RESUMEN 2DO PARCIAL

Autor	Juan Pablo Frascino
Reviewed	☑

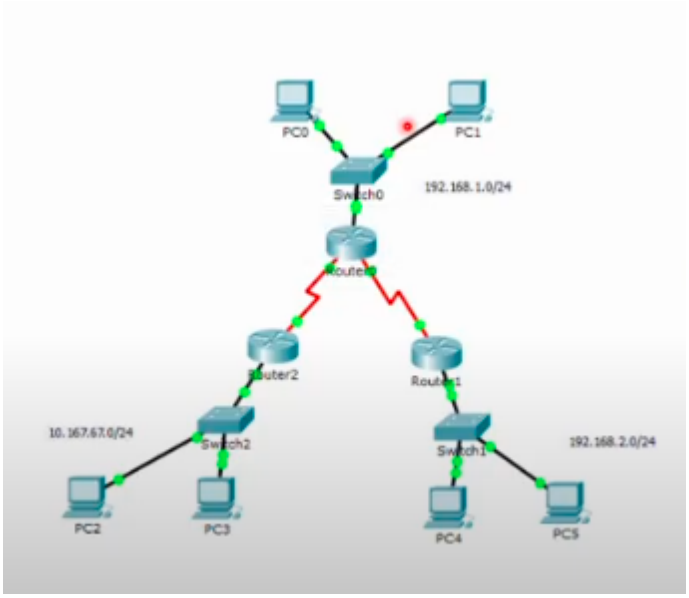
RUTEO/ROUTING

Comunicaciones entre redes separadas. Algoritmos que nos permiten encontrar las redes a las que nos queremos comunicar.

Existen 2 categorias de algoritmos de ruteo:

- ESTATICOS: Un administrador agrega manualmente las redes remotas
- DINAMICO: Las redes remotas son descubiertas automaticamente por medio de un PROTOCOLO

ESTATICO

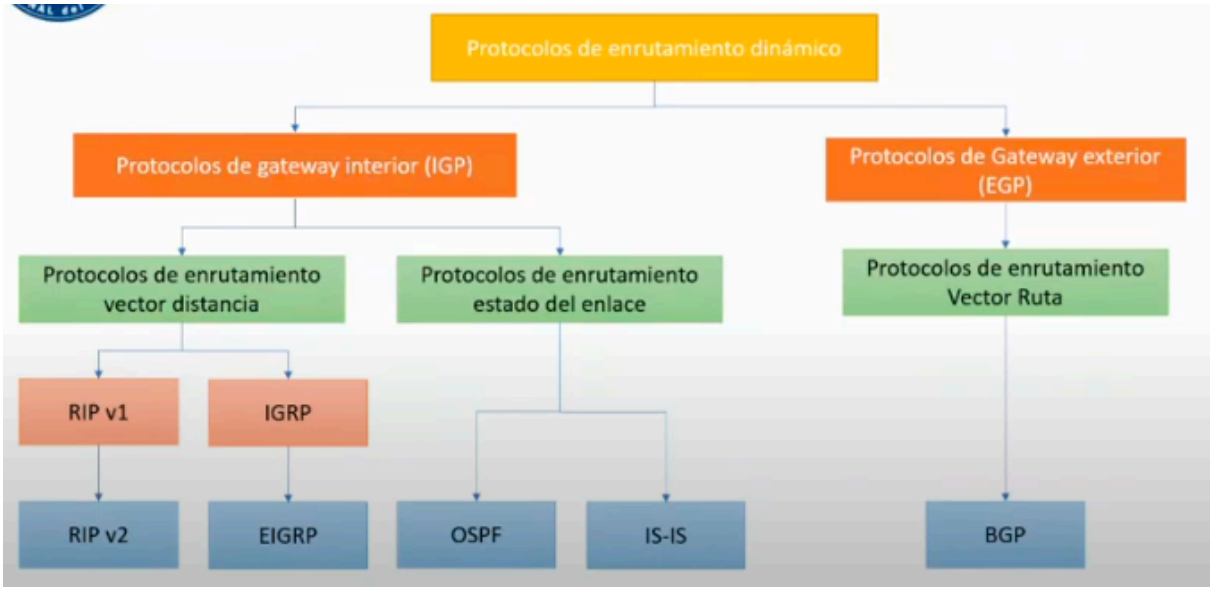


(Los enlaces rojos son enlaces series utilizados para conformar WAN a partir de varias LAN)

En este caso, si utilizaramos los algoritmos estaticos deberiamos generar reglas manualmente en cada router para ir fijando las rutas que deben tomar ciertos paquetes dependiendo de que red vienen y a que red van.

Ventajas	Desventajas
Fácil de implementar en una red pequeña	Adecuado solamente para topologías simples o fines específicos, como una ruta estática predeterminada.
Muy seguro. No se envían anuncios, a diferencia del caso del ruteo dinámico.	La complejidad de la configuración aumenta significativamente cuando el tamaño de la red es mayor.
La ruta al destino siempre es la misma	Se requiere intervención manual para volver a enrutar el tráfico.
Dado que no se requieren algoritmos de ruteo ni mecanismos de actualización, no se necesitan recursos adicionales (CPU / RAM)	

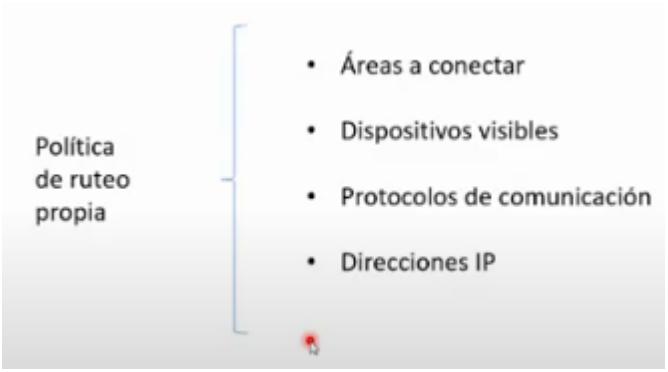
DINAMICO



En esta categoria de enrutamiento existen 2 grandes tipos de protocolos de enrutamiento dinamico:

PROTOCOLOS DE GATEWAY INTERIOR(IGP):

Son usados para intercambiar informacion dentro de un sistema autonomo(AS=grupo de redes IP que comparten una politica de ruteo propia e independiente)



desde afuera el AS es visto como una entidad unica, cada AS tiene un IDENTIFICAR PROPIO, ASN(autonomous system number), puede ser de 16 o 32 bits y es asignado por diferentes asociaones a los largo del globo.

por ejemplo los proveedores de servicio de internet los utilizan puertas adentro para conectar redes propias y de clientes. Dentro de esta categoria existen 2 grandes grupos:

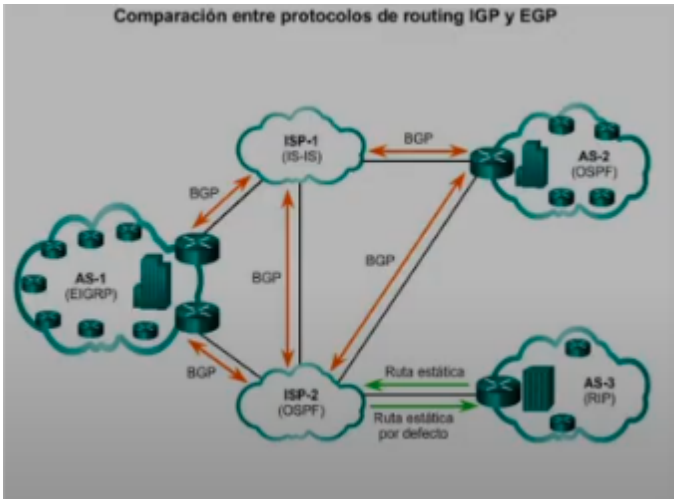
- PROTOCOLOS DE ENRUTAMIENTO VECTOR DISTANCIA(RIP, EIGRP):
  RIP=es por SALTOS,
  EIGRP= tiene en cuenta el ancho de banda, retardos, confiabilidad y carga de los enlaces
- PROTOCOLOS DE ENRUTAMIENTO ESTADO DE ENLACE(OSPF):
  OSPF=Open shortest path first, Genera areas

PROTOCOLOS DE GATEWAT EXTERIOR(EGP):

Son usados par intercambiar informacion entre distintos sistemas autonomos, osea hacia afuera d los sistemas autonomos, dentro de esta categoria se utilizan protocolos del tipo:

- PROTOCOLOS DE ENRUTAMIENTO VECTOR RUTA(BGP):
  BGP=Comunicacion entre AS

EJ: IGP & EGP



	Protocolos de Gateway Interior (IGP)				Protocolo de Gateway Exterior (EGP)
	Vector distancia		Estado de enlace		Vector ruta
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-MP

CONVERGENCIA

Se llama convergencia al estado de la red donde TODOS los routers tienen informacion COMPLETA y PRECISA de TODA la red.

El tiempo de convergencia es el tiempo que los routers tardan en compartir informacion, calcular las mejotes rutas y actualizar sus tablas de ruteo.

Cada protocolo de ruteo dinamico tiene su tiempo de convergencia haciendo que algunos sean mas rapidos de otros.

Para enrutar dinamicamente se necesitan 3 cosas:

- Estructuras de datos: tablas, bases de datos internas, y otros datos utilizados para sus operaciones

- Mensajes de protocolo de ruteo: existen varios tipos de mensajes para descubrir redes y rutas
- Algoritmos de ruteo: calculos/pasos para determinar la mejor ruta

Objetivos de los protocolos dinamicos:

Descubrir redes remotas, mantener la informacion de ruteo actualizada, buscar el mejor camino hacia las redes de destino, encontrar otro camino nuevo si la ruta actual deja de estar disponible.

Y para realizar esto se utiliza METRICAS, que es un valor medible q el protocolo le asigna a cada ruta para determinar la mejor ruta, dependiendo del protocolo son metricas distintas.

Ventajas	Desventajas
Adecuado en todas las topologías donde se requieren varios routers	La implementación puede ser más compleja.
Por lo general, es independiente del tamaño de la red.	Menos seguro. Se requieren opciones de configuración adicionales para proporcionale protección.
Si es posible, adapta automáticamente la topología para volver a enrutar el tráfico.	La ruta depende de la topología actual
	Requiere CPU, RAM y ancho de banda de enlace adicionales.

TIPOS DE PROTOCOLOS

Antes de comenzar a ver uno por uno hay que tener en cuenta que hay una sub division importante entre estos. Que pueden ser con clase o sin clase.

- PROTOCOLO DE RUTEO CON CLASE:
  No se utilizan actualmente, por ej RIP v1 y IGRP, no se usan porque no informan las mascaras de red por lo tanto no es valido con el subnetting.

- PROTOCLO DE RUTEO SIN CLASE:
  Incluyen informacion de mascara de subred en las actualizaciones de ruteo, permitiendo la utilizacion del subnetting tanto VLSM como CIDR, tambien soportan protocolos de ruteo ipv6.
  EJ sin clase: RIPV2, EIGRP, OSPF

PROTOCLOS IGP

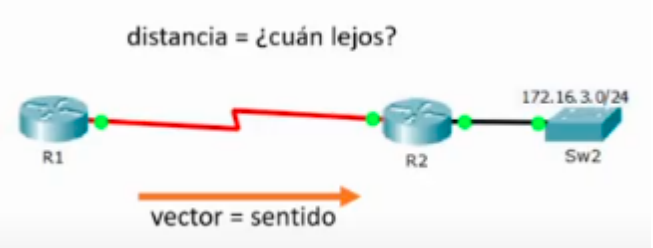
PROTOCOLO VECTOR DISTANCIA:

Los mas utilizados son el RIP v2 y el EIGRP

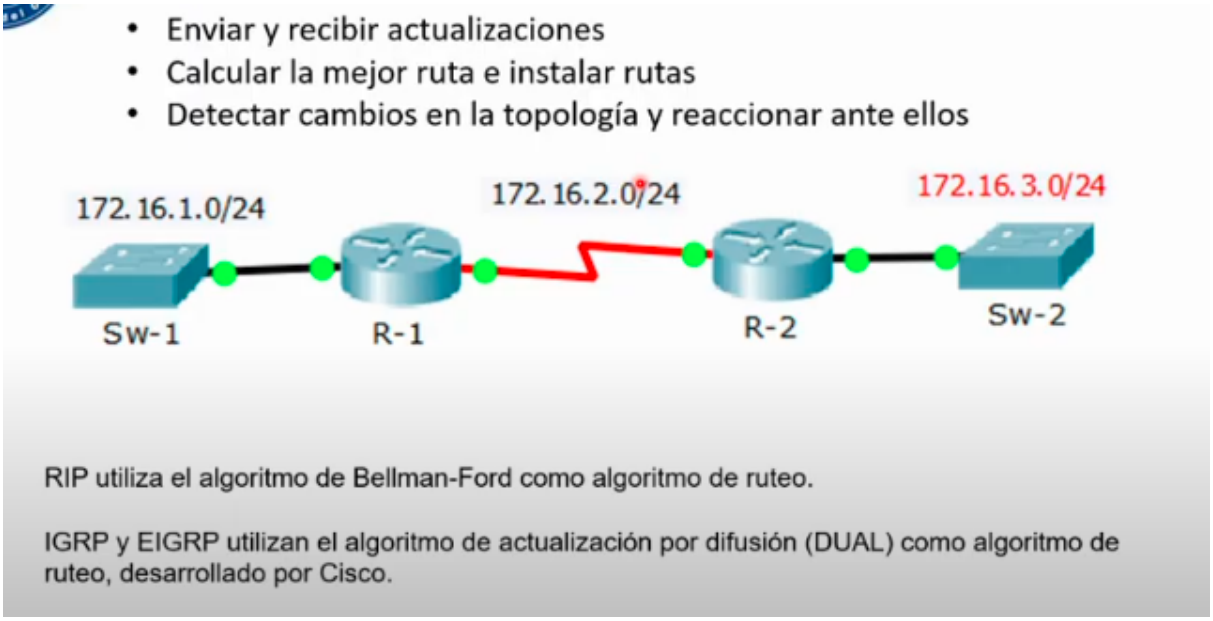
Como funcionan? Con actualizaciones y calculo de distancias.

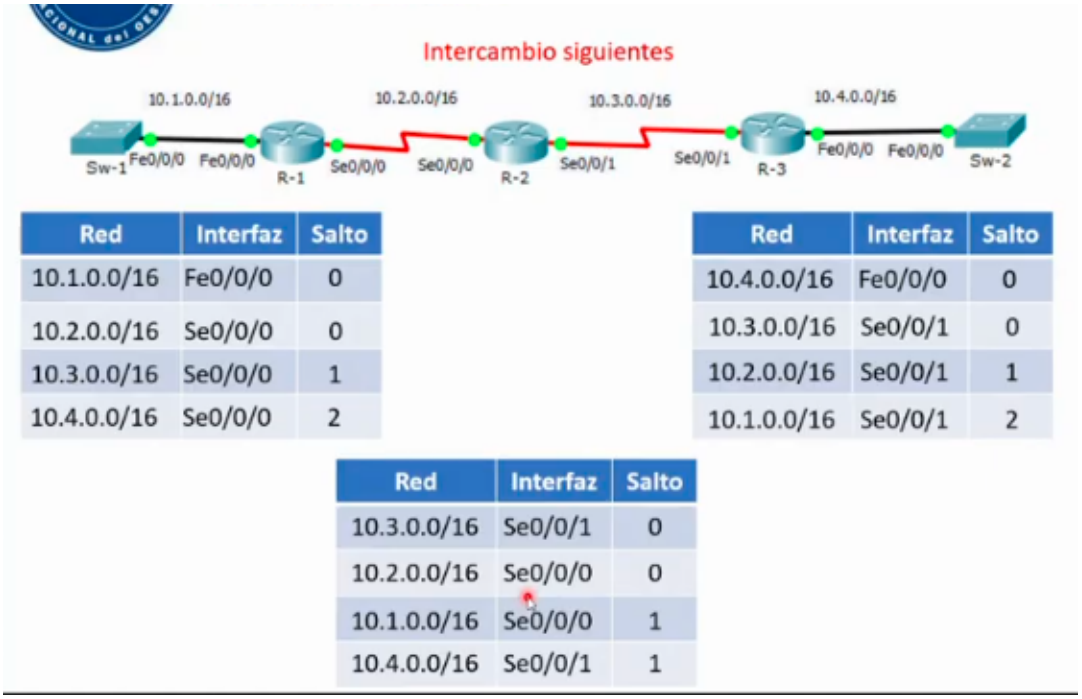
Que son las actualizaciones? Cada n segundos van informando a sus vecinos mediante multifusion cual es el estado de su red, el protocolo no tiene conocimiento de la topologia de la red, sino que cada red conoce sobre las redes al rededor mediante las actualizaciones de estado, estas consumen ancho de banda y recursos.

Como se calculan las distancias? Utiliza un vector y la distancia. El vector es el sentido, y la distancia es cuanto routers tengo pasar para llegar a destino(cada router que paso se le llama un salto)



Para el R1, 172.16.3.0/24 está a un salto (distancia); puede alcanzarse a través del R2 (vector).





Red	Interfaz	Salto
10.1.0.0/16	Fe0/0/0	0
10.2.0.0/16	Se0/0/0	0
10.3.0.0/16	Se0/0/0	1
10.4.0.0/16	Se0/0/0	2

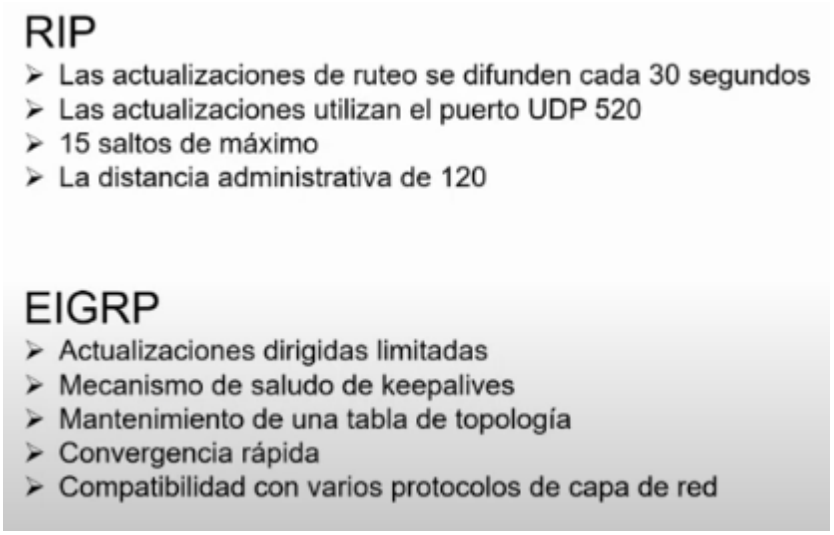
Red	Interfaz	Salto
10.4.0.0/16	Fe0/0/0	0
10.3.0.0/16	Se0/0/1	0
10.2.0.0/16	Se0/0/1	1
10.1.0.0/16	Se0/0/1	2

Red	Interfaz	Salto
10.3.0.0/16	Se0/0/1	0
10.2.0.0/16	Se0/0/0	0
10.1.0.0/16	Se0/0/0	1
10.4.0.0/16	Se0/0/1	1

Cada router tiene su tabla con todas las redes accesibles, por cual interfaz llegar y a cuantos saltos de distancia se encuentra. Primero cada router llena la tabla con las redes inmediatamente conectadas, es decir de salto 0, y luego comiezan a compartir por multidifusion esta informacion permitiendo que otros routers vecinos llenen sus tablas con estas actualizaciones.

La diferencia de EIGRP con RIP es que EIGRP ademas de tener en cuenta los saltos/distancia como RIP, tambien tiene en cuenta el ancho de banda del enlace, es decir, ante 2 enlaces del mismo ancho de banda va priorizar la

cantidad de saltos menor, y viceversa, antes 2 enlaces de la misma cantidad de saltos va a priorizar el mayor ancho de banda disponible.

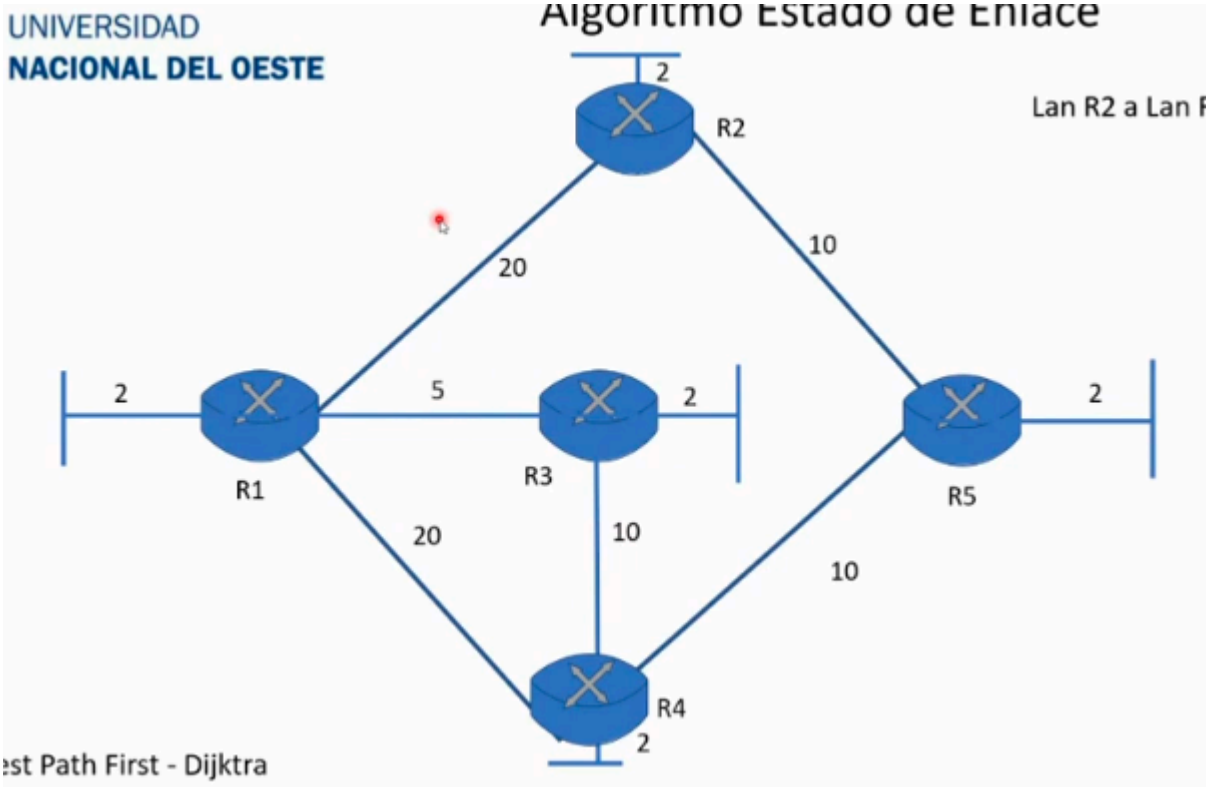


PROTOCOLO DE ESTADO ENLACE:

El mas conocido es OSPF

Aca cada router va manteniendo su propia base de datos en donde en cada base de datos va mateniendo el estado de los enlaces junto con otra informacion como velociada, latencia, rpund trip, etc.

Lo primero que hace cada router es enviar un paquete de “saludo” a sus vecinos(redes conectadas mediante interfaces de red). Luego cada router prepara y crea un paquete de link state(LSP) que incluye el estado de cada enlace directamente conectado, y procese a saturar la red con el LSP a todos los vecinos que luego almacenan la info de los LSP en una base de datos. Luego utilizan la bbdd para construir un mapa completo de la topologia y calcular el mejor camino hacia cada subred de destino.



Utiliza la base de datos para ir poniendole costos a los caminos y luego utiliza un algoritmo para encontrar el camino mas corto primero(open shortest path fisrt) por ejemplo un dijsktra.

DESVENTAJAS DEL OSPF:

Alto consumo de ram y cpu, toma mucha cpu y recursos correr el spf en cada router, entonces lo que se hace es generar pequeñas subareas de pequeñas cantidades de router que tienen router limitadores de area llamado router de borde, una vez que se logra la converecia dentro del subarea, el router de borde informa al area 0(la principal) la informacion recaudada. Siempre existe un area 0 y todas las demas areas se conectan a esa.

COMPARACION ALGORITMOS DINAMICOS

	Vector - Distancia				Estado Enlace	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Velocidad de convergencia	Lento	Lento	Lento	Rápido	Rápido	Rápido
Escalabilidad tamaño de la red	Pequeño	Pequeño	Pequeño	Grande	Grande	Grande
VLSM	NO	SI	NO	SI	SI	SI
Uso de recursos	Bajo	Bajo	Bajo	Medio	Alto	Alto
Implementación y mantenimiento	Simple	Simple	Simple	Complejo	Complejo	Complejo

DISTANCIA ADMINISTRATIVA: Cada protocolo tiene un vlaor, mientras mas pequeña la distancia administrativa va a ser lo preferible al momento de router, si alguna red esta conectada directamente la distancia es cero, si una ruta es estatica la distancia es 1, y para los demas protocolos hay distintos valores predeterminados que va a determinar la prioridad de uso de esa ruta.

PROTOCOLOS EGP

PROTOCOLOS DE ENRUTAMIENTO VECTOR RUTA:

El mas conocido y utilizado es el BGP(Border gateway protocol). Comunica los distintos sistemas autonomos y va realizado diferentes operaciones incrementales cada SA le comunica a otro SA que redes tiene.

Cada router va a analizar las redes que tiene conectadas a traves de los distintos protocolos internos, una vez que recolecto estas tablas con la informacion interna de la red la debe comenzar a comunicar a los AS vecinos. Esto lo realiza mediante 2 procesos diferentes:

- Proceso de entrada(Aprender): El router de frontera recibe informacion de sus enrutadores pares(peers) por BGP, y va a tratar de buscar la maejor ruta para alcanzar los distintos AS, las tablas de BGP siguen la siguiete forma. X red, de X sistema autonomo, la alcanzo por X interfaz
- Proceso de salida(Anunciar): El router de frontera anuncia por BGP a sus vecinos la mejor trayectoria que tiene para llegar a distintos AS, comunica que AS tiene, que redes tienen y que distancia tiene.

Es un protocolo bastante costoso. Los AS el BGP los va conectando por cascada, cada AS anuncia lo de el y lo de los anteriores AS al siguiente AS.

CAPA DE TRANSPORTE TCP/UDP

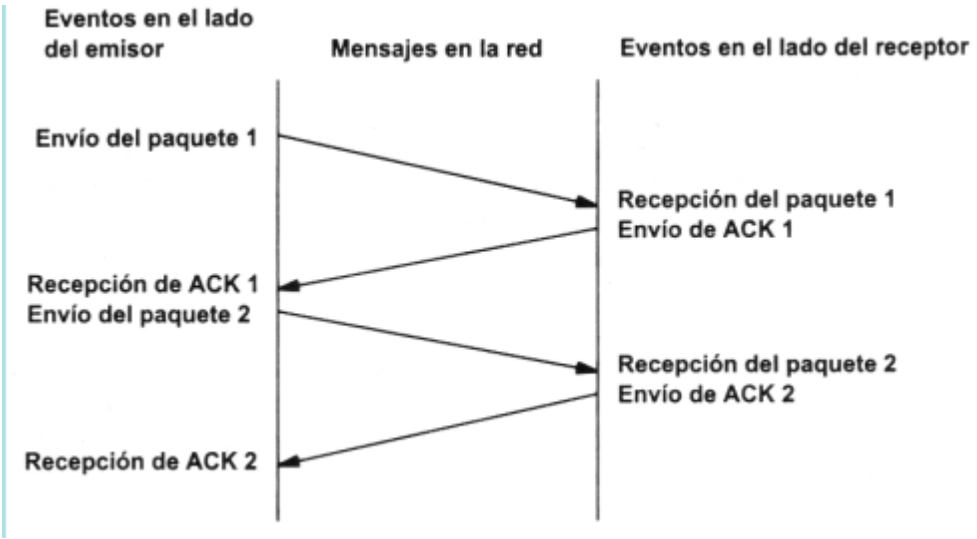
Provee comunicacion entre sistemas finales(extremo a extremo). Utiliza un protocolo llamado TCP/IP que se subdivide en 2:

- TCP: ORIENTADO A LA CONEXION
- UDP: NO ORIENTADO A LA CONEXION

TCP(TRANSMISION CONTROL PROTOCOL)

- Orientado a la conexion, es decir es necesario establecer una conexion entre los extremos.
- Fiable, la informacion que envia el emisor llega de forma segura al receptor
- Utiliza como unidad de datos a los bytes u octetos(de bits), y se agrupan en segmentos.

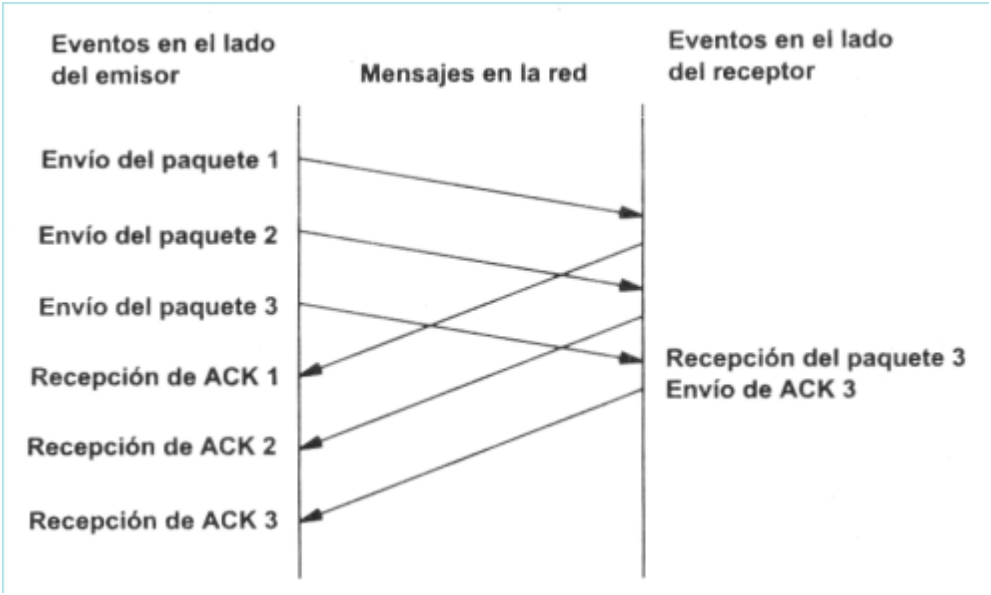
La forma de establecer una comunicacion fiables es asegurando que los segmentos lleguen a destino y para realizarlo se implementando CONFIRMACIONES o ACKNOWLEDMENT(ACK)



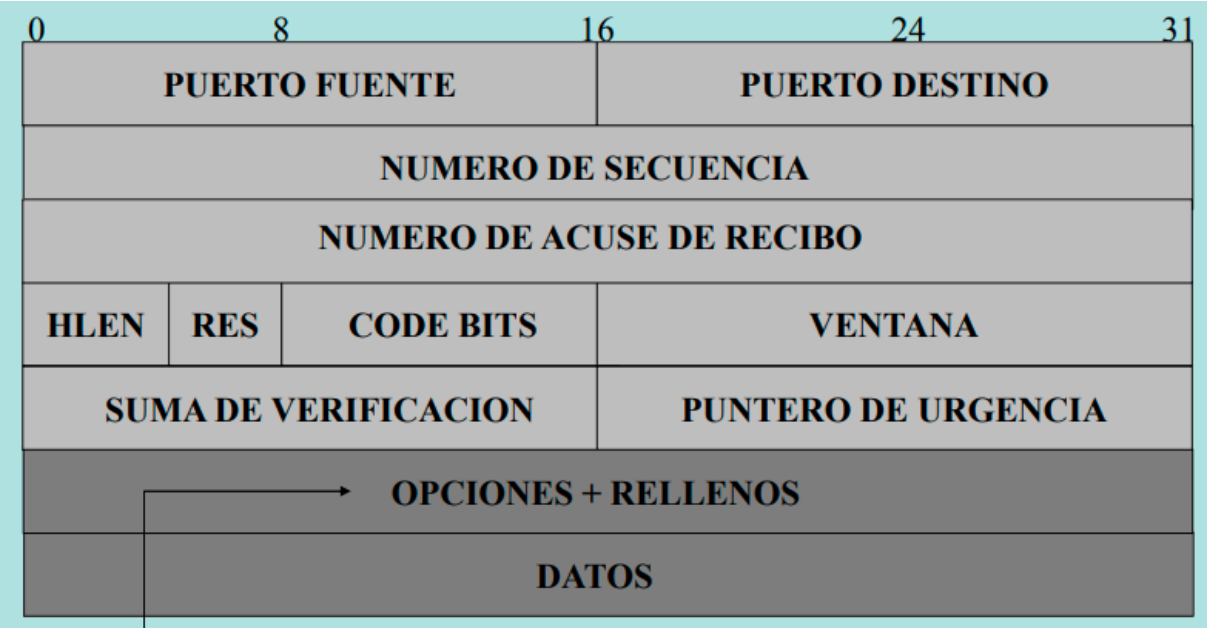
(Envio paquete, recibo confirmacion de que llego, y asi sucesivamente)

Para darnos cuenta de la perdida de un paquete, al enviarlo se activa un temporizador que en caso de que nunca llegue el ACK, se vencera y nos avisara que no llego la confirmacion, por lo tanto el paqute se ha perdido.

La eficiencia de las transmisiones tcp se mejora al enviar los datos bajo el concepto de una VENTANA DESLIZANTE, es decir en vez de mandar un segmento y esperar a la confirmacion para mandar el siguiente lo que hago es que voy mandando segmentos a la vez que espero sus confirmaciones.



FORMATO DE LOS SEGMENTOS TCP(en bits)



PUERTO FUENTE:-Indica el puerto del equipo origen, tiene 16 bits

-Número desde 1025 a 65536

PUERTO DESTINO:Indica el puerto del equipo destino, tiene 16 bits
-Número hasta 1024
-Relacionados con el servicio, ejemplo http 80

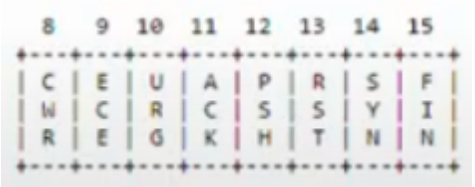
NUMERO DE SECUENCIA: Inicia como el primer byte del primer octeto de datos que nosotros estamos mandando, va incrementando con la cantidad de bytes que nosotros vamos enviando luego del primer paquete

NUMERO DE ACUSE DE RECIBO: Indica el numero de secuencia del siguiente byte que esperamos recibir

HLEN(4bits): Longitud del header, medido en multiplos de 4, valor minimo 5(20 bytes)

RES(4bits): reservado, sin uso

CODE BITS: 8 bits de control, utilizados para controlar congestiones, sesiones y el 3 way handshake, cada uno indica una flag(si esta en uno, sino en cero)



CWR: Congestion Window Reduced
ECN: Explicit Congestion Notification
URG: Habilita el Campo Puntero Urgente
ACK: Habilita el Campo de Confirmación
PSH: Habilita la función de forzado
RST: Habilita la función de interrumpir la conexión
SYN: Habilita la función de sincronizar la conexión
FIN: Habilita la función de terminar la conexión

VENTANA: Numero de bytes u octetos que el emisor esta dispuesto a aceptar por parte del destino, por el tamaño del buffer

SUMA DE VERIFICACION: es el checksum del segmento, pero tambien incluye una pseudo cabecera que contiene datos de la cabecera del protocolo ip

PUNTERO DE URGENCIA: Se utiliza para enviar datos urgentes, si este campo esta encendido mostrara el numero del byte de los datos urgentes a partir del numero de secuencia

OPCIONES: Si el hlen indica mas de 5 palabras seran de opciones como en el protocolo ip(si no estan completas se rellenan hasta llegar a 32 bits)

DATOS: Luego se envian en el resto de palabras los datos a transmitir

Las redes que utiliza tcp pueden CONGESTIONARSE por las siguientes razones:

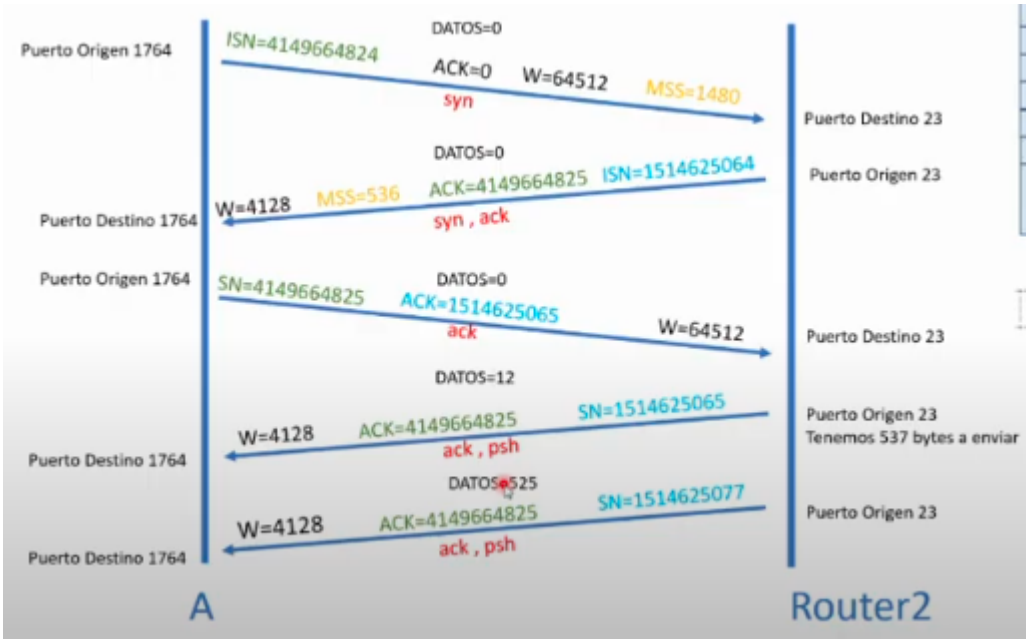
- perdida de paquetes
- latencia alta
- fluctuaciones de throughput
- injusticia en la asignacion de recursos

Para evitar esto se controla la red mediante CONTROL DE FLUJO, busca evitar que el emisor sobrecargue al receptor para eso tenemos el campo de ventana, y luego el CONTROL DE CONGESTION, busca que el emisor sobrecargue la red.

CAMINO DE LAS 3 VIAS/ 3 WAY HANDSHAKE

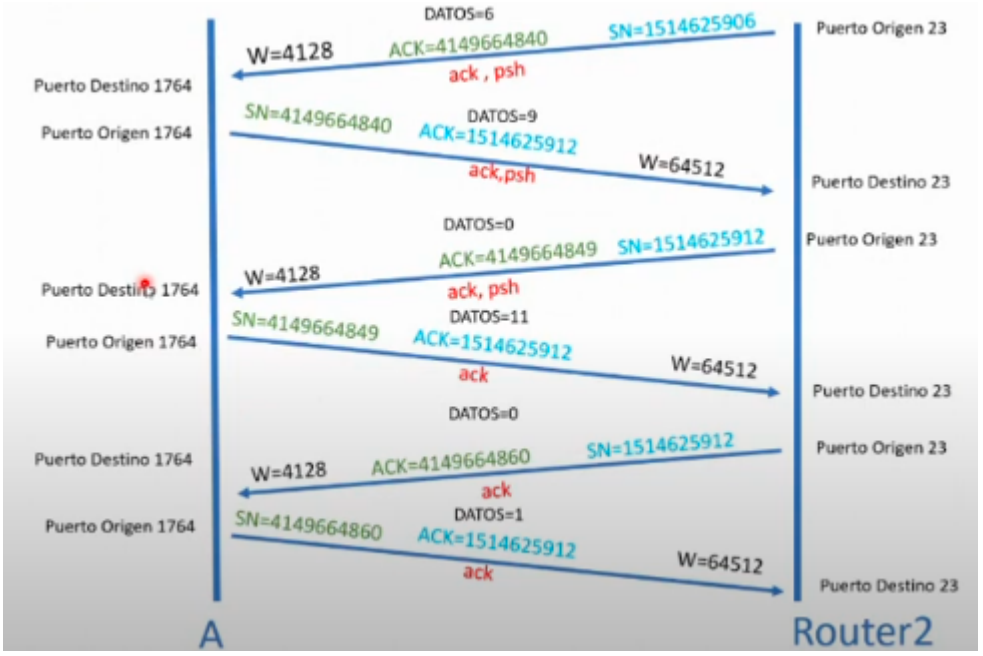
Es el mecanismo utilizado para establecer la conexion entre emisor y receptor

SYN, SYN/ACK, ACK



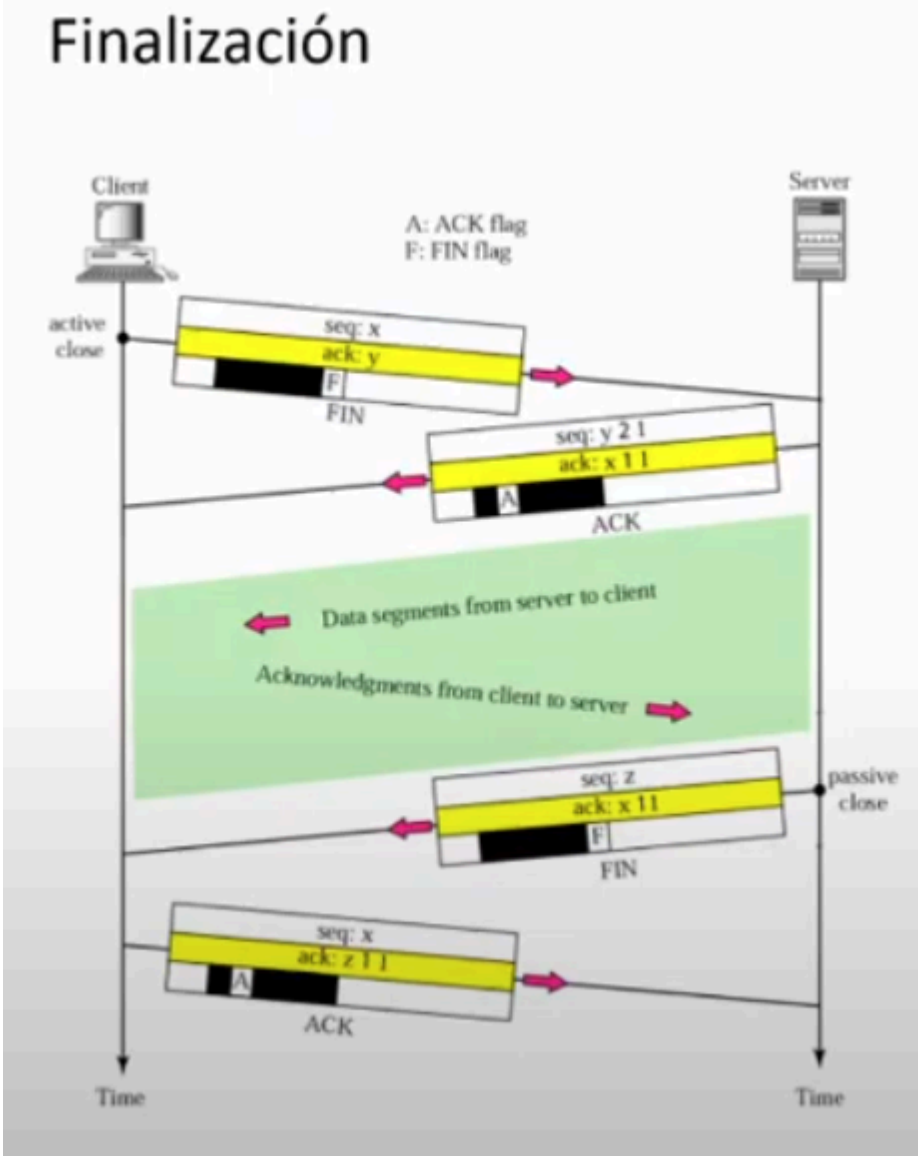
EJEMPLO DE ENVIO DE SEGMENTOS EN UN 3 WAY HANDSHAKE

fijarse que cuando estoy haciendo el camino de 3 vias, el sn aumenta en 1 por cada envio.



EJEMPLO DE ENVIO DE SEGMENTOS EN UNA TRANSMISION DE DATOS

Fijarse en como cuando envio datos, el SN se le suma en la siguiente tramision la cantidad de datos transmitidas en la ultima, en el ack va el sn del otro, los ack tienen 0 datos



TEMPORIZADORES Y ESTADOS

El temporizador que espera que llegue un ack se llama timeout. Si el timeout es muy corto tengo muchas retransmisiones, pero si es muy largo tengo una reaccion muy lenta ante las perdidas.

Entonces para calcular un tiempo adecuado uso el ROUND TRIP(tiempo de ida y vuelta, desde envio a ack) y partir de eso utilizo una formula para ir calculando un timeout adecuado

Otros temporizadores que tiene el TCP y que se utiliza para varios calculos:

- temporizador de retransmision: cuando no hay ack se retransmite regularmente

- temporizador de persistencia: verifica periodicamente que no hay un cambio en el tamaño de la ventana de buffer para no sobrepasarlo
- temporizador de mantenimiento: detecta regularmente si el otro extremo de la transmision se bloquea o se reinicia
- temporizador de 2M: mide si la conexion esta e TIME_WAIT(tiempo que espero para asegurarme que todos los segmentos restantes de la conexion hayan expirado)

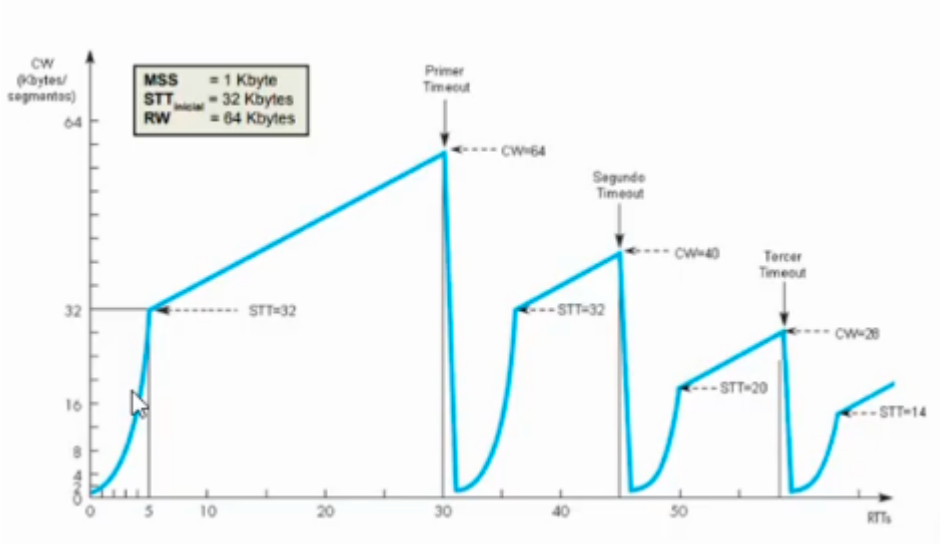
MECANISMOS DE CONTROL DE CONGESTION BASICOS

- SLOW START: inicio con una tasa de transferecia baja y medida que pasa el timepo la voy aumentando a la maxima tasa posible en el momento de manera exponencial
- CONGESTION AVOIDANCE: una vez que alcanzo cierto umbral de congestion usando el slow start, se comienza aumentar la tasa pero no de manera exponencial sino de de manera lineal mediante un MSS(Maximun segment size) a la vez
- FAST RETRANSMIT: mejora la eficiencia reduciendo el tiempo necesario para recuperarse ante la perdida de paquetes, asume perdidas sin esperar que el timeout expire, generando una respuesta mas rapida ante la perdida de paquetes
- FAST RECOVERY: una vez que se retransmite el paquete perdido, en vez de volver al slow start tcp entra en un estado de recuperacion rapida, donde la ventana de congestion se reduce a la mitad del tamaño que tenia cuando se detecto la perdida

Despues existen unos mas avanzados que son reimplementaciones de esots basicos:

- Tahoe
- Reno y New Reno
- CUBIC
- BRR

Implementacion:



vemos como aumenta exponencial con slow start, luego llega la umbral y aumenta en lineal con el congestion avoidance, en este caso no hay fast recovery por lo que llega al timeout y en vez de comenzar a transmitir desde cero lo hace desde la mitad con el fast recovery.

ej ejercicio tcp

Rendimiento TCP (bits/s) = Tamaño de ventana TCP (bits) / Latencia (s)

Distancia (km)	RTT (ms)
1000	15
4000	50
8000	120

Tenemos un enlace gigabit Ethernet entre servidores con una latencia RTT de 30 ms. Necesitamos enviar un archivo de gran tamaño de un servidor a otro por FTP. ¿Qué ancho de banda real podemos esperar?

Considerando tamaño ventana TCP estándar 64KB (65536 B = 524288 bits)

Rendimiento máximo de TCP = 524.288 bits / 0,030 s = 17.476.266 bps = 17,4 Mbps

Para aumentar este throughput(cantidad de bits enviados por segundo) podemos:

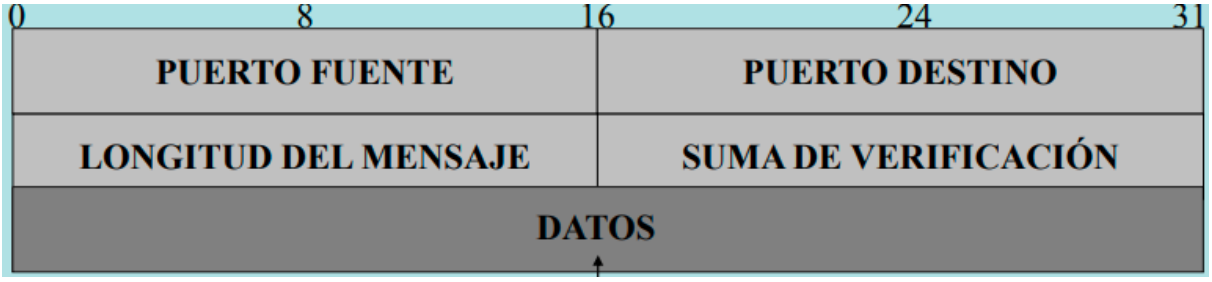
- reducir la latencia RTT
- Abrir multiples conexion tcp simultaneas

- Modificar la configuracion del tcp en ambos extremos

UDP(USER DATAGRAM PROTOCOL)

Es utilizado en transmisiones donde nos importa mas la velocidad que la fiabilidad de los datos, ej: llamadas telefonicas, servicios de streaming, videojuegos online, etc

- No orientado a la conexion, es decir no se establece una conexion previa al envio de datos.
- No fiable, la informacion que envia el emisor puede perderse o dañarse antes de llegar al receptor
- Utiliza como unidad de datos a los bytes u octetos(de bits), y se agrupan en segmentos.



El segmento es mas simple que el tcp, el header tiene solo 4 campos de 16 bits, los puertos como en tcp, luego la longitud total del mensaje expresada en bytes(incluye tanto a datos como a cabecera) y luego el checksum como tcp. y los datos.

WAN y HDLC

Las WAN(WIDE AREA NETWORK) son redes de area amplia que interconectan diferentes redes lan, en forma privada, son vinculos internos, en forma publica, es la internet.

En las WAN se usan multiples protocolos que trabajan en la capa d enlace, por ej:

• High Level Data Link Control (HDLC)
• Point to Point Protocol (PPP)
• Asynchronous Transfer Mode (ATM)
• Frame Relay (FR)
• Syncronous Data Link Controller (SDLC)
• Logical Link Control (LLC)

HDLC

Es uno protocolos de WAN mas importantes y utilizados, sus caracteristicas son:

- Es un protocolo de comunicaciones punto a punto y punto a multipunto
- proporciona recuperacion de errores
- ofrece una comunicacion fiable entre transmisor y receptor
- orientado al bit y sincronico
- permite una transmisión transparente, independientemente del código de nivel superior.

Funciona definiendo estaciones que pueden ser de 3 tipos:

- PRIMARIAS: Genera ORDENES, es la encargada de controlar el funcionamiento del enlace
- SECUNDARIAS: Genera RESPUESTAS, es controlada por una estacion primaria.
- COMBINADAS: Genera ORDENES o RESPUESTAS, puede ser una estacion primario o secundaria

A su vez el enlace puede estar:

NO BALANCEADO: Esta formado por una estación primaria y una o más secundaria

BALANCEADO: Esta formado por dos estaciones combinadas.

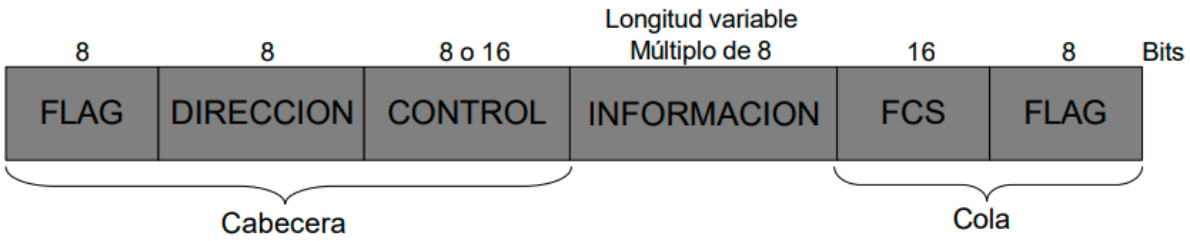
(ambos pueden trabajar en full o half duplex)

Tambien se debe definir el modo de operacion sobre el que opera el enlace:

- MODO DE RECUPERACION NORMAL(NRM): Utilizado en configuraciones no balanceadas. La estación primaria emite ordenes y la o las secundarias envían respuestas.
- MODO BALANCEADO ASINCRONICO(ABM): Utilizado en configuraciones balanceadas. Cualquiera de las estaciones combinadas puede iniciar la comunicación.
- MODO DE RESPUESTA ASINCRONICO(ARM): Utilizado en configuraciones no balanceadas. La estacion secundaria puede iniciar la comunicacion, pero la primaria sigue siendo la responsable de la comunicaciom.

El modo ABM es el más utilizado en enlace punto a punto full duplex.

ESTRUCTURA DE LA TRAMA HDLC

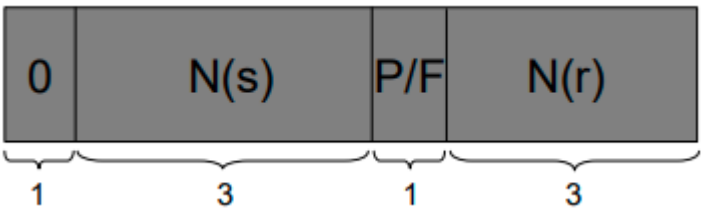


FLAGS: Son los campos delimitadores de la trama(inicio y final) y siempre tienen la forma “01111110” (7E) que la identifica, tambien se garantiza que en el campo de datos no apararezca ninguna combinacion de bits igual al flag, por lo que si aparecen 5 unos seguidos, se inserta un cero que luego es quitado por el receptor.

DIRECCION: normalmente son 8 bits, pero puede ser ampliado a varios bloques de 7 bits, en ese caso cada bloque utiliza el ultimo bit para avisar si hay otro bloque(0) o no (1), es utilizado solo para enlaces punto a multipunto, donde indico las estaciones secundarias.

CONTROL: Es un campo de longitud variable(1 o 2 bytes) e implementa los mecanismo de control de flujo y enlace, existen 3 tipos de tramas:

- INFORMACION(I): se utiliza para enviar datos de usuarios (capa superior a HDLC), aceptación de tramas, información de tramas enviadas.



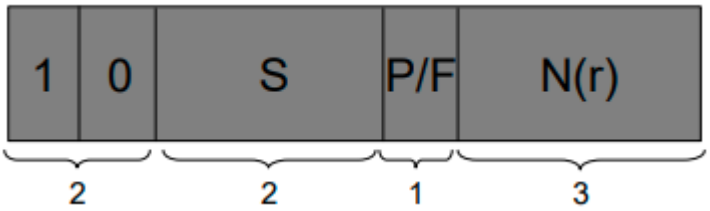
El primer bit es un cero

N(s): Número asociado a las tramas enviadas.
N(r): Número de secuencia de la próxima trama que se espera recibir.
P/F: Poll / Fin

(La funcion del P/F depende el contexto, la estacion principal utiliza el P(POLL) para solicitar una respuesta de estado a una secundaria, y la secundaria responde con una trama de informacion o supervision y el bit F, que indica final de trasmision de la secundaria en NRM)

- SUPERVISION(S): Se utilizan para tareas de supervisión(Aceptación de tramas, Solicitud de transmisión de tramas, Suspensión temporal de la transmisión)

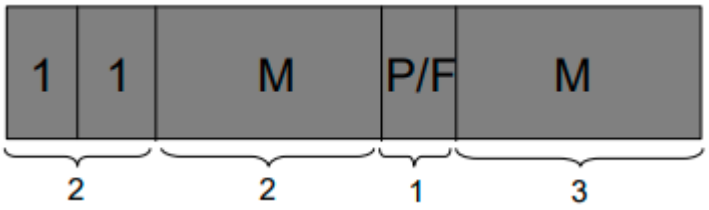
  EJ de estas tramas: RR/00(RECEPTOR READY), RNR/10(RECEPTOR NO READY), REJ/01 (RECHAZO SIMPLE), SREJ/11(RECHAZO SELECTIVO)



Los primeros 2 bits son 10

N(r): Número de secuencia de la próxima trama que se espera recibir.
S: Codifica el tipo de trama de supervisión.
P/F: Polling / Fin

- NO NUMERADAS(N): Se utilizan para tareas de gestion(conexion/desconexion del enlace, control del enlace)



Los primero 2 birs son 11

M: Codifica ordenes y respuestas en este tipo de tramas. 5 bits define 32 comandos y 32 respuestas
P/F: Polling / Fin

INFORMACION: Campo solo presente en las tramas de informacion, es de logitud variable pero siempre la cantidad de bits debe ser multiplo de 8

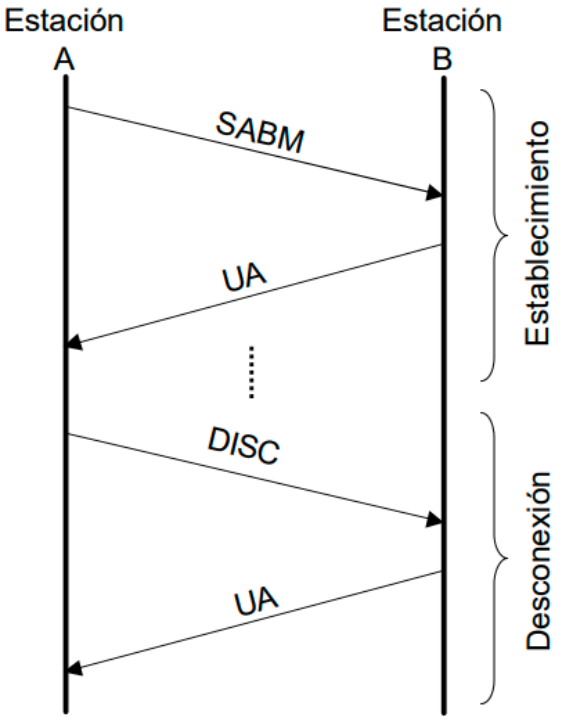
FCS: FRAME CHECK SEQUENCE, codigo de deteccion de erroes que excluye a los delimitadores, normalmente es un crc de 16 bits

COMUNICACION EN HDLC

Consiste en el intercambio de tramas entre 2 estaciones, y se divide en 3 fases:

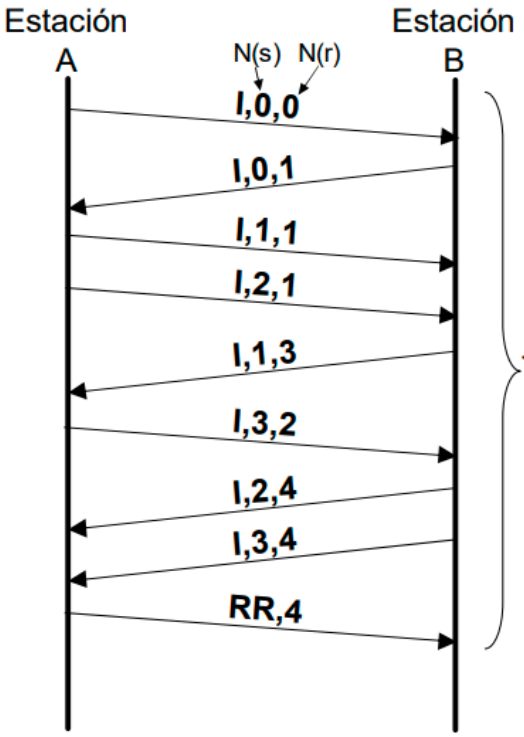
– Establecimiento de la conexión
– Transferencia de datos
– Liberación de la conexión

Establecimiento y Fin de Conexión

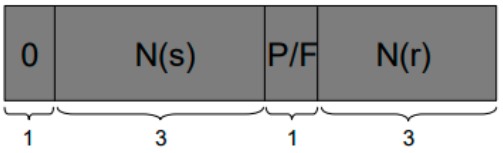


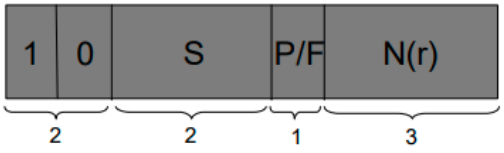
SABM: Establecimiento de la conexión en modo asincrónico balanceado.
UA: Aceptación de la solicitud.
DISC: Pedido de desconexión.

Ejemplo Transferencia de Datos

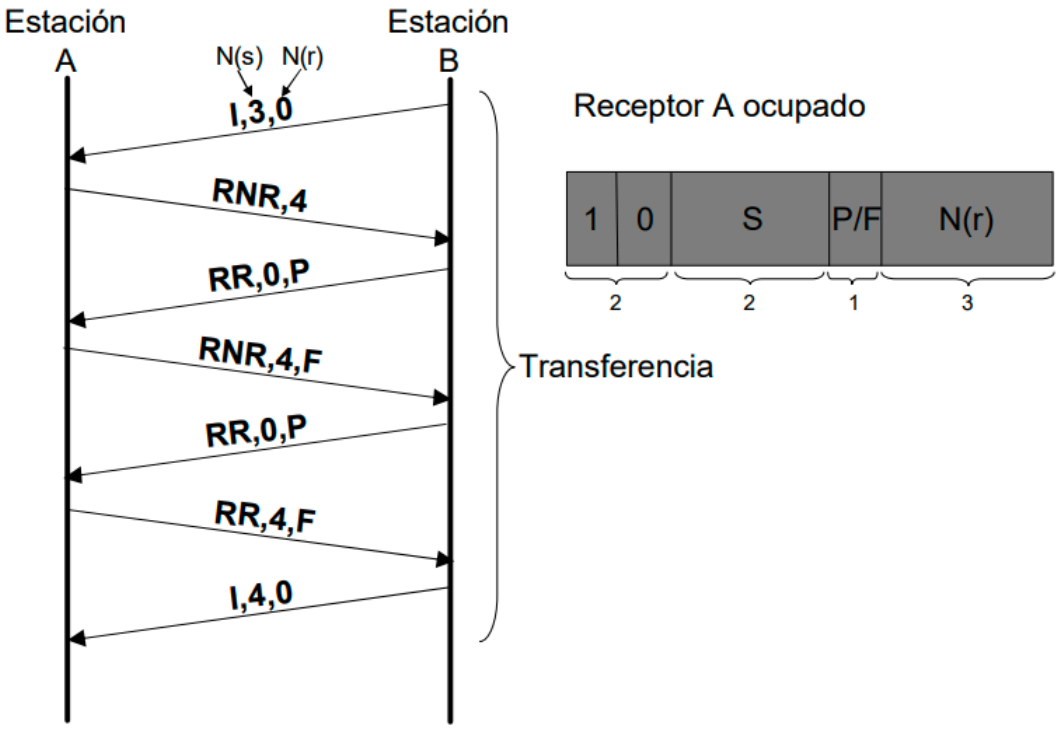


Intercambio de datos en ambos sentidos

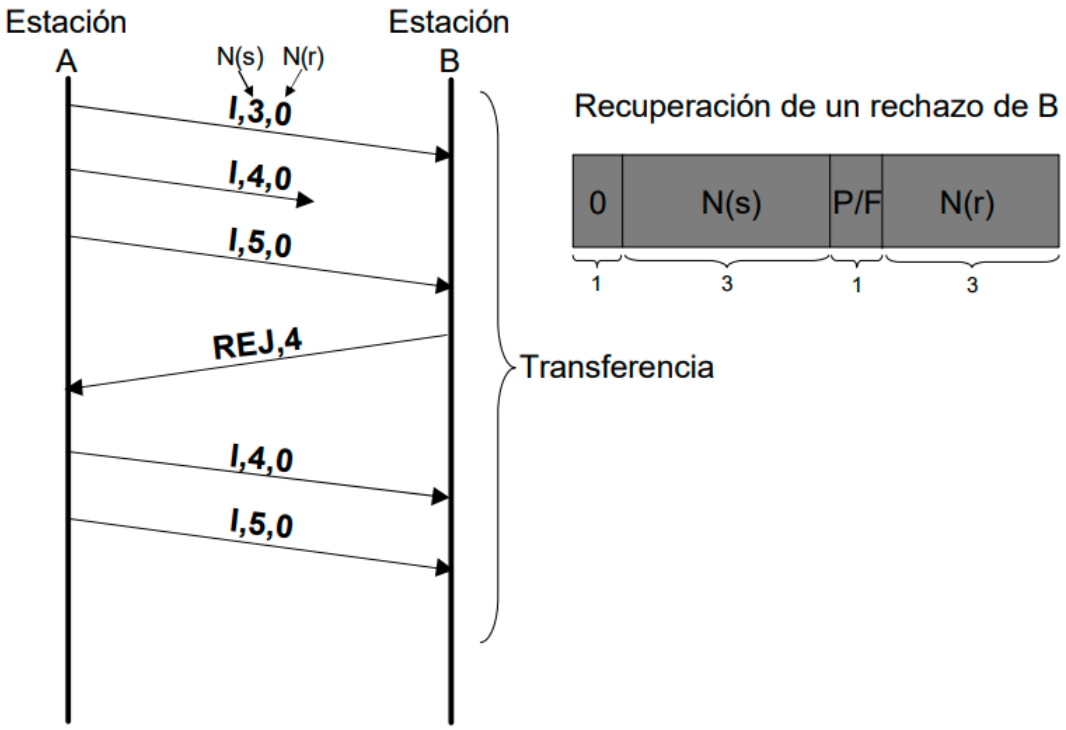




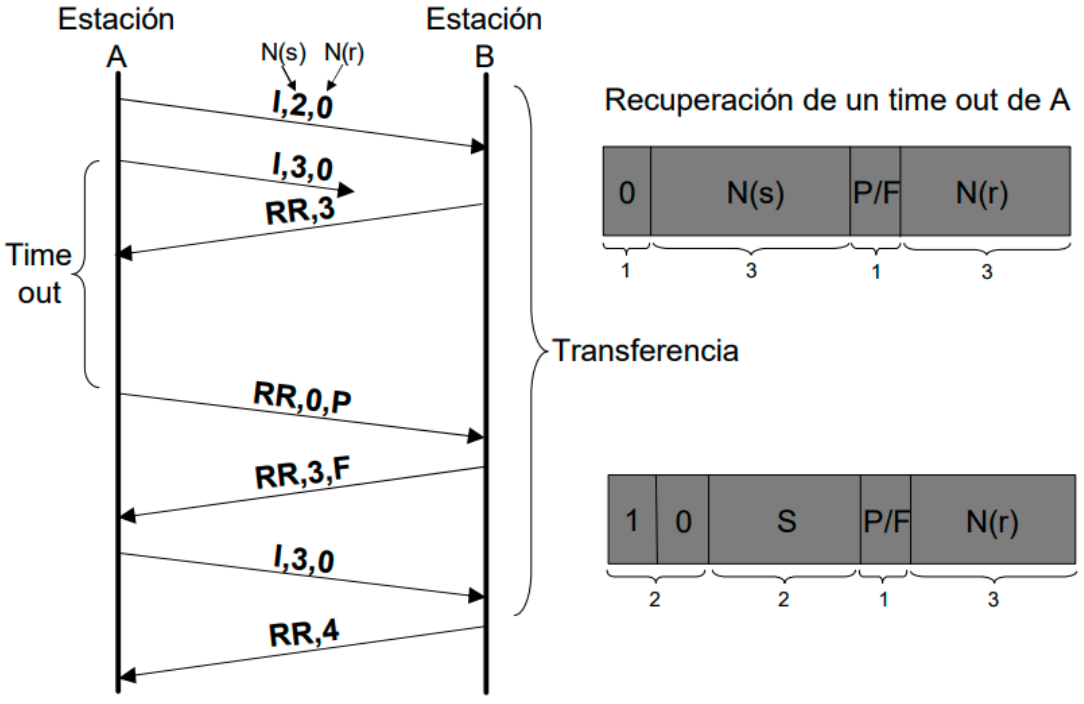
Ejemplo Transferencia de Datos



Ejemplo Transferencia de Datos



Ejemplo Transferencia de Datos



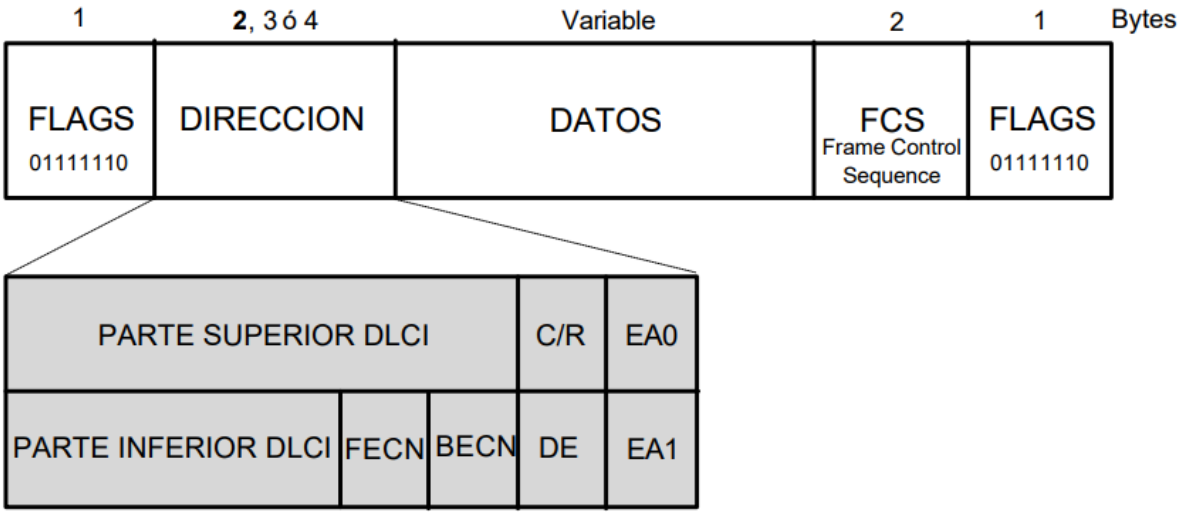
FRAME RELAY

Frame relay es otro protoclo utilizado en las WAN y que trabaja sobre la capa de enlace. Nace como necesidad de un protocolo que se adecue mas a la nuevas velocidades de las redes.

Caracteristicas:

- Utiliza una tecnica de conmutacion de tramas, trabaja como si fuera un switch a nivel wan
- Permite transmitir voz, videos y datos a mayor velocidad
- Encapsula varios protocolos(IP, IPX, SNA, etc)
- Trabaja con enlaces punto a punto siempre
- Orientado a la conexion pero NO CONFIABLE, es decir, establece una conexion previa al envio de datos, pero puede llegar a perderlos durante la transmision.
- Se pueden realizar 2 tipos de conexiones:
  - PERMANENTES(PVC): La conexion esta siempre activa(gasto recursos
  - SWITCHEADA(SVC): Genero la conexion en el momento que la necesito usar
- No corrige errores y no tiene control de flujo
- Utiliza la señal de banda base HDB3

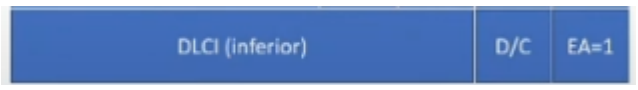
FORMATO DE LA TRAMA FRAME RELAY(ESTA EN BYTES)



CAMPO DE DIRECCIONES(ESTA EN BITS)

DLCI: Data Link Connection Identifier, es un identificador unico del enlace pero es local a cada red, osea que cada red le puede asignar un dlci distinto que refiera al mismo enlace.
C/R: Comando/Respuesta
EA: Extensión de la Dirección, si esta en 0 indica que el dcli continua, permitiendo mayor cantidad de enlaces, si esta en 1 termian ahi el campo de direcciones
FECN: Notificación Explícita de Congestión hacia delante
BECN: Notificación Explícita de Congestión hacia atrás
DE: Discard Eligibility, si esta marcada para el descarte o no, es decir, si llega a haber congestion puede ser descartada si esta en 1.

Se le puede agregar un octeto mas

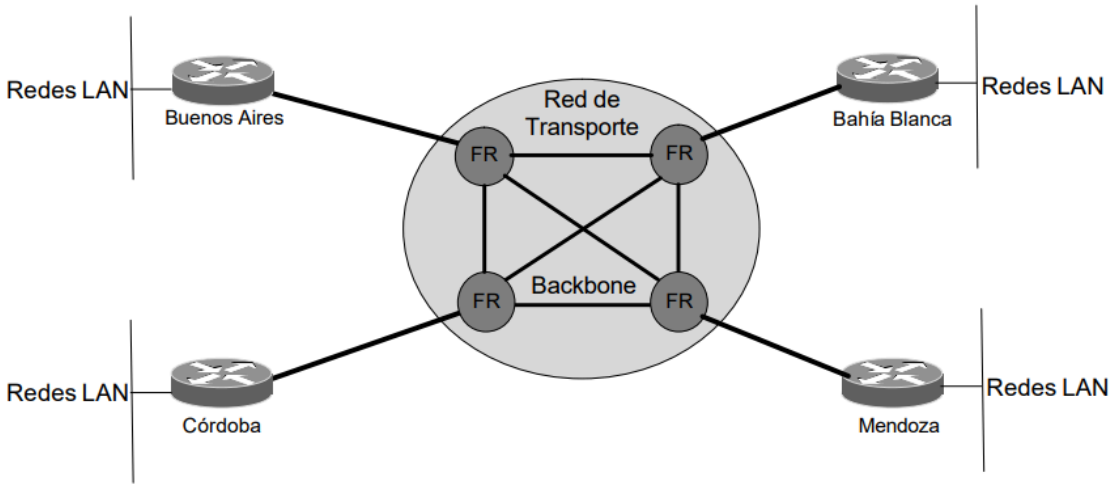


O dos

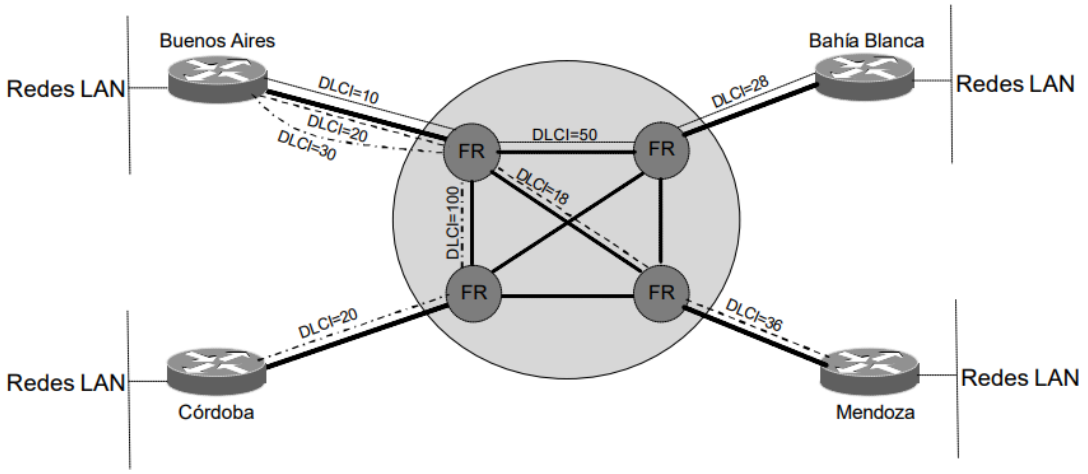
permitiendo que el dcli sea cada vez mas grande.

Entonces, con 2 octeto son 10 bits de dlci, con 3 octetos son 16 bits y con 4 octetos son 23 bits de dcli

ARQUITECTURA DE UNA RED FR



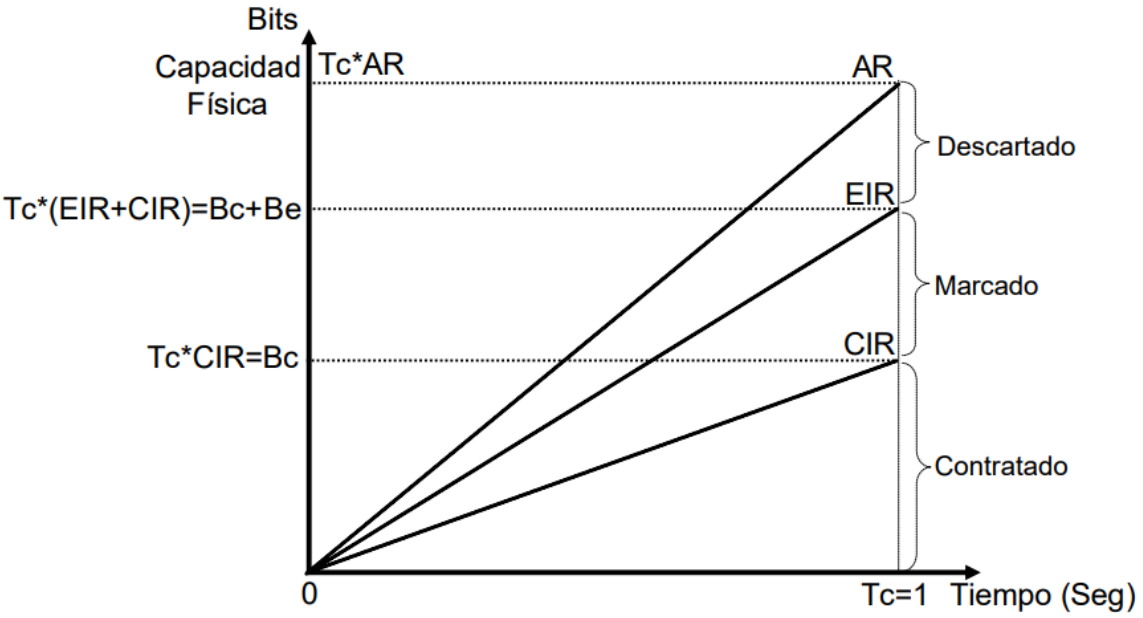
Supongamos que tengo una casa central en buenos aires y quiero conectarme con las demas casas



CVP1: DLCI 10 + DLCI 50 + DLCI 28 → Buenos Aires – Bahía Blanca
CVP2: DLCI 20 + DLCI 18 + DLCI 36 → Buenos Aires – Mendoza
CVP3: DLCI 30 + DLCI 100 + DLCI 20 → Buenos Aires – Córdoba

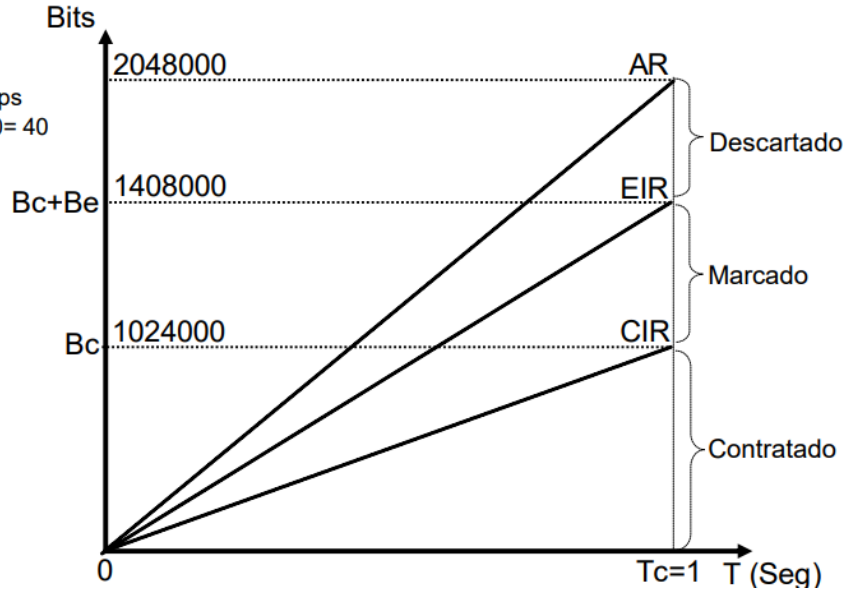
Vemos como para cada red, el dlci de la conexion es distinto, pero al fin y al cabo refiere a la misma conexion

TRAFICO Y PROBLEMAS



Problema: Supongamos que se contrata un acceso FR con una línea física E1 (AR= 2048 Kbps). Además se define un PVC con un CIR=1024 Kbps. El proveedor configura el enlace con un EIR=384 Kbps y establece el valor de Tc=1 segundo. En esta situación se desea enviar un flujo de video en tiempo real a un destino remoto, suponiendo que el envío de datos se hace siempre utilizando tramas de 6250 bytes (50000 bits), siendo el flujo de datos de 2000 Kbps, se desea conocer cuantas tramas se inyectan al nodo FR, cuantas serán aceptadas, cuantas marcadas y cuantas descartadas.

Trama = 50000 bits
Flujo de Datos (V) = 2000000 bps
Cant. Tramas = 2000000/50000= 40
TG = 1024000/50000=20
TM = 384000/50000= 8
TD = 640000/50000=12



Para sacar cantidad de tramas hago FLUJO DE DATOS/TAMAÑO DE TRAMAS

Para sacar cantidad de tramas aceptadas hago CIR/TAMAÑO DE TRAMAS

Para sacar cantidad de tramas marcadas hago EIR/TAMAÑO DE TRAMAS

Para las descartas resto las dos anteriores al total.

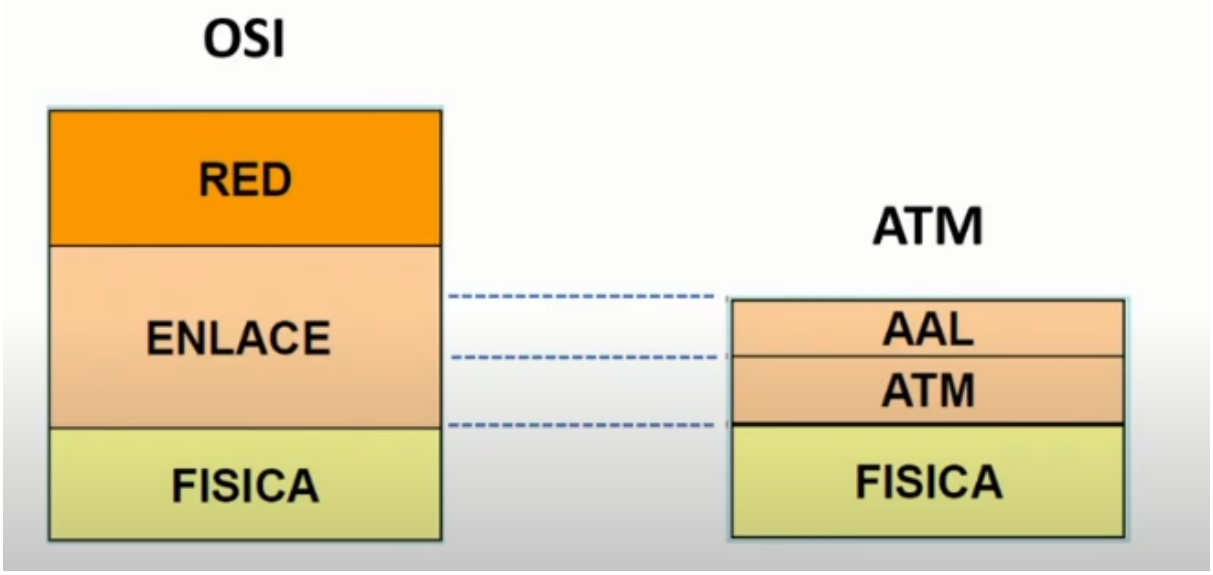
ATM

Ultimo protocolo de WAN, ATM, ASYNCHRONOUS TRANSFER MODE)

CARACTERISTICAS:

- En lugar de utilizar tramas utiliza CELDAS de longitud fija
- Utiliza multiplexacion de varias conexion logicas a traves de una unica interfaz fisica.
- Tiene un MINIMA capacida de control de errores y de flujo(un solo campo)
- Puede trabajar a muy ALTAS VELOCIDADES, a diferencia de FR que llegana a los 3mbps, esta puede ir desde los 25 mbps hasta los 40 gbps

- Orientada a la conexion, y tiene los 2 mismos tipos de circuitos que FR:
  - PERMANENTES(PVC)
  - SWITCHEADOS/CONMUTADOS(SVC)
- Utiliza una codificaion llamada par VPI/VCI para establecer las conexiones entre circuitos virtuales, uno define el circuito/ruta(VPI) y otro el canal dentro de esa ruta(VCI), dentro un VPI puede haber varios VCI.
- Cuando se establece la conexion se reservan los recursos para garantizar la calidad de servicio establecida



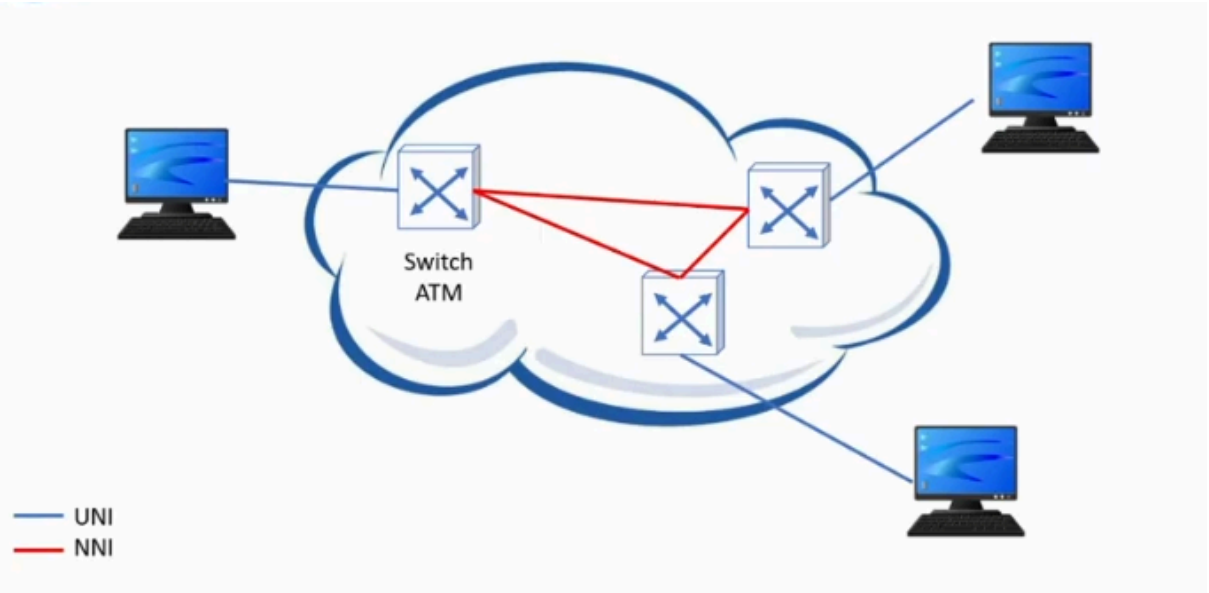
ATM desvaria un poco del clasico modelo osi, para empezar en la capa fisica se utiliza principalmente fibra optica(eso es lo que nos permite las altas velocidades). Y luego en la capa de enlace se divide en 2, la capa ATM(encargada del control de flujo, multiplexa y demultiplexa, maneja los headers, se encarga de los vpi/vci, etc) y la capa AAL(encargada la convergencia, segmentancion y reemsamble de las celdas)

CELDAS ATM

Tienen un tamaño fijo de 53 bytes, y 5 bytes son de cabecera, por lo tanto tengo un campo de informacion de maximo 48 bytes.

Estas celdas pequeñas reducen el retardo en las colas para las celdas de alta prioridad, tambien las celdas de tamaño fijo por una caracteristica fisica se

pueden conmutar de forma más facil y eficiente.

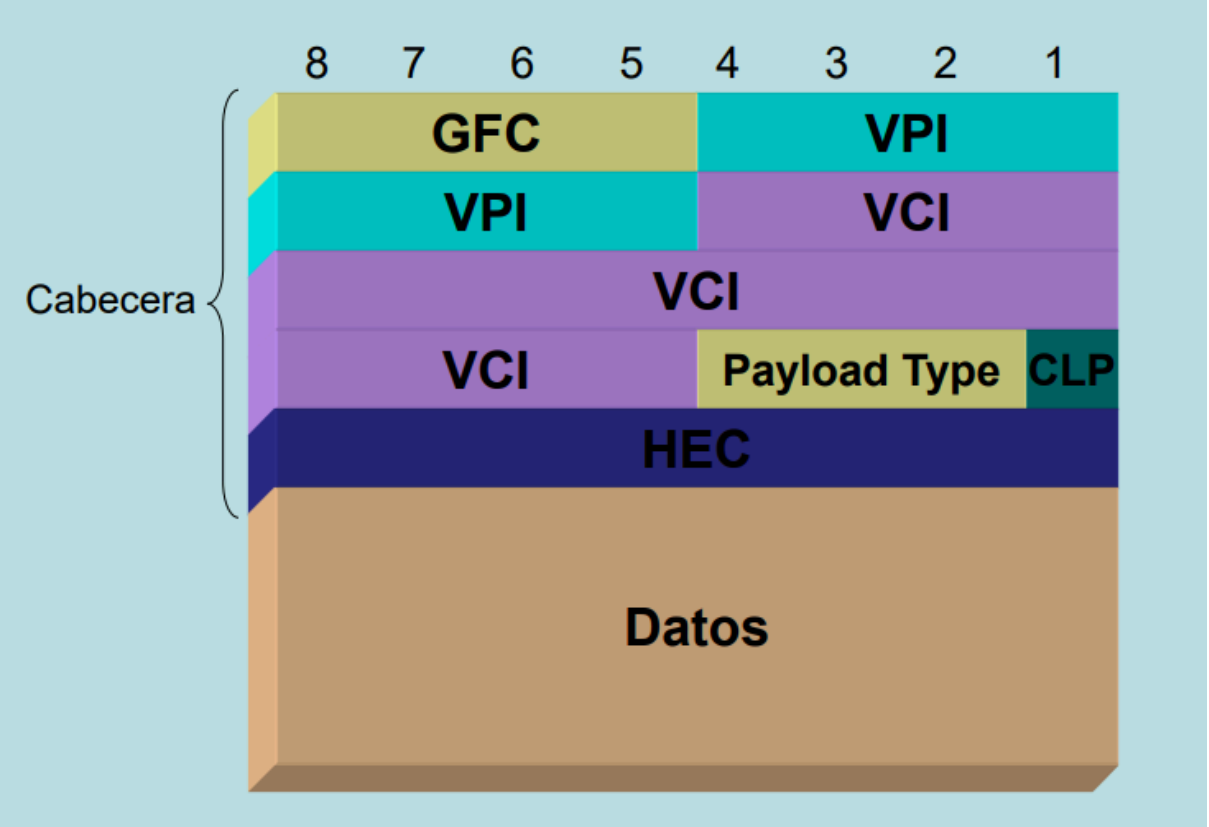


Dependiendo de donde se encuentre la conexion tiene nombres distintos porque las tramas son distintas:

- UNI (user network inteface): Interfaces entre la red y el usuario, redes orientadas al usuario final con capacidades especiales, pueden llegar a ser de cobre en vez de fibra
- NNI : Interfaces red a red, entre los switches ATM(dentro de la red del proveedor de servicio), son todas de fibra optica, tienen anchos de bandas mucho mayores a los de las UNI

Los switches atm tienen como objetivo conmutar la mayor cantidad de celdas con la menor tasa de error y ademas todas las celdas que entran a un nodo nunca se reordenan, tal cual como llegan se despachan, no hay buffer.

FORMATO CELDA UNI(EN BITS)



GFC (Generic Flow Control, 4 bits): Controla el flujo de tráfico en la interfaz usuario-red

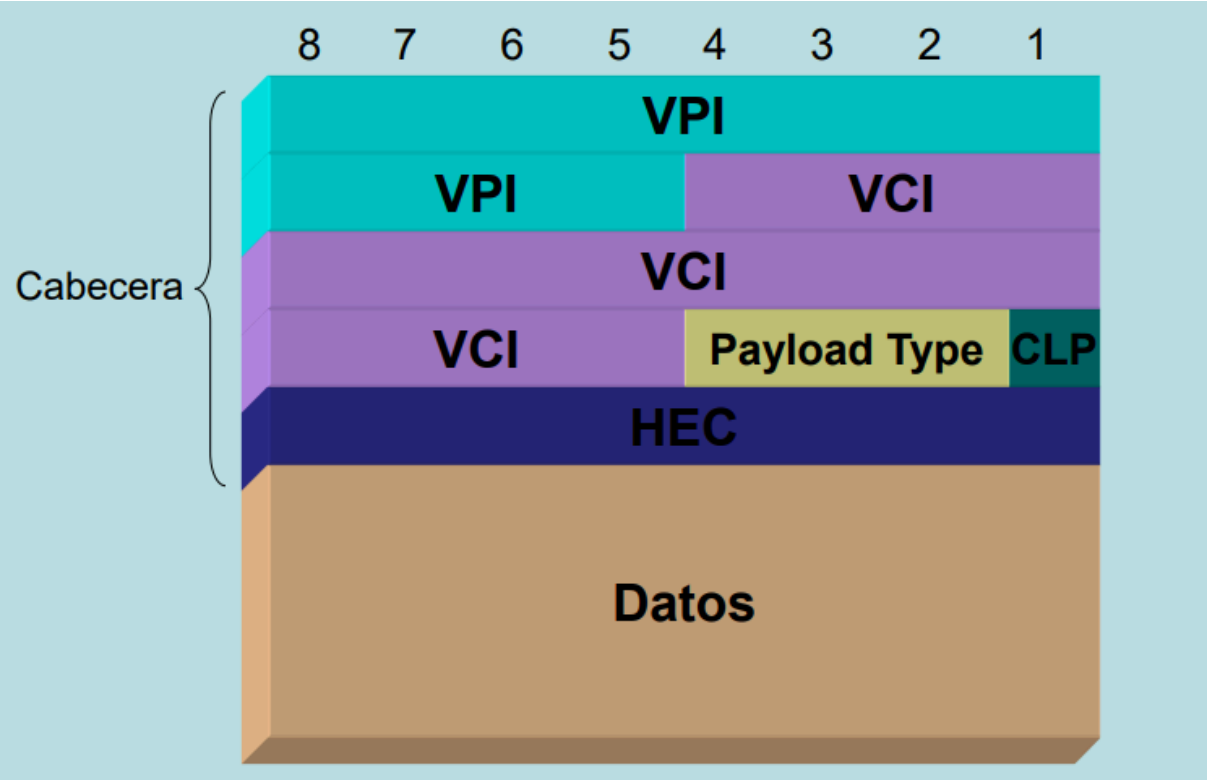
VPI (Virtual Path Identifier, 8 bits) y VCI(Virtual Circuit Identifier, 16 bits): Se utilizan
para indicar la ruta de destino o final de la celda

PTI (Payload type, 3 bits): identifica el tipo de datos de la celda (datos del usuario o control)

CLP (Prioridad, Cell Loss Priority, 1 bit): Indica el nivel de prioridad de las celdas, si este bit esta activo cuando la red ATM esta congestionada la celda puede ser descartada.

HEC (Header Error Correction, 8 bits): contiene un código de detección de error que sólo cubre la cabecera, permite detectar un buen número de errores múltiples y corregir errores simples

FORMATO CELDA NNI(EN BITS)



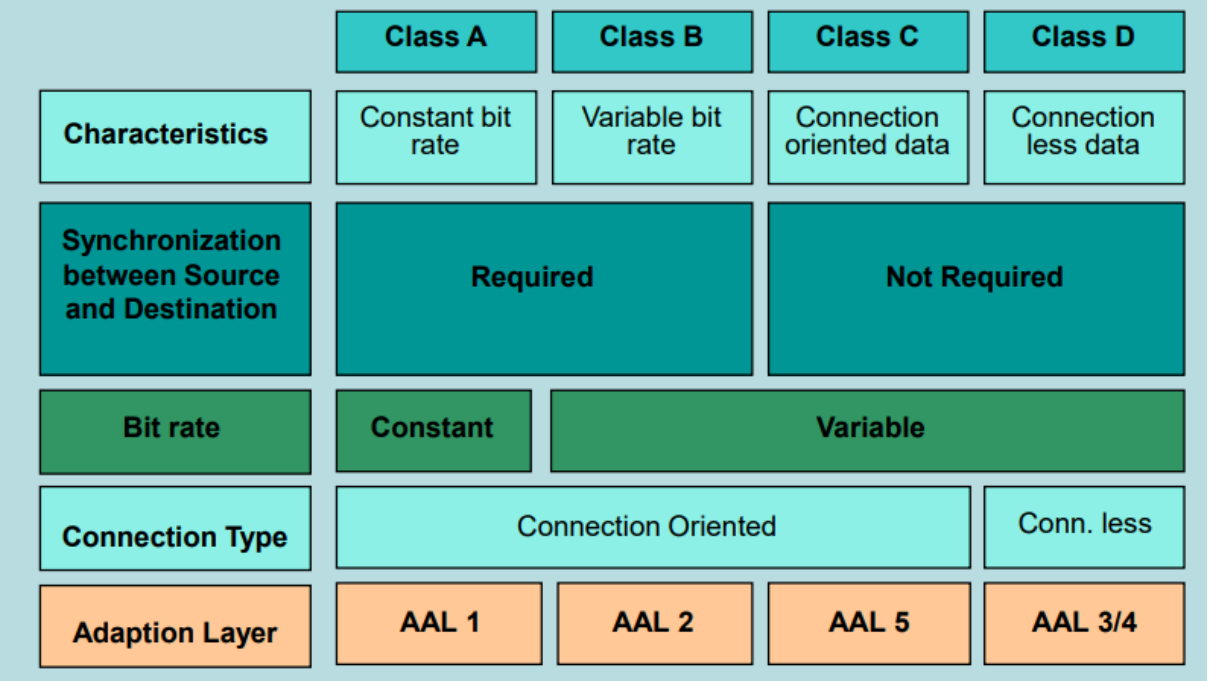
Lo unico que cambia es que desaparece el campo de control de flujo de trafico y esos bits se los asigna al VPI pasando a tener 12 bits, permitiendole tener muchas mas rutas/caminos

Como vimos, en la capa de enlace se divide en ATM y AAL, este AAL es una capa de adaptacion de servicio que va a cambiar dependiendo de la categoria de servicio:

*bit rate es la tasa de transferencia de datos

Estos servicios tambien se pueden categorizar en funcion del tiempo

- Servicios a tiempo real
- Constant Bit Rate (CBR)
- Real-Time Variable Bit Rate (VBR)
- Serivicios NO a tiempo real
- Non-Real-Time Variable Bit Rate (nrt-VBR)
- Available Bit Rate (ABR)
- Unespecified Bit Rate (UBR)



Si estudiaste de mi resumen pagate unas medialunas 😛😛😛😛😛😛😛😛😛

Alias: jp.frascino.mp