Unidad de trabajo 2

Conceptos Básicos de Redes e Internet

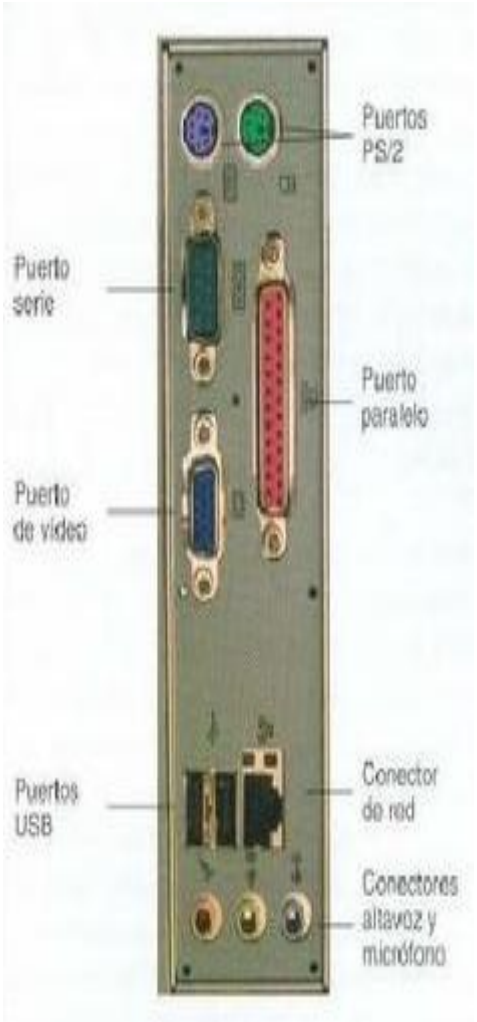
Contenido

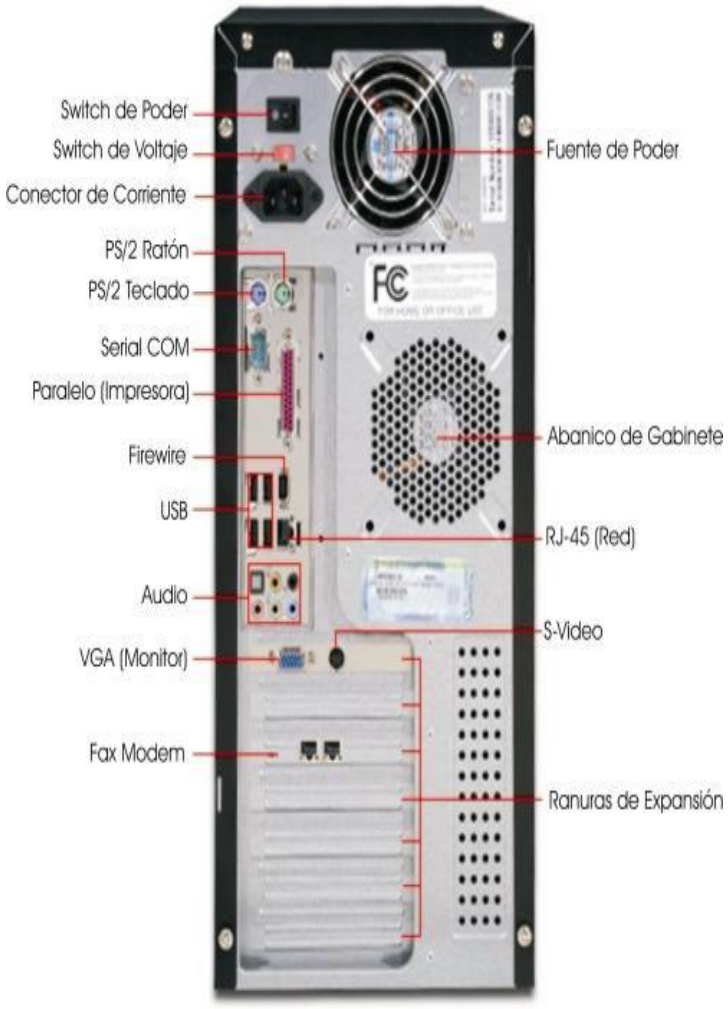
1. Definiciones previas

1.1. QUÉ ES UN PUERTO

En la informática, un**puerto**es una forma genérica de denominar a unainterfaza través de la cual los diferentes tipos dedatosse pueden enviar y recibir. Dicha interfaz puede ser de **tipo físico**, o puede ser a nivel desoftware(por ejemplo, los puertos que permiten la transmisión de datos entre diferentesordenadores), en cuyo caso se usa frecuentemente el término **puerto lógico**.

Un puerto es una conexión o un enchufe -los físicos- el cual es utilizado para conectar dispositivo de Hardware como impresoras o Mouse, permitiendo el intercambio de datos con otro dispositivo. Dicho de otra forma todo puerto es una interface o medio de acceso de un punto a otro.





Los **puertos físicos** más comunes son:

1. Puertos Serie: Sólo pueden transmitir un dato a la vez, por lo que son lentos y se utilizan para módems externos, ratones, etc.
2. Puertos Paralelo: Son más rápidos que los puertos serie (donde 8 bits de datos, forman un byte, y se envían simultáneamente sobre ocho líneas individuales en un solo cable.) Suelen utilizarse para conectar escáner e impresora.
3. Puertos USB (Universal Serial Bus): Creado a principio de 1996. La velocidad de transferencia muy alta, y además permiten conectar y desconectarlos sin necesidad de apagar el ordenador. Hay dos tipos diferenciados por la velocidad: USB 1 y USB 2.
4. Puertos Firewire: Similares a los USB 2, un poco más rápidos. Suelen utilizarse en videocámaras digitales.
5. Puerto RCA es un tipo de conector eléctrico común en el mercado audiovisual.
6. Conector de Video VGA: El equipo utiliza un conector D subminiatura de alta densidad de 15 patas en el panel posterior para conectar al equipo un monitor compatible con el estándar VGA (Video GraphicsArry).
7. Puertos RJ-11: Es un conector utilizado por lo general en los sistemas telefónicos y es el que se utiliza para conectar el MODEM a la línea telefónica de manera que las computadoras puedan tener acceso a Internet.
8. Puertos RJ-45: Es una interfaz física utilizada comúnmente en las redes de computadoras, sus siglas corresponden a "Registered Jack" o "Clavija Registrada".
9. PCI (PeripheralComponentInterconnect) son ranuras de expansión de la placa madre de un ordenador en las que se pueden conectar tarjetas de sonido, de vídeo, de red, etc.
10. PCI-Express: Nuevas mejoras para la especificación PCIe 3.0 que incluye una cantidad de optimizaciones para aumentar la señal y la integridad de los datos, incluyendo control de transmisión y recepción de archivos.
11. Puertos de Memoria: A estos puertos se conectan las tarjetas de memoria RAM. Los puertos de memoria son aquellos puertos, o bahías, donde se pueden insertar nuevas tarjetas de memoria, con la finalidad de extender la capacidad de la misma;

12. Puertos Inalámbricos: Las conexiones en este tipo de puertos se hacen, sin necesidad de cables, a través de la conexión entre un emisor y un receptor utilizando ondas electromagnéticas (infrarrojos, bluetooth).

Puertos Lógicos.

ElPuerto Lógicoes una zona, o localización, de la memoria de un ordenador que se asocia con un puerto físico o con un canal de comunicación, y que proporciona un espacio para el almacenamiento temporal de la información que se va a transferir entre la localización de memoria y el canal de comunicación.

Los puertos lógicos son, al igual que los puertos físicos, necesarios para que nuestros programas puedan comunicarse con el exterior. La diferencia es que se enlazan virtualmente con los programas, para tener una referencia, y que los otros programas puedan conectarse a los nuestros y traspasar información.

- ✓ Los puertos de 1 a 1024 se llaman **puertos reservados**. Tienen una función específica que mandan los estándares. La organización que se encarga de establecer los estándares es la IANA (Internet AssignedNumbersAuthority), que se puede encontrar en www.iana.org. Por ejemplo:
  - ✓ HTTP puerto 80 transferencia de hipertexto por Internet
  - ✓ FTP puerto 20 transferencia de datos
  - ✓ HTTPS puerto 443 transferencia segura
  - ✓ SMTP puerto 25 correo electrónico
- ✓ Los puertos 1024 a 49.151 son **puertos registrados**, no son estándar, pero la IANA se encarga de asignarlos a distintas aplicaciones, que lo necesitan.
- ✓ Los puertos 49.152 a 65.535 son **puertos efímeros** y son utilizados como puertos temporales, sobre todo por los clientes (el navegador, el cliente de correo, el cliente de FTP) que los eligen aleatoriamente para establecer desde ellos la conexión a los puertos servidores y, si la conexión cae, se liberan y pueden ser usados por cualquier otra aplicación o protocolo más tarde.

1.2. ¿QUÉ ES UN DATAGRAMA?

Un datagrama es un fragmento de paquete (análogo a un telegrama) que es enviado con la suficiente información para que la red pueda simplemente encaminar el fragmento

hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes.

Los datagramas también son la agrupación lógica de información que se envía como una unidad de capa de red a través de un medio de transmisión sin establecer con anterioridad un circuito virtual. **Los datagramas IP son las unidades principales de información de Internet.**

1.3. ¿QUÉ ES NAT?

NAT (**Network AddressTranslation** - **Traducción de Dirección de Red**) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

Dos de los principales problemas que posee Internet son la escasez de direcciones IP y el creciente tamaño de las tablas de rutas. La facilidad NAT (Network AddressTranslation) permite a la red IP de una empresa aparentar, de cara al resto de redes IP, que está usando un espacio de direccionamiento distinto al que internamente está usando. Por tanto NAT permite a una empresa que utiliza direcciones privadas (direcciones locales), y que por tanto no son accesibles por tabla de rutas de Internet, conectarse a Internet **al convertir dichas direcciones privadas en públicas** (direcciones globales) que sí son accesibles desde Internet. NAT está descrito en la RFC 1631.

NAT tiene diversas aplicaciones, siendo algunas:

- Se quiere tener conectividad con Internet, pero no todos los equipos poseen direcciones IP globales (permitidas). En este caso se configura un router NAT como enlace entre el dominio privado (red local) y el dominio público (red pública: en este caso Internet). El router NAT traduce las direcciones locales en direcciones globales antes de enviar los paquetes al exterior.
- Una empresa requiere conectividad IP entre oficinas remotas. Dichas oficinas remotas posee redes IP internas que no cumplen con un plan de direccionamiento con lo que las tablas de rutas para lograr conectividad entre ellas es grande o imposible. En este caso sería suficiente con configurar NAT en los routers frontera de cada oficina, realizar así la transformación entre las redes internas de las oficinas a redes globales, que ahora sí cumplen con el plan de direccionamiento.

- Se necesitan cambiar la direcciones internas de muchos equipos. En lugar de realizar dicho cambio que sería muy costoso en tiempo se podría realizar NAT.

http://www.lab.dit.upm.es/~labrst/config/manuales-teldat/Dm720v10-5_Protocolo_NAT.pdf

1.4. REDES DE ORDENADORES.

Una **red de ordenadores** o **red informática**, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos con la finalidad de compartir información y recursos.

2. ¿QUÉ ES UN PROTOCOLO?

En informática y telecomunicación, un protocolo de comunicaciones **es un conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen** entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos

El protocolo define, entre otros:

- ✓ El formato y orden de los mensajes a intercambiar.
- ✓ Las acciones a realizar en cada caso.

3. TIPOS DE REDES.

Las redes se clasifican según su alcance, el tipo de conexión, su relación funcional, su topología, la direccionalidad de los datos, su grado de autentificación, el de difusión, el servicio o la función que desempeñan.

En todas las redes de área local encontramos siempre un modo de transmisión / modulación (banda base o banda ancha), un protocolo de acceso (TDMA, CSMA/CD, TokenPassing, FDDI), un soporte físico (cables de pares trenzados, coaxiales o fibra óptica), una topología (bus, anillo, estrella), etc.

Por su alcance

- ✓ **Red de área personal** o *PAN*
- ✓ **Red de área local** o *LAN* es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión.
- ✓ **Red de área de campus** o *CAN* es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar.
- ✓ **Red de área metropolitana** es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa.
- ✓ **Red de área de almacenamiento**, en inglés *SAN* es una red concebida para conectar servidores, matrices de discos y librerías de soporte.
- ✓ **Red de área local virtual** (*Virtual LAN, VLAN*) es un grupo de computadoras con un conjunto común de recursos a compartir.

Por tipo de conexión

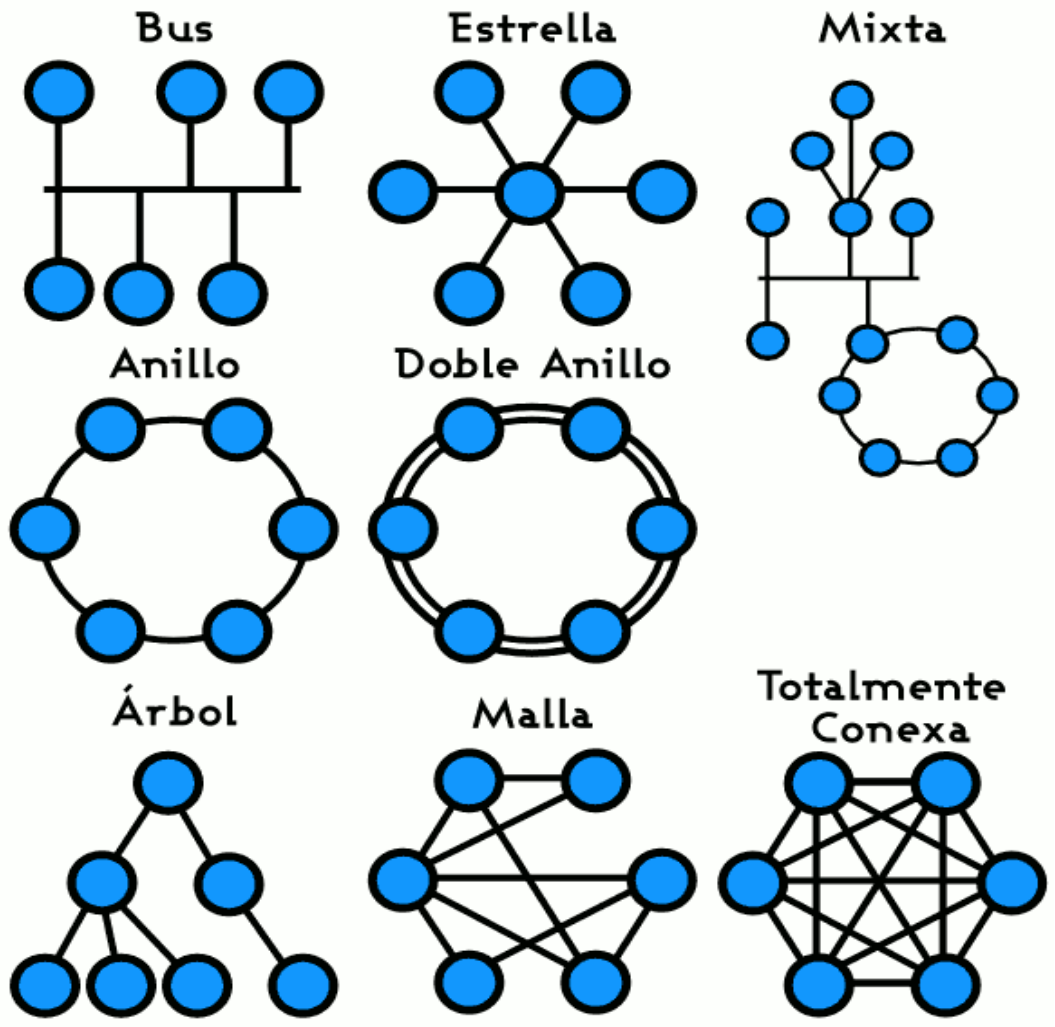
- ✓ **Medios guiados**
  - El cable **coaxial** se utiliza para transportar señales eléctricas de alta frecuencia.
  - El cable de **par trenzado** es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia.
  - La **fibra óptica** es un medio de transmisión empleado habitualmente en redes de datos se compone de un hilo muy fino de material transparente por el que se envían pulsos de luz que representan los datos a transmitir.
- ✓ **Medios no guiados**
  - Red por **radio**
  - Red por **infrarrojos**
  - Red por **microondas**

Por su relación funcional

- ✓ **Cliente-servidor** consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.
- ✓ **Peer-to-peer** (entre iguales, entre pares o punto a punto) todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

Por topología

- ✓ **Red en bus**: se caracteriza por tener un único canal de comunicaciones al cual se conectan los diferentes dispositivos.
- ✓ **Red en anillo**: cada estación está conectada a la siguiente y la última está conectada a la primera.
- ✓ **Red en estrella**: las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.
- ✓ **Red en malla**: cada nodo está conectado a los otros.
- ✓ **Red en árbol**: la conexión es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central.
- ✓ **Red mixta**: se mezclan cualquiera de las anteriores.



Por la direccionalidad de los datos

- ✓ **Unidireccional**: un Equipo Terminal de Datos transmite y otro recibe.
- ✓ **Half-Duplex o Bidireccional**: sólo un equipo transmite a la vez.
- ✓ **Full-Duplex:** ambos pueden transmitir y recibir a la vez una misma información.

Por grado de autentificación

- ✓ **Red Privada**: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.
- ✓ **Red de acceso público:** una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal.

Por su grado de difusión

- ✓ **Intranet** es una red de computadoras que utiliza alguna tecnología de red para usos comerciales, educativos o de otra índole de forma privada, esto es, que no comparte sus recursos o su información con redes ilegítimas.
- ✓ **Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP.

Por el servicio o la función que desempeñan

- ✓ **Red comercial** proporciona soporte e información para una empresa u organización.
- ✓ **Red educativa** proporciona soporte e información para una organización educativa dentro del ámbito del aprendizaje.
- ✓ **Red para el proceso de datos** proporciona una interfaz para intercomunicar equipos que vayan a realizar una función de cómputo conjunta.

3.1 SERVICIOS DE RED E INTERNET

La finalidad de una red es que los usuarios de los sistemas informáticos de una organización puedan hacer un mejor uso de los mismos mejorando de este modo el rendimiento global de la organización Así las organizaciones obtienen una serie de ventajas del uso de las redes en sus entornos de trabajo, como pueden ser:

- ✓ Mayor facilidad de comunicación.

- ✓ Mejora de la competitividad.
- ✓ Mejora de la dinámica de grupo.
- ✓ Reducción del presupuesto para proceso de datos.
- ✓ Reducción de los costos de proceso por usuario.
- ✓ Mejoras en la administración de los programas.
- ✓ Mejoras en la integridad de los datos.
- ✓ Mejora en los tiempos de respuesta.
- ✓ Flexibilidad en el proceso de datos.
- ✓ Mayor variedad de programas.
- ✓ Mayor facilidad de uso. Mejor seguridad

4. Método de Acceso al Medio

El **método de acceso** se refiere al conjunto de reglas que definen la forma en que un equipo coloca los datos en la red y toma los datos del cable. Una vez que los datos se están moviendo en la red, los métodos de acceso ayudan a regular el flujo del tráfico de la red. También podemos definir el método de acceso al medio como la herramienta que se encarga de mediar entre el equipo y el entorno de red para la transmisión de información; a fin de que los datos lleguen al receptor justo como fueron enviados desde el emisor.

El acceso al medio no es un elemento independiente del resto de la tecnología que se utiliza en las redes de computadoras, muchas veces el método de acceso está condicionado a otros factores como la topología y la estructura física que se utilice.

Algunos métodos de acceso son:

- ✓ **CSMA. Acceso múltiple con detección de portadora y detección de colisiones.** Se basa en que cada estación monitoriza o "escucha" el medio para determinar si éste se encuentra disponible para que la estación puede enviar su mensaje, o por el contrario, hay algún otro nodo utilizándolo, en cuyo caso espera a que quede libre. Todos los otros nodos escucharán y el nodo seleccionado recibirá la información.

  En caso de que dos nodos traten de enviar datos por la red al mismo tiempo, cada nodo se dará cuenta de la colisión y esperará una cantidad de tiempo aleatoria antes de volver a hacer el envío. Cada paquete enviado contiene la dirección de la estación destino, la dirección de la estación de envío y una secuencia variable de bits que representa el mensaje transmitido.

- ✓ **Token**. En el método de acceso conocido como paso de testigo, circula por el cable del anillo equipo en equipo un paquete especial denominado testigo. Cuando un equipo del anillo necesita enviar datos a través de la red, tiene que esperar a un testigo libre. Cuando se detecta un testigo libre, el equipo se apodera de él si tiene datos que enviar y una vez haya terminado, volverá a dejar libre el testigo y lo enviará a la próxima estación.

5. Introducción a los modelos OSI y TCP/IP

Las primeras redes de ordenadores tuvieron unos inicios muy similares a los primeros ordenadores: las redes y los protocolos se diseñaban pensando en el hardware a utilizar en cada momento, sin tener en cuenta la evolución previsible, ni por supuesto la interconexión y compatibilidad con equipos de otros fabricantes.

A medida que la tecnología avanzaba y se mejoraba la red se vivieron experiencias parecidas a las de los primeros ordenadores: los programas de comunicaciones, que habían costado enormes esfuerzos de desarrollo, tenían que ser reescritos para utilizarlos con el nuevo hardware, y debido a la poca modularidad prácticamente nada del código era aprovechable.

El problema se resolvió de forma análoga a lo que se había hecho con los ordenadores. **Cada fabricante elaboró su propia arquitectura de red, que permitía independizar las funciones y el software del hardware concreto utilizado.** De esta forma cuando se quería cambiar algún componente sólo la función o el módulo afectado tenía que ser sustituido. La primera arquitectura de redes fue anunciada por IBM en 1974 y se denominó SNA (Systems Network Architecture).

La arquitectura SNA se basa en la definición de siete niveles o capas, cada una de las cuales ofrece una serie de servicios a la siguiente, la cual se apoya en esta para implementar los suyos, y así sucesivamente. Cada capa puede implementarse en hardware, software o una combinación de ambos. El módulo (hardware y/o software) que implementa una capa en un determinado elemento de la red debe poder sustituirse sin afectar al resto de la misma, siempre y cuando el protocolo utilizado se mantenga inalterado. Este modelo de capas ha sido la base de todas las arquitecturas de redes actualmente en uso.

Después de la especificación de SNA por parte de IBM cada fabricante importante definió su propia arquitectura de redes; así la evolución de los productos de comunicaciones estaba garantizada, pero **no** se había resuelto el problema de la **interoperabilidad** entre diferentes fabricantes. Debido a la posición de hegemonía que

IBM disfrutaba en los años 70 y principios de los 80 la compatibilidad con IBM era un requisito necesario, por lo que la mayoría de los fabricantes tenían implementaciones de los protocolos SNA para sus productos, o estas estaban disponibles a través de terceros. Así, la forma más sencilla de interconectar dos equipos cualesquiera era conseguir que ambos hablaran SNA.

6. MODELO OSI (Interconexión de sistemas abiertos)

En 1977 la ISO (International OrganizationforStandardization) consideró que esta situación no era la más conveniente, por lo que entre 1977 y 1983 definió la arquitectura de redes OSI con el fin de promover la creación de una serie de estándares que especificaran un conjunto de protocolos independientes de cualquier fabricante.

Se pretendía con ello no favorecer a ninguna empresa a la hora de desarrollar implementaciones de los protocolos, cosa que inevitablemente habría ocurrido si se hubiera adoptado alguna de las arquitecturas existentes, como la SNA de IBM o la DNA (Digital Network Architecture) de Digital. Se esperaba llegar a convertir los protocolos OSI en el auténtico Esperanto de las redes telemáticas. Por diversas razones el éxito de los protocolos OSI en la práctica ha sido mucho menor de lo inicialmente previsto.

Seguramente la aportación más importante de la iniciativa OSI ha sido precisamente su arquitectura. Ésta ha servido como marco de referencia para describir multitud de redes correspondientes a diversas arquitecturas, su generalidad y no dependencia de ningún fabricante en particular, la hacen especialmente adecuada para estos fines.

https://www.youtube.com/watch?v=gmFv4ZD_h4w

https://www.youtube.com/watch?v=naPcsq3nFtg

https://www.youtube.com/watch?feature=player_detailpage&v=J4fyeLWeq-Q

1. La capa física:

La capa física tiene que ver con la **transmisión de bits** por un canal de comunicación. Las consideraciones de diseño pretenden asegurar que cuando en un extremo se envíe un bit 1, se reciba en el otro lado como bit 1, no como bit 0.

2. Capa de Enlace de Datos:

Se encarga del **direccionamiento físico** "MAC y LLC"de la red. Del **acceso al medio**, de la detección de errores, de la distribución ordenada de tramas y del control de flujo.

3. Capa de Red:

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. En este nivel se realiza el **direccionamiento lógico** y la determinación de la **ruta** de los datos hasta su receptor final.

4. Capa de Transporte:

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son:

- seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino,
- segmentación de datos y gestión de cada porción,
- reensamble de segmentos en flujos de datos de aplicación, e identificación de las diferentes aplicaciones.

Seguimiento de Conversaciones individuales

Cualquier host puede tener múltiples aplicaciones que se están comunicando a través de la red. Cada una de estas aplicaciones se comunicará con una o más aplicaciones en hosts remotos. Es responsabilidad de la capa de Transporte mantener los diversos streams de comunicación entre estas aplicaciones.

Segmentación de datos

Debido a que cada aplicación genera un stream de datos para enviar a una aplicación remota, estos datos deben prepararse para ser enviados por los medios en partes manejables. Los protocolos de la capa de Transporte describen los

servicios que segmentan estos datos de la capa de Aplicación. Esto incluye la encapsulación necesaria en cada sección de datos. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de Transporte para indicar la comunicación a la cual está asociada.

Reensamble de segmentos

En el host de recepción, cada sección de datos puede ser direccionada a la aplicación adecuada. Además, estas secciones de datos individuales también deben reconstruirse para generar un stream completo de datos que sea útil para la capa de Aplicación. Los protocolos de la capa de Transporte describen cómo se utiliza la información de encabezado de dicha capa para reensamblar las secciones de datos en streams y enviarlas a la capa de Aplicación.

Identificación de las aplicaciones

Para poder transferir los streams de datos a las aplicaciones adecuadas, la capa de Transporte debe identificar la aplicación de destino. Para lograr esto, la capa de Transporte asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador número de puerto. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en ese host. Este número de puerto se utiliza en el encabezado de la capa de Transporte para indicar con qué aplicación está asociada esa sección de datos.

La capa de Transporte es el enlace entre la capa de Aplicación y las capas inferiores, que son responsables de la transmisión en la red. Esta capa acepta datos de distintas conversaciones y los transfiere a las capas inferiores como secciones manejables que puedan ser eventualmente multiplexadas a través del medio.

Las aplicaciones no necesitan conocer los detalles de operación de la red en uso. Las aplicaciones generan datos que se envían desde una aplicación a otra sin tener en cuenta el tipo de host destino, el tipo de medios sobre los que los datos deben viajar, el paso tomado por los datos, la congestión en un enlace o el tamaño de la red.

Además, las capas inferiores no tienen conocimiento de que existen varias aplicaciones que envían datos en la red. Su responsabilidad es entregar los datos al dispositivo adecuado. Luego la capa de transporte ordena estas secciones antes de entregarlas a la aplicación adecuada.

5. Capa de Sesión:

Esta capa es la que se encarga de crear y mantener diálogos entre las aplicaciones de origen y destino, es decir, mantener y **controlar el enlace** establecido entre dos computadores que están transmitiendo datos de cualquier índole.

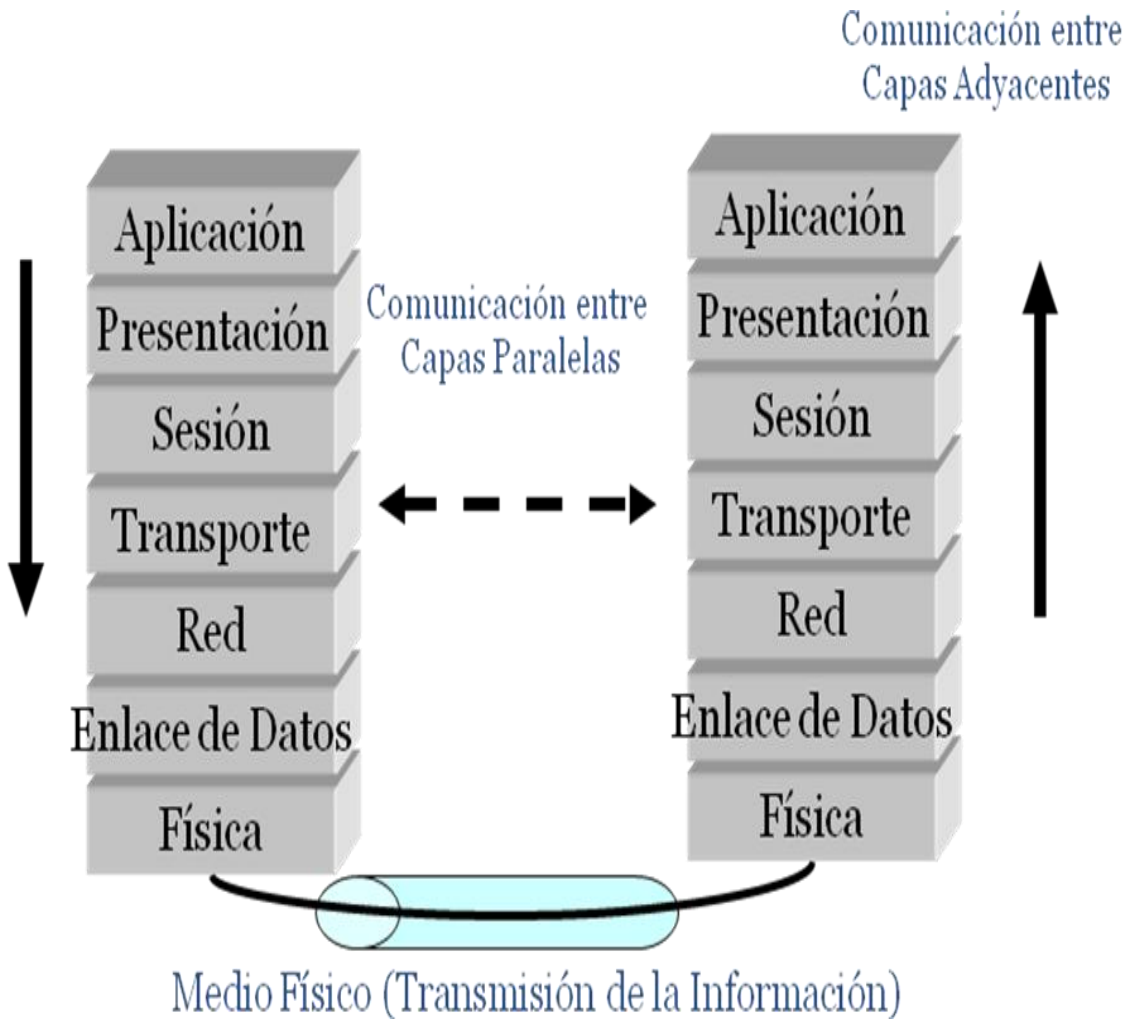
La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o desactivaron durante un periodo de tiempo prolongado.

6. Capa de Presentación:

El objetivo es encargarse de la **representación de la información**, de manera que aunque distintos equipos puedan usar diferentes formatos de representaciones interna los datos lleguen de manera reconocible.

7. Capa de Aplicación:

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos, servidor de ficheros, etc.



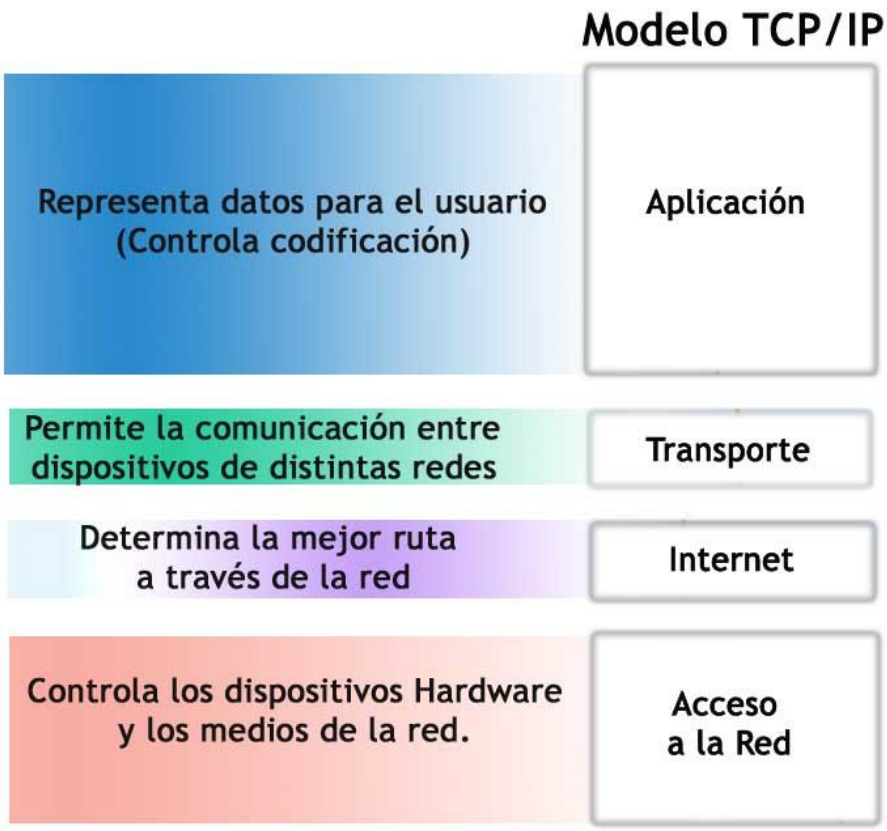
7. Capa de Aplicación	Aplicaciones de usuario
6. Capa de Presentación	Formato de datos común.
5. Capa de Sesión	Diálogos y conversaciones
4. Capa de Transporte	Calidad de servicio y confiabilidad.
3. Capa de Red	Selección de ruta, direccionamiento lógico y enrutamiento
2. Capa de Enlace de Datos	Direccionamiento físico. Tramas y control de acceso al medio
1. La capa física	Señales y medios

6.1 ARQUITECTURA TCP/IP. ARPANET

En 1969 la agencia **ARPA** (AdvancedResearchProjects Agency) del Departamento de Defensa de los Estados Unidos inició un proyecto de interconexión de ordenadores mediante redes telefónicas. Al ser un proyecto desarrollado por militares en plena guerra fría un principio básico de diseño era que la red debía poder resistir la destrucción de parte de su infraestructura (por ejemplo a causa de un ataque nuclear), de forma que dos nodos cualesquiera pudieran seguir comunicados siempre que hubiera alguna ruta que los uniera. Esto se consiguió en 1972 creando una red de conmutación de paquetes denominada **ARPAnet**, la primera de este tipo que operó en el mundo. La conmutación de paquetes unida al uso de topologías malladas mediante múltiples líneas punto a punto dio como resultado una red altamente fiable y robusta.

ARPAnet fue creciendo paulatinamente, y pronto se hicieron experimentos utilizando otros medios de transmisión de datos, en particular enlaces por radio y vía satélite; los protocolos existentes tuvieron problemas para interoperar con estas redes, por lo que se diseñó un nuevo conjunto o pila de protocolos, y con ellos una arquitectura. Este nuevo conjunto se denominó **TCP/IP** (**Transmission Control Protocol/Internet Protocol**), nombre que provenía de los dos protocolos más importantes que componían la pila; la

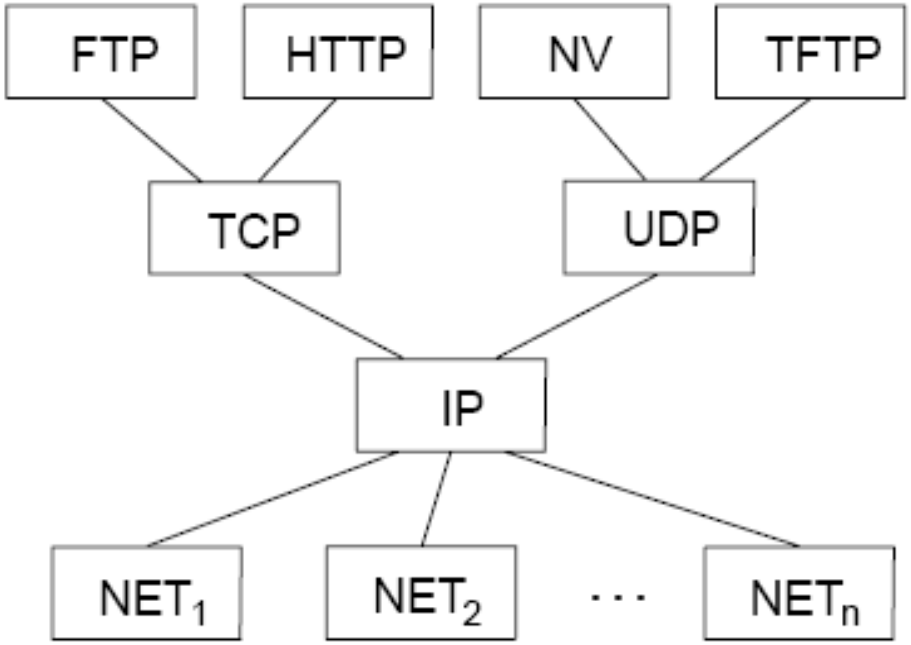
nueva arquitectura se llamó sencillamente modelo TCP/IP, los nuevos protocolos fueron especificados por vez primera por Cerf y Kahn en un artículo publicado en 1974. A la nueva red, que se creó como consecuencia de la fusión de ARPAnet con las redes basadas en otras tecnologías de transmisión, se la denominó Internet.



Mientras que en el caso de OSI se emplearon varios años en definir una arquitectura de capas donde la función y servicios de cada una estaban perfectamente definidas, y sólo después se planteó desarrollar los protocolos para cada una de ellas, en el caso de TCP/IP la operación fue a la inversa; primero se especificaron los protocolos, y luego se definió el modelo como una simple descripción de los protocolos ya existentes. Por este motivo el modelo TCP/IP es mucho más simple que el OSI. También por este motivo el modelo OSI se utiliza a menudo para describir otras arquitecturas, como por ejemplo TCP/IP, mientras que el modelo TCP/IP nunca suele emplearse para describir otras arquitecturas que no sean la suya propia.

El modelo TCP/IP ofrece la máxima flexibilidad, en la capa de aplicación, para los creadores de software.

TCP/IP es un conjunto de protocolos. En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos.



La capa host-red o de acceso a la red

Esta capa engloba realmente las funciones de la capa física y la capa de enlace del modelo OSI. El modelo TCP/IP dice que debe ser capaz de conectar el host a la red por medio de algún protocolo que permita enviar paquetes IP. Se podría afirmar que para el modelo TCP/IP esta capa se comporta como una 'caja negra'. Cuando surge una nueva tecnología de red (por ejemplo ATM) una de las primeras cosas que aparece es un estándar que especifica de que forma se pueden enviar sobre ella paquetes IP; a partir de ahí la capa internet ya puede utilizar esa tecnología de manera transparente.

Capa de red o capa de Internet

Esta capa define aquí un formato de paquete y un protocolo, llamado IP (Internet Protocol), que se considera el protocolo 'oficial' de la arquitectura, siendo el más popular de todos.

Su papel equivale al desempeñado por la capa de red en el modelo OSI, es decir, se ocupa de encaminar los paquetes de la forma más conveniente para que lleguen a su destino, y de evitar que se produzcan situaciones de congestión en los nodos intermedios. Debido a los requisitos de robustez impuestos en el diseño, la capa Internet da únicamente un servicio de conmutación de paquetes no orientado a conexión. Los paquetes pueden llegar desordenados a su destino, en cuyo caso es responsabilidad de las capas superiores en el nodo receptor la reordenación para que sean presentados al usuario de forma adecuada.

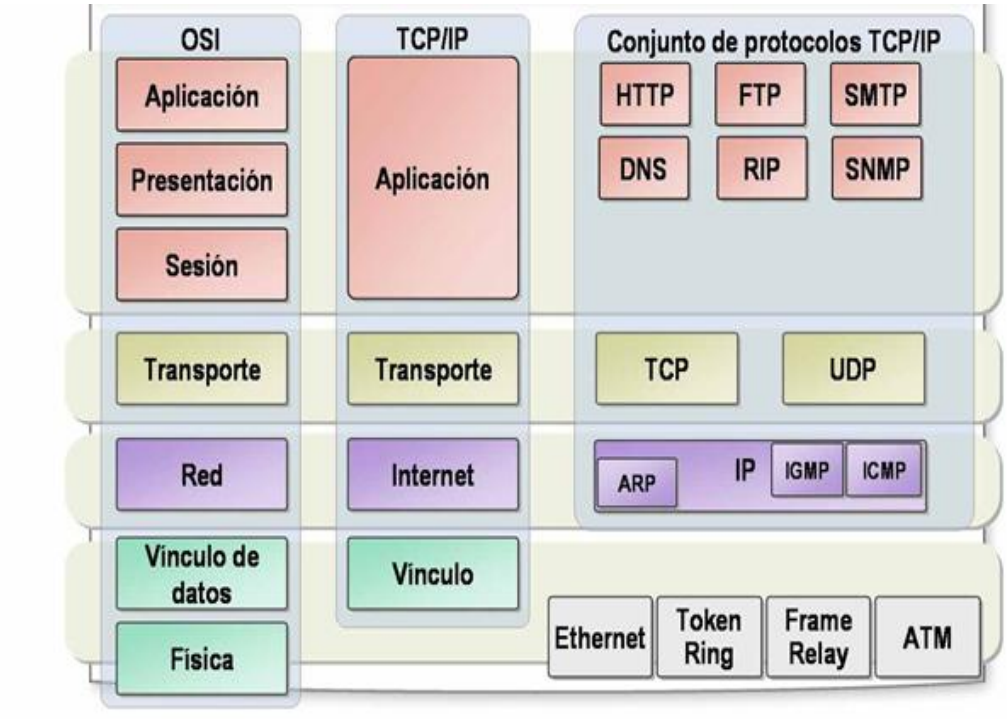
La capa de transporte

Esta capa recibe el mismo nombre y desarrolla la misma función que la cuarta capa del modelo OSI, consistente en permitir la comunicación extremo a extremo (host a host) en la red.

La capa de aplicación

Esta capa desarrolla las funciones de las capas de sesión, presentación y aplicación del modelo OSI.

6.2 PROTOCOLOS DEL MODELO TCP/IP



6.3 PROTOCOLOS DE LA CAPA DE APLICACIÓN

Esta capa proporciona la interfaz entre la red por la cual se transmiten los datos y el usuario; contiene protocolos que son utilizados para intercambiar datos entre los programas de origen y destino.

- Protocolo de transferencia de archivos (**FTP):** es utilizado para transferir archivos de manera interactiva entre sistemas.
- Sistema de nombres de dominio **(DNS**): utiliza un formato simple llamado mensaje, el cual se utiliza para todos los tipos de solicitudes que hagan los clientes y da respuestas del servidor.
- Hipertext Transfer Protocol**(HTTP):** especifica una actividad de solicitud-respuesta, cuando el cliente envía en un explorador un mensaje de solicitud al servidor, HTTP define los tipos de mensajes que el cliente utiliza para solicitar la página y envía los mensajes que el servidor necesita para responder.
- Protocolo simple de transferencia de correo, Protocolo de oficina de correos **(SMTP/POP):** para recibir los e-mails desde un servidor el cliente del correo puede utilizar un POP, al enviar el e-mail desde un cliente se utiliza el protocolo SMTP.
- Protocolo de configuración dinámica de host **(DHCP):** éste servicio permite a los dispositivos de red obtener las direcciones IP, por medio de un servidor DHCP el cual elije una dirección de un rango denominado "*pool"* y se le asigna al host por un periodo determinado. El servidor DHCP ordena una única dirección a cada usuario, lo que permite a los administradores de red configurar sencillamente la trayectoria IP del cliente.
- **Telnet** proporciona una forma de utilizar una computadora, conectada a través de la red, para acceder a un dispositivo de red como si el teclado y el monitor estuvieran conectados directamente al dispositivo.
- **Etc.**

6.4 PROTOCOLOS DE LA CAPA DE TRANSPORTE

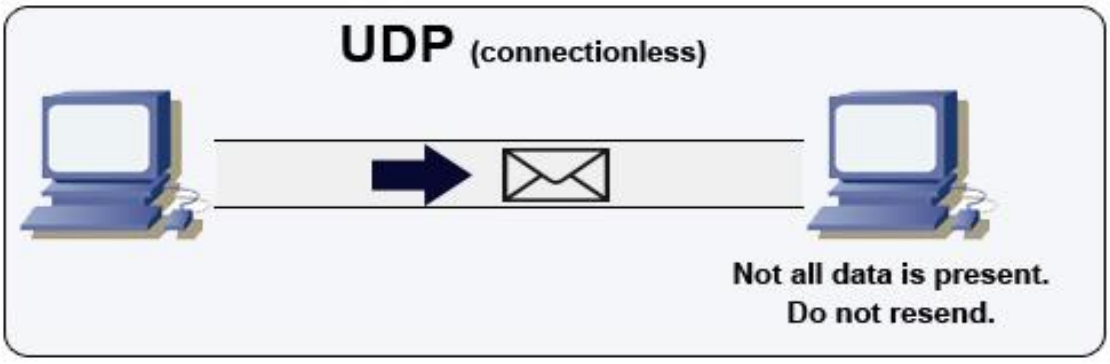
La capa de transporte permite la comunicación extremo a extremo (host a host) en la red. Aquí se definen dos protocolos:

https://www.youtube.com/watch?v=sdzKhSWmMm0&src_vid=gmFv4ZD_h4w&feature=iv&annotation_id=annotation_681209

UDP (UserDatagramProtocol, protocolo de datagrama de usuario)

Es un protocolo muy simple que da un servicio **no orientado a conexión y no fiable**. UDP no realiza control de errores ni de flujo. Es decir cuando una maquina A envía paquetes a una maquina B, el flujo es unidireccional. La transferencia de datos es realizada sin haber realizado previamente una conexión con la máquina de destino (maquina B), y el destinatario recibirá los datos sin enviar una confirmación al emisor (la maquina A). Esto es debido a que la encapsulación de datos enviada por el protocolo UDP no permite transmitir la información relacionada al emisor. Por ello el destinatario no conocerá al emisor de los datos excepto su IP.

Una aplicación típica donde se utiliza UDP es la transmisión de voz y vídeo en tiempo real; aquí el retardo que introduciría el control de errores produciría más daño que beneficio: es preferible perder algún paquete que retransmitirlo fuera de tiempo.

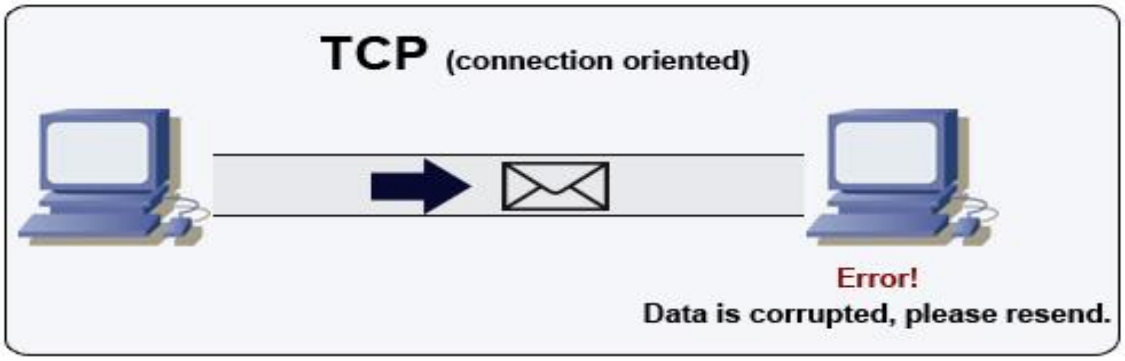


TCP (Transmission Control Protocol, Protocolo de control de transmisión)

TCP ofrece un servicio **fiable**, con lo que los paquetes (aquí llamados segmentos) llegan ordenados y sin errores. TCP se ocupa también del control de flujo extremo a extremo, para evitar por ejemplo que un host rápido sature a un receptor más lento.

Es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. TCP es un protocolo **orientado a conexión**, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

Cuando una máquina A envía datos a una máquina B, la máquina B es informada de la llegada de datos, y confirma su buena recepción. Aquí interviene el control CRC de datos que se basa en una ecuación matemática que permite verificar la integridad de los datos transmitidos. De este modo, si los datos recibidos son corruptos, el protocolo TCP permite que los destinatarios soliciten al emisor que vuelvan a enviar los datos corruptos.



Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura (gracias al sistema de acuse de recibo del protocolo TCP) independientemente de las capas inferiores.

Esto significa que los routers (que funcionan en la capa de Internet) sólo tienen que enviar los datos en forma de datagramas, sin preocuparse con el monitoreo de datos porque esta función la cumple la capa de transporte (o más específicamente el protocolo TCP).

El protocolo **TCP** permite garantizar la transferencia de datos confiable, a pesar de que usa el protocolo IP, que no incluye ningún monitoreo de la entrega de datagramas.

TCP está pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, pérdida de paquetes, orden en el que llegan los paquetes, duplicados de paquetes...) que gestiona el propio protocolo.

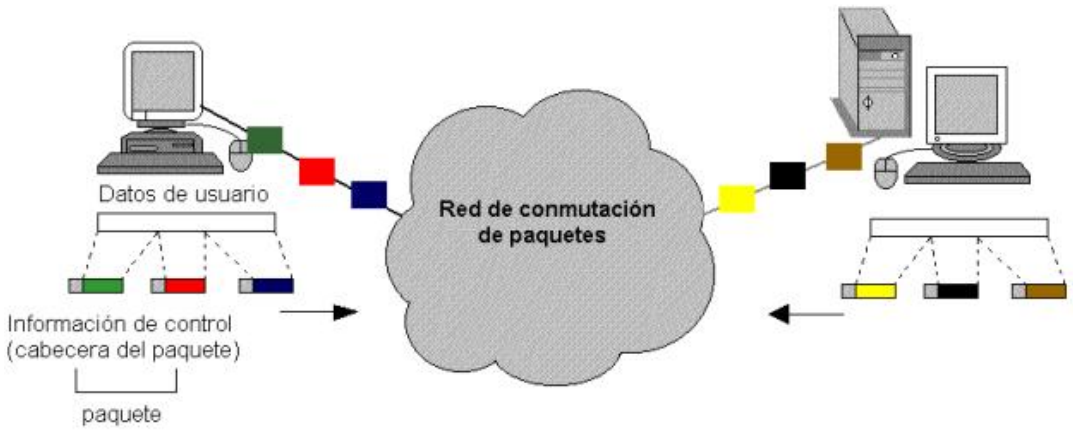
Cuando es más importante la velocidad que la fiabilidad, se utiliza UDP. En cambio, TCP asegura la recepción en destino de la información para transmitir.

7. PROTOCOLOS DE LA CAPA DE INTERNET. PROTOCOLO IP.

7.1 PROTOCOLO IP (INTERNET PROTOCOL)

Se trata de un protocolo **no** orientado a conexión, usado tanto por el origen como por el destino para la transmisión de datos a través de una red de **paquetes conmutados**. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas. En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

No añade fiabilidad, control de flujo o recuperación de errores para el protocolo de interfaz de red subyacente. Los paquetes que envía IP se pueden perder, estar fuera de orden, o incluso duplicar. IP no tratará estas situaciones, es tarea de las capas superiores proporcionar estas facilidades.



7.2 DIRECCIONAMIENTO IP Y ENRUTAMIENTO

Quizás los aspectos más complejos de IP son el **direccionamiento y el enrutamiento**. El direccionamiento se refiere a la forma como se asigna una dirección IP y cómo se dividen y se agrupan subredes de equipos.

El enrutamiento consiste en encontrar un camino que conecte una red con otra y, aunque es llevado a cabo por todos los equipos, es realizado principalmente por routers, que no son más que computadoras especializadas en recibir y enviar paquetes por diferentes interfaces de red.

http://www.areas.net/comofunciona/conexion/3.htm

7.3 DIRECCIONAMIENTO DE RED IPV4

Se trata de la cuarta versión del protocolo IP, usa direcciones de 32 bits muchas de las cuales están dedicadas a redes locales, actualmente no quedan direcciones ipv4 disponibles para compra debido a la evolución al ipv6.

7.4 DIRECCIONAMIENTO DE RED IPV6

La principal innovación de IPv6 es el uso de direcciones más extensas que con IPv4. Están codificadas con 16 bytes (128 bits) y esto permite que se resuelva el problema que hizo que IPv6 esté a la orden del día: brindar un conjunto prácticamente ilimitado de direcciones de Internet.

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables

En general, IPv6 no es compatible con IPv4, pero es compatible con todos los demás protocolos de Internet, incluyendo TCP, UDP, ICMP, IGMP, OSPF, BGP y DNS.

Sus características principales son:

- **Mayor espacio de direccionamiento (**RFC [1]2373 **)**

[1] Las RFC (Peticiones de comentarios) son un conjunto de documentos que sirven de referencia a la comunidad de Internet , que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.

Las direcciones pasan de los 32 a 128 bits, o sea, de 2^{32} direcciones (4.294.967.296) a 2^{128} direcciones (3.402823669 10^{38}).

Esto hace que:

- Desaparezcan los problemas de direccionamiento del IPv4 actual.
- No sean necesarias técnicas como el NAT para proporcionar conectividad a todos los ordenadores/dispositivos de nuestra red.
- Por tanto, todos los dispositivos actuales o futuros (ordenadores, PDAs, teléfonos GPRS o UMTS, neveras, lavadoras, etc.) podrán tener conectividad completa a Internet.

- **Seguridad (**RFC 2401 **y** RFC 2411**)**

  Uno de los grandes problemas achacable a Internet es su falta de seguridad en su diseño base. Este es el motivo por el que han tenido que desarrollarse, por ejemplo, el SSH o SSL, protocolos a nivel de aplicación que añaden una capa de seguridad a las conexiones que pasan a través suyo.

  IPv6 incluye **IPsec**, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.

- **Autoconfiguración (**RFC 2462**)**

  Al igual que ocurría con el punto anterior, en el actual IPv4 han tenido que desarrollarse protocolos a nivel de aplicación que permitiesen a los ordenadores conectados a una red asignarles su datos de conectividad al vuelo. Ejemplos son el DHCP o BootP.

  IPv6 incluye esta funcionalidad en el protocolo base, la propia pila intenta autoconfigurarse y descubrir el camino de conexión a Internet (routerdiscovery)

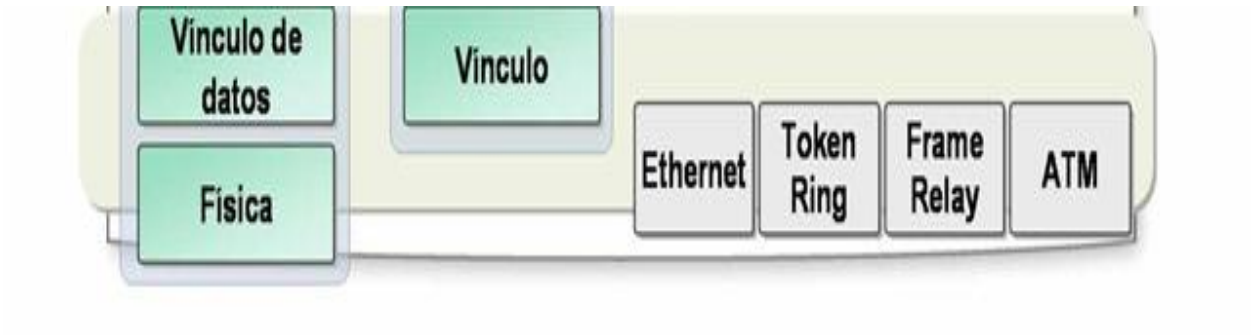
- **Movilidad (**RFC 3024**)**

  Con la movilidad (o roaming) ocurre lo mismo que en los puntos anteriores, una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.

IP v4 versus IP v6

Característica	IPv4	IPv6
Longitud de direcciones	32 bits	128 bits
Clases de direcciones	Clase A, Clase B, Clase C	Direcciones sin clase (Classless)
Tipo de direcciones	Unicast, Multicast, Broadcast	Unicast, Multicast, Anycast
Configuración de dirección	Estática (a través de ficheros de configuración) o por DHCP	Autoconfiguración (plug and play) o por DHCP
Formato cabecera	Complejo. Longitud variable	Simple. Longitud fija
Calidad de servicio	Sí, aunque no soportado totalmente por routers	Sí
Soporte tráfico en tiempo real	No	Sí
Seguridad	No	Sí

8. PROTOCOLOS DE LA CAPA DE ACCESO A LA RED.



En la capa de acceso al medio se determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico. Se responden preguntas del tipo: ¿puede un puesto dejar información en el cable siempre que tenga algo que transmitir?, ¿debe esperar algún turno?, ¿cómo sabe un puesto que un mensaje es para él?

Un organismo de normalización conocido como IEEE (Instituto de ingenieros eléctricos y electrónicos) ha definido los principales protocolos de la capa de acceso al medio conocidos en conjunto como estándares 802. Los más importantes son los IEEE 802.3 y IEEE 802.5 que se estudian a continuación.

El protocolo utilizado en esta capa viene determinado por las tarjetas de red que instalemos en los puestos. Esto quiere decir que si adquirimos tarjetas Ethernet sólo podremos instalar redes Ethernet. Y que para instalar redes Token ring necesitaremos tarjetas de red especiales para Token ring. Actualmente en el mercado únicamente se comercializan tarjetas de red Ethernet (de distintas velocidades y para distintos cableados).

7.1 TOKEN RING (802.5)

Las redes Token ring (paso de testigo en anillo) fueron utilizadas ampliamente en entornos IBM desde su lanzamiento en el año 1985. En la actualidad es difícil encontrarlas salvo en instalaciones antiguas de grandes empresas.

El cableado se establece según una topología de anillo. En lugar de utilizar difusiones, se utilizan enlaces punto a punto entre cada puesto y el siguiente del anillo. Por el anillo Token ring circula un mensaje conocido como token o ficha. Cuando una estación desea transmitir espera a recibir el token. En ese momento, lo retira de circulación y envía su mensaje. Este mensaje circula por el anillo hasta que lo recibe íntegramente el destinatario. Entonces se genera un token nuevo.

Las redes Token ring utilizan una estación monitor para supervisar el funcionamiento del anillo. Se trata de un protocolo complejo que debe monitorizar en todo momento el buen funcionamiento del token (que exista exactamente uno cuando no se transmiten datos) y sacar del anillo las tramas defectuosas que no tengan destinatario, entre otras funciones.

Las redes Token ring de IBM pueden funcionar a 4 Mbps o a 16 Mbps utilizando cable par trenzado o cable coaxial.

7.2 ETHERNET (802.3)

Ethernet es un estándar de redes de área local para ordenadores con acceso al medio por contienda CSMA/CD. ("Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

El protocolo de red Ethernet fue diseñado originalmente por Digital, Intel y Xerox por lo

cual, la especificación original se conoce como Ethernet DIX. Posteriormente, IEEE ha definido el estándar Ethernet 802.3. La forma de codificación difiere ligeramente en ambas definiciones.

Es el método de conexión más extendido en la actualidad. El estándar 802.3 fue diseñado originalmente para funcionar a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps (802.3u) o 1 Gbps.

Una red Ethernet tiene las siguientes características:

- **Canal único**. Todas las estaciones comparten el mismo canal de comunicación por lo que sólo una puede utilizarlo en cada momento.
- Es de **difusión** debido a que todas las transmisiones llegan a todas las estaciones (aunque sólo su destinatario aceptará el mensaje, el resto lo descartarán).
- Tiene un **control de acceso** distribuido porque no existe una autoridad central que garantice los accesos. Es decir, no hay ninguna estación que supervise y asigne los turnos al resto de estaciones. Todas las estaciones tienen la misma prioridad para transmitir.
- El protocolo de comunicación que utilizan estas redes es el **CSMA/CD** (CarrierSenseMultiple Access / CollisionDetect, acceso múltiple con detección de portadora y detección de colisiones). Esta técnica de control de acceso a la red ha sido normalizada constituyendo el estándar IEEE 802.3. Veamos brevemente el funcionamiento de CSMA/CD:

7.3 COMPARACIÓN DE ETHERNET Y TOKEN RING.

En Ethernet cualquier estación puede transmitir siempre que el cable se encuentre libre; en Token ring cada estación tiene que esperar su turno. Ethernet utiliza un canal único de difusión; Token ring utiliza enlaces punto a punto entre cada estación y la siguiente. Token ring tiene siempre una estación monitor que supervisa el buen funcionamiento de la red; en Ethernet ninguna estación tiene mayor autoridad que otra. Según esta comparación, la conclusión más evidente es que, a iguales velocidades de transmisión, Token ring se comportará mejor en entornos de alta carga y Ethernet, en redes con poco tráfico.

En las redes Ethernet, cuando una estación envía un mensaje a otra, no recibe ninguna confirmación de que la estación destino haya recibido su mensaje. Una estación puede estar enviando paquetes Ethernet a otra que está desconectada y no advertirá que los paquetes se están perdiendo. Las capas superiores (y más concretamente, TCP) son las

encargadas de asegurarse que la transmisión se ha realizado de forma correcta.

9. Diferencias entre el Modelo OSI y el Modelo TCP/IP

- ✓ OSI distingue de forma clara los servicios, interfaces y protocolos. TCP/IP no lo hace.
- ✓ OSI fue definido antes de implementar protocolos por lo que algunas funcionalidades necesarias fallan o no existen, TCP/IP por el contrario fue definido después por lo tanto engloba todas las funcionalidades de cada protocolo.