REDES Y SERVICIOS DE LA TELECOMUNICACIÓN (RSTC)

Gabriel Cereceda

TEMA 1: REVISIÓN DE FUNDAMENTOS.

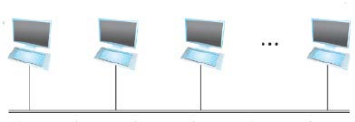
Vamos a repasar los conceptos fundamentales con los que vamos a trabajar en esta asignatura:

Topología de la red: consiste en los elementos físicos (equipos, medios) y la interconexión que componen una red

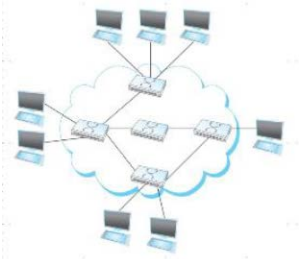
- Enlace directo: no es una red, es la conexión directa entre dos equipos, se suele conocer como conexión punto a punto.

El medio no necesariamente tiene que ser un cable, puede ser inalámbrico, radio…

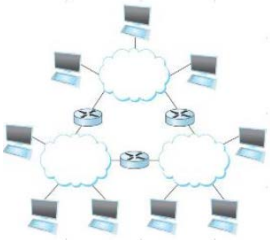
- Enlace compartido: se trata de equipos interconectados por el mismo medio.



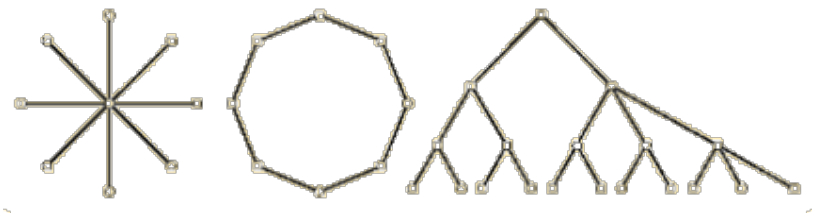
- Red: conjunto de medios mediante los cuales los equipos pueden conectarse entre sí.



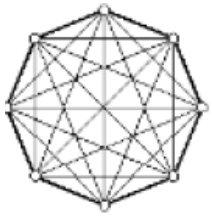
- Internet: se puede definir como una red de redes formada por equipos, medios y redes interconectadas.



- Tipos de topología: son las "formas" que adquiere el dibujo de la red. Pueden ser tipo estrella, anillo, árbol…



También podemos encontrar redes que conecten, todos con todos o MESH como podemos ver en la siguiente figura:



Donde el número de enlaces necesario para conectar todos los equipos viene determinado por la siguiente expresión: $\binom{\boldsymbol{n^{\underline{o}}\ de\ equipos}}{\mathbf{2}} = \frac{\boldsymbol{n(n-1)}}{\mathbf{2}}$ que se corresponde con la conexión de n equipos tomados de dos en dos.

NOTA:

Para hacer ejercicios de esta parte, normalmente suelen pedir el número medio de saltos (entre routers) o el número de enlaces medio…

En estos casos lo que hay que hacer es caracterizar una variable aleatoria (número de saltos) y después calcular lo que nos pidan.

Por ejemplo, si nos dicen que existe una topología de árbol y 2^n-1 routers, y que la probabilidad es uniforme (todos los caminos son posibles) se calcula el número de saltos medio como $\sum_i^{n-1} Pi\ Xi$.

Puede ayudar a calcular la probabilidad el entender estos ejercicios como "el número de enlaces/caminos/routers totales que puedo escoger entre todos los posibles".

Es decir dando n saltos, llego a x routers de los m posibles, tal y como vemos aquí: $P(n\ saltos) = \frac{n^{\underline{o}}\ de\ router\ que\ puedo\ llegar\ en\ esos\ saltos}{n^{\underline{o}}\ de\ routers\ existentes}$

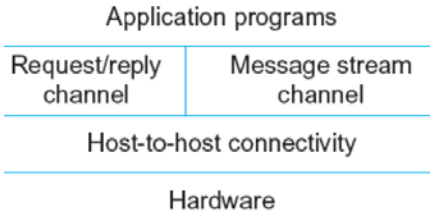
Si tuviésemos 5 routers y quisiéramos saber de cuantas maneras podríamos conectarlos con una determinada topología, basta con saber cuantos enlaces hay entre ellos y hacer una variación con el número de topologías a estudiar (4 tipos de enlaces y 10 enlaces saldrían a 4^{10} posibles topologías.

Por último si tuviésemos 8 routers conectados y quisiésemos saber el retardo medio que hay entre router y router, lo que tenemos que hacer es calcular el número medio de saltos que se pueden dar.

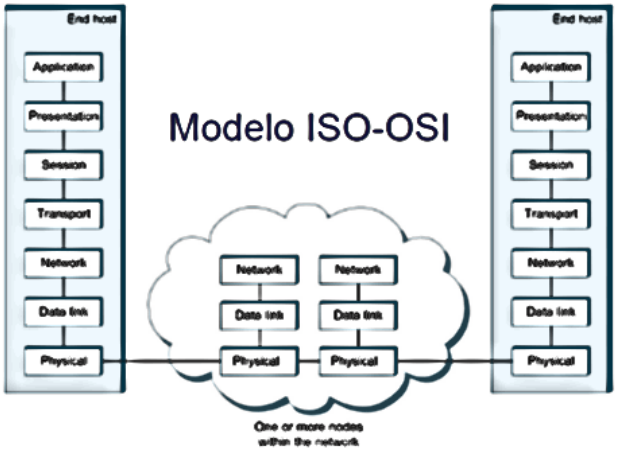
La probabilidad de dar un salto es igual al número de routers que llego dando un salto, partido por los routers que hay.

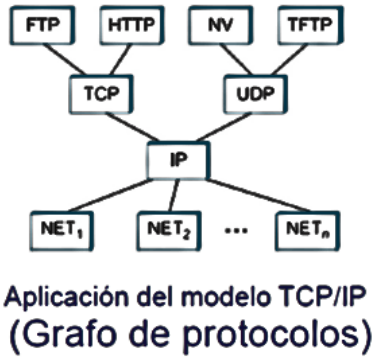
Arquitectura de la red: es el conjunto de topologías mas las funciones que realizan cada equipo.

- Funciones: las funciones que realiza un equipo para comunicarse con otro se gestiona mediante protocolos.
- Protocolo: es un mecanismo para hacer que dos equipos funcionen entre sí (para que se "entiendan").
- Torre de protocolos: es un conjunto de protocolos jerarquizados necesarios para realizar una función o dar un servicio. Cada protocolo se abstrae del nivel anterior y da servicio al protocolo superior.



Para estandarizar estos modelos existen dos típicos, el OSI y el TCP/IP





Aplicación del modelo TCP/IP
(Grafo de protocolos)

Tenemos que distinguir dos tipos de comunicación:

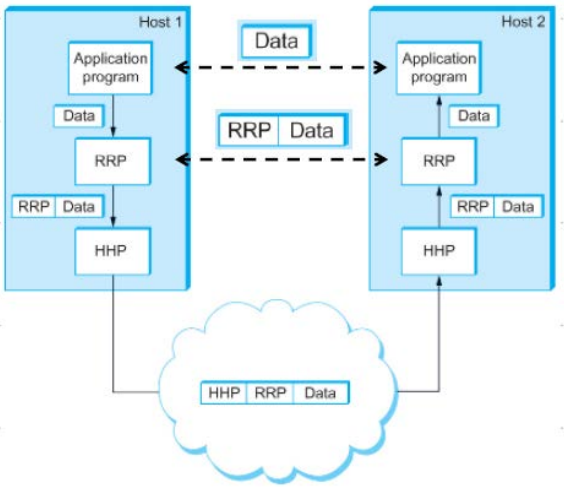
- Comunicación física: la que se hace mediante hardware y cable.
- Comunicación virtual: la existente entre protocolos, los protocolos de cada host se entienden con los respectivos del otro host.

Si atendemos a la siguiente figura:

La aplicación de un programa genera unos datos que quiere enviar a un host 2.

Pasa por un protocolo RRP que le pone una cabecera a los datos, para que el RRP del host 2 lo entienda.

Seguidamente pasa por un protocolo HHP el cual también le pone otra cabecera que entenderá el semejante del host 2.



Viaja por la red hasta que llega a su destino, en el cual, pasa por el protocolo HHP, lo "entiende", pasa por el protocolo RR, lo entiende, y finalmente el dato es transmitido a la otra máquina.

Prestaciones:

Fiabilidad de un sistema: pueden presentarse distintos tipos de errores como los siguientes:

- Errores de bit: cambiar 0 por 1 o viceversa.
- Errores de ráfaga: muchos bits alterados.
- Errores de paquete: cuando se pierden por cogestión (colas).
- Errores de enlace o nodo: tiempo medio entre fallos.
- Desorden o duplicación de los paquetes.

Se dice que una red es fiable si es capaz de resolver ese tipo de problemas.

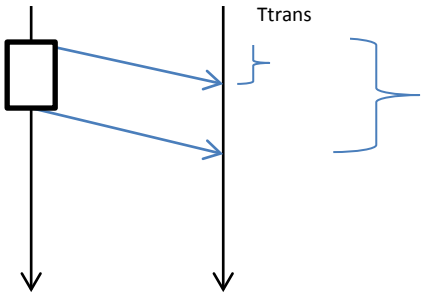
Ancho de banda (bandwidth): en esta asignatura entendemos el ancho de banda como el número de bits que pueden transmitirse en un segundo. El ancho de bit, es el tiempo que dura un bit.

Retardo (delay): retardo, es el tiempo total que tarda en llegar la información de un sitio a otro. En general, $R = T_{procesamiento} + T_{transmisión} + T_{propagación} + T_{colas}$

Pueden definirse además:

Tiempo de propagación: $\frac{distancia}{velocidad\ de\ la\ luz\ en\ el\ medio}$

Tiempo de transmisión: $\frac{tamaño\ del\ paquete}{ancho\ de\ banda}$



RTT (Round trip time): Es el tiempo que se emplea en ida y vuelta. Los protocolos son sensibles al RTT, si es muy grande el protocolo puede no funcionar.

Capacidad del tubo: Es el producto del retardo por el ancho de banda.

Jitter: Variación del retardo (cómo varía el retardo a lo largo de una transmisión). No todos los paquetes tienen el mismo retardo, entre otras cosas debido al camino que siga, colas… etc.

Caudal: $\frac{tamaño\ de\ la\ transferencia}{Tiempo\ de\ transferencia\ /bps)}$

Tiempo de transferencia = $RTT + \frac{Tamaño}{Ancho\ de\ banda}$.

De cara a los ejercicios a realizar en esta parte, resaltamos lo siguiente:

Variaciones sin repetición: todas las maneras de elegir m elementos de entre los n posibles de manera que los conjuntos elegidos son distintos

$$\frac{n!}{(n-m)!}$$

Variaciones con repetición: todas las maneras de elegir n elementos tomados de m en m sin tener en cuenta la repetición.

$$\boldsymbol{n^m}$$

Combinaciones sin repetición: combinaciones de n elementos tomados de me en m (todas las maneras disponibles de de elegir m elementos de entre los n disponibles).

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!}$$

Combinaciones con repetición: combinaciones de n elementos tomados de me en m (todas las maneras disponibles de de elegir m elementos de entre los n disponibles).sin importar que se repitan

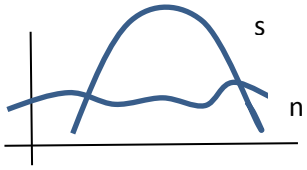
$$\binom{n+m-1}{m} = \frac{(n+m-1)!}{m!\,(n-1)!}$$

TEMA 2: ACCESO A LA RED (I)

Enlaces punto a punto:

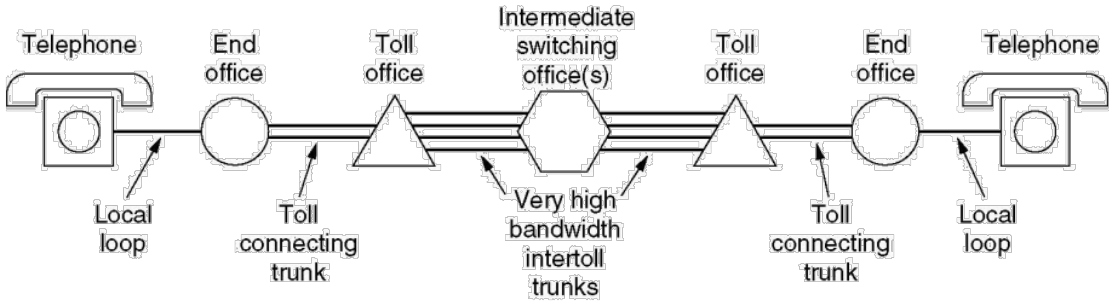
Si definimos el ancho de banda (B), y la relación señal/ruido (S/N), podemos encontrar la capacidad máxima que tiene un canal según el **límite de Shannon**:

$$C = B\ log_2(1 + {}^{S}/_{N})$$



Acceso a la red telefónica (PSTN)

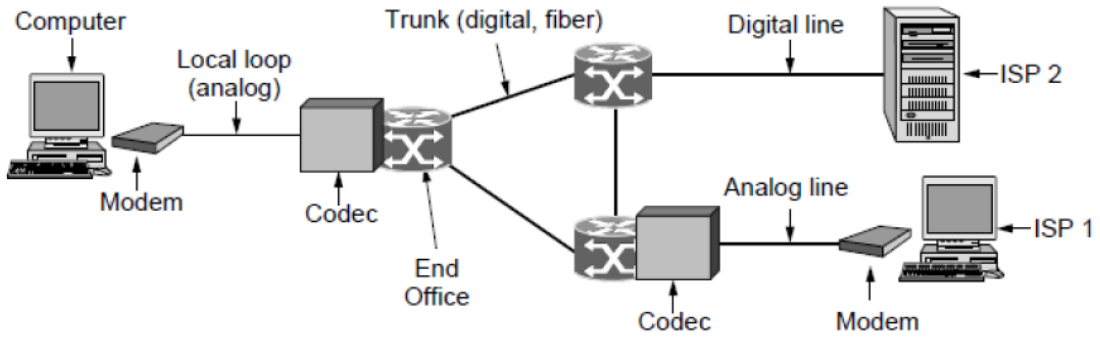
La red telefónica está compuesta de una serie de equipos y elementos interconectados.



El usuario se conecta mediante el bucle de abonado (local loop) a una central local (end office), ésta está conectada mediante un enlace troncal a una central de nivel superior (toll office) que permite llamadas de larga distancia.

Naturalmente las se pueden conectar varias end office, y toll office formando una gran red de niveles superiores de comunicación.

La información viaja de la siguiente manera:



La información analógica que sale del ordenador viaja por la red de manera digital, gracias a la conversión que hacen los códec en ella.

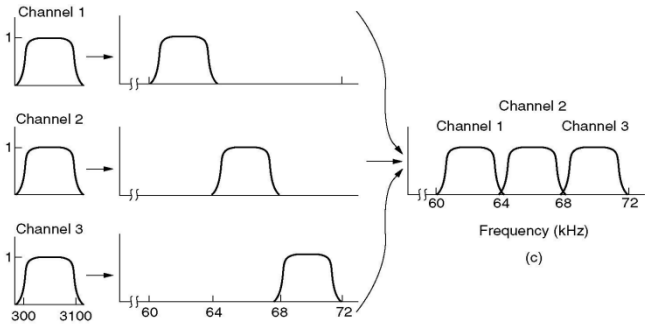
Multiplexación:

El método de Multiplexación consiste en unir varios caminos diferentes y juntarlos en uno solo.

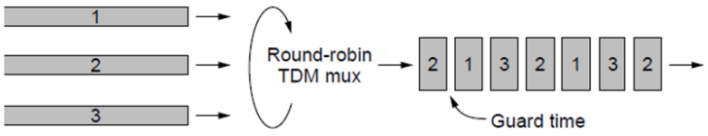
Es un reparto estático, ya que a cada enlace le reserva una parte de enlace común, y centralizado.

Existen diversos tipos de Multiplexación (FDM, TDM…)

- Multiplexación por frecuencia (FDM): consiste en juntar distintas bandas de frecuencia en un único canal con un ancho de banda suficientemente amplio para albergarlas a todas

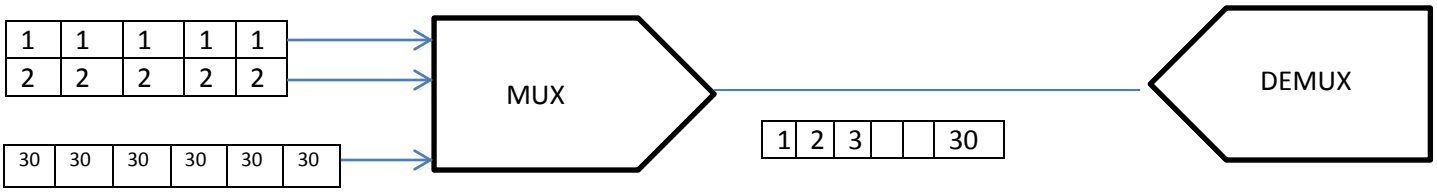


- Multiplexación por división de tiempos(TDM):consiste en en mezclar varios canales (troceados) y enviarlos todos por un mismo canal. Se respeta el orden de los canales y la velocidad a la que están siendo enviados.



Norma E1: (para canales de 64Kb)

Explicación paso a paso:



64Kbps

Tenemos 30 canales de abonados que llegan a un multiplexor, a una velocidad de 64Kbps.

La información que llega de cada canal la dividimos en paquetes de 8 bits (slots), de tal manera que por el canal se transmiten los slots mezclados por orden.

Un slot (de 8 bits) tarda en transmitirse $\frac{8}{64Kbps} = 125\mu s$ es decir, que deben transmitirse por el canal común a esa misma velocidad.

En principio, para que todo fuese a la velocidad debida sin pérdidas de información, errores… la velocidad del canal debiera ser 30 x 64Kbps.

Definimos la **trama** como el conjunto de slots de los canales así como de señalización y control de canal. Una trama está formada por los primeros slots de cada canal, otra por los segundos y así sucesivamente formando una comunicación por multitrama.

Ahora bien, es necesario señalizar los comienzos de trama para que el demultiplexor sepa cuando llega y el que.

Para ello se añade un slot al comienzo de la trama. (La trama ya tiene 31 slots)

Así mismo se va a añadir un slot adicional para señalización de canal en la posición 16 con la siguiente estructura:

C1	C7

De manera que cada 15 tramas serán señalizados todos los canales. El primero de estos slots (en la primera trama) contiene información de sincronismo para la multitrama.

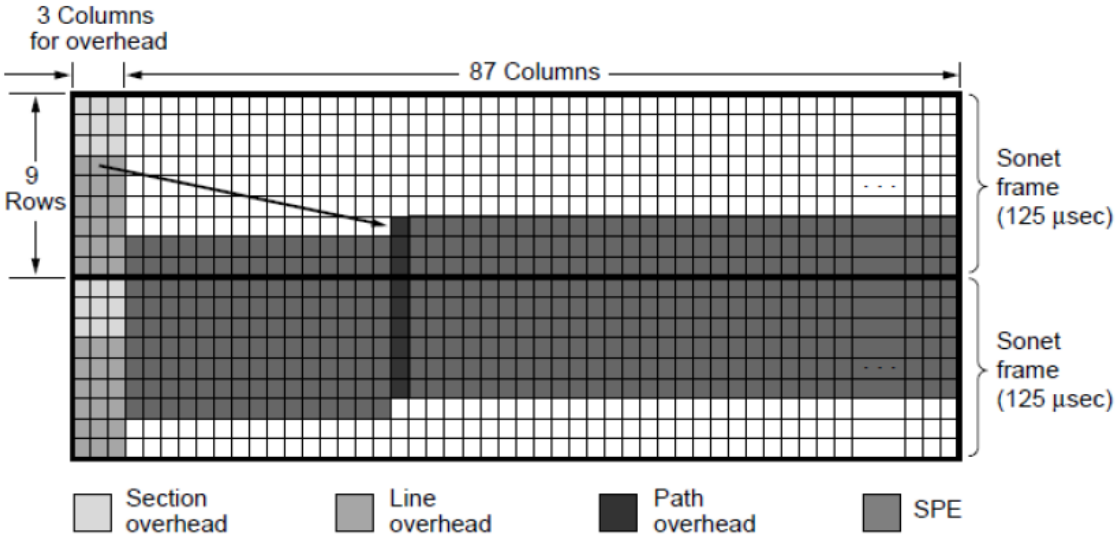
De manera que la trama queda de la siguiente manera:

0	1	2		16		30

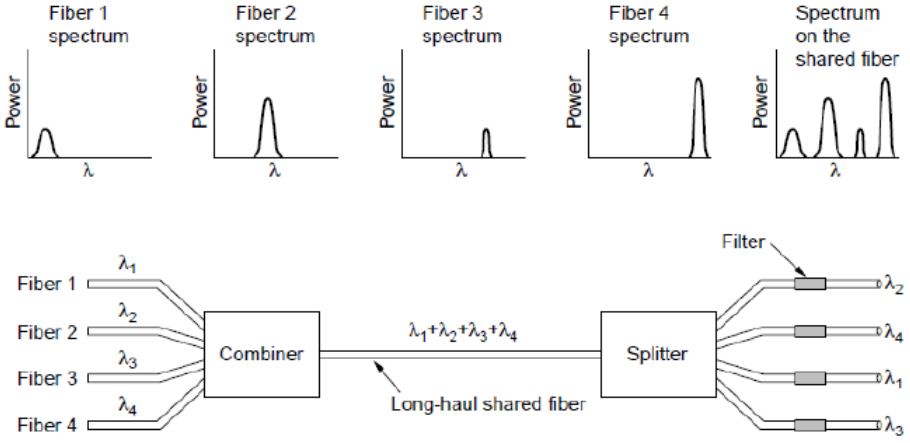
Y la velocidad del canal debe ser **32 x 64Kbps**.=**2048Kbps**

Existe otros tipo de multiplexación:

- SONET/SDH o multiplexación síncrona: utilizan una trama de 90 bytes en cada celda, y un total de 9 celdas. (no entramos mucho en detalle, dejamos el esquema de la trama)



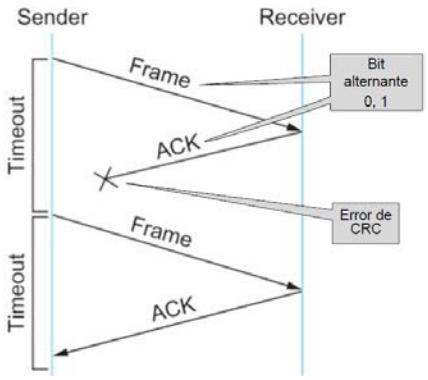
- Multiplexación por longitud de onda: similar a la de frecuencia en el ámbito de la fibra óptica pero que se detalla de la siguiente manera:



Transmisión fiable y eficiente:

Durante la transmisión de un mensaje, ya sea una trama o un paquete, pueden producirse errores de tal manera que pueda perderse información o corromperse el paquete en cuestión.

Para resolver este problema se utiliza el protocolo de parada y espera: en el cual, se envía un paquete al destino. Si tras un tiempo determinado no se recibe el ACK de asentimiento, se renvía el mismo paquete.



Cuando se reciba el ACK pertinente el emisor enviará el siguiente paquete y así sucesivamente hasta realizar el envío completo.

Este protocolo funciona a su vez con el bit alternante, CRC… y demás sistemas para evitar errores en los ACK.

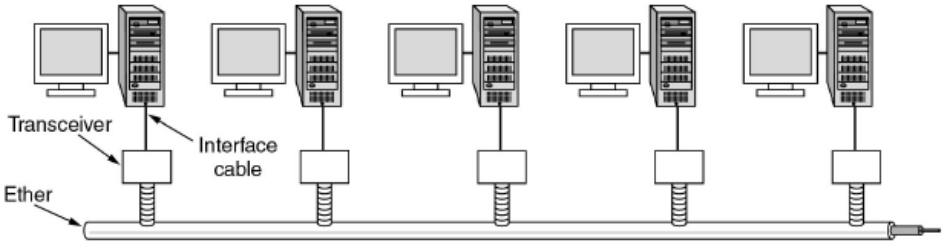
Así mismo, para que la emisión sea eficiente los paquetes debieran usar todo el canal de tal manera que enviase constantemente paquetes hasta que se recibe el 1º ACK del primer mensaje.

Una vez recibido se procede a enviar el segundo mensaje utilizando todo el canal para enviar paquetes.

ETHERNET BÁSICA, WIFI Y REDES CELULARES:

ETHERNET BÄSICA:

Una red Ethernet consiste en mantener conectados al mismo medio distintos sistemas. (típicamente cable). Tal y como vemos en la figura:



Es en el medio donde se da el dominio de colisión donde no puede confluir la información de 2 hosts distintos a la vez.

En el caso de que colisionen, se detecta y se retransmite tras un tiempo aleatorio.

Todos los hosts tienen una única dirección MAC, que se representa como el conjunto de 6 bytes de una forma como esta: 00:35:F3:03:14:47

Por el medio viaja la información con información Ethernet que todos los hosts entienden.

La dirección Ethernet tiene la siguiente estructura:

Preámbulo, (64 bits)	Dirección de destino (48bits)	Dirección de emisor (48 bits)	Tipo del paquete (16 bits)	CUERPO del paquete (46 bits)	CRC:código de errores. (32 bits)

Cuando un host se comunica con otro host, funciona mediante paquetes Ethernet, pero existe la posibilidad de que un host hable con todos los que están conectados mediante la utilización de una dirección reservada FF: FF: FF: FF: FF: FF

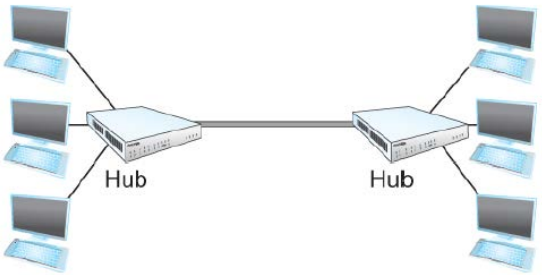
El protocolo **CSDA**

"Acceso múltiple con escucha de portadoras y detección de colisiones".

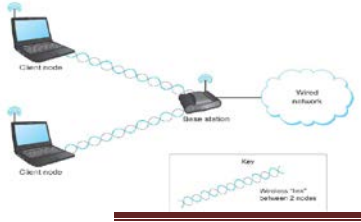
Es el protocolo que funciona para la buena comunicación (sin colisiones) de los host en la red Ethernet, y funciona de la siguiente manera:

- Escucha si hay alguien enviando por el canal. Hay ocasiones en las que no se escucha nada pero si que se está utilizando el canal.
- Tras un tiempo de t=2d los usuarios averiguan que se ha dado lugar a una colisión.
- Se retransmite de manera aleatoria.

La red Ethernet evolucionó y se utilizan unos "hubs" o repetidores, los cuales se encargan de difundir todo lo que le llega, por todos sus puertos.



WIFI: la estructura WIFI se compone básicamente de los siguientes elementos:

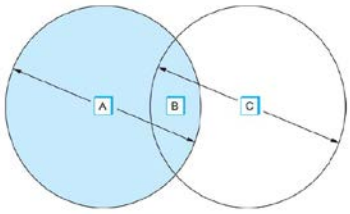


Donde vemos que está formado por ordenadores o clientes, conectados de manera inalámbrica a una estación base que es la encargada de conectarlos a internet.

En este tipo de infraestructura cuyo medio es radio, no es homogéneo ni estable, y adquiere gran importancia los mensajes de asentimiento, ACK.

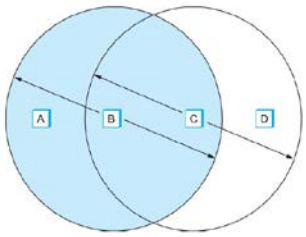
En este tipo de redes nos encontramos con una serie de problemas a tener en cuenta:

- El problema del nodo oculto: si nos fijamos en la imagen, podemos observar que tenemos tres emisores con sus radios de alcance.



Vemos que C no escucha la señal de A, por tanto puede pensar que la red esta libre, (no escucha nada) pero si que puede haber tráfico.
B por su parte, escucha a C y a A y no habrá problemas para transmitir cuando le toque.
Por tanto, si A y C deciden transmitir a la vez (mutuamente no se escuchan) habrá colisiones en la transmisión.

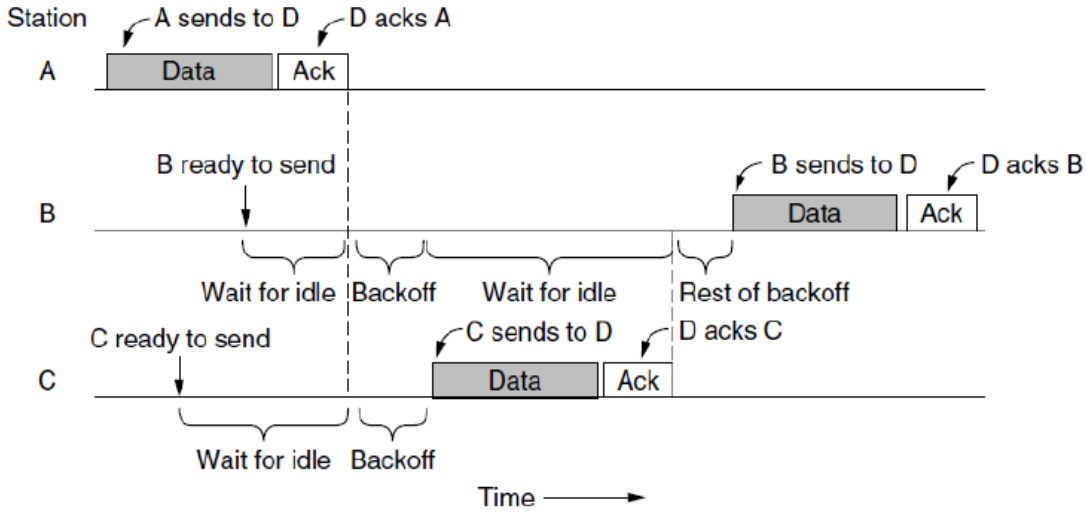
- El problema del nodo expuesto: ahora vemos como son 4 los que emiten señal.



si se da el caso en que B se comunica con A, C que está escuchando señal piensa que no puede comunicarse con D a pesar de que sí puede.

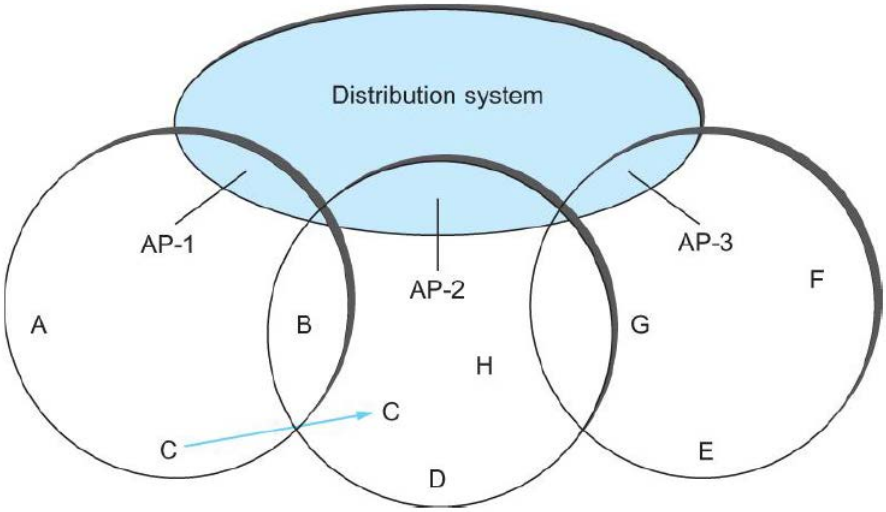
Es un error, no puede efectivamente comunicarse con A o B pero sí con D.

El protocolo para WIFI es el CSMA-CA y funciona de la siguiente manera:



"wait for idle" es esperar durante un tiempo aleatorio, y "back off" es el tiempo de espera desde que se ha enviado a un paquete hasta que otro nodo pueda transmitir.
Este sistema es ineficiente para el problema del nodo oculto.

WIFI extendida, distribución y movilidad:



Dado el siguiente mapa de situación, vemos como hay varios Access Point (AP), que conectan los host a internet.

Existen dos métodos para conectarse a un AP:

- Método activo: el host A manda un paquete de prueba (probe) y si el AP lo envía bien, le llegará un ACK y se conectará a ese AP
- Método pasivo: los AP envían un paquete baliza que leen todos los host, y el host en función de cómo lo reciba y con qué potencia de señal, decidirá conectarse a ese AP o a otro.
- Movilidad: se A se mueve, en algún momento perderá señal, el host reescanea de nuevo y se engancha a otro AP.
  Entre los AP existe una comunicación para ver que clientes están conectados o desconectados entre ellos.

Sistemas móviles Celulares:

Generaciones:

- 1º Generación: voz analógica.
- 2º Generación: GSM voz digital
- 3º Generación: 3G-UMTS voz digital y datos.
- 3,5 ,4 ..Generación: voz digital y datos a alta velocidad (con OFDM)

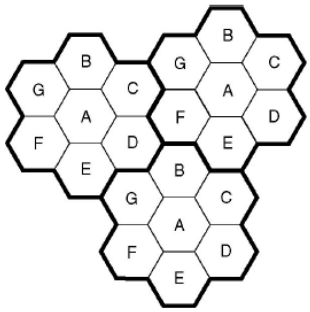
Sistema celular:

En un principio se planteó la disposición de una antena a la que se conectaban los teléfonos dentro de un radio de acción bastante grande.

Esto suponía que para que el móvil estuviese en contacto con la antena, tenía que utilizar mucha potencia lo cual era perjudicial incluso para la salud. Así mismo, el sistema sólo tendría para todos los móviles conectados **n** canales dúplex para establecer las llamadas.

Para resolver este problema se propuso un sistema basado en celdas, de tal manera, que estuviesen organizadas en un número finito de éstas (cluster), con un radio menor de actuación que disminuía la necesidad de potencia de los terminales, y la reutilización de los canales para cada cluster.

Vemos en la siguiente imagen como se disponen.



con esta organización, si el operador dispone de 100 canales, ya puede dar servicio a esos 100 canales en cada cluster, puesto que no se interfieren.

Se define entonces el $factor\ de\ reutilización = \frac{Portadoras\ en\ el\ sistema}{Portadoras\ en\ cada\ celda}$

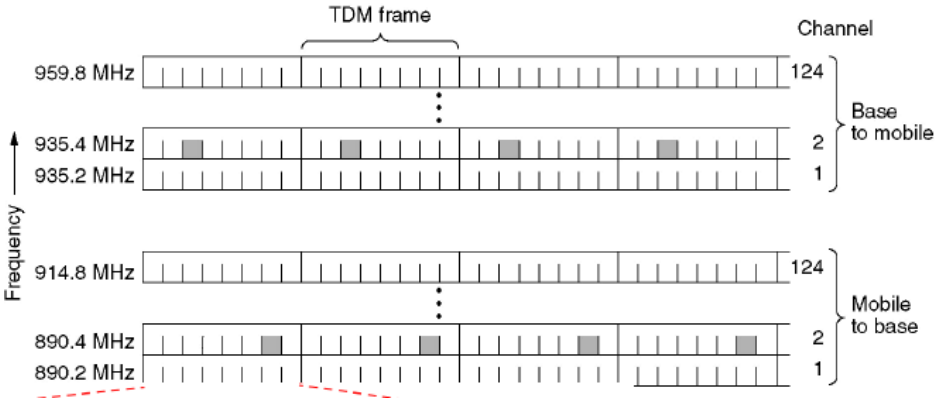
Que incluye además un sistema de movilidad (hand off, hand over) que permite al usuario pasar de una celda a otra de manera transparente y sin necesidad de cortar la conversación.

Los canales pueden ser de 4 tipos:

- Control: (base-móvil) gestionan el sistema
- Anuncios: (base-móvil) llamadas entrantes
- Acceso: (bidireccionales)
- Datos: (bidireccionales)

GSM:

Este sistema permite transmitir muchas conversaciones a la vez de la siguiente manera:



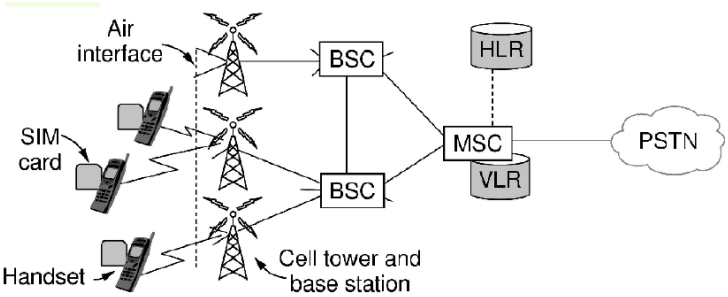
A cada portadora se le da una estructura en el tiempo de tramas de 4,6 ms de duración. Dentro de una trama caben 8 slots. Durante la conversación, la portadora utiliza el mismo slot.

A esto se le llama canal, es decir, cada slot de la trama es una conversación, un canal de voz.

En los slots hay 114 bits de información por lo que hay una velocidad de 114/4,6 ms = 24,7Kbps. Pero como hay que protegerlo, se reduce a una velocidad de 13Kbps.

En la misma frecuencia (canal) hablan hasta 8 móviles a la vez, por lo que se alcanza una gran eficiencia en el sistema.

Vemos como es la arquitectura GSM



donde BSC es la base de datos de control.

MSC es un conmutador de llamadas.

VLR son las bases de visitantes del sistema.

ACCESO DIGITAL EN REDES DE ABONADOS:

xDSL, tiene distintas variantes, como por ejemplo ADSL

ADSL: (asymmetrical digital suscriber line) se trata de un protocolo a nivel físico de transmisión de datos bidireccional asimétrico por los pares de cobre telefónico.

Es asimétrico porque la velocidad de bajada y subida son distintas.

Tiene muchas ventajas como por ejemplo:

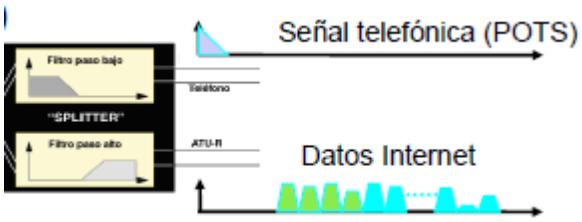
- Reutiliza la infraestructura, por lo que necesita una baja inversión y se despliega rápidamente.
- Llega prácticamente a donde llegue el teléfono.
- Puede utilizarse conjuntamente con el servicio telefónico.
- Podemos estar siempre conectados a una velocidad asimétrica relativamente alta.

El inconveniente es que pierde calidad conforme el abonado se aleja de la central.

El escenario típico es el siguiente:

Vemos como el proovedor mediante el enlace telefónico hace llegar internet a casa.

En casa un repartidor (splitter) se encarga de separar las frecuencias de voz de las frecuencias de datos de la siguiente manera:



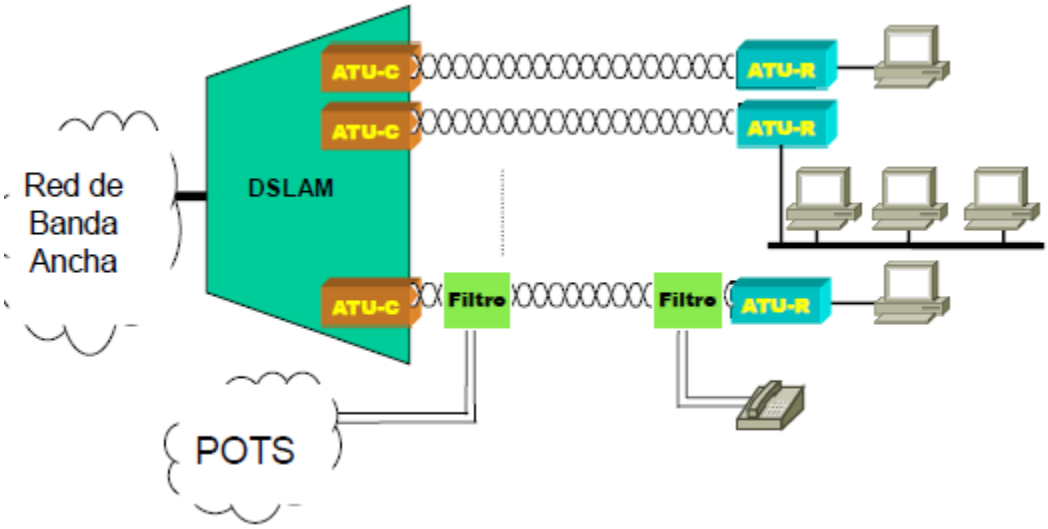
el filtro paso bajo separa la señal telefónica, y el filtro paso alto separa la señal de datos.

Existirá tantos splitter en casa, como teléfonos haya con el fin de no interferir voz con datos.

ATU (ADSL Terminal Unit) procesa las señales digitales que para enviarlas por el bucle de abonado. Puede ser ATU-R (remoto) o ATU-C (central).

POTS significa Plane Old Telephone System.

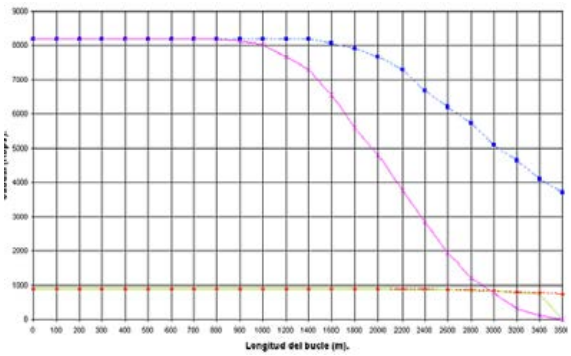
Estructura:



Un proovedor de servicios se sirve de una DSLAM (Digital Suscriber Line Acces Multiplexer) para llegar a todos sus abonados.

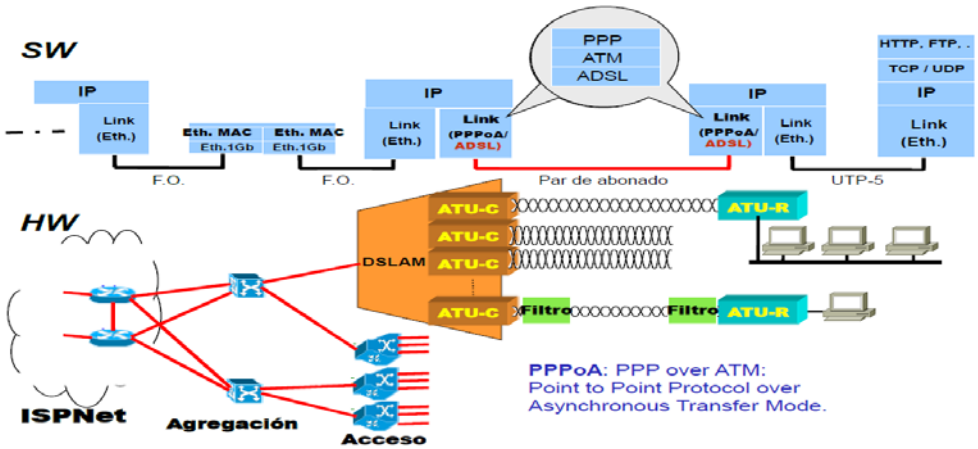
Las ATU-C son unos moduladores/desmoduladores que tratan a nivel físico con el abonado. Por tanto, en la DSLAM habrá tantos ATU-C como abonados existan.

Naturalmente, como ya hemos mencionado antes conforme más lejos esté el abonado de la central, peor será la calidad con la que le llegue el servicio, entre otras cosas por:



- Distancia
- Diámetro del cable
- Diafonías e interferencias.
- Derivaciones sin terminar…

La arquitectura de la red XDSL viene detallada desde el punto de vista del software y del hardware en la siguiente imagen.



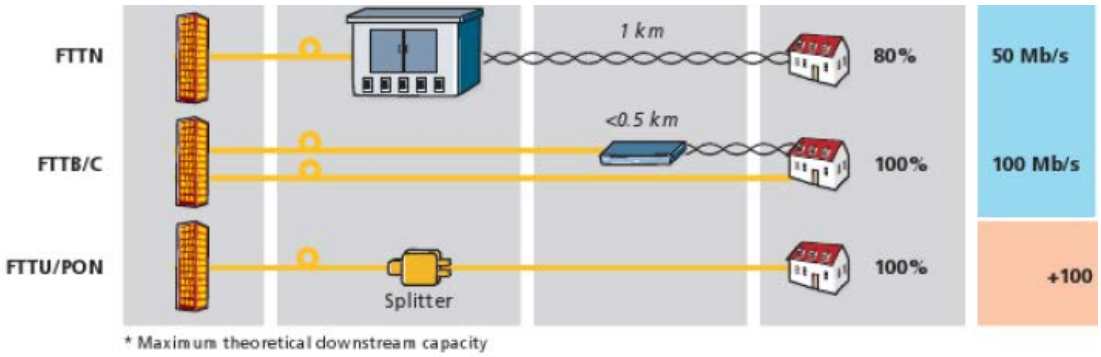
Vemos que se utilizan dos protocolos a nivel de software para la comunicación por XDSL.

- PPT: Point to Point Protocol, se encarga de la señalización de comienzo y fin de paquete. Incorpora un sistema de detección de errores.
- ATM: Asynchronous Transfer Mode está orientado a conexión no fiable. Fragmenta las PDU´s en paquetes de 53 bytes que se transmiten físicamente por el ADSL.

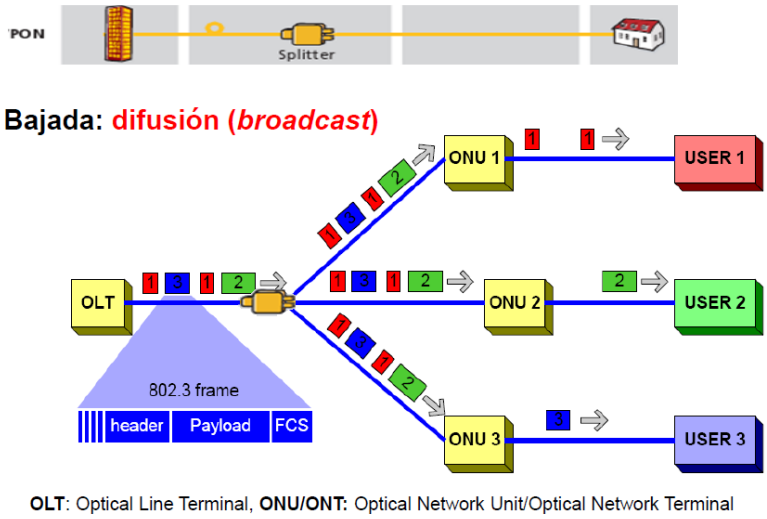
XPON: se trata de redes que utilizan fibra óptica para encaminar los servicios. Existen entre otros dos tipos:

- GPON: Gygabit Pon.
- GEPON: Gygabit Ethernet Pon

Podemos ver un gráfico de los diferentes tipos de Xpon, así como su velocidad dependiendo de si mezcla o no cable.



La red típica de una Xpon es la que sigue: en el caso de bajada



OLT: Optical Line Terminal, **ONU/ONT:** Optical Network Unit/Optical Network Terminal

OLT: Optical Line Terminal

Se envían tramas tipo Ethernet por un único hilo de fibra, el cual llega a un Splitter óptico que es distinto al del ADSL.

Este splitter actúa como repetidor, es decir envía a todos los abonados toda la información.

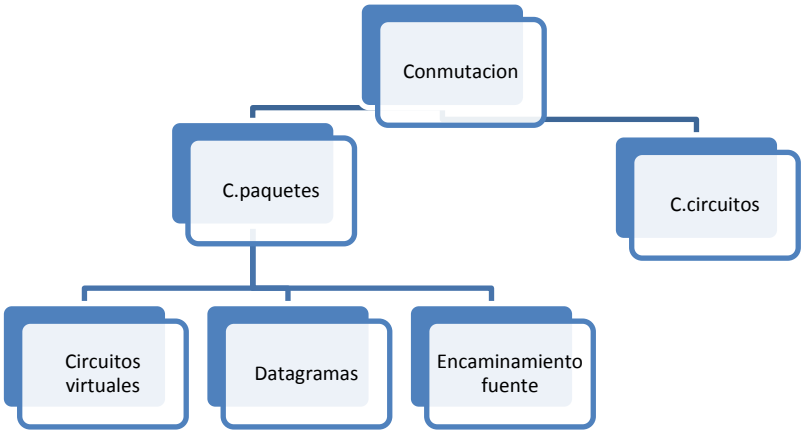
La ONU (Optical Network Unit) propiedad de cada abonado se encarga de recoger la información que le pertenece y rechazar la que no es para él.

Se utiliza la multiplexación por intervalos de tiempo (TDMA) para llevar acabo el proceso.

En el caso de subida, actúa exactamente igual pero en sentido contrario, el splitter recoge la información de todos y la encamina hacia el OLT.

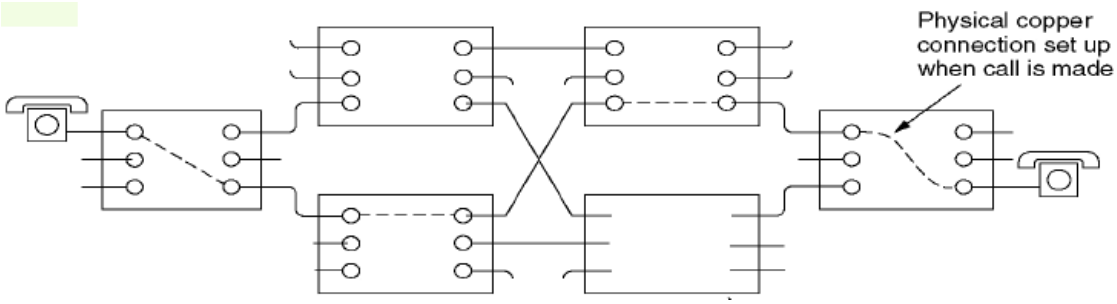
TEMA 3: Conmutación en redes de datos:

Vemos un pequeño esquema de los tipos de conmutación que vamos a ver:



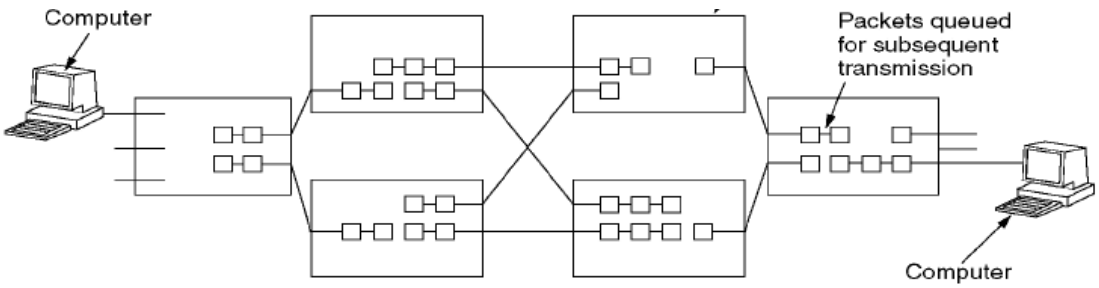
Comenzamos explicando la conmutación de circuitos:

La conmutación de circuitos se basa en una "unión física" extremo a extremo continua durante la comunicación.



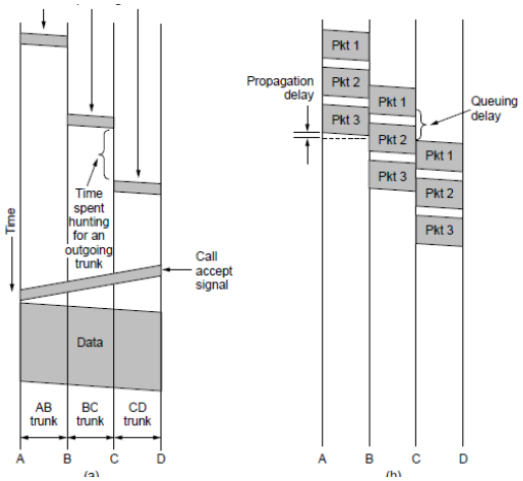
Este tipo de comunicación está ya en desuso y se utilizaba sobre todo para las centrales telefónicas antiguas.

La conmutación de paquetes se basa en una red formada por switches o conmutadores, que van dirigiendo los paquetes desde el origen hasta el final, por distintos caminos según la velocidad de los enlaces, los costes… el destino es quien se encarga de ordenarlos o pedirlos de nuevo si es que se han perdido.



Es el tipo de encaminamiento más usado hoy en día.

Para dejar clara la diferencia entre conmutación de circuitos y la conmutación de paquetes, esta imagen muestra como se comporta cada una en un cronograma de tiempos:



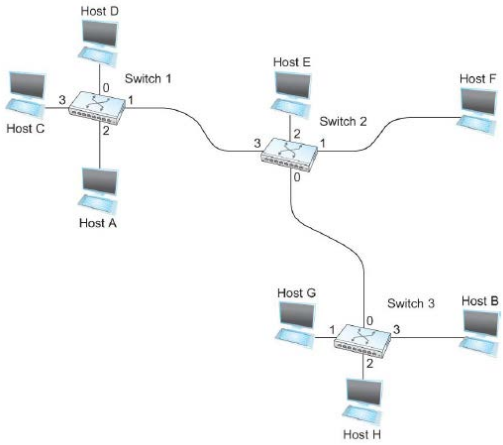
Vemos cómo en la conmutación de circuitos la conexión se mantiene constante mientras se está intercambiando información, (es el ejemplo de una conversación telefónica).

Por el contrario la conmutación de paquetes envía continuamente los paquetes por la red, que siguen diferentes caminos. Además éstos tienen unas protecciones contra errores para que la información no se pierda o llegue errónea al destinatario.

Conmutación de paquetes

Datagramas:

Si suponemos que tenemos una red dispuesta de la siguiente manera:



La red de datagramas consiste en que cada switch contiene una tabla de forwarding que sirve para encaminar los paquetes que le llegan por sus puertos de entrada, al destino por sus puertos de salida.

Las tablas tienen la siguiente estructura:

A dónde quiero ir	Por qué puerto debo ir

Con el ejemplo de la figura, la tabla de forwarding del switch 2 es:

A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0

Estas tablas se crean automáticamente mediante una serie de algoritmos, o bien el administrador de la red las crea de manera estática.

En una red de datagramas, cada paquete tiene una cabecera con la dirección de destino.

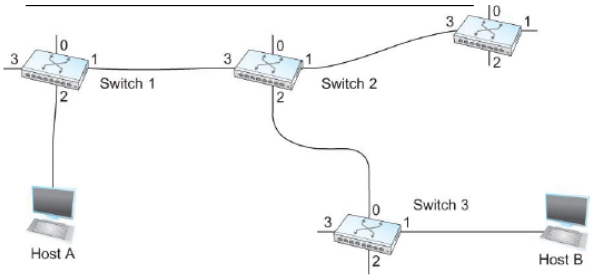
Existe una búsqueda para cada paquete. Y cada switch almacena la información de la posición de todos hosts de la red, lo que puede generar ineficiencias ya que las tablas pueden ser de dimensiones muy grandes.

Como solución a los problemas e ineficiencias de la conmutación de paquetes por datagramas, se creó la conmutación por:

Circuitos virtuales.

Adquiere este nombre porque se crea un circuito en base a la señalización de los paquetes.

Si tenemos una red con la siguiente estructura:



Cada switch tiene su tabla de forwarding pero que sólo usa para señalizar el origen y el destino, no interviene más en el proceso.

Las tablas que se manejan ahora tienen la siguiente estructura:

Lo que viene por el puerto	Con el número	Sale por el puerto	Con el número

De esta manera a cada paquete se le asigna un número y se crea una nueva tabla.

Los número de los circuitos son locales, es decir, sólo los distinguen los routers de cada enlace.

Es esta tabla no hay una búsqueda sino que hay una indexación, por lo que se hace muy rápidamente. Por ejemplo la tabla del switch 2 sería: (no están incluidos todos los caminos)

3	1	2	1
0	1	2	1
1	1	3	1
2	1	1	1

Hay que tener cuidado con no equivocarse a la hora de rellenar las tablas para no poner dos caminos iguales.

Por último vamos a ver el último tipo de conmutación que es el:

Encaminamiento fuente o (source routing).

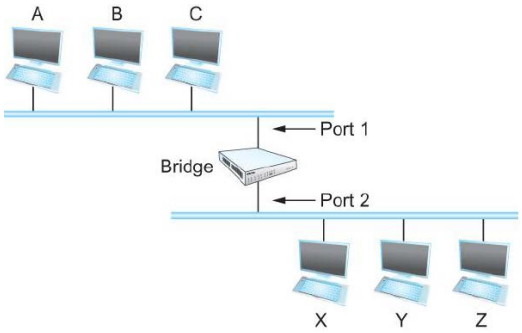
En este modo de conmutación, el paquete desde el origen, lleva toda la información acerca del encaminamiento que debe seguir hasta llegar a su destino.

Existen varios modos de llevar a cabo esta conmutación: (siendo la flecha el paso de un router a otro)

- Rotación: DCBA→ADCB→BADC→…
- Eliminación: DCBA→DCB→DC→…
- Puente: Ptr DCBA→ Ptr DCBA→ Ptr DCBA→..(donde Ptr es un “puente” que señala que información escoger en cada momento.

Conmutación en Ethernet (Switching):

El esquema típico es el siguiente:



El Bridge no es un repetidor, es un conmutador que entiende de tramas Ethernet y sus dominios de colisión.

En el switch existe una tabla de forwarding como la que sigue para nuestro ejemplo:

HOST	PUERTO
A	1
B	1
C	1
X	2
Y	2
Z	2

Esta tabla no se rellena manualmente, la autorrellena el propio switch, que inicialmente está vacía.

Si un paquete desde A quiere ir a B, manda un paquete tipo Ethernet (recordar trama).

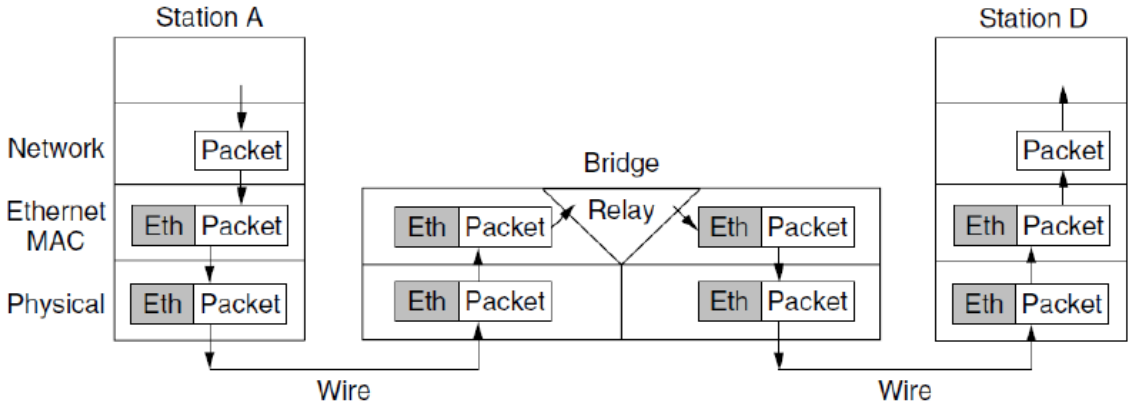
Como el switch inicialmente no sabe nada, difunde el paquete por todos los puertos. De esta manera, ya memoriza por que puerto se conecta A y la guarda en la tabla.

Se puede resumir la creación de la tabla en los siguientes pasos:

- No sabe nada, difunde por todos los puertos.
- Los hosts envían paquetes de tal manera que el switch aprende de las fuentes.
- Olvida si la tabla permanece inactiva y reaprende.

La pega de estas tablas es que a gran escala no son viables por su gran volumen de datos.

La estructura del Software del switch es la siguiente, como vemos, entiende de Ethernet.



Spanning Tree Protocol (STP)

Este protocolo sirve para resolver el problema que surge cuando es posible llegar al mismo sitio por distintos caminos formando bucles.

El protocolo crea un único camino, en forma de árbol (ramificado) de modo que no existen bucles. Para ello asigna un estado a los puertos de cada switch de modo que los inhabilita o deja abiertos con unas características que ahora veremos.

Para formar el árbol, los bridges/switches se envían BPDU's con la siguiente estructura:

Raíz	Coste	Bridge ID	Puerto ID

De tal manera que todos saben quien es el más pequeño y los costes entre enlaces.

Para determinar el estado de los puertos, hacemos los siguientes pasos:

- Escogeremos el puerto Raíz (ROOT) como el puerto con el ID más bajo (puede ser su MAC el número de bridge… lo que se use para identificarlos).
- Se toma un puerto designado para cada red.
    - el que menor coste tenga a la raíz y de ID más bajo.
    - es el que se encarga de copiar el tráfico de la red, a esa red.
- Para cada Puente se designa un puerto Raiz que es el que comunica con el camino más corto hasta el Root.
- Para cada Puente marcamos puertos designados, que son los que comunican con otras redes para las que son el puente designado.
- Los puertos que no sean raíz o designados, se bloquean, es decir, dejan de copiar tráfico en la red y así se rompen los bucles.

Tema 4.Internetworking (IP)

Introducción:

Definimos una inter-red como una colección de redes (pueden ser de distinto tipo) interconectadas para entregar un servicio de intercambio de datagramas entre sistemas finales.

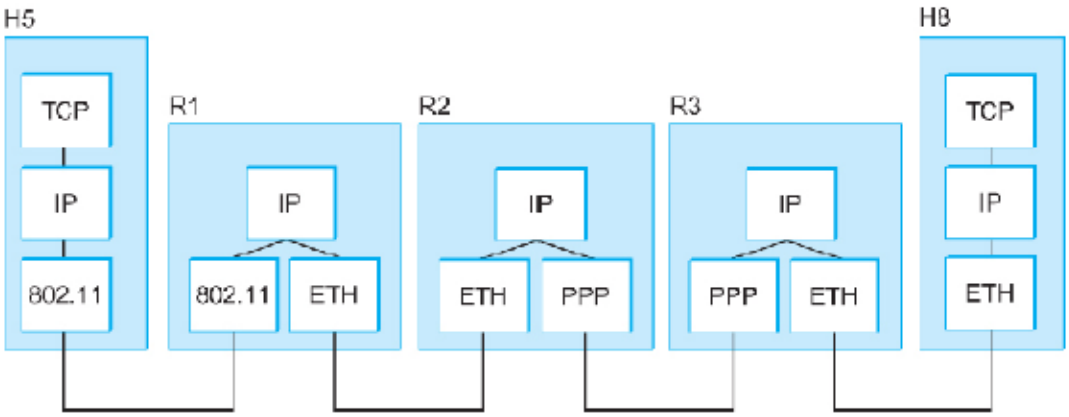
Cada red entiende sobre su propia topología, por ejemplo las redes tipo WIFI, “entienden” de WIFI, las de Ethernet, de Ethernet.

Lo que buscamos es un protocolo, que permita que las redes se puedan comunicar independientemente del tipo que sean. Un lenguaje universal.

Para ello nace el protocolo **IP**

IP es un protocolo nuclear que sirve para construir redes heterogéneas escalables que se ejecuta entre sistemas finales y routers.

Por ejemplo vemos la torre de protocolos que sigue un paquete a lo largo de todas las redes



Donde vemos que cada router entiende de la topología a la red que está conectado, pero sobre ello está el protocolo IP que los comunica entre sí.

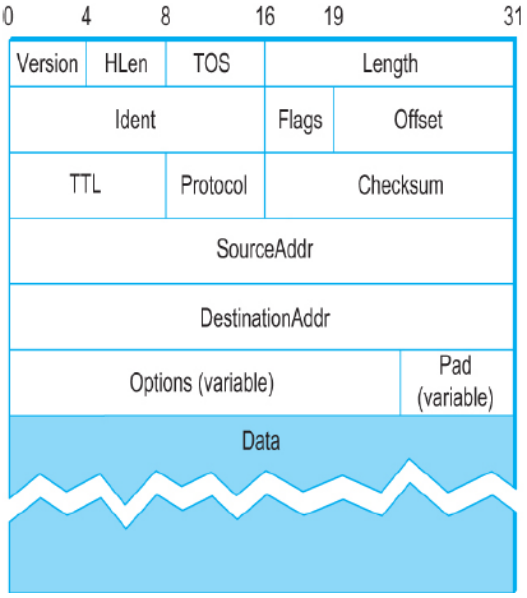
El modelo de servicio IP es un servicio de datagramas con las siguientes características:

- Envío de datos sin conexión
- Envío de datos al modo (best effort) que “intento que lleguen pero sino…”
    - La PDU puede perderse
    - La PDU puede desordarse
    - Pueden duplicarse o perderse los paquetes.

Se busca entonces un mecanismo de direccionamiento universal, global.

Formato PDU del protocolo IP

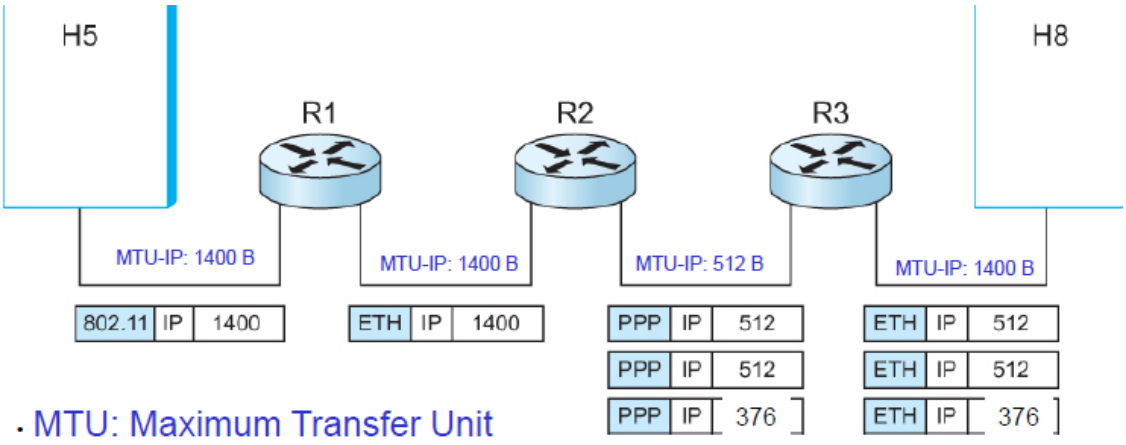
Ayudándonos del siguiente gráfico:



Vemos que son tramas de un total de 32 bytes, que se dividen en los siguientes apartados:
Versión: número de versión del protocolo.
HLEN: indica el número de palabras de 32 bits que forman la cabecera.
TOS: calidad del servicio (QoS).
Length: número de bytes total del datagrama.
Ident: información para fragmentar.
Flags: número del fragmento
Offset: de qué trozo del paquete se trata
TTL:time to live, contador de saltos
Protocol: indica qué protocolo de transferencia usa.
Checksum: es una suma de la cabecera, mira si se ha perdido algo(contra errores).
Source y Destination: información de destino y fuente.

Fragmentación y reensamblado:

Vemos un esquema en que podemos ver el proceso de cómo el paquete se va troceando a medida que avanza por la red:



En el primer paso no fragmente porque la SDU de Ethernet tiene más capacidad de la que le llega. Hay fragmentación cuando PDU>MTU.

En ese caso se dividen los fragmentos teniendo en cuenta las cabeceras en paquetes de tamaños enteros, cuya suma sea la MTU de ese router.

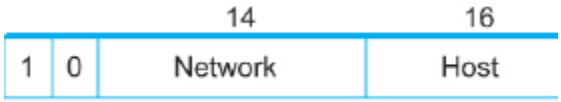
Si algún paquete se pierde por el camino, los tira todos. Ya los pedirá de nuevo.
Si llegamos a una red que tiene una MTU más pequeña que el fragmento, se juntan todos y se refragmenta de nuevo de acuerdo a la red.

Direccionamiento global:

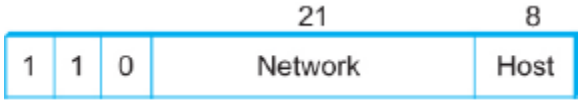
A cada red se le direccionan un número de máquinas, y cada red tiene un número de red, por ejemplo, 138.4.32.2
Las direcciones universales se corresponden con los siguientes tipos:

- Tipo A: (10.3.2.4) donde permite crear 128 redes de 16277126 host conectados a ella.

- Tipo B: (128.33.43.95) donde permite crear 16384 redes con 65535 host conectados.



- Tipo C: (192.12.68.77) que permite crear 2097152 redes con 256 host conectados.



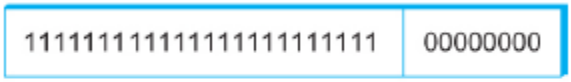
Como se puede ver, es un sistema de asignación muy rígido, si quisiera crear una red por ejemplo para conectar 500 maquinas, debería contratar una de tipo B que haría que perdiese recursos.

Por ello, para crear un sistema más dinámico, nace el concepto de subred.

De modo que ahora las direcciones se estructuran de la siguiente manera:

Donde se indica cuántos bits son para señalar el número de la red, y cuantos bits para señalar el número de hosts.

Un ejemplo de máscara de subred es:



Subnet mask (255.255.255.0)

Mask = número de bits de identificación de red
=> 2^{mask} redes de $2^{32-mask}$ SFs cada una.
Identificación de red =

Subnetted address

Vemos que dependiendo del número de bits que designemos para señalar las redes, tendremos más o menos bits para señalar el número de host conectados a ellas.

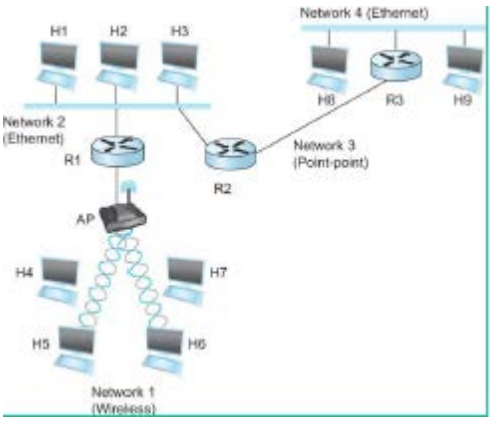
Todas las redes tienen su dirección IP, este concepto nace para crear subredes con números de hosts determinados dentro de esas redes.

Forwarding de los datagramas IP:

Los Routers IP tienen unas tablas de forwarding en las que almacenan los caminos para llegar a los sistemas finales, similar a la de conmutación de datagramas, con la siguiente estructura:

Dirección de red del destino	Siguiente paso para llegar a ella.

Por ejemplo, si tenemos la siguiente distribución:



La tabla de forwarding del router será

Dirección del destino	Siguiente paso
Red 1	Ir al router 1
Red 2	Interfaz 1
Red 3	Interfaz 2

Cada host, envía datagramas con la siguiente información:

- IP (160.5.1.8)
- Red (160.5.1.0)
- Mask (255.255.255.0)

En la tabla de forwarding de cada router, se busca si el destino final pertenece a esa subred.
En caso negativo, se mira la columna de siguiente paso y se envía por la red.

Este proceso va rellenando la tabla de forwarding automáticamente.

Existe un "default router" que se usa cuando no se conoce la dirección en las tablas de forwarding que típicamente es el router de salida de la red.

Traducción de direcciones (ARP):

Cuando necesitamos conocer la dirección MAC Ethernet de los host de la red, utilizamos el protocolo ARP que funciona de la siguiente manera:

- El host 1 hace ping al host 2 (obtiene direcciones IP).
- Difundo a toda la red a la que pertenece el host 2 la pregunta ¿quién es esta IP?
- El host 2 responde al host 1 dándole su MAC
- Finalmente se almacenan las IP con sus MAC.

DHCP: configuración automática de sistemas:

El DHCP server es el responsable en una red, de decir a cada host qué IP debe usar, cómo señalizarla, su máscara… con el fin de no crear conflictos.

Cada vez que un Host arranca, le pide la información al DHCP y éste le contesta con toda la información mencionada antes para su correcto funcionamiento.

Señalización de errores:

Para asegurarnos la fiabilidad del tráfico IP de la red, surge como también hemos visto en otras ocasiones un protocolo de errores. En este caso el protocolo ICMP.

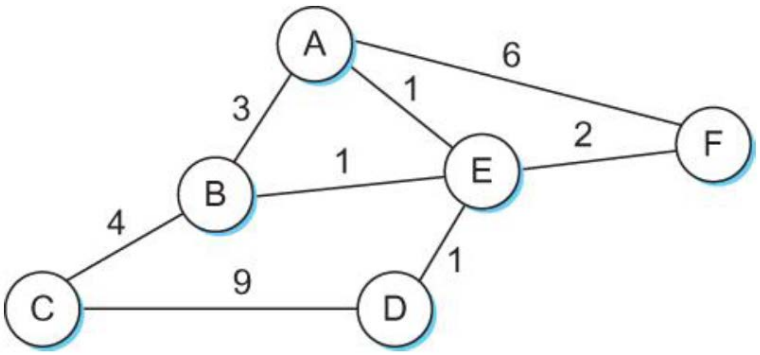
El ICMP(Internet Control Managment Protocol) define un conjunto de PDU's de señalización de nivel inter-red para manejar todas las operaciones en el tráfico de la red.

Sigue la siguiente estructura:

ICMP packet	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
IP Header (160 bits OR 20 Bytes)	Version/IHL	Type of service	Length	
	Identification		*flags and offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Payload (64+ bits OR 8+ Bytes)	Type of message	Code	Checksum	
	Quench			
	Data (*optional*)			

Tema 4.2. Encaminamiento:

Los encaminamientos dentro de una red se basan en las posibilidades de ir al destino final por distintos caminos, lo mas usual es que busquemos el camino óptimo. Para ver la estructura de una red, dibujamos lo que se llama grafo de red:



Donde vemos que está formado por nodos, ya sean routers, switch…

Por enlaces que son caminos entre nodos.

Y el concepto de costes, que se trata de una clasificación de la viabilidad de los caminos, dependiendo de diversos factores como pueden ser la velocidad, la carga del enlace, el tipo de enlace…

El objetivo del encaminamiento ha de ser encontrar el camino más óptimo, y debe ser:

- Correcto
- Simple (de algoritmo sencillo)
- Robusto
- Estable (no oscilante)
- Justo y óptimo (equitativo con todos los nodos)
- Adaptable a los cambio topológicos de la red

Principio del camino óptimo:

Si se conoce un camino óptimo por ejemplo, A→C→F→B→H…

Sabemos pues que cualquier camino dentro de él es el óptimo, es decir, si quisiera ir de F a H, debiera pasar por B.

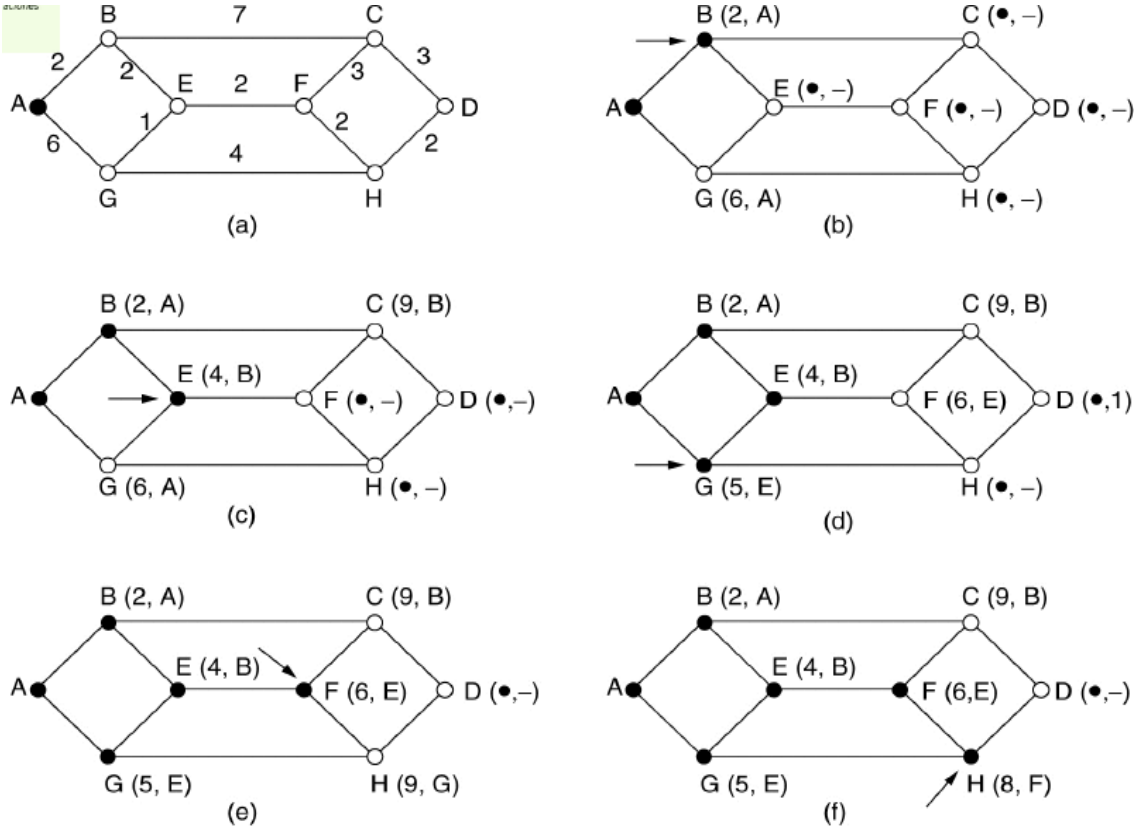
Algoritmo del camino más corto (Dijkstra):

Partimos del grafo de la red con el conocimiento de los nodos, los enlaces y los costes.

El algoritmo es el siguiente:

- Definimos un nodo confirmado que será "permanente" y conocemos que es el más óptimo. (En la práctica será el origen del camino que nos piden buscar).
- Actualizamos los nodos adyacentes al confirmado la siguiente información (coste hasta llegar aquí, desde el nodo) ejemplo: B(2,A)
- De los adyacentes, hacemos permanentes el de menor coste hasta el origen.
- Repetimos el paso 2 hasta llegar al origen.
- ¿He hecho el destino permanente? Si es que si, he obtenido el camino más corto, sino, vuelvo a empezar.

Vemos un esquema de cómo funciona el algoritmo paso a paso:



Para buscar el camino más corto también puede usarse lo que se conoce como inundación.

Flooding (inundación):

El proceso de este procedimiento es el siguiente:

- Como no sabe nada, envía información a todos los caminos.
- Hasta que encuentra el camino óptimo.

Encuentra el camino óptimo si o si, puesto que los recorre todos, el problema que existe es la generación de bucles, pero se pueden controlar de la siguiente manera:

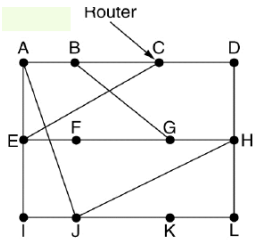
- Limitando el número de saltos (TTL) no elimina el bucle pero si que los delimita
- Hacer una memoria de los paquetes que ya han pasado por el nodo. Se le asigna un número de secuencia, y si el nodo detecta que ya ha pasado previamente por ahí, se lo carga. Este procedimiento sí que elimina los bucles.

Vemos que estos procedimientos para hallar el camino más corto son muy estáticos y no son adaptables a un cambio repentino de la topología de la red.

Para ello existen unos tipos de encaminamientos dinámicos:

Distance Vector (DV):

Dada una disposición como la siguiente:



El proceso es el siguiente:

- Un nodo lo primero que hace es conocer a sus vecinos y sus distancias hacia ellos. De modo que por ejemplo, J tendría una tabla inicial como esta:

destino	siguiente paso	la mejor distancia conocida
A	A	8
B	-	-
C	-	-
D	-	-
E	-	-
F	-	-
G	-	-
H	H	12
I	I	10
J	J	0
K	K	6
L	-	0

- Se produce un intercambio entre él y sus vecinos de la tabla de distance vector . Provocando que la tabla inicial de J evolucione con la información de cada uno de ellos.
  Por ejemplo, dada la tabla de distance vector de A vemos como evoluciona la de J

destino	siguiente paso	la mejor distancia conocida
A	A	8
B	A	12+8
C	A	25+8
D	A	40+8
E	A	22
F	A	31
G	A	18+8
H	H	12 (no lo toco)
I	I	10 no lo toco)
J	J	0 no lo toco)
K	K	6 no lo toco)
L	-	37

Sucesivamente intercambiándola con todos los vecinos obtendríamos una tabla de distance vector final de J como:

destino	siguiente paso	la mejor distancia conocida
A	A	8
B	A	20
C	I	28
D	H	20
E	I	17
F	I	30
G	H	18
H	H	12 (no lo toco)
I	I	10 no lo toco)
J	J	0 no lo toco)
K	K	6 no lo toco)
L	K	15

Los problemas que tiene este sistema son que:

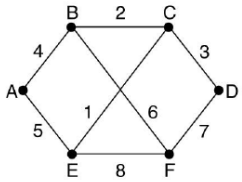
- Puede tardar mucho en converger a la tabla final
- Si el nodo origen se quita, la cuenta de costes aumenta de forma engañosa hasta infinito.

Estado de los enlaces (link state)

El procedimiento es el siguiente:

- Conocer los vecinos y sus costes
- Construir un LSP (Link State Packet)
- Enviar un LSP a todos los routers (Flooding) conociendo así la topología de la red.
- Calcular el camino más corto (Dijkstra).

Vemos una imagen de cómo son los LSP según una red determinada:



A		Link: B		State: C		D		Packets: E		F	
Seq.		Seq.		Seq.		Seq.		Seq.		Seq.	
Age		Age		Age		Age		Age		Age	
B	4	A	4	B	2	C	3	A	5	B	6
E	5	C	2	D	3	F	7	C	1	D	7
		F	6	E	1			F	8	E	8

La distribución de estos paquetes se hace con la siguiente estructura:

			Send flags			ACK flags			
Source	Seq.	Age	A	C	F	A	C	F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Donde Send flags es el apartado para decir a quien enviar, y ACK Flags el apartado para ver quien tiene que responder.