Escuela Técnica
Superior de Ingeniería

Universidad de Huelva

Departamento de Ing. Electrónica,
Sistemas Informáticos y Automática

TERCER CURSO. REDES DE COMPUTADORES

TEMA 1
Fundamentos de comunicaciones y redes de datos

ÍNDICE

BIBLIOGRAFÍA:

Apuntes de Redes de Comunicaciones. Universidad de Oviedo.

Stallings, W.; "Comunicaciones y Redes de Computadores". 6ª Edición; Prentice-Hall; 2000 (681.324 STA com).

CCNA 1 (Cisco)

1.- Introducción.

Las últimas décadas han estado protagonizadas por la tecnología de la información, es decir, todos los aspectos relacionados con la recolección, procesamiento y distribución de la información. Estas áreas han ido convergiendo, y las fronteras entre captura, transporte, almacenamiento y procesamiento de la información, son cada vez más tenues. El crecimiento de la demanda de estos servicios es exponencial. A medida que aumenta la capacidad para recoger, procesar y distribuir la información, las exigencias de procesamientos más sofisticados crecen con mayor rapidez. El resultado de esta evolución ha sido la aparición de *redes de ordenadores* como una solución más barata, fiable y flexible para muchas situaciones prácticas, y a la vez ha abierto la puerta a nuevas aplicaciones.

En este escenario donde múltiples tecnologías hardware y software se combinan para formar redes de equipos interconectados, resulta imprescindible encontrar un marco de referencia sobre el que situar cada uno de los elementos responsables en el proceso de la comunicación. Este marco nos permitirá construir una base de conocimientos ordenada sobre los sistemas de comunicaciones, que es el enfoque principal de este capítulo.

2.- Conceptos de comunicaciones.

Desde un punto de vista de las comunicaciones, podríamos hacer las siguientes definiciones:

- **Señal**: Es una codificación eléctrica o electromagnética de información.
- **Señalización**: Es el acto de propagar la señal a través de un medio adecuado.
- **Transmisión**: Se define como la comunicación de los datos mediante la propagación y el procesamiento de señales.
- **Redes de computadores**: Se denomina así al conjunto de ordenadores que se comunican entre sí mediante una red de comunicaciones.

Un sistema de transmisión de datos está formado por una fuente de los datos, generalmente un computador que extrae esos datos del usuario a través de un teclado o de disco y un transmisor que es el encargado de adecuar la información al sistema de transmisión empleado, realizando para ello la generación de la señal que se va a transmitir. Dicha señal se propaga por un sistema de transmisión que tiene como finalidad hacer llegar una señal legible de un punto a otro separados geográficamente.

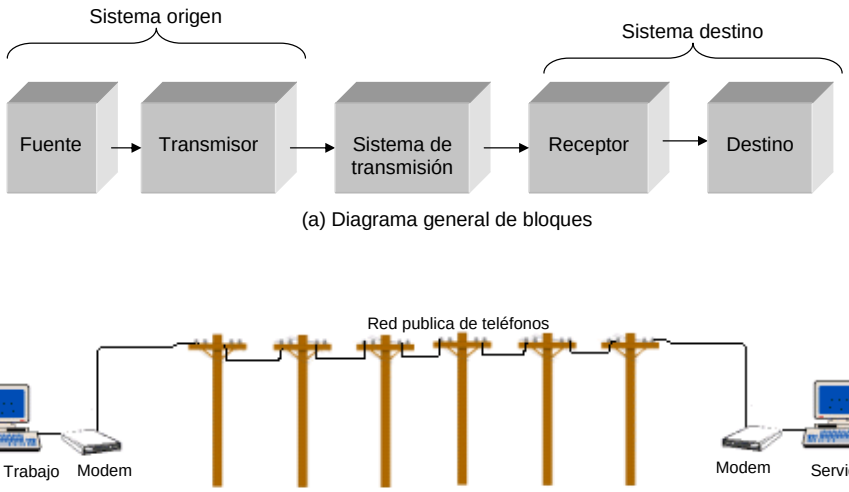


Fig. 1: Esquema genérico de un proceso de comunicación

El receptor realiza el proceso inverso, extrayendo del medio o sistema de transmisión la señal distorsionada o degradada previsiblemente proveniente del transmisor y convirtiéndola mediante tareas de decisión en datos digitales. Estos datos digitales se deben interpretar en el Destino, por el receptor final del mensaje, que puede ser el usuario a través de un terminal de datos o un sistema de almacenaje en disco.

Dado que normalmente la comunicación es bidireccional, el equipo que hace de transmisor también tiene las funciones de receptor y viceversa. A dicho dispositivo se le suele denominar "**DCE**" o Equipo de Comunicación de Datos. Ejemplos típicos de DCE es una tarjeta de red Ethernet o Wifi, o un modem ADSL.

Tanto al equipo fuente como al de destino se les suele denominar "**DTE**" o Equipo Terminal de Datos, que es la parte del hardware destinada a emitir o recibir información. En este caso sería un PC, un teléfono, un televisor, etc.

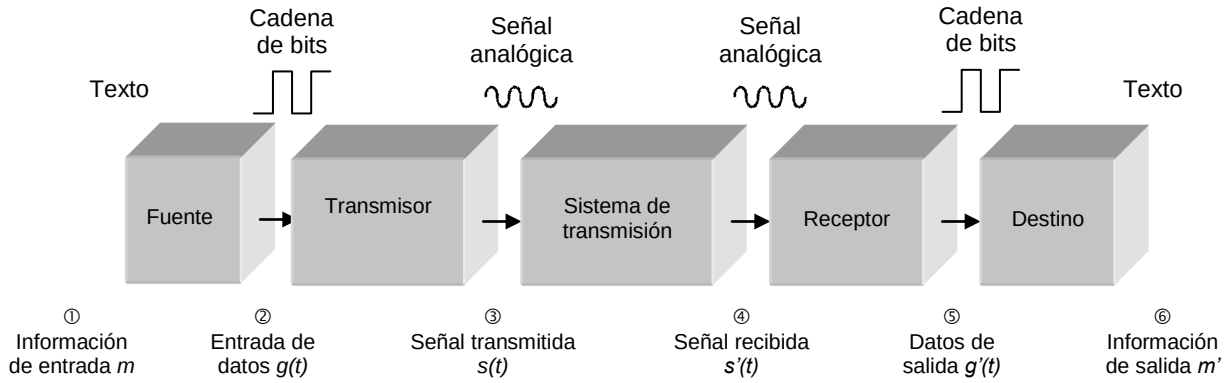


Fig. 2: Señalización en un proceso de comunicación.

2.1- Componentes Hardware de una red.

En cuanto al sistema de transmisión puede estar preparado para propagar señales analógicas, como es el caso de la red de telefonía tradicional, o bien señales digitales como en el caso de las redes de dato actuales. Las redes tradicionales de telefonía estaban compuestas por cables de cobre: par trenzado en la línea que llegaba al usuario final, y cable coaxial para unir los equipos de comunicaciones. Dichos equipos consistían en:

-**Centralitas** (también llamadas PBX): Equipos destinados a conmutar circuitos entre el cliente y el destinatario de la llamada. Si la llamada era local la conmutación conectaba directamente a los dos usuarios implicados. Si no era local, la comunicación se derivaba por un enlace troncal a conmutadores de mayor jerarquía.

-**Conmutadores o switches**: Equipos que conmutaban canales de múltiples circuitos (comunicaciones de varios barrios, o de toda una provincia). Se pueden asimilar a centralitas de mucha mayor capacidad, donde los caudales de tráfico eran mucho mayores.

-**Multiplexores**: Equipos capaces de agregar varios circuitos o canales en una única señal de comunicación que usaba un único cable o medio de transmisión. También realiza el proceso inverso.

-**Amplificadores**: Equipos que aumentan la potencia de la señal. A medida que la señal atraviesa un medio de transmisión pierde energía debido a que ésta es absorbida por el medio o dispersada mediante irradiación. Por tanto precisa ser amplificada cada cierto número de tramos (distancia). A estos equipos, combinados usualmente con los dos siguientes, se les llama también **repetidores** de señal.

-**Ecualizadores**: Equipos destinados a corregir la "no linealidad" o distorsión que causan los amplificadores.

-**Filtros**: Equipos que seleccionan ciertos componentes de una señal con respecto a otros en función de su frecuencia.

Los sistemas de transmisión digital usan señales digitales, es decir, señales que se decodifican directamente en una secuencia de ceros y unos. Aquí los medios de transmisión son muy variados (cobre, fibra óptica, infrarrojos, inalámbricos…). Los equipos típicos de este tipo de redes son:

-**Hub** o concentrador o repetidor: Son equipos que repiten la señal digital que les llega por una boca (puerto de acceso) hacia todas las demás bocas.

-**Switch** o conmutador: Cuando les llega un mensaje a una de sus bocas, averiguan en el mismo cuál es el destinatario y, en función de ello, seleccionan la boca por la que han de retransmitirlo. Sólo pueden hacer esto entre equipos que están físicamente conectados al switch.

-**Router** o enrutador o encaminador: También reenvían mensajes hacia sus destinatarios, como el switch. La diferencia es que en este caso los equipos origen y destino de los mensajes no tienen

necesariamente que estar conectados físicamente al router, sino que pueden estar en redes muy lejanas.

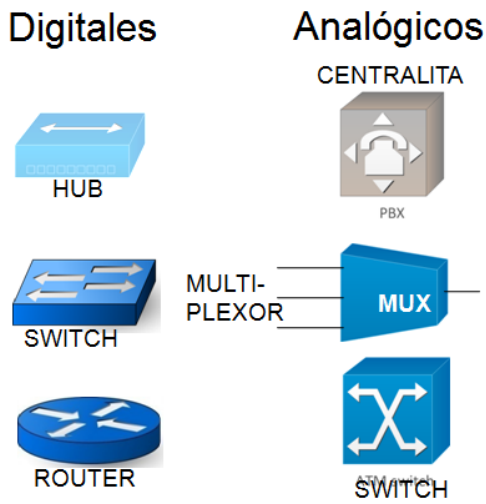


Fig. 3: Simbología de equipos de comunicación

2.2- Componentes Software de una red.

Un DTE puede ser un teléfono, una impresora, un ordenador… El caso del ordenador sería el más genérico desde el punto de vista del software, por tanto consideremos dos ordenadores conectados entre sí por un hub (fig. 4). Dentro de cada ordenador hay una serie de elementos software que interactúan entre sí para poder realizar el proceso de la comunicación.

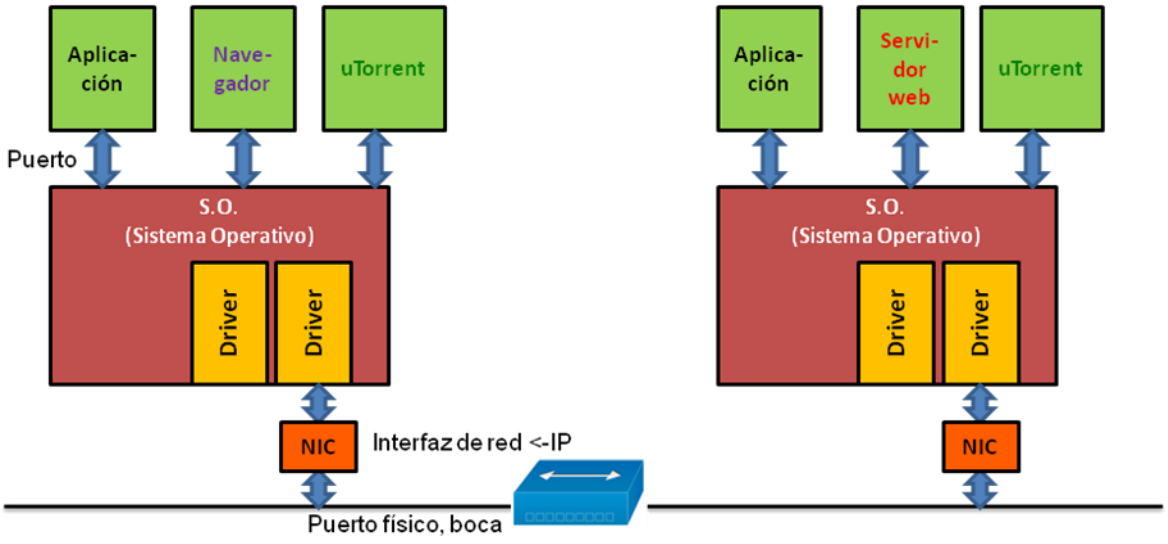


Fig. 4: Elementos software del proceso de comunicación

Un ordenador mantiene en ejecución un sistema operativo. Dicho sistema operativo gestiona el hardware del ordenador a través de unas librerías de código específicas para dicho hardware denominadas drivers o controladores. Las tarjetas de red o NICs (Network Interface Cards) son uno de esos elementos de hardware. Por tanto, cada vez que el sistema operativo necesita usar una NIC para transmitir información ha de pasar necesariamente por esos drivers. Por otro lado el usuario

utiliza aplicaciones que están instaladas sobre ese sistema operativo, como por ejemplo el navegador web, el correo electrónico, aplicaciones de descarga de archivos tipo torrent, etc.

Cuando un usuario solicita una página web, la aplicación navegador construye un mensaje con dicha solicitud y lo pasa al sistema operativo. Éste identifica la comunicación con esa aplicación con un número, denominado puerto, incorpora datos al mensaje y llama a una función del driver. El driver convierte el mensaje en una secuencia de ceros y unos que la NIC transmite por el medio físico que en este caso sería el cable de red. El hub retransmite el mensaje hasta el otro ordenador, donde tendría lugar el proceso inverso.

2.3- Esquema típico de una red.

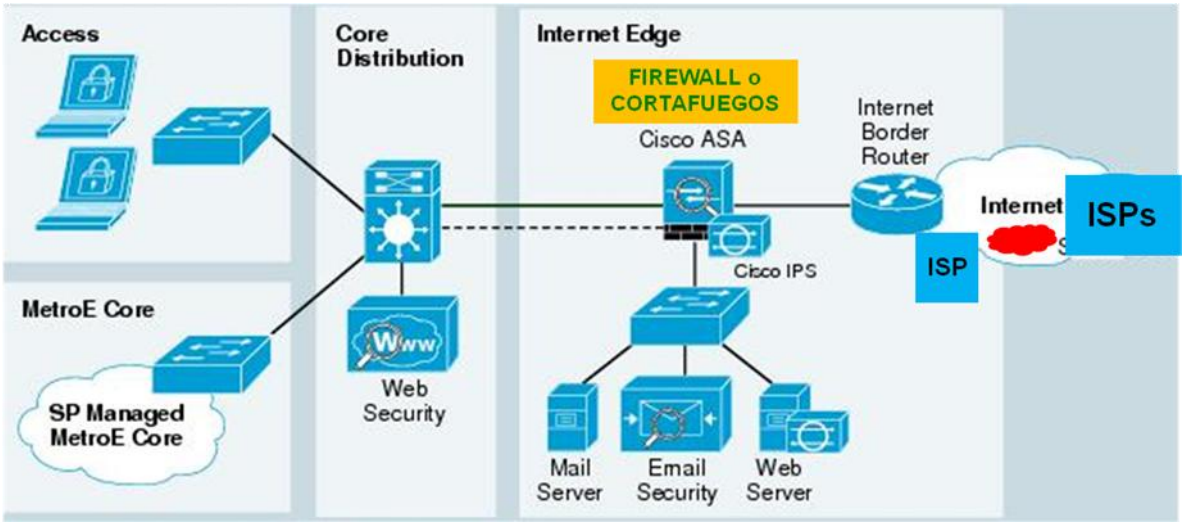


Fig. 5: Esquema de la red típica de una empresa

La red usual de una empresa comienza con la conexión a través de uno o varios routers a la compañía de telecomunicaciones o **ISP** (Internet Service Provider) que le ofrece acceso a internet. A partir de aquí la red de la empresa o **intranet** (red privada gestionada por una misma entidad) puede ser más o menos grande. En el caso más general se dividirá en tres partes: borde, distribución y acceso. En la parte de borde o frontera es donde se disponen los equipos de seguridad (**firewalls** o cortafuegos) que filtran los mensajes maliciosos. La parte de distribución consiste una serie de switches o routers de altas prestaciones que se ramifican más o menos profusamente según el tamaño de la red, siguiendo una estructura de árbol. La parte de acceso son switches de menor capacidad destinados a la conexión de los ordenadores o servidores.

Mediante este esquema los equipos de la intranet pueden conectarse a cualquier otro equipo en internet y viceversa. En este sentido hay un conjunto de equipos dentro de internet con los que las empresas deben tener diferente consideración a nivel de seguridad: los equipos de proveedores, colaboradores y clientes. A este conjunto de equipos concreto se le denomina **extranet**.

En la figura 6 podemos observar un ejemplo concreto de comunicación. En un ordenador de la intranet un usuario abre la aplicación Chrome (navegador web) para consultar las noticias. Teclea el nombre del sitio que desea visitar y pulsa enter. A continuación el navegador envía la petición al sistema operativo, en este caso Windows, que le asigna un número de puerto a dicha aplicación. El sistema operativo selecciona la NIC por la que transmitir, que tiene también un número único asignado denominado IP. Esta información es añadida al mensaje y pasa a los drivers que controlan

la NIC. Ésta realiza la señalización eléctrica por un cable de cobre que está conectado a un switch. El switch, que tiene múltiples entradas o bocas, también denominadas puertos, conmuta internamente para que la señal se remita por la boca que mira hacia su destino, en este caso un router. El router hace algo similar a lo que hace el switch, pero en lugar de hacerlo a nivel hardware como el switch, éste opera a nivel software, como lo haría un ordenador. Es decir, tiene un sistema operativo y un microprocesador general que ejecuta programas. Esto lo hace más lento pero más flexible y funcional que el switch. El router decide por dónde reenviar el mensaje atendiendo a un conocimiento amplio de la red. El siguiente nodo en el camino puede ser otro router, o un switch o un hub. En cualquier caso el mensaje es señalizado según el medio que tenga que atravesar en cada caso (cable UTP, fibra óptica, vía inalámbrica…). Finalmente el mensaje llega a su destino. La NIC destinataria pasa el mensaje al sistema operativo, en este caso Linux. Éste reconoce la aplicación de destino gracias al número de puerto y se lo entrega. La aplicación es un servidor Apache que reconoce la petición y responde enviando la página web completa.

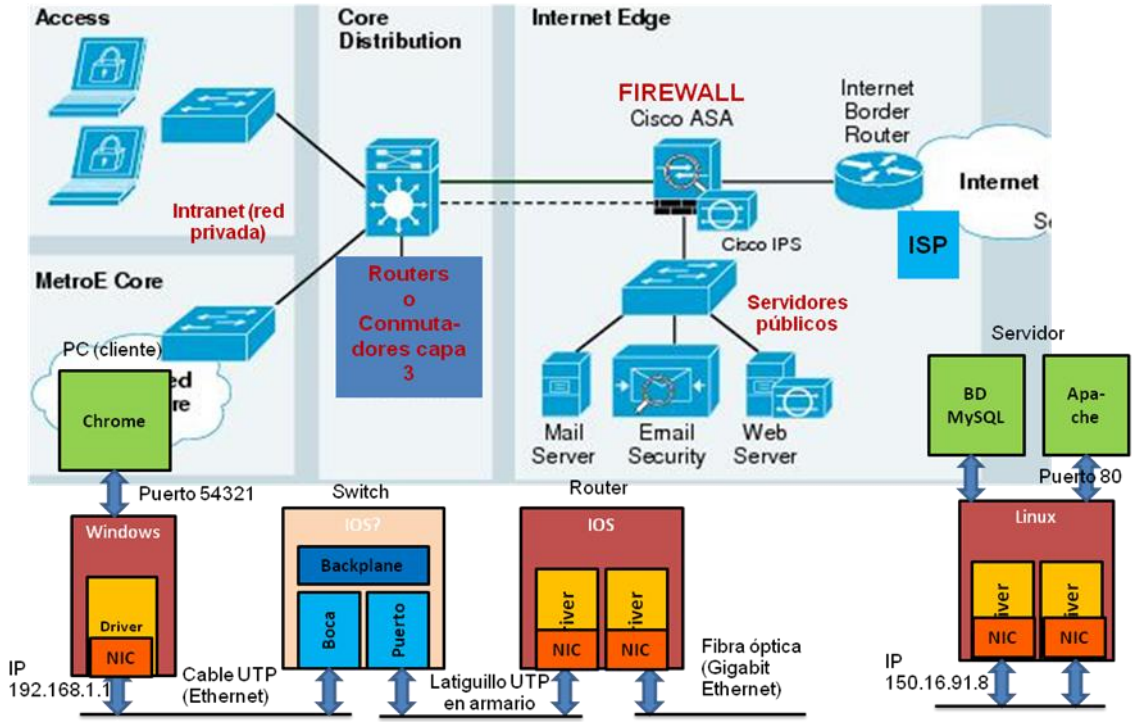


Fig. 6: Ejemplo de comunicación desde la intranet a un servidor externo

Para que el sistema funcione, el servidor debe estar permanentemente encendido y a la escucha de posibles mensajes, con el puerto asignado por el sistema operativo establecido, y además, debe ser un puerto conocido por el equipo que hace la solicitud. Esta solución se denomina "**Cliente-Servidor**", donde el equipo o la aplicación que solicita la comunicación se denomina **cliente**, y el equipo o el software que está continuamente conectado y a la espera se denomina **servidor**. En esta disposición el servidor no puede conectar con el cliente a menos que éste lo llame. Esta solución es la más extendida, y ejemplo de ello son los servicios web, de correo electrónico, descarga de ficheros, juegos, servicios en nube, etc.

Otra solución diferente consiste en que todos los equipos hacen de servidor y cliente a la vez. De este modo todos pueden contactar con cualquiera en cualquier momento. A esta solución se la denomina descentralizada o **P2P** (Peer-to-Peer) o comunicación entre iguales. Ejemplo de este enfoque serían

las aplicaciones para compartir archivos (torrent, Kademlia, eDonkey), los blockchains (bitcoin, ethereum, etc.), ciertos juegos, etc.

3.- Tipos de Redes.

3.1- Según su topología.

Los elementos que conforma una red pueden conectarse de diferentes formas. La figura 7 muestra diferentes estructuras que suelen aparecer según como se conecten físicamente los nodos de la red.

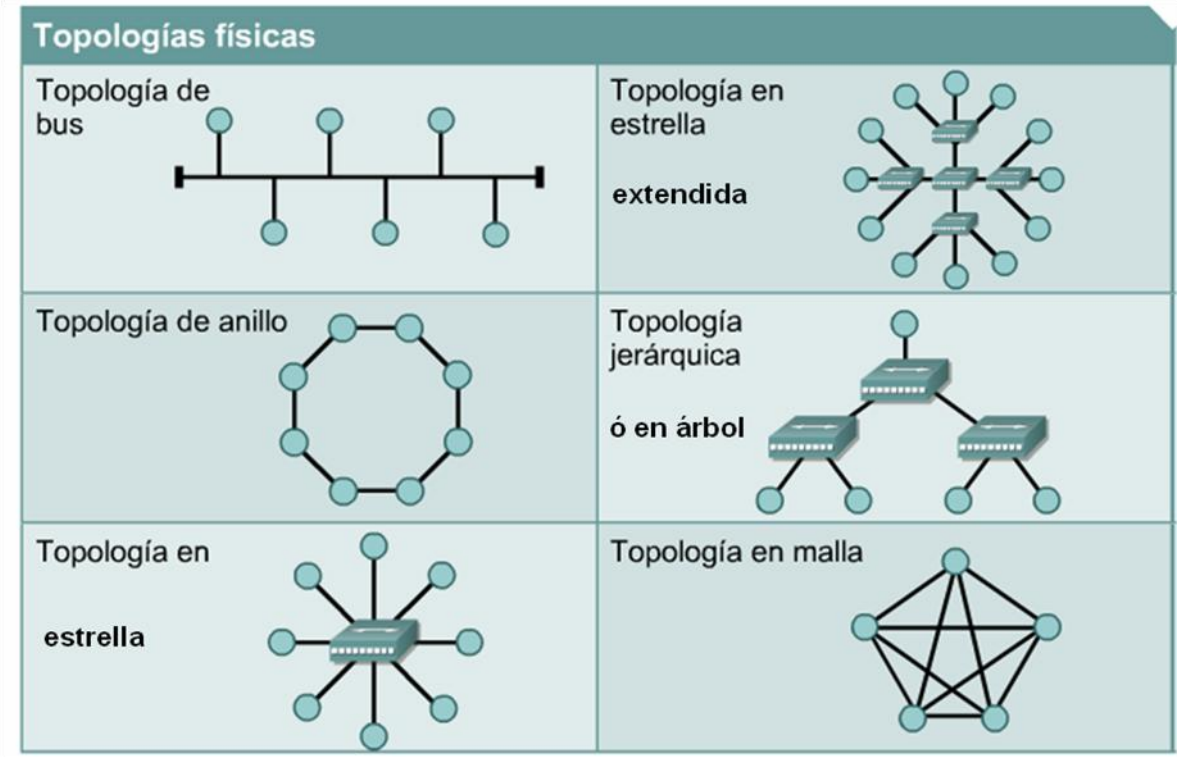


Fig. 7: Topologías físicas.

La topología en **bus** describe cualquier sistema en el que los equipos comparten un mismo medio de comunicación (el aire si es inalámbrico, o un mismo par de hilos de cobre al que se conectan en bus). Tal y como puede observarse en la figura siguiente se simbolizan de dos formas:

Fig. 8: Simbología de redes de medios compartidos, o de bus, o de difusión.

En bus, al ser un **medio compartido**, cuando un equipo emite un mensaje, éste es recibido por todos. Por eso a estas redes también se las llama redes de **difusión** o redes **broadcast**. Aquí se da la

circunstancia de que cuando dos equipos tratan de señalizar a la vez en este medio, las señales se combinan produciendo un resultado ininteligible. A este evento se le denomina **colisión**, y las NICs tienen que tener una forma de detectarlo y evitarlo.

La topología en anillo exige que los mensajes pasen de nodo en nodo siguiendo el círculo hasta llegar a su destino. Es una topología que supera en eficiencia a la de bus cuando hay alto tráfico.

La topología estrella extendida y árbol en realidad son la misma y es la que suele conformar la intranet. Era la topología tradicional de las redes de telefonía y es la topología típica de la mayoría de las intranets.

La topología mallada es típica de sistemas donde se desea redundancia de caminos entre diferentes nodos para conferir robustez (si cae un nodo o un enlace, quedan caminos alternativos entre los demás nodos de la red). Por tanto en la zona troncal de internet (y de algunas intranets) suele combinarse una estructura jerárquica con un mallado parcial.

Independientemente de cómo estén conectados los equipos, éstos pueden seguir una lógica de comunicación diferente. Por ejemplo, hay sistemas que utilizan medios inalámbricos como ZigBee y que por tanto están conectados en una topología de bus, sin embargo sus nodos se organizan de forma jerárquica y van transmitiendo sus mensajes de nodo en nodo siguiendo esa jerarquía. Es decir, a nivel físico siguen una topología bus, pero a nivel lógico funcionan con una topología tipo árbol. Otro ejemplo sería TokenBus que usa también un cable común a todos los dispositivos (topología física tipo bus), pero que se organizan en una secuencia circular donde cada nodo va pasando un mensaje denominado testigo y sólo pueden usar el medio compartido cuando les llega dicho testigo (topología lógica tipo anillo).

3.2- Según su funcionamiento.

Tal y como se observa en la sección anterior, dado un conjunto de equipos en el que uno quiere enviar un mensaje a otro, o bien la red es de difusión y simplemente se envía al medio compartido, o bien no lo es y el mensaje viaja de nodo en nodo hasta llegar a su destino (resto de topologías). En este último caso se habla de redes **unicast** (en contraposición a broadcast), redes **conmutadas** (porque cada nodo conmuta o selecciona al siguiente nodo en el camino) o redes **punto a punto** (porque los nodos están unidos por enlaces o cables no compartidos, es decir, enlaces sólo compartidos por sus dos nodos extremos).

Las redes conmutadas pueden adoptar una de las siguientes estrategias:

Redes de conmutación de circuitos: Son redes en las que el proceso de comunicación sigue la secuencia siguiente:
1-Establecimiento de la conexión (llamada): El DTE que desea iniciar la comunicación avisa a su nodo más próximo indicando qué otro DTE va a ser el destinatario de la llamada. A continuación dicho nodo se comunica con los siguientes pasándose la petición de llamada de uno a otro. De este modo los nodos involucrados realizan una conmutación interna entre puertos y una reserva de recursos de tal forma que se garantice un canal para esa llamada. Cuando esos recursos están disponibles se informa a los DTEs de que hay un canal disponible para poder comunicarlos entre sí.
2-Transmisión de la información: Una vez el canal está establecido (conmutaciones internas fijadas), queda a disposición de los DTEs para que puedan usarlo en la transmisión de información. Las líneas o canales que forman parte de ese canal no pueden ser usadas por otros equipos, ni siquiera en los

intervalos de tiempo en los que los DTEs conectados no estén transmitiendo nada (como ocurre en una conversación telefónica).
3-Cierre de la conexión (llamada): Uno de los DTEs informa de que no va a transmitir nada más al nodo al que está conectado. Éste propaga el aviso a los demás para que deshagan la conmutación y liberen recursos de manera que los enlaces vuelvan a quedar disponibles para futuras llamadas.

Este enfoque era el tradicional de las redes de telefonía. Los nodos de conmutación eran en este caso las denominadas **centralitas** o **PBX** (Private Branch eXchange) cuando se situaban en el extremo del usuario. Desde ahí la red seguía una topología jerárquica con conmutadores de mayores prestaciones. La red telefónica tradicional tiene varias siglas sinónimas: **RTC** (Red Telefónica Conmutada), **RTB** (Red de Telefonía Básica) o **PSTN** (Public Switched Telephone Network).

No obstante, las redes de conmutación de circuitos presentan ciertas desventajas con respecto a su uso para transmitir datos en lugar de voz. En primer lugar se paga por el tiempo de conexión, independientemente de su uso. El tráfico de datos es de tipo ráfagas, es decir, durante un tiempo muy corto se precisa un máximo de caudal de tráfico, pero luego, durante la mayoría del tiempo, hay silencio. Es decir, en datos, o bien se está continuamente estableciendo y liberando conexiones, o bien se mantiene una conexión continua lo cual es muy costoso.

En segundo lugar, los canales conmutados establecidos son circuitos a los que no tienen acceso nadie más que los DTEs conectados. Es decir, supone un desperdicio de recursos, sobre todo en las conexiones troncales de la red, sabiendo que hay muchos intervalos de silencio que podrían ser aprovechados.

Redes de conmutación de paquetes. Son redes en los que la información que se desea transmitir se encapsula en mensajes (paquetes) cada uno de los cuales tiene toda la información que se precisa para llegar a su destino, es decir, remitente y destinatario. En estas redes el proceso es mucho más simple. Cuando un DTE desea transmitir, envía directamente su mensaje al nodo más cercano. Cada nodo en la red inspecciona los mensajes que les van llegando y, en función del destinatario, decide (conmuta) por qué puerto reenviarlo.

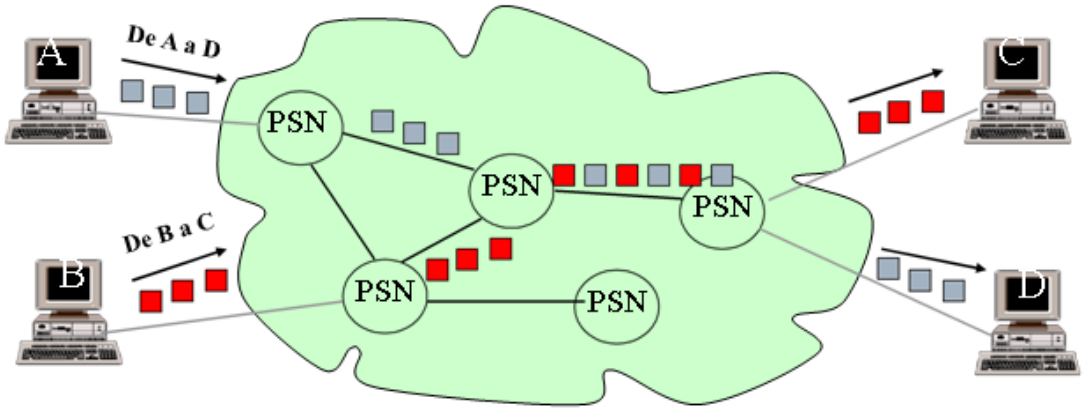


Fig. 9: Redes de conmutación de paquetes

En estas redes se paga por caudal máximo de tráfico y no hay que realizar un lento proceso de establecimiento de conexión, sino que se transmiten los mensajes o paquetes directamente. Dado que los nodos conmutan paquetes y no circuitos, los silencios no tienen ninguna reserva de recursos y los paquetes de varias comunicaciones aprovechan secuencialmente los enlaces troncales de forma

natural. Es decir, se realiza un uso mucho más eficiente de la red. Por estas razones la red tradicional conmutada ha sido sustituida progresivamente por distintas tecnologías de conmutación de paquetes.

3.3- Según su tamaño.

Redes de Área Local (LAN)

En general, una LAN (Local Area Network) es una red privada cuya extensión está limitada en el espacio: un edificio, un campus o en general una extensión inferior a un kilómetro. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas y fábricas para compartir recursos e intercambiar datos y aplicaciones. Las topologías más típicas son las conexiones en bus o estrella. El medio de transmisión más utilizado es el cobre combinado con fibra óptica a alto nivel.

Dentro de las redes LAN se pueden definir tipos de LAN más pequeñas como las redes de área personal (**PAN**) que son las que abarcan el habitáculo que rodea al usuario: un salón, una habitación, un vehículo. Una PAN usualmente conectará dispositivos que dan servicio en dicho habitáculo al usuario. Un ejemplo sería una red Bluetooth entre dispositivos de audio y pantalla táctil en un coche. Debido a la proximidad las PAN tienen diferentes requisitos técnicos que las LAN.

Otra denominación emergente son las BAN (Body Area Network), que comunica dispositivos unidos o en contacto con el cuerpo del usuario: relojes inteligentes, sensores biométricos, auriculares, móvil…

Redes de Área Extensa (WAN)

Una WAN se caracteriza por ocupar una gran área geográfica (hasta un continente entero). Los medios de transmisión son muy variados y la topología suele ser mallada, con conexiones troncales (backbones) habitualmente en anillo y fibra óptica. Las redes WAN son muy caras debido a que los nodos troncales requieren altas prestaciones y los que no lo son suelen ser muy numerosos, además las líneas pueden ser de varios kilómetros y suelen requerir proyectos de ingeniería civil para tenderlas (excavación de zanjas, entubado, postes, etc.). Esos costes implican que la actualización de tecnologías en redes WAN sea muy lenta y provoque la coexistencia de sistemas obsoletos con los más modernos. En consecuencia aparecen soluciones técnicas complejas para poder traducir las comunicaciones entre diferentes sistemas. Esta complejidad aumenta cuando hay que interconectar redes gestionadas por diferentes compañías o ubicadas en diferentes países con regulaciones técnicas diferentes. La tabla siguiente muestra las diferencias entre ambos tipos de redes.

TABLA I

REDES DE ÁREA EXTENSA (WAN)	REDES DE ÁREA LOCAL (LAN)
Distancias de hasta miles de Kilómetros	Distancias inferiores a un kilómetro
Protocolos complejos	Protocolos simples
Suelen ser públicas y administrada por empresas u organismos nacionales	Suelen ser privadas y administradas por sus propietarios
Habitualmente usa circuitos de la red telefónica para sus conexiones	Suele emplear comunicaciones digitales sobre cables propios
Tasas de error altas (1 bit erróneo entre cada 10^5 bits transmitidos).	Tasas de error bajas (1 bit erróneo entre cada 10^9 bits transmitidos)
Suele emplear enlaces punto a punto	Suele emplear redes broadcast o estrella

Redes de Área Metropolitana (MAN)

Son redes de carácter intermedio entre las LAN y las WAN. Poseen características de ambas aunque se diferencian de las LAN en que su área se extiende a toda una ciudad, y de las WAN en que presenta más homogeneidad en cuanto a topología y medios de transmisión. Un ejemplo de red MAN serían LMDS y MMDS, dos tecnologías inalámbricas destinadas a dar servicio de red vía inalámbrica a toda una ciudad. Las antenas del ISP se disponen regularmente en los edificios más altos de modo que su alcance divida en celdas toda la ciudad. Las antenas de los clientes se orientan hacia la más cercana para obtener un enlace de datos.

Redes de Almacenamiento (SAN)

Son redes LAN dedicadas al almacenamiento de datos. Exclusivamente los servidores acceden a ellas, que disponen una infraestructura de altas velocidades de transferencia. Al ser redes separadas, se evita el tráfico cliente-servidor. Las características más relevantes son:

- **Rendimiento**: Las SAN (Storage Area Network) permite el acceso concurrente de dos o más dispositivos a sus matrices de datos a elevada velocidad.
- **Disponibilidad**: Tienen elevada tolerancia a fallos (transferencias seguras hasta 10 km).
- **Escalabilidad**: Existen multitud de tecnologías disponibles que permiten la transferencia de archivos entre sistemas.

Una SAN puede verse como un gran disco duro al que acceden los servidores como si fuera propio. De hecho los servidores solicitan la lectura de sectores de disco. Por el contrario existen otro tipo de estrategias de almacenamiento de información como las **NAS** (Network Attached Storage) que atienden solicitudes de archivos en lugar de sectores de disco. Las NAS son servidores en sí que pueden ser accedidos desde la red.

Redes Privadas Virtuales (VPN)

Son redes privadas que se construyen usando la infraestructura de una red pública. Utilizan el cifrado para generar túneles seguros entre los dispositivos a comunicar. Si el cifrado lo hace el router, el resto de equipos se comunica por la VPN como si fuera una LAN. Es decir, aunque a nivel físico una VPN es una WAN, a nivel lógico es una LAN. Existen tres tipos:

- **VPN de acceso**: Permiten conectar a un usuario desde cualquier punto físico de la red pública a la sede de su empresa. Suele utilizarse para conectar pequeñas oficinas (SOHO) mediante cable telefónico, DSL, RDSI(ISDN) o cablemodem. También sirve para conectar trabajadores que actúen desde casa o en cualquier lugar público. La seguridad debe lidiar con dispositivos cuya dirección no es fija (IP dinámica) y el cifrado lo hace el propio DTE, por lo que las aplicaciones que usen la VPN han de ser compatibles con el software de cifrado. Esto limita la funcionalidad de las VPNs a determinados servicios (web, e-mail).
- **Redes internas de VPN**: Conectan a un usuario en un punto físico fijo (una oficina local) a la sede. Sólo pueden acceder por tanto, usuarios de la empresa. Dado que la dirección es fija y que el equipamiento es de la propia empresa, este tipo de VPN se configura en el enrutador. De este modo se puede conseguir que los equipos entre oficina y sede se vean a nivel lógico como si estuvieran en la misma LAN, todo el camino WAN que han de atravesar para conectarse se ve como un único enlace punto a punto. El router cifra la comunicación que vaya a dicho enlace.

- **Redes externas VPN**: Igual que las anteriores pero con terminales en oficinas de otras empresas (proveedores o clientes). Aquí tienen acceso los usuarios de la extranet, por lo que la seguridad ha de ser diferente.

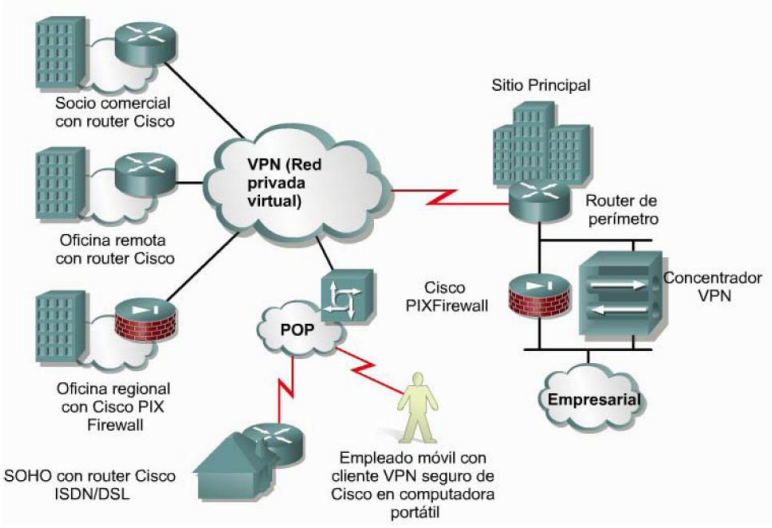


Fig. 10: Redes VPN

Internet:

Internet es una red WAN de ámbito mundial formada en su núcleo por un conjunto de compañías de telecomunicaciones (ISPs) dedicadas a vender el servicio de acceso a la misma, y en su periferia por usuarios o empresas clientes dedicadas a ofrecer o solicitar información. Internet nació como una nueva arquitectura de comunicación para datos. En un principio sólo estaban adscritos a dicha red un conjunto de ordenadores de diferentes universidades. Posteriormente se fueron uniendo a la misma las LAN de diferentes empresas. Las conexiones se hicieron en un principio aprovechando la infraestructura de telecomunicaciones existente, que en ese momento era la red de telefonía (RTB). Luego, la red fue creciendo incorporando líneas y equipos propios. Por tanto, físicamente Internet es una amalgama de redes LAN conectadas con conexiones WAN pertenecientes a la red de telefonía y otras conexiones WAN propias de esta red datos.

A nivel lógico Internet es una red de conmutación de paquetes donde los nodos siguen una estructura tipo árbol, excepto en el núcleo donde se vuelve una red mallada con conexiones redundantes. Aunque cada ISP es dueño de hacer lo que quiera en sus routers, o cada empresa en su LAN, todos eligen seguir las normas promulgadas por el IETF, una entidad que no obedece a ningún país en concreto y en el que puede participar todo el que lo desee aportando una cantidad. De este modo todos se benefician del funcionamiento de la red.

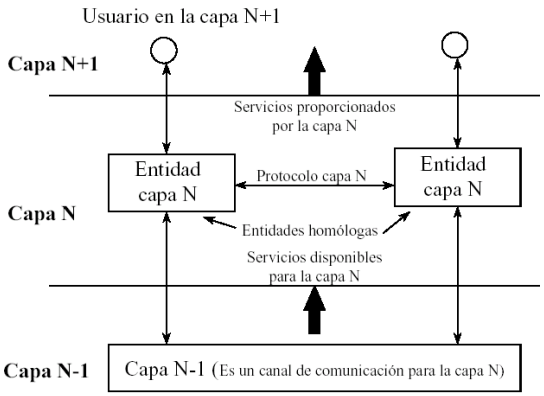
3.- Arquitectura de Red.

He aquí la definición algunos elementos previos:

- **Sistema abierto**: Sistema capaz de interconectarse con otros de acuerdo con unas normas establecidas. La Interconexión de Sistemas Abiertos se ocupará del intercambio de información entre sistemas abiertos y su objetivo será la definición de un conjunto de normas que permitan a dichos sistemas cooperar entre sí.
- **Capa o nivel**: Conjunto de funciones o servicios en que se divide el proceso de comunicación.. Las capas están jerarquizadas y cada capa añade nuevas características a partir de los servicios que proporciona la capa inmediatamente inferior.
- **Entidad**: Elemento que lleva a cabo las funciones asignadas a la capa en la que se encuentra. Las entidades equivalen a procesos software o dispositivos electrónicos inteligentes. Entidades pertenecientes a capas equivalentes en dos equipos diferentes de llaman ***entidades homólogas (peers)***.
- **Protocolo**: Conjunto de reglas (semánticas, sintácticas y de temporización) que gobiernan la comunicación entre entidades de una misma capa. Es decir, en el protocolo de la capa N, una entidad intercambia información con su homóloga en la máquina destino, de cara a proporcionar los servicios asignados a esa capa. Para ello, hará uso de los servicios que proporciona la capa anterior.
- **Arquitectura de red**: Conjunto de capas y protocolos que constituyen un sistema de comunicaciones.

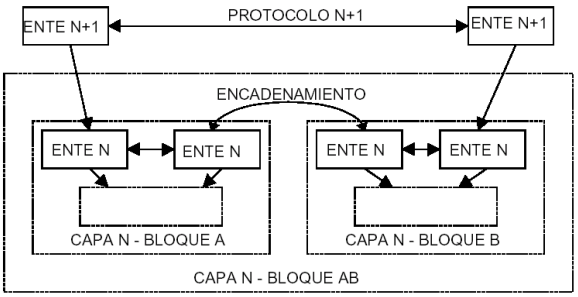
Con la definición de estos términos ya puede vislumbrarse la estructura en que se descompone un sistema de comunicación, que puede resumirse así:

a) El sistema de comunicación está formado por un conjunto de *entidades* situadas en diferentes *capas*.
b) Las *entidades* de una determinada *capa* N cooperan entre sí de acuerdo con un determinado *protocolo* N.
c) Las *entidades* de una *capa* N utilizan los *servicios* N-1 proporcionados por las *entidades* de las *capas* inferiores, mediante un *acceso* a ellos. La estructura de estas *capas* es desconocida para la *capa* N, la cual, sólo tiene en cuenta los *servicios* proporcionados por lo que se ha denominado *bloque* N-1.
d) Las *entidades* de una *capa* N realizan unas determinadas *funciones* N, utilizando los *servicios*.



e) Una capa, la N, proporcionará a la capa inmediatamente superior, la N+1, una serie de servicios. Para ello puede usar los servicios ofrecidos por la capa N-1. Por ejemplo, a partir de un enlace físico con errores, se podría construir un enlace lógico libre de errores.

Según ISO, el modelo que hemos definido es válido para configuraciones simples como sería el caso de una línea punto a punto dedicada. Pero para cubrir configuraciones más complejas como es el caso de interconexiones a través de una red pública de transmisión de datos, se elaboró otro modelo en el que se ha permitido el encadenamiento entre bloques o capas.

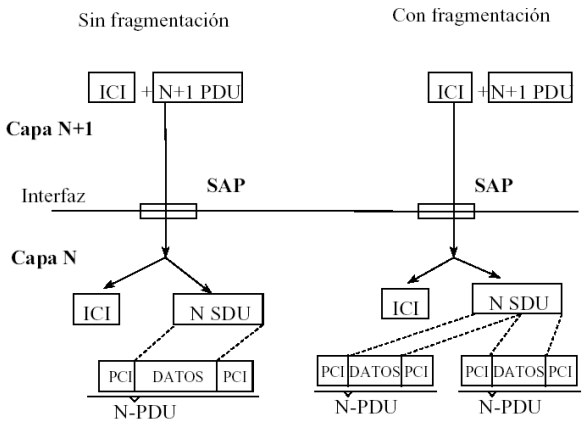


3.1.- Unidades de información transmitidas en la comunicación.

Para acceder a un servicio, se recurre a un ***SAP*** (Punto de Acceso al Servicio), que puede entenderse como el punto en el que interactúan dos capas contiguas de una misma estación. Puede haber más de un SAP entre dos capas. Cada SAP tiene una dirección que lo identifica. En UNIX, los SAP son los puertos o sockets y su dirección el número del puerto o socket.

Para permitir la comunicación entre dos capas, debe existir un conjunto de reglas que definan la interfaz. Así, la interfaz definirá aspectos físicos (conectores, niveles eléctricos) y/o lógicos (estructuras de datos, temporización, etc.) que permitan la interconexión de las capas. Cada máquina puede tener sus propias interfaces entre capas sin que esto afecte a la comunicación entre capas equivalentes.

En una comunicación típica, la capa N+1 pasa una ***IDU*** (Unidad de Datos de la interfaz) a través de un SAP a la capa N dentro de la misma máquina. Una IDU está compuesta por una información de control de la interfaz (***ICI***) y una parte de datos o ***SDU*** (Unidad de Datos del Servicio). La SDU es la información para la que se requiere el servicio, mientras que la ICI es la información que necesita la interfaz para proporcionar el servicio en la forma deseada.
Mientras la ICI puede variar de una máquina a otra, la SDU permanece invariable. La SDU de la capa N junto con la cabecera y la cola que forman la información de control del protocolo (PCI), integran la llamada ***N-PDU*** (Unidad de Datos del Protocolo) de la capa N. Si la información no se fragmenta, la información de la SDU de la capa N coincide con los datos de la PDU de la capa N. Si por el contrario, la información es fragmentada, se formarán varias PDU de capa N. Estos trozos deberán ser reensamblados en el destino para obtener la SDU.



Un servicio ofrecido por una capa puede mapearse directamente sobre un servicio de la capa inferior, o bien, la capa puede disponer de un protocolo que le permita mejorar el servicio que ofrece la capa inferior (por ejemplo corrección de errores). En cualquier caso, el usuario de los servicios de una capa, debe ver a ésta como una caja negra.

3.2- Funciones de los sistemas de comunicación.

Hemos visto que en cada capa existen unas funciones o servicios a realizar. Entre estas funciones están las siguientes.

Nombres y direcciones.

En la comunicación, la identificación de las partes que intervienen es fundamental. No sólo hay que saber qué nos están diciendo sino que hay que saber quién lo dice. En general, distinguiremos entre ***nombres, direcciones*** y ***rutas*** a la hora de identificar una estación, o de forma más general, un recurso. Mediante el nombre identificaremos el recurso al que queremos acceder. Su dirección nos indicará en que punto de la red se encuentra, y la ruta nos definirá el camino óptimo a seguir para llegar al recurso. La función que se optimiza puede ser el coste de la comunicación, la fiabilidad, el tiempo, o una ponderación de varios de estos criterios.

Fragmentación y reconstrucción de mensajes.

Resulta evidente que la longitud de la información que se desea enviar o se va a recibir no tiene que coincidir necesariamente con el tamaño del paquete que realmente circula por la red. En ese caso, el mensaje original debe se fragmentado en trozos más pequeños para su envío a través del canal de comunicación. Esta situación obliga a que la estación receptora sea capaz de identificar los diferentes bloques y reensamblarlos con el fin de obtener la información original.

Compactación.

En ocasiones, para aumentar la eficiencia de un canal, pueden enviarse en un mismo paquete varios bloques pequeños de información. Es obligación del sistema de comunicación hacer esta tarea transparente al usuario.

Establecimiento de conexiones y Multiplexación.

Para poder establecer una comunicación que involucre varios mensajes es necesario establecer una sesión o una conexión. La sesión mantiene información sobre el estado de las comunicaciones para permitir la recuperación de la misma tras un error, o bien para ordenar la secuencia de mensajes. En este sentido, una conexión puede verse como un flujo de mensajes entre dos estaciones. Por otra parte, puede ocurrir que una estación tenga un único canal de comunicación, pero quiera mantener simultáneamente varias sesiones abiertas. Esto obliga a que las distintas sesiones existentes compartan el canal mediante su Multiplexación. También puede ocurrir lo contrario, es decir, que una sesión desee emplear varios canales disponibles en una máquina con el fin de aumentar la capacidad de la conexión. Esta multiplexación / demultiplexación del canal exige un control adicional sobre el flujo de mensajes.

3.5.- Control de errores.

En la comunicación es importante disponer de canales fiables, es decir, libres de errores. Esto incluye tres aspectos fundamentales: detección, corrección y recuperación de errores. Las principales causas de error son el ruido en la línea de transmisión, el deterioro de la información en algún nodo intermedio o la pérdida de paquetes. Así pues, deben detectarse:

- Deterioros en la información (errores a nivel de bit)
- Pérdidas de mensajes
- Duplicación de mensajes
- Mensajes fuera de secuencia.

La detección de errores de bits se logra añadiendo información redundante, por ejemplo usando bits de paridad. Los errores de secuencia se detectan añadiendo a los mensajes identificadores de secuencia únicos. En general, cuando se detecta un error, la solución suele ser la petición de retransmisión del paquete o paquete afectados.

Congestión y control de flujo.

Un sistema de comunicación puede sufrir los mismos problemas de congestión que las carreteras. Esto es debido a que un gran número de usuarios comparten un número limitado de recursos. Si en un momento dado hay una gran demanda de dicho recurso, éste puede llegar a saturarse y no ser capaz de atender todas las peticiones que recibe. Estamos ante una congestión.

Los ***mecanismos de control de congestiones***, son los medios de que dispone la red para evitar un bloqueo de la misma a medida que aumenta el tráfico de información. Los ***mecanismos de control de flujo*** permiten regular el intercambio de información entre dos entidades de forma que una no envíe más información de la que la otra es capaz de procesar.

Sincronización.

Para que pueda existir comunicación entre dos entidades, es necesario que exista una sincronización a distintos niveles:

- **Nivel de bit:** El receptor debe conocer o ser capaz de determinar el comienzo y duración de cada elemento de señal para poder leerla de forma correcta.

- **Nivel de byte:** Muchos sistemas intercambian información en forma de caracteres de 8-bits (byte), aunque varios bytes pueden empaquetarse en un único mensaje para su transmisión.

Por ello, el receptor debe ser capaz de distinguir el comienzo y final de cada byte dentro del paquete.

- **Nivel de bloques:** Es necesario determinar el inicio y final de un bloque de bytes. La información contenida un bloque suele tener un significado u otro en función de su posición. Es habitual que los bytes iniciales actúen como cabecera y contengan información que permite al protocolo de la capa controlar la comunicación.

- **Nivel de acceso al medio de comunicación:** En el caso de acceder a un medio de comunicación con estructura de bus, es importante asegurar que sólo un usuario tiene acceso al medio en un instante determinado.

- **Nivel de protocolo:** Dos entidades pares que se comunican, y que mantienen información sobre el estado de la comunicación deben estar sincronizadas al comienzo de la misma o tras un error grave de la comunicación, para poder recuperarla.

- **Nivel de proceso:** Este tipo de sincronización es necesaria para acceder a un recurso compartido como por ejemplo datos comunes almacenados en un disco.

Gestión de Prioridades.

Con el fin de establecer jerarquías a la hora de competir por el acceso a un recurso, pueden establecerse distintos niveles de prioridad para los mensajes. En general, mensajes de alta prioridad sufrirán retardos menores. Un uso típico es la transmisión de alarmas en aplicaciones de control, indicar la parada de una aplicación, o el uso de mensajes de control de comunicación.

3.3.- El modelo de referencia OSI de ISO.

El modelo OSI (Open Systems Interconnection) de ISO (International Standards Organization) fue una propuesta para la standarización de las redes de ordenadores. Este modelo tiene siete capas, diseñadas con arreglo a los siguientes principios:

1. Una capa se creará en situaciones en las que se requiera un nivel diferente de abstracción.
2. Cada capa deberá realizar una función bien definida.
3. La función que realiza cada capa deberá seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfaces.
4. El número de capas será suficientemente grande como para que funciones diferentes no estén en la misma capa, y suficientemente pequeño para que la arquitectura no sea difícil de manejar.

El modelo OSI por si mismo, no es una arquitectura de red puesto que no especifica el protocolo que debe usarse en cada capa, sólo indica un reparto de servicios factible para a partir de ahí definir los protocolos oportunos.

Capa física

La capa física se ocupa de la transmisión de bits a través de un canal de comunicación. Debe asegurar que cuando un extremo envía un bit con valor 1, sea recibido como tal en el otro extremo. Los problemas de diseño a considerar aquí son los aspectos mecánico, eléctrico, de interfaz y el

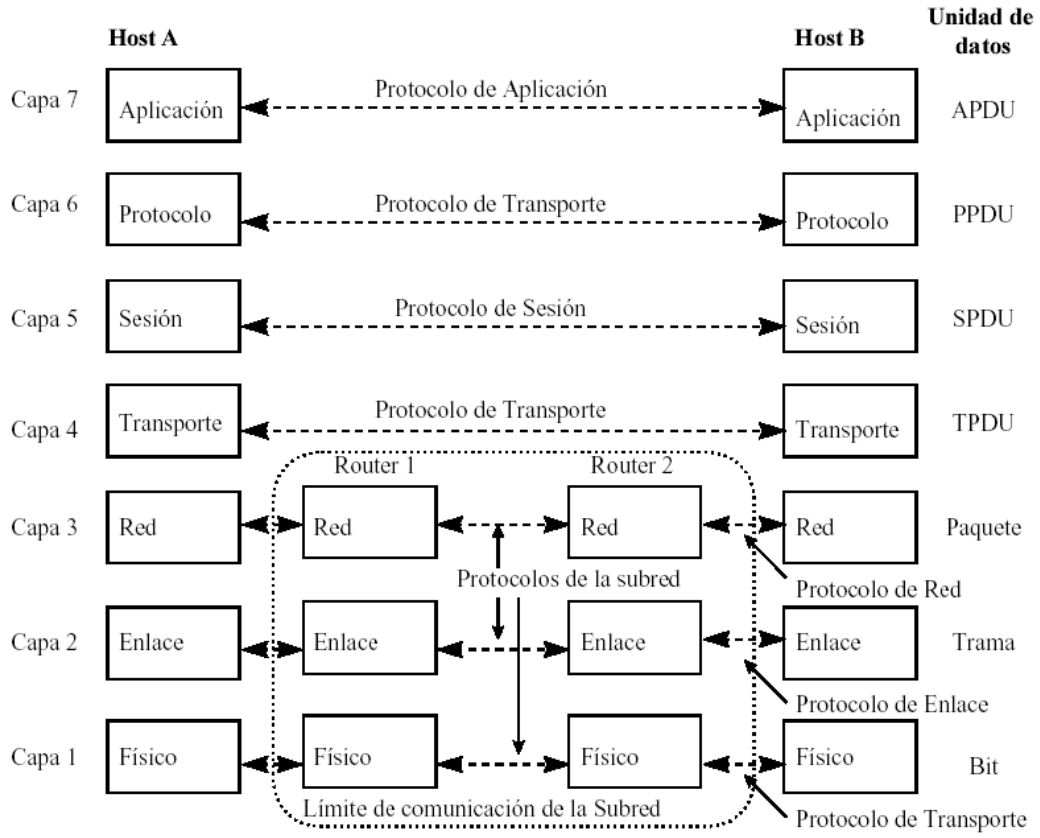
medio de transmisión física. Como servicios que puede implementar son de sincronización y control de errores.

Capa de enlace

Su principal tarea consiste en proporcionar una línea sin errores a partir de un medio de transmisión cualquiera. Esta capa debe crear y reconocer los límites de las tramas. Además debe resolver los problemas creados por el deterioro, pérdida o duplicidad de tramas. La capa de enlace ofrece distintos servicios a la capa de red, cada uno con distinta calidad y precio. De nuevo sincronización y errores son servicios propios de esta capa. Además incluye el servicio de control de congestión o control de flujo que permite evitar que un emisor muy rápido sature a un receptor muy lento. También pueden verse en esta capa procesos de multiplexación y de compactación. La PDU de esta capa se denomina **trama**.

Capa de red

La capa de red se ocupa del control de la operación de la subred. Un punto vital de su diseño, es la decisión sobre como encaminar los paquetes del origen al destino. El encaminamiento puede basarse en unas tablas estáticas o bien determinarse dinámicamente en función del tráfico de red. También debe detectar y corregir problemas de congestión de tráfico. En ocasiones también incluye funciones de contabilidad para el cobro de los servicios de subred. La capa de red también debe resolver los problemas de comunicación entre distintas redes, fragmentando por ejemplo los paquetes en unidades inferiores cuando sea necesario. La PDU de esta capa se llama **paquete**.



Capa de transporte

La principal función es aceptar los datos de la capa de sesión, dividirlos si es necesario y pasarlos a la capa de red. Además debe asegurar que todos lleguen correctamente al otro extremo. Este trabajo debe hacerse de forma eficiente para aislar la capa de sesión de cambios en el hardware.

Lo habitual es establecer una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión. Si la conexión de transporte necesita un gran caudal, ésta podría crear múltiples conexiones de red. Por otra parte, si el mantenimiento de una conexión de red es costoso podría multiplexar varias conexiones de transporte sobre la misma conexión de red.

La capa de transporte determina qué tipo de servicio debe dar a la capa de sesión. El tipo de conexión más habitual es el punto a punto libre de errores. La capa de transporte es la primera capa extremo a extremo dentro de la jerarquía. Debe preocuparse del establecimiento y liberación de conexiones así como proporcionar mecanismos de control de flujo y de congestiones. La PDU de transporte se denomina **segmento**.

Capa de sesión

Una capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. Un servicio de la capa de sesión es gestionar el control de diálogo, es decir, actúa como moderador en una reunión donde varios individuos desean comunicarse. Puede permitir que el tráfico vaya en las dos direcciones simultáneamente, o bien alternativamente, en cuyo caso determinará que estación tiene el turno.

Otro servicio asociado a la capa de sesión es la administración del testigo si existe. También debe encargarse de la sincronización. Esto implica la inserción de puntos de verificación en el flujo de datos, en los que puede retomarse la conversación en caso de fallo.

Capa de presentación

La capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que transmite. También puede ocuparse de la compresión y encriptación de los datos intercambiados.

Capa de aplicación

Contiene una cantidad de protocolos usados frecuentemente, como por ejemplo ofrecer servicios de terminal virtual, transferencia de archivos, correo electrónico, ejecución remota de procesos, etc.

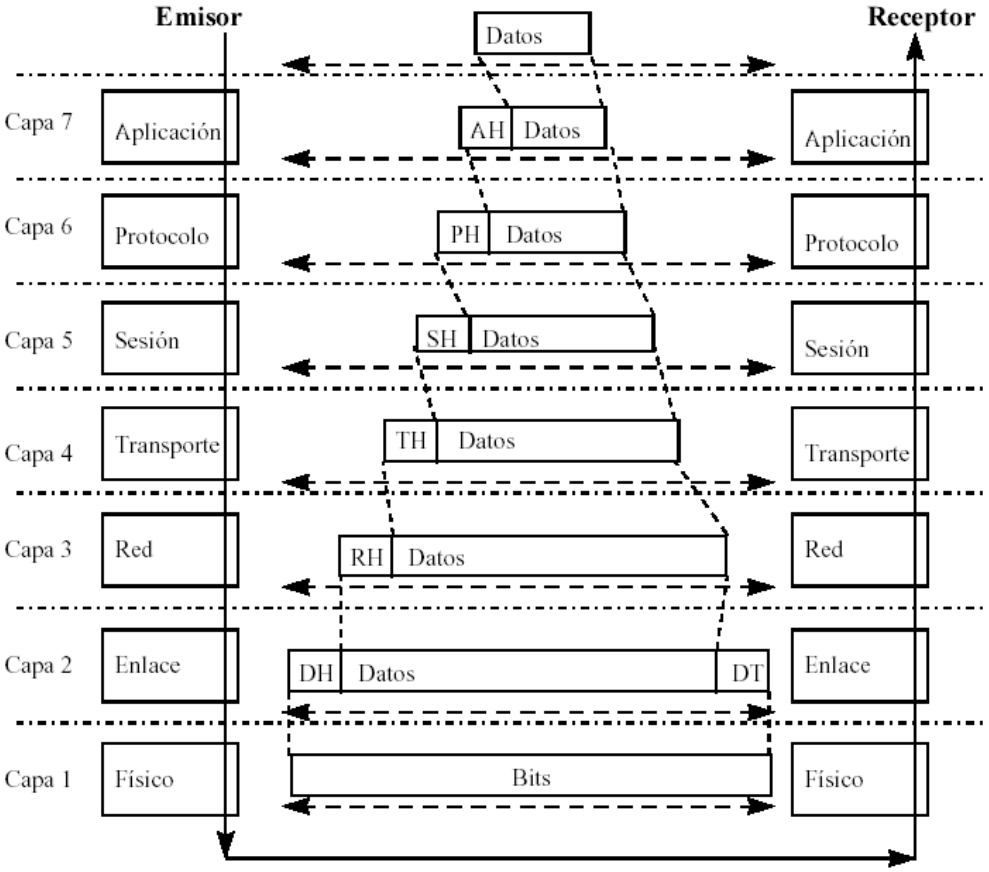
3.4.- Transmisión de datos en el modelo OSI

Una vez vistas las distintas capas que especifica el modelo de referencia OSI, conviene estudiar la forma en que se produce una comunicación. Supongamos que el proceso emisor tiene una información que enviar, para ello, entregará los datos a la capa de aplicación. La capa de aplicación añade a la información que recibe una cabecera (que puede ser nula) que permite a la capa seguir el protocolo que tenga definido. El conjunto formado por los datos originales y la cabecera de aplicación es entregado a la capa de presentación.

La capa de presentación transforma este bloque de distintas formas, en función del servicio pedido, y añade una nueva cabecera, la correspondiente a la capa de presentación.

El nuevo conjunto de datos es entregado a la capa inmediatamente inferior, la capa de sesión. Es importante destacar que la capa de presentación no distingue que parte de los datos que recibió corresponden a la cabecera de la capa de aplicación y que parte son los datos del usuario.

Es importante hacer notar que en una o varias de las capas, el conjunto de datos que recibe la capa N de la N+1 pueden ser fragmentados en bloques más pequeños para su entrega a la capa N-1. En ese caso, cada bloque recibirá su propia cabecera y además la capa que realiza la fragmentación deberá ser la encargada (en la máquina receptora) de reensamblar los bloques hasta formar el conjunto inicial de datos, y entregarlos a la capa superior.



El proceso se repite hasta llegar a la capa física, momento en el cual los datos son enviados a través del canal físico disponible hacia la máquina de destino. La capa física de la estación receptora recibirá el conjunto de bits del mensaje y comenzará el proceso inverso. Capa a capa deberá ir eliminando las distintas cabeceras y transmitiendo el resultado hacia las capas superiores hasta llegar al proceso receptor.

Evidentemente, el objeto de añadir y eliminar las cabeceras no es tener algo que hacer, sino que las cabeceras permiten a cada capa suministrar el servicio que le fue requerido por la capa superior de acuerdo al protocolo establecido para la capa. De esta manera, la comunicación funciona como si cada capa se comunicase directamente con su homóloga en la máquina de destino a través de un canal lógico proporcionado por el resto de capas en ambas máquinas.

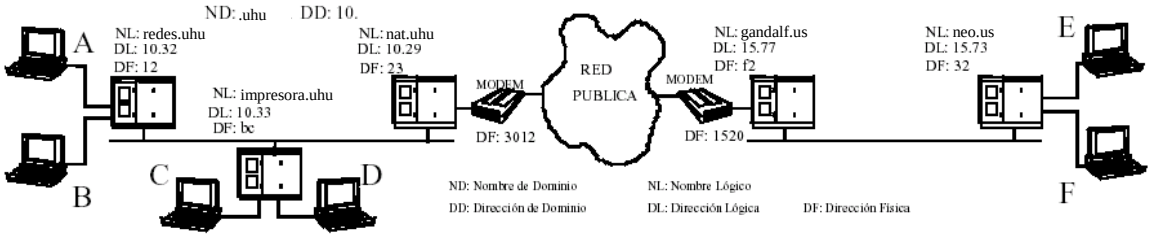
Aunque la idea puede parecer rebuscada, es similar a lo que sucede en la comunicación entre personas. Inicialmente tenemos una idea que queremos comunicar a nuestro contertulio. Esa idea es entrega a la zona del cerebro encarga del lenguaje. A su vez, el área del lenguaje se encargará de generar los impulsos nerviosos necesarios para hacer vibrar nuestras cuerdas vocales. Esta vibración

se transformará en un sonido recogido por el oído de nuestro interlocutor. Los impulsos nerviosos generados por su oído serán enviados al cerebro que los transformará en palabras, y de ellas extraeremos la idea.

El proceso de la comunicación es similar si el área del lenguaje decide enviar la información al área encargada de la escritura. En este caso, el área del lenguaje estará pidiendo un servicio diferente a la capa inferior: escribir en lugar de hablar. Además, el medio físico empleado será distinto, papel en lugar del aire. En cualquier caso nosotros sólo somos conscientes de que enviamos o recibimos un pensamiento.

Ejemplo

A modo de ejemplo en las páginas siguientes se muestra como dos sistemas abiertos interconectados realizan el intercambio de información. Se ha supuesto una red formada por dos dominios constituidos por redes locales y unidos a través de una red pública de transmisión de datos. Dentro de cada red, local o pública, las interfaces de cada nodo están identificadas mediante una dirección física (que en el caso de la red pública puede ser un número de abonado) impuesta por el propio hardware de red y que normalmente el usuario no puede modificar.



Por razones nemotécnicas a los nodos y dominios se les dan nombres que permitan recordar su denominación en la red fácilmente. Estos nombres están asociados a direcciones lógicas, que son las que realmente utiliza el sistema de comunicaciones para identificar cada nodo y dominio. Por lo general el nombre o dirección de un nodo se compone de la identificación del dominio donde se encuentra junto con su identificación individual dentro de ese dominio. Las identificaciones lógicas son asignadas por los usuarios a los nodos, generalmente bajo la supervisión de un administrador de la red.

Cuando se transmite un mensaje, pasa de la capa 7 a la 1 del sistema emisor, y cada capa añade su propia cabecera o trata el mensaje de alguna forma. Las tramas que constituyen el mensaje se transmiten sobre el medio hasta el sistema receptor en el que pasan de la capa 1 a la 7, eliminándose las cabeceras y reconstituyéndose el mensaje. Cuando las funciones de una capa en particular no son necesarias, se emplea una capa nula.

En el primer ejemplo el mensaje va destinado a un nodo que se encuentra en la misma red física que el nodo emisor. Por ello, las funciones de encadenamiento entre entidades no son necesarias y la capa de red y la distinción entre direcciones lógicas y físicas pierden sentido al no ser necesario para realizar el encaminamiento.

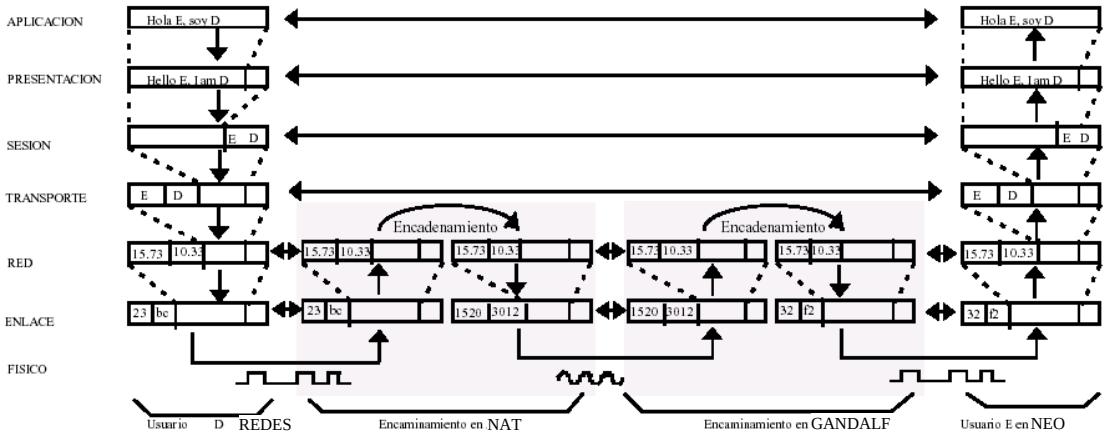
El mensaje es adquirido por la capa de aplicación, que se implementaría como el software necesario para recoger el mensaje del teclado del usuario del terminal B de “redes” y enviarlo por la red. Una vez obtenido el mensaje la aplicación lo entregaría al modulo o programa que implementa la capa de presentación, que adecuará el mensaje a la sintaxis de la red. En este caso se ha ejemplificado como una traducción a idioma de la red, que podríamos suponer que es el inglés. En la realidad la capa de

presentación adecua estructuras de datos, representaciones de datos enteros, de coma fija, de coma flotante, comprime, encripta, etc. A unas estructuras estándar para el sistema de comunicaciones.

La capa de sesión mantiene la sesión de trabajo de cada usuario dentro de un mismo nodo, identificando a cada usuario para diferenciar su sesión de la de los demás. Todas estas sesiones convenientemente identificadas (generalmente mediante la identificación tanto del origen, B, como del destinatario, C) se multiplexan en la capa de transporte que transfiere a la capa de red los datos destinados a cada nodo (correspondientes a una o varias sesiones) dando su identificación lógica en la red (10.33 como destino y 10.32 como origen).

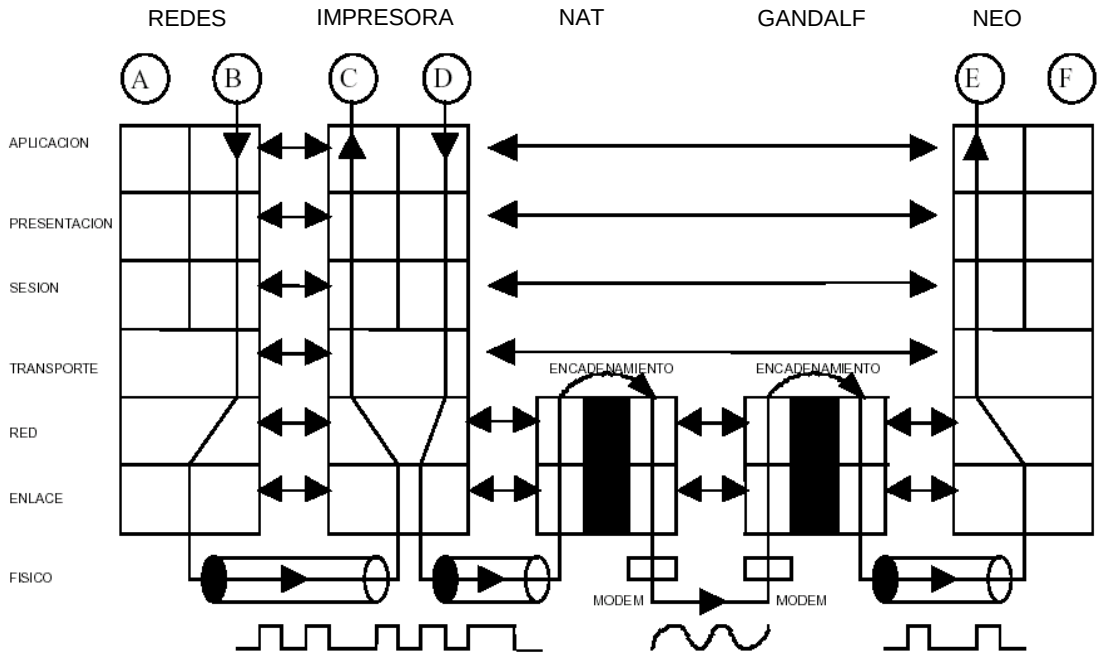
Cuando el nodo destinatario se encuentra en la misma red, esta capa simplemente entrega a la de enlace los datos a enviar con la identificación de la interfaz física (bc) que corresponde al destinatario. La trama de datos creada por la capa de enlace es convertida en señales eléctricas (en este caso) que se propagan por el medio de transmisión.

Una vez captadas las señales por la interfaz física del destinatario, se convierten de nuevo en una trama. La capa de enlace se encarga de determinar si está dirigida al nodo en el que se encuentra mediante la comprobación de la dirección física que viene en la trama. Si es así la acepta y la entrega para ser procesada por la capa de red, sino la rechaza.



La capa de red comprueba la dirección lógica de destino, y si es la suya entrega los datos a la de transporte. Esta identifica los datos que vienen para las distintas sesiones y los demultiplexa entre ellas (en este caso la sesión del usuario C). La capa de sesión elabora sus datos para el mantenimiento de la misma y pasa en mensaje aún en la forma de representación de la red a la capa de presentación. Esta lo descomprime, desencripta y/o adecua su representación a la utilizada en el nodo destinatario (que no tiene por que se la misma que la del nodo de origen). Finalmente la

aplicación correspondiente hará aparecer el mensaje en la pantalla del terminal del usuario destinatario.



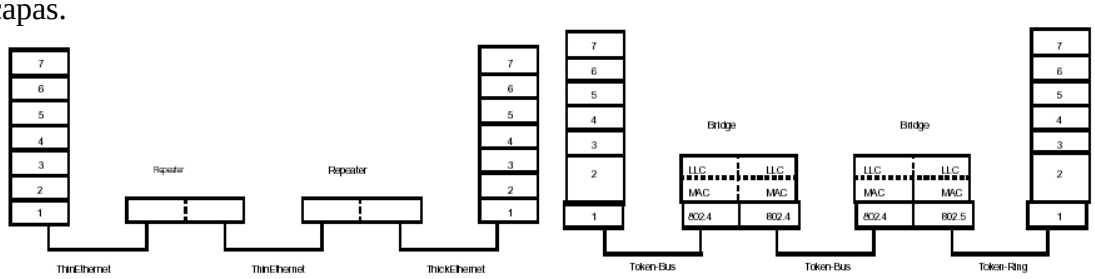
En el segundo ejemplo la transmisión se realiza entre dos nodos localizados en dominios diferentes, "redes.uhu" y "neo.us". Esto obliga a la información a pasar por nodos intermedios en su camino entre el usuario D, origen de la transmisión, y el destinatario E.

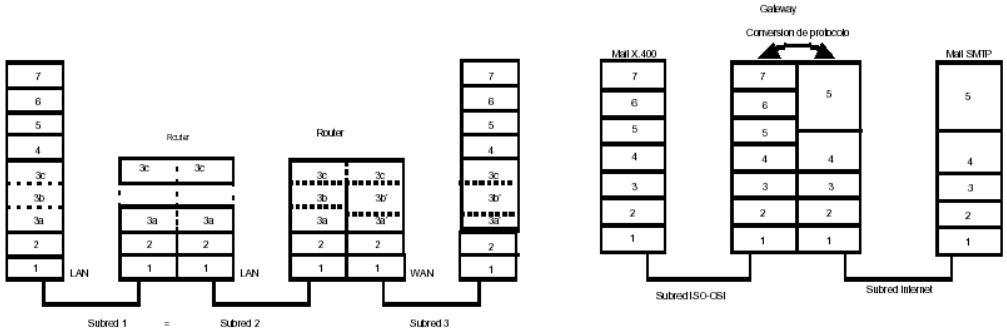
En principio todo el proceso es igual al anterior hasta que la información llega a la capa de red, encargada precisamente del encaminamiento entre subredes. Esta capa se encuentra con el problema de que si entrega la información a la capa de enlace indicando como destinatario la dirección física de "neo.us" (32), nadie en su subred atenderá esa trama de datos. Sin embargo si conoce la dirección física en su red del nodo que le sirve de enlace con nodos de de otros dominios, "nat.uhu" (23) y a esa dirección física dirige la trama.

La trama es aceptada por la capa de enlace de "nat.uhu" pues está dirigida su dirección física. Pero cuando los datos llegan a la capa de red este detecta que la dirección lógica del destinatario no es la suya. Sin embargo, "nat.uhu" está preparada para estas situaciones ya que se encarga del encaminamiento del tráfico que va y viene desde fuera de la subred local. Dispone de dos interfaces de comunicación con características y sintaxis de dirección diferentes, y de unas tablas de encaminamiento que le permiten saber en función de la dirección lógica del destinatario a que red y a que dirección física ha de dirigir la información. En este caso decide pasar a la capa de red implementada para la red pública los datos, y ésta los destina a través de la capa de enlace hacia la dirección física "1520" que corresponde al nodo que realiza funciones similares en la red "us".

La información se transmite a través de la red pública con señales eléctricas de características muy distintas a las de la red local, y son aceptadas por la capa de enlace de "gandalf.us". Su capa de red detecta también una dirección lógica de destino distinta a la suya para realizar a continuación un proceso similar al de "nat". Ahora los datos pasan de nuevo a unas capas relacionadas con la red local "us" (que puede ser un estándar diferente a la red que se utiliza en "uhu") y son dirigidos, ahora si, a la dirección física del destinatario, "neo.us" (32). El proceso hasta llegar a la pantalla del usuario del terminal E es el ya descrito en el ejemplo anterior.

En la tercera figura se muestran los caminos seguidos por la información a través de las capas y se pueden observar los fenómenos de multiplexación sobre la capa de transporte y que esta es la primera de las capas que mantiene un diálogo extremo a extremo en la comunicación entre subredes. La cuarta figura muestra distintos dispositivos en los que se producen encadenamientos en distintas capas.



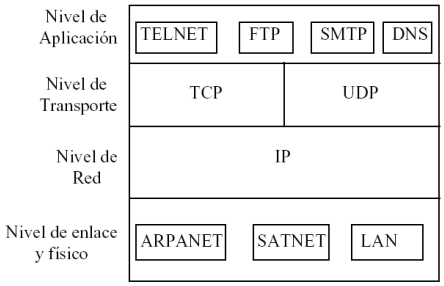


3.5.- El modelo de referencia TCP/IP.

Este modelo es el usado por ARPANET, el abuelo de las redes de ordenadores.

La capa Internet

Por diversas razones, en el caso de ARPANET se eligió una red basada en conmutación de paquetes sobre un servicio de red sin conexión. Esta capa de red es la capa internet. Su función es permitir que los host inserten paquetes en cualquier red, y que estos viajen independientemente hacia su destino (que quizá sea una red distinta). Incluso pueden llegar en distinto orden del que fueron enviados, en cuyo caso, es obligación de las capas superiores reordenarlos si fuese preciso.



La capa internet define un tipo oficial de paquete y un protocolo llamado IP (internet protocol). La principal obligación de la capa es distribuir los paquetes hacia su destino, por ello su función es el encaminamiento de los mensajes y evitar atascos, aunque sus mecanismos de control de congestiones son bastantes limitados. Equivale a la capa de red del modelo OSI.

La capa de transporte

Es la siguiente capa en el modelo TCP/IP. Está diseñada para permitir el diálogo entre entidades homólogas extremo a extremo, al igual que la capa de transporte de modelo OSI. Utiliza dos protocolos: TCP (Transmision Control Protocol) y UDP (User Datagram Protocol). El primero es un protocolo orientado a conexión, libre de errores, que permite enviar bloques de bytes de una máquina a otra por un canal libre de errores. TCP también administra el control de flujo. El protocolo UDP es un protocolo sin conexión basado en datagramas simples. Se penso para aquellos casos en los que la capa de sesión necesitase un canal lógico distinto del que proporciona TCP.

Capa de aplicación

El modelo TCP/IP no tiene las capas de presentación ni de sesión. La experiencia ha demostrado que esta aproximación es la correcta. Esta capa contiene todos los protocolos de alto nivel como por ejemplo: TELNET (terminal remoto), FTP (transferencia de ficheros), SMTP (correo electrónico), DNS (servidor de nombres), etc. Más recientemente se le han añadido otros protocolos como NNTP (news) y HTTP.

Capa de acceso a red

En TCP/IP aglutina tanto la capa física OSI como la de enlace. En realidad sólo especifica que el host debe estar unido a la red a través de algún protocolo que permita el envío de paquetes IP.

3.6.- Comparación entre los modelos OSI y TCP/IP

El modelo OSI y el TCP/IP tienen muchas cosas en común. Ambos se basan en la idea de una pila de protocolos independientes. Además, la funcionalidad de las capas es bastante similar. Por ejemplo, en ambos modelos, las capas hasta la de transporte deben proporcionar un servicio de transporte extremo a extremo independiente de la red, a procesos que desean comunicarse. En ambos casos, las capas que están por encima de la capa de transporte son usuarios de los servicios, que ésta proporciona, orientados a la aplicación.

Aún así, también poseen muchas diferencias. El modelo OSI tiene tres conceptos básicos: servicios, interfaces y protocolos. Probablemente, la principal contribución del modelo OSI es hacer explícita la distinción entre estos conceptos. Cada capa realiza unos servicios para la capa superior. La definición de los servicios indica qué es lo que hace la capa, no cómo es el acceso de las capas superiores o como funcionan las mismas.

La interfaz de una capa indica cómo acceder a los servicios que ofrece, pero tampoco dice nada sobre como funciona interiormente. Finalmente el protocolo de la capa es un problema exclusivo de la misma. Sólo debe ser capaz de asegurar que la capa proporciona correctamente sus servicios. Su modificación no debería afectar al software de las demás capas.

En su origen, el modelo TCP/IP no hizo esta distinción, aunque con el tiempo se ha adecuado a estos propuestos por el modelo OSI. Como consecuencia, los protocolos del modelo OSI están mejor escondidos que en el modelo TCP/IP. El modelo OSI se planteó antes de definir los protocolos de cada capa por ello el modelo no se desvió en favor de ningún protocolo en particular. El principal inconveniente es que los diseñadores del modelo no tenían mucha experiencia y por ello no sabían muy bien en qué capa incluir cada servicio.

Por ejemplo, la capa de enlace estaba pensada para redes punto a punto. Cuando aparecieron las redes broadcast hubo que insertar una subcapa para acomodarlas. Cuando se comenzaron a diseñar sistemas basados en OSI con los protocolos que existían, se dieron cuenta que no encajaban con los servicios requeridos de la capa. Los miembros del comité ISO pensaban que cada país tendría una red, controlada por el gobierno y adecuada al modelo OSI. El problema es que las cosas no evolucionaron así.

Con TCP/IP sucedió lo inverso: primero se definieron los protocolos y el modelo resultó ser una descripción de los mismos. Evidentemente, los protocolos se ajustan al modelo, pero el modelo no se ajusta a ningún otro conjunto de protocolos, por lo que no es útil para describir redes que no sean de tipo TCP/IP.

Otra diferencia está en el tipo de conexión. El modelo OSI soporta servicios sin conexión y orientados a conexión en la capa de red, pero la capa de transporte sólo acepta servicios orientados a conexión. El modelo TCP/IP sólo soporta servicio de datagramas en la capa de red, pero admite ambas formas de servicio en la capa de transporte, con lo que el usuario puede elegir. Esto es importante para aplicaciones basadas en un protocolo simple de pregunta / respuesta.

4.- Breve historia de las redes de comunicación.

4.1.- Arpanet.

ARPANET (Red de la Agencia de Proyectos de Investigación Avanzada) es la creación de ARPA, que es la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de EEUU. Su programa, iniciado en los últimos años de la década de los 60, comenzó por estimular la investigación en temas relacionados con redes de ordenadores, mediante la canalización de recursos a los departamentos de ciencias de la computación de varias Universidades de Estados Unidos, así como a algunas compañías privadas. Esta investigación produjo una red experimental de cuatro nodos, que se dio a conocer públicamente en diciembre de 1969. Desde entonces, creció en forma substancial, hasta llegar a tener varios centenares de hosts, cubriendo casi la mitad de la Tierra. En 1983, una vez demostrada su capacidad para establecer un servicio fiable de comunicaciones, ARPA cedió la administración de la red a la DCA (Defense Communications Agency), para que la utilizase como una red operacional. Lo primero que hizo la DCA fue separar la parte militar en una subred separada, llamada MILNET, con fuertes restricciones para su acceso desde otras redes externas. En 1990, fue sustituida por otras redes que ella misma había creado, de forma que fue cerrada y desmantelada, aunque MILNET sigue operativa.

A comienzos de los años 60, Paul Baran había sugerido la idea de la conmutación de paquetes frente a la conmutación de circuitos propia de las líneas telefónicas. ARPA decidió que esta novedosa solución debía ser la base para las comunicaciones entre los ordenadores militares dado que resultaba más segura en caso de ataque, pues la destrucción de un nodo de comunicaciones no implicaría la interrupción automática de las mismas. Por ello, la red que se desarrollara debía ser una red de conmutación de paquetes, formada por una subred y unos host que la utilizan.

La subred estaba formada por una serie de minicomputadores llamados IMP (Interfaz Message Processors) conectados entre sí por líneas de transmisión de datos. Para mayor seguridad, cada IMP debía estar conectado al menos a otros dos, de esta forma si alguna línea o algún IMP resultaba destruido, los mensajes continuarían circulando por caminos alternativos.

Cada nodo de la red consistiría en un IMP y un host, en la misma habitación y conectados por un cable que permitiese comunicaciones fiables a alta velocidad. Un host podría enviar mensajes a un IMP de hasta 8063 bits. El IMP lo fragmentaría en trozos menores de 1008 bits y los enviaría de forma independiente hacia su destino. Cada paquete debía ser recibido entero antes de que un nodo intermedio lo reenviase hacia el destino final.

ARPA seleccionó a BBN, una empresa de Massachusetts, para que construyera la subred en diciembre de 1968. BBN eligió un modelo modificado de los DDP-316 de Honeywell, con 12K palabras de 16-bits como memoria principal para utilizarlos como IMP. Los IMP no tenían discos, ya que las partes móviles se consideraban poco fiables. Los IMP estaban conectados entre sí por líneas alquiladas de 56 Kbps.

El software se dividió en dos partes: el host y la subred. El software de la subred incluía los protocolos de comunicación entre dos IMP consecutivos y entre IMP origen - IMP destino. El software del host se encargaba de las comunicaciones host - IMP, host - host, y el software de aplicación.

Para resolver el problema del software del host, ARPA convocó un encuentro entre investigadores, la mayor parte estudiantes de graduado. Los estudiantes esperaban encontrar a algún experto en redes para que les explicase el diseño de las mismas y de su software, para después asignar a cada uno una parte del trabajo. La realidad es que no hubo ningún experto, y ellos mismos tuvieron que hacer todo el trabajo.

Sin embargo, una primera red experimental comenzó a funcionar a finales de 1969 con cuatro nodos: UCLA, UCSB, SRI y UTAH. Se eligieron estas cuatro universidades por el número de contratos que ya tenían con ARPA, y además porque sus ordenadores de proceso eran totalmente incompatibles entre sí. La red creció rápidamente y se añadieron más IMP. En menos de tres años estaba extendida por todo Estados Unidos.

Posteriormente, el software de los IMP se modificó para permitir la conexión de terminales a los IMP, sin necesidad de un host intermedio. A este tipo de IMP se les denominó TIP (Terminal Interfaz Processor). También se permitió la conexión de varios
hosts a un mismo IMP para ahorrar dinero, la conexión de un host a varios IMP para aumentar la seguridad y la separación entre host e IMP.

Para favorecer la difusión de ARPANET, ARPA también financió la investigación sobre redes vía satélite y redes vía radio. Llegado este punto, se concluyó que los protocolos de que se disponían no eran los más adecuados para enfrentarse a redes heterogéneas. Como consecuencia se buscaron nuevos protocolos, lo que culminó con la propuesta en 1974 de TCP/IP por parte de Cerf y Kahn. TCP/IP estaba específicamente concebido para la comunicación entre diversos tipos de redes. Esto favoreció que nuevas redes se incorporasen a ARPANET.

Para facilitar la difusión de estos protocolos ARPA financió a BBN y la Universidad de California en Berkeley para que los integrasen en el Unix de Berkeley. Se crearon así los sockets, como interfaz del sistema con la red, y escribieron muchas aplicaciones, utilidades y programas de administración para facilitar su uso.

El momento fue el idóneo, coincidió con la compra de nuevos VAX en muchas universidades y redes locales para interconectarlos, pero no tenían el software. La aparición de Unix BSD 4.2 fue providencial, y su uso se generalizó rápidamente. Es más con TCP/IP era fácil conectar la LAN a ARPANET. La expansión de la red hizo necesario crear un nuevo protocolo para organizar las máquinas en dominios y mapear los nombres de las máquinas con sus direcciones IP. El nuevo protocolo fue DNS (Domain Naming System).

4.2.- Nfsnet.

A finales de los 70, NSF (la Fundación Nacional para la Ciencia de Estados Unidos) se fijó en el enorme impacto que ARPANET estaba teniendo sobre la investigación universitaria, permitiendo que investigadores de todo el país compartiesen datos y colaborasen en proyectos de investigación. Sin embargo, para conectarse a ARPANET, la universidad debía tener algún contrato de investigación con el Departamento de Defensa.

Esta dificultad para el acceso a ARPANET llevó a NSF a crear una red virtual, llamada
CSNET (Red de Ciencias de la Computación) entorno a una máquina de BBN que tenía líneas módem y conexiones a ARPANET. Usando CSNET, los investigadores podían llamar y dejar correo electrónico para que otros los leyesen más tarde. Era simple, pero funcionaba.

Hacia 1984 NSF comenzó el diseño de una red de alta velocidad que sucediese a ARPANET, y estuviese abierta a todos los grupos de investigación universitarios. Para comenzar, NSF estableció una red base que conectase sus seis centros de supercomputación. El software sobre el que corrían las comunicaciones fue TCP/IP desde el comienzo.

NSF financió la creación de diversas redes regionales conectadas a NSFNET y constituyó la base para intercomunicar universidades, centros de investigación, bibliotecas y museos. NSFNET tenía también conexiones con ARPANET. El éxito fue inmediato.

A medida que la red fue creciendo, NSF se dio cuenta de que no podría seguir financiando el servicio para siempre. Además, existían empresas que deseaban conectarse a NSFNET pero lo tenían prohibido debido las restricciones impuestas por NSF. De esta forma, NSF animó a MERIT, MCI e IBM a formar una corporación sin ánimo de lucro, ANS, como paso intermedio hacia la comercialización de la red. En 1990, ANS se hizo cargo de NSFNET y actualizó los enlaces de 1.5 Mbps a 45 Mbps formando ANSNET.

En 1991, el Congreso de Estados Unidos autorizó la financiación de NREN, el sucesor de NSFNET para la investigación, para su funcionamiento a velocidades de Gigabits. El objetivo es tener una red nacional a 3 Gbps antes del próximo siglo. Es un prototipo de la pretendida superautopista de la información.

4.3.- Usenet.

Cuando apareció el Unix por primera vez, y se utilizó ampliamente en los laboratorios Bell, los investigadores descubrieron que necesitaban una forma de copiar archivos de un sistema Unix a otro. Para resolver este problema, escribieron el ***uucp*** (Unix to Unix Copy). A medida que los sistemas Unix adquirieron módems de llamada automática, fue posible copiar archivos entre máquinas distantes, mediante el programa uucp, de forma automática. Vino el surgimiento de redes informales, en las que una máquina central con un marcador telefónico automático se encargaba de llamar a un grupo de máquinas, durante la noche, para acceder y transferir archivos y correo electrónico entre ellas. Dos máquinas que tuviesen módems, pero sin llamada automática, podían comunicarse al hacer que la máquina central llamara a la primera, cargase los archivos ycorreo pendientes, y luego llamase al destino para descargarlos.

Estas redes crecieron muy rápido debido a que todo lo que se necesitaba para que uno se uniera a la red, era el sistema UNIX con un modem, algo que prácticamente cualquier departamento de ciencias de la computación tenía. Estas redes, se unieron para formar una sola red que se denominó UUCP, constituida por aproximadamente 10.000 máquinas y un millón de usuarios.

La rama europea correspondiente se denominó EUNET y disponía de una estructura más organizada. Cada país europeo tenía una sola máquina de entrada operada por un único administrador. Los administradores mantienen un contacto permanente para administrar el tráfico de la red. Todo el tráfico internacional circula entre los puntos de entrada de los diferentes países. La conexión con Estados Unidos se hacía a través de un enlace entre Amsterdam y Virginia. También existían ramas en Japón, Corea, Australia y otros países.

El único servicio que ésta red ofrecía era el correo electrónico, pero una red similar llamada USENET, que se creó entre las universidades de Duke y Carolina del Norte, ofrecía un servicio de noticias. En la práctica todas las máquinas de EUNET y UUNET disponen de ambos servicios, por ello, se suele utilizar el nombre de USENET para referirse a todas ellas.

En el servicio de ***news***, se establecen infinidad de grupos de noticias a los que puede subscribirse cualquier usuario. Algunos grupos son de tipo técnico, aunque otros están relacionados con hobbies, política, ... Cada usuario puede poner mensajes en los grupos a los que está subscrito y leer los enviados por los demás. Estos mensajes se copian mediante uucp y se distribuyen a todas las máquinas que actúan como servidores.

4.4.- El nacimiento de Internet.

El número de redes, máquinas y usuarios conectados a ARPANET creció rápidamente después de que TCP/IP se convirtiese en el protocolo "oficial". Cuando NSFNET y ARPANET se interconectaron, el crecimiento se hizo exponencial. Hacia mediados de los 80, se comenzó a ver todo este conjunto de redes y subredes como la Internet, aunque no hubo ningún acto oficial que inmortalizase el momento.

El crecimiento ha seguido siendo exponencial, y hacia 1990 Internet contaba ya con 3000 redes y 200.000 ordenadores conectados. En 1992, se llegó al millón de hosts. En 1994 se estimó que el número de hosts se duplicaba cada año. El pegamento que une todas estas redes es el modelo de referencia TCP/IP junto con sus protocolos.

Pero, ¿qué significa estar en Internet?. Podemos considerar que una máquina está en Internet si ejecuta los protocolos del modelo TCP/IP, tiene una dirección IP, y la capacidad de enviar paquetes IP a otras máquinas que tienen las mismas características. El concepto queda oscurecido por el hecho de que muchos ordenadores personales tienen la capacidad de conectarse a servicios de Internet a través de un intermediario mediante el uso del modem.

Con la expansión sufrida, no es posible administrar la red con el estilo informal con que se hacía. En 1992, se fundó la **Internet Society** para promover el uso de Internet e incluso poder hacerse cargo de su administración.

Las cuatro aplicaciones básicas de Internet son:

1. ***Correo electrónico.***

2. ***Servicio de Noticias (news).***
3. ***Login remoto:*** Telnet, ssh, rlogin…
4. ***Transferencia de ficheros (ftp).***

Hasta comienzos de los 90, Internet era usada fundamentalmente por las universidades, organismos gubernamentales y algunas compañías con fuertes departamentos de investigación. La aparición de una nueva aplicación, el ***World Wide Web*** lo cambió todo y atrajo a millones de usuarios. Esta aplicación desarrollada en el CERN, consistia en un programa para interfaz gráfica y se denominó Mosaic. En sí no cambiaba los servicios básicos, sino que simplemente facilitaba su uso sin más que usar el ratón. Luego llegó la lucha de los Navegadores de Internet, Internet Explorer, Netscape, Mozilla, Opera, etc, ero eso ya es otra historia…

4.5.- Novell Netware.

Es la red local para ordenadores personales más extendida del mundo. Se diseñó para su uso en compañías que sustituían sistemas basados en mainframes por grupos de ordenadores personales. Cada usuario posee un PC que hace las veces de cliente de otros más potentes, que actúan como servidores de ficheros, de bases de datos, ofrecen colas de impresión, etc.

NetWare usa una arquitectura de red propia, basada en el antiguo sistema XNS de Xerox. Esta arquitectura, anterior a OSI, es más parecida a TCP/IP. De hecho, consta de 5 capas, con funciones similares a los de TCP/IP, pero el conjunto de protocolos es distinto.

Las capas física y de enlace se pueden elegir de entre varios estándares como Ethernet, TokenRing o ARCnet. Sobre ellos, define un nivel de red en el que usa el protocolo IPX que proporciona un servicio sin conexión no fiable. Su funcionalidad es muy similar a IP.

Sobre IPX, en la capa de transporte se dispone de un protocolo orientado a conexión y libre de errores, llamado NCP y que es el núcleo fundamental de NetWare. Hay otro protocolo que sólo proporciona servicios de datagramas, que es el SPX. Otra posible opción es el uso de TCP. Cada aplicación de la capa superior (transferencia de ficheros, anuncio de servidor, correo, ...) puede elegir el servicio de transporte que desea utilizar.

5.- Estándares y Agencias de Normalización.

Existen muchos fabricantes y suministradores de redes de ordenadores, cada uno con sus propias ideas sobre como deben funcionar las comunicaciones entre ordenadores. Por ejemplo, IBM tenía más de una docena de protocolos propios. Esta situación hacía que fuese difícil construir redes de ordenadores si éstos pertenecían a distintos fabricantes.

El caos generado por esta situación dio lugar a la exigencia de que se estableciesen normas. El objeto de la normalización no solo era facilitar la interconexión de equipos diferentes, sino lograr un incremento del mercado para aquellos productos que se acogiesen a la norma, lo que conduciría a una economía de escala que permitiría la reducción de costes y con ello un mercado aún mayor.

Las normas se dividen en dos categorías que pueden definirse como: de facto y de jure. Las normas ***De Facto***, son aquellas que se han establecido sin ningún planeamiento formal. Por ejemplo, las normas IBM-PC y sus sucesoras son normas de hecho porque docenas de fabricantes decidieron copiar fielmente las máquinas que IBM sacó al mercado.

Por el contrario, las normas ***De Jure*** (de derecho), son normas formales, adoptadas por un organismo que se encarga de su normalización. Las autoridades internacionales encargadas de la normalización se dividen, por lo general, en dos clases: la establecida por convenio entre gobiernos nacionales, y la establecida voluntariamente sin un tratado entre organizaciones. En el área de normas de redes de ordenadores, existen dos organizaciones principales, de cada uno de los dos tipos.

Las normalizaciones tienen las siguientes ventajas:

- Las normalizaciones aseguran un gran mercado. Se estimula la producción masiva y en algunos casos la utilización de alta y muy alta escala de integración lo que reduce mucho los costos.
- Un estándar permite que productos de diferentes suministradores se comuniquen entre sí, dotando al comprador de mayor flexibilidad en la selección y uso de los equipamientos.

Pero por otro lado tienen las siguientes desventajas:

- Los estándares tienden a congelar la tecnología. Mientras un estándar se desarrolla, se revisa y se adopta, se habrán desarrollado otras técnicas más eficaces.
- Hay varios estándares para la misma función. Recientemente, las organizaciones dedicadas a desarrollar estándares han comenzado a cooperar más estrechamente para que esto no suceda.

5.1.- Organizaciones de Estándarización en Comunicaciones.

El status legal de las compañías telefónicas en el mundo varía considerablemente de un país a otro. En un extremo está Estados Unidos que tiene unas 1500 compañías distintas, todas ellas privadas. Antes de su fragmentación en 1984, AT&T era la mayor de estas compañías, prestando servicio al 80 % de la población de Estados Unidos y cubriendo más de la mitad de su área geográfica. Las demás compañías daban servicio al resto de usuarios, principalmente en áreas rurales. En el otro extremo, están los países en los que el gobierno detenta un monopolio sobre las comunicaciones, como suele suceder en muchos países europeos.

Es clara la necesidad de que los servicios de comunicación sean compatibles a escala mundial, para asegurar que la gente (y los ordenadores) de un país pueden comunicarse con los de otro país diferente. Esta coordinación la ofrece una agencia de las Naciones Unidas llamada, ***UIT*** (Unión Internacional de Telecomunicaciones). La UIT tiene tres órganos principales, dos de ellos se ocupan sobre todo de la difusión internacional de radio y el otro está fundamentalmente relacionado con sistemas telefónicos y de comunicaciones de datos.

A este último grupo se le conoce como ***UIT-T*** o ***CCITT*** (Comité Consultivo Internacional Telegráfico y Telefónico). El CCITT tiene cinco clases de miembros:

- Miembros A, que son las compañías telefónicas nacionales, o los ministerios de telecomunicaciones.
- Miembros B, que son los reconocidos como administraciones privadas (por ejemplo AT&T).
- Miembros C, que son las organizaciones científicas e industriales.
- Miembros D, que corresponden a otras organizaciones internacionales.
- Miembros E, que corresponden a aquellas organizaciones cuya misión fundamental está en otro campo, pero que están interesadas en el trabajo de la CCITT.

La tarea del CCITT consiste en promover las recomendaciones técnicas sobre aspectos telefónicos, telegráficos e interfaces de comunicación de datos. Esta labor ha producido normas que tienen un reconocimiento internacional como por ejemplo la norma V.24 (EIA RS-232 en Estados Unidos), y la norma X.25 que especifica la interfaz entre un ordenador y una red de ordenadores (conmutación de paquetes).

5.2.- Agencias de Normalización Internacionales.

Las normas internacionales son producidas por la ***ISO*** (International Standards Organization), que es una organización voluntaria, fuera de tratados y fundada en 1946, cuyos miembros son las organizaciones nacionales de normalización correspondientes a los 89 países miembros, y otros 85 organismos.

La ISO emite normas en una gama amplia de temas, que van desde las tuercas y los tornillos, hasta los recubrimientos de los postes telefónicos. La ISO tiene casi 200 comités técnicos (TC), cuyo orden de numeración se base en el momento de su creación, ocupándose cada uno de ellos de un tema específico. Por ejemplo, TC1 está relacionado con temas relativos a tuercas y tornillos, mientras que el TC 97 está relacionado con ordenadores y procesamiento de información. Cada uno de los TC tiene subcomités (SC), los cuales se dividen a su vez en grupos de trabajo (WG).

Los WG, constituidos por unos 100.000 voluntarios distribuidos en todo el mundo, son los que realizan el trabajo. Varios de estos "voluntarios" son por lo general asignados por las propias compañías, representantes de gobiernos nacionales o expertos provenientes del mundo académico.

La ISO y el CCITT algunas veces cooperan (de hecho, ISO es un miembro de clase D del CCITT), con respecto a la emisión de normas sobre telecomunicaciones, con objeto de evitar el absurdo de dos normas internacionales oficiales, mutuamente incompatibles.

El procedimiento que utiliza la ISO para el establecimiento de normas, está diseñado para conseguir el mayor consenso posible. El proceso comienza cuando alguna de las organizaciones nacionales considera necesario el establecimiento de una norma internacional. Entonces, se forma un grupo de trabajo que llega a plantear una propuesta de trabajo (DP). Una vez que se genera la DP se hace circular entre todos los miembros, los cuales cuentan con seis meses, a partir de ese momento, para plantear sus comentarios y críticas. Si una mayoría significativa aprueba la propuesta, se produce un documento revisado, denominado DIS (Anteproyecto de Norma Internacional), el cual se hace circular nuevamente con objeto de tener más comentarios y realizar una votación al respecto. Con base en los resultados de esta vocación, se prepara, aprueba y publica el testo final de la IS (norma internacional). En algunas de las áreas, en donde existe una gran polémica, la DP o DIS probablemente tenga que pasar por varias versiones, en su planteamiento, antes de adquirir el número de votos necesarios para su aprobación. El proceso completo puede llevar varios años.

Existen otros organismos que también establecen normas a distintos niveles. Por ejemplo ***NIST*** (National Institute of Standards and Technology) de Estados Unidos se encarga de establecer normas de obligado cumplimiento para las adquisiciones que realiza el gobierno de Estados Unidos, con excepción de las que realiza directamente el ministerio de Defensa, que tiene sus propias normas (normas MIL).

Otro participante importante en el mundo de las normas es el ***IEEE***, que es la organización profesional más grande del mundo. Esta institución, además de publicar numerosas revistas y programar un número muy importante de conferencias anuales, ha establecido un grupo dedicado al desarrollo de normas en el área de ingeniería eléctrica y computación. La norma 802 del IEEE, para una red de área local, es la norma clave para el desarrollo de las LAN. Posteriormente, fue adoptada por la ISO como base para la norma ISO 8802.

Otras organizaciones con normas importantes son las siguientes, todas norteamericanas de nivel nacional: **ANSI** (Instituto Nacional Americano de Normalización) **EIA** (Asociación de industrias electrónicas) y **TIA** (Asociación de industrias de telecomunicaciones)

5.3.- Normas sobre Internet.

Internet tiene sus propios mecanismos de estandarización, diferentes de los del CCITT y la ISO. De forma sencilla, podemos decir que los participantes en los encuentros de UIT o de la ISO llevan trajes. Las personas que llegan a las reuniones para estandarización de Internet llevan vaqueros o uniformes militares.

UIT-T e ISO están pobladas por funcionarios y representantes de las grandes empresas que han hecho de la estandarización su trabajo. Por el contrario, la gente relacionada con Internet busca un acuerdo para que las cosas funcionen, pero sin que sea un fin en sí mismo.

Cuando se creo ARPANET, el departamento de defensa creó un comité informal para su desarrollo. En 1983, el comité se renombró y se denominó ***IAB*** (Internet Activities Board). Recibió una serie de encargos adicionales cuyo objetivo básico era lograr que los investigadores involucrados en ARPANET e Internet avancen en la misma dirección. Posteriormente, el acrónimo "IAB" se cambió por Internet Architecture Board. Actualemte el IAB está gobernado por la ISOC, una ONG sin ánimo de lucro en la que puede participar cualquiera sin más que aportar una cuota.

Cada uno de los diez miembros del IAB encabeza un grupo de trabajo (task force) sobre algún aspecto de especial relevancia. El IAB tiene varias reuniones al año para discutir resultados y comunicarlos al ministerio de Defensa y al NSF. Cuando se necesita un standard, el IAB elabora el nuevo standard y lo distribuye para que se elaboren distintas implementaciones. Las comunicaciones se realizan en forma de ***RFC*** (Request For Comments). Las RFC se encuentran disponibles a través de la red y pueden ser consultadas por cualquiera. Su numeración sigue un estricto orden cronológico y en la actualidad es de unas 2000.

Con la difusión de Internet, esta forma de trabajo no era efectiva. En 1989, el IAB se reorganizó de nuevo. Los investigadores formaron el ***IRTF*** (Internet Research Task Force), y al ***IETF*** (Internet Engineering Task Force), ambos dependientes del IAB. El IAB se amplió para incluir representantes de otras organizaciones. El IRTF se debe hacer cargo de la investigación a largo plazo, mientras que el IETF debe resolver los problemas técnicos a corto plazo.

Otra entidad relevante en internet es la **ICANN** que es responsable de la asignación de direcciones IP y la preservación de los nombres de dominio. Antes esta labor recaía en la IANA que era gubernamental.

RESUMEN

Definiciones: Arquitectura de red, sistema abierto, protocolo, capa, SAP, LAN, MAN, WAN, SAN, VPN(y subtipos), NIC, PDU(y sus nombres por nivel), DTE, DCE y NIC.
Diferencias LAN-WAN
Pila OSI: funciones de cada nivel.
Pila TCP/IP: diferencias con OSI.
Ventajas/desventajas de las normalizaciones.
Organismos importantes: ISO,ITU-T,IEEE, ANSI, EIA, TIA, IETF (con los RFCs).