td></tr>
</table>

Clase A: susceptibles al delay (ej: videoconferencia).

Características de MPLS

- orientado a la conexión.
- Ofrece control de tráfico (seguridad).
- Ofrece control de ancho de banda.
- Adaptabilidad de calidad de servicio.
- Tiene la facultad de operar con cualquier protocolo de red (IP, IPX, etc).
- Crea circuitos virtuales para unir redes distribuidas entre lugares físicamente distantes. Estos circuitos se denominan LSP (Label Switched Paths).

Componentes de MPLS

- LSR (Label Switching Router): son nodos internos de la red, analizan el label del paquete recibido y a partir de su tabla de ruteo interno, determina el camino a seguir (puerto de salida) y el nuevo label que reemplazará al actual. Leen la etiqueta, no les hace falta abrir el paquete.
- LER (Label Edge Router): son nodos que están en la periferia de la red, y son los que se unen a las distintas redes IP externas.
- LSP (Label Switched Path): son la concatenación de un LER de ingreso, una serie de combinaciones de LSR y un LER de egreso.
- LER de ingreso: hace el mayor trabajo. Observa la dir IP del paquete, determina la ruta a seguir internamente asignando un LSP, y le agrega un label como encabezado.
- LER de egreso: remueve el label del paquete y se lo entrega a la red IP correspondiente.
- LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- FEC (Fowarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

Etiqueta MPLS: datos de usuario + cabecera IP + cabecera MPLS + cabecera nivel 2 + …

Cabecera MPLS

- Label (20 bits): es el valor de la etiqueta MPLS.
- Exp (3 bits): se usan para identificar la clase del servicio.
- Stack (S, 1 bit): cuando S=1, es la primera de la pila, la última etiqueta. El resto tiene S=0.
- Time To Live (TTL, 8 bits): se decrementa en 1 en cada enrutador y al llegar a 0, el paquete se descarta. Generalmente sustituye el campo TTL de la cabecera IP.

Funcionamiento

- El único análisis de enrutamiento que se realiza es en el router LER de ingreso. Los siguientes LSR o LER de egreso simplemente siguen el enrutamiento en base a los label y sus tablas internas.
- En MPLS, el label es usado para establecer la ruta, y por lo tanto no es necesario llevar información adicional sobre la ruta a seguir en cada paquete.
- El label asignado representa una combinación de enrutamiento, prioridad y calidad de servicio.

Modo de operación de MPLS

0- Al comienzo, cada red conectada a un LER es detectada por éste, quien agrega un registro en su tabla interna por cada red.
1- Intercambio de redes IP: todos los LSR y LER involucrados intercambian las redes que conocen de acuerdo al protocolo IGP configurado. Los LSR receptores actualizan su tabla con la info recibida y a cada entrada de la tabla le asignan una label y un puerto.
2- Establecimiento de sesiones LDP: cada LSR/LER levanta una sesión LDP con sus vecinos directos para intercambiar etiquetas.
3- Creación de caminos: los caminos (LSP) son creados luego de establecidas las sesiones LDP; el camino óptimo es escogido según las métricas del IGP (> AB, < cant de saltos, etc). Existen dos métodos (tipos de distribución y retención de etiquetas):
    a. Unsolicited downstream, opción “liberal label retention”.
    b. Downstream on demand, opción “liberal/conservative label retention”.

    Valores válidos para etiquetas: 16 hasta 20^{20} (modo trama).

    Tipo de control de distribución:
    - Control ordenado: un LSR no propaga etiquetas a otros LSRs sin haber recibido previamente una etiqueta desde sus LSRs vecinos para el mismo FEC (camino).
    - Control independiente: un LSR puede propagar etiquetas en cualquier momento a cualquier LSR.

Modo LDP / MPLS	**Control**	**Distribución**	**Retención**
Modo trama	Independent	Unsolicited	Liberal
Modo celda o MPLS-TE (RSVP)	Ordered	On demand	Conservative

4- Envío de tráfico: todo paquete IP que ingrese a la red MPLS es etiquetado y conmutado hacia su destino a través de los LSR. El destino puede estar ubicado dentro o fuera de la red MPLS.

El MPLS básico no es de gran utilidad sin sus aplicaciones, las cuales se pueden levantar una vez creada la red MPLS. Éstas agregan gran valor a la tecnología. (Ej: VPN, Qos, PWE3, etc).

Resumen del modo de operación:

- Creación de la etiqueta y distribución.
- Creación de la tabla en cada router.
- Creación de un label switched path.
- Inserción de la etiqueta / lookup en la tabla.
- Fowarding del paquete:
    - El nodo de entrada a la red hace la asignación de cada paquete a un FEC.
    - El FEC se indica mediante una etiqueta que viaja con el paquete.
    - En saltos siguientes no hay necesidad de identificar el FEC pq se tiene la etiqueta.
    - La etiqueta se emplea como índice en una tabla que especifica un siguiente salto y una nueva etiqueta.
    - La etiqueta que traía el paquete se sustituye por la nueva.
    - Reenvío MPLS no requiere que los nodos sepan procesar la cabecera del nivel de red (u otro protocolo encapsulado).

<u>MPLS con QoS</u>

- Prioridades:
    - Real Time (P1) – Prioridad más alta: voz, video interactivo, señal de llamadas.
    - Critical Data (P2): ruteo, datos de misión crítica, datos transaccionales.
    - Preferred (P3): video en streaming, gestión de redes.
    - Best Effort (P4): basurero (scavenger), best effort).
- En VPN-WAN basada en internet, todos estos procesos están en la misma escala de prioridad (best effort).
- Las reglas de QoS hacen que el AB se mantenga constante y respete la cantidad asignada según la prioridad.+

<u>Niveles de QoS</u>

1- El mejor esfuerzo (IP, IPX, Apple Talk): es propio de la capa 3. Su función es hacer el mayor esfuerzo por entregar un paquete pero sólo especifica eso, no informa nada respecto al AB, delay, jitter, etc.
2- Diferenciado – DIFFSERV (Primero, clases, etc.): en este nivel se le brinda un poco más al cliente, y es decir que en caso de congestión va a haber paquetes privilegiados, pero tampoco se puede garantizar nada.
3- Garantizado (AB, demora, jitter): en este nivel se pueden especificar los parámetros de calidad del servicio brindado, es el más serio y es el nivel más alto, típico de ATM. Es el más caro.

Disponibilidad mensual del servicio: es el porcentaje de tiempo durante el cual el canal contratado está operativo y en correcto funcionamiento en un periodo de un mes calendario. Se mide en hs.

Retardo de tránsito (Round Trip Delay)

- El RTD extremo a extremo es el tiempo de ida y vuelta [mseg] de un paquete de 100 bytes entre una sede origen y otra destino, pertenecientes a la misma VPN.
- Para cada una de las sedes pertenecientes a una VPN, el cliente deberá seleccionar una destino, es decir, la ruta sobre la que se realizarán las mediciones de los SLAs específicos.

Jitter o Variación de retardo

- El jitter define con qué regularidad llegan los paquetes al receptor.
- Es la variación del delay o latencia.
- Un jitter muy pequeño indicaría que todos los paquetes llegan con un retardo muy similar (que puede ser bajo o alto, pero es más o menos constante), mientras que un jitter muy alto nos indicaría que las diferencias de retardo entre los distintos paquetes son considerables, es decir, unos paquetes llegan con un retardo muy bajo y otros, con uno muy alto.
- El jitter se expresa en milisegundos y el periodo de observación es un mes de calendario.
- Es muy importante para el tráfico multimedia en tiempo real, pues las aplicaciones necesitan unas variaciones de retardo muy bajas, ya que mediante técnicas de buffering retrasan la reproducción de los flujos para poder reproducir la señal sin cortes.
- Si un paquete llega con un retardo superior al jitter estimado, será descartado ya que no habrá llegado a tiempo para participar de la reconstrucción de la señal.

Calidad de servicio	Valor del jitter (%)	Valor pérdida paquetes (%)
Bronce	N/A	N/A
Plata	N/A	< 1%
Oro	N/A	< 1%
Multimedia	< 30 mseg	< 0,5%

Tecnología de la red

- La red multiservicio es una red basada en tecnología ATM que permite el transporte de flujos de información Frame Relay y ATM.
- Capacidad de conmutación de cientos de Gbps, con enlaces disponibles para entregar hasta 20 Gbps y escalamiento según demanda.
- Acceso desde cualquiera de los nodos de la red multiservicio.

- Los equipos de acceso a la red IP permiten la conexión de enlaces de cliente de entre 64 kbps y 622 Mbps en arquitecturas tipo WAN, y de entre 10 Mbps y 10 Gbps en arquitecturas tipo LAN.
- Los protocolos de acceso a la red que se pueden usar son todos los que permite el protocolo IP y la red multiservicio (ej: PPP, HDLC, FR, ATM, IEEE 802.3).

VPN IP MPLS: Configuración del acceso en función de las QoS

% Tiempo Real + % Misión Crítica + % Estándar = AB Acceso [kbps]

El precio del servicio será dependiente de esta configuración.

Acceso a internet

- Como valor adicional a la VPN se incorpora en cada sitio la posibilidad de acceder a Internet, manteniendo las características de privacidad de la VPN, es decir que este adicional **no** transforma a la VPN en una solución de Internet VPN.
- El AB para tráfico de Internet debe estar considerado en el AB de QoS Estándar.
- Solo se puede configurar el AB de Internet hasta un 50% de la capacidad del vínculo de acceso y hasta el 100% de la QoS Estándar.

Integración de tecnologías

Múltiples tecnologías conviven en una misma red permitiendo el enrutamiento de los datos en forma óptima y sin congestión: data center, accesos dial up, accesos ADSL, Interworking con ATM y FR.

Conclusiones

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles 3 y 2, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura. (En resumen, es importante separar los servicios críticos).

Por otro lado, el hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte (no solo sobre infraestructuras ATM) facilitará de modo significativo la migración para la próxima generación de la internet óptica, en la que se acortará la distancia entre el nivel de red IP y la fibra.