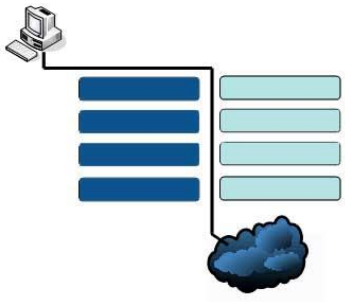
Redes, tipos y sus aplicaciones

- Concepto de red
- Clasificaciones de redes
- Conmutación de circuitos, conmutación de paquetes
- Topologías de red

Modelos de referencias de redes, protocolos y servicios



- Modelo OSI
- Las 7 Capas del modelo (Resumen) URL
- El modelo TCP/IP
- Protocolos
- Gráfico de protocolo TCP/IP
- Comparación entre el modelo OSI y el modelo TCP/IP
- Encapsulamiento de datos

Capa Física

Es el nivel más bajo. El medio físico por el cual se transmite la información. Puede ser cable coaxil, par trenzado, fibra óptica o incluso el aire (mediante el uso de wifi, o similar)

- La placa de red (NIC)
- ¿Qué es un modem? ¿Qué tipos de modems se utilizan en la actualidad?
- ¿Qué es un hub? ¿Cómo funciona?
- La alternativa WIFI el Acces point

Capa Enlace

La capa de enlace o acceso a la red determina la manera en que las Pc’s envían y reciben la información a través del soporte físico proporcionado por la capa anterior. Una vez que tenemos un cable, ¿cómo se transmite la información por ese cable?

- Cableado estructurado
- Dirección física (MAC)
- Swtich - Bridge

Capa Red

La capa de red define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino.

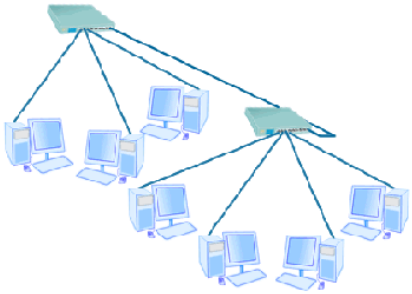
- El Protocolo IP
- Direcciones IP
- ¿Qué es un Router?
- ¿Cómo averiguo mi IP pública?
- ¿Cómo obtener mi IP privada?
- ¿Qué es el IP V6?

Capa Transporte

La capa de transporte ya no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza. Protocolos relacionados: UDP, TCP.

- La capa de transporte y la calidad del servicio
- El Protocolo TCP
- Puertos TCP

Capa Aplicación



La capa de aplicación es la que está en contacto con el usuario, Proporciona los distintos servicios de Internet: Correo electrónico (SMTP, POP, IMAP), páginas Web (HTTP, DNS), Transmisión de archivos (FTP, SFTP), conexiones remotas (Telnet, SSH), entre otros.

- ¿Qué es un Proxy?
- El protocolo HTTP
- El protocolo FTP
- Protocolos de correo electrónico (SMTP, POP, IMAP)
- El protocolo DNS
- El protocolo DHCP
- Telnet vs SSH

Redes, tipos y sus aplicaciones

1. Concepto

Una red es un conjunto de computadoras –dos o más – que comparten recursos, aplicaciones, información y dispositivos de hardware.
Existen redes de diversos tipos: desde la simple conexión en red de dos computadoras contiguas mediante un cable, a la gran red mundial que es Internet.
La posibilidad de «compartir», generalmente va a estar ligado íntimamente con las políticas de seguridad de cada red, esto significa que se tendrá acceso a tal o cual recurso, si estamos autorizados para tal fin. En este sentido es importante conocer el modo en que se estructura y distribuye el servicio de red de una organización y quiénes son los responsables y sus criterios al tomar las decisiones respecto a la seguridad y acceso.
Existe una gran variedad de dispositivos de interconexión, pudiendo conectar sitios distantes a miles de kilómetros o separados sólo por algunos metros. Pueden ser enlaces satelitales, módems, fibras ópticas y enlaces de radio entre otros.
De este modo, las redes de computadoras pueden llegar a infinidad de lugares brindando una cantidad de servicios, tendientes a facilitar la comunicación entre diferentes sitios. En
este sentido el avance tecnológico marca enormes cambios en el estilo de vida de la población y fundamentalmente, nuevas posibilidades en el ámbito del trabajo.
Los servicios que brindan las redes, se ven limitados:

- por la capacidad del dispositivo de interconexión, lo que llamaremos «ancho de banda», que es la medida de la cantidad de información que puede transportar;
- por la misma computadora, ya sea por sus recursos físicos, (memoria, procesador, etc.), como sus aplicaciones de software.

Las redes de computadoras han pasado a formar parte de nuestra vida cotidiana, ya sea desde una terminal de cobro de impuestos, un cajero automático, la tarea diaria en una oficina, y claro está, la Red Internet con todos sus servicios, web, correo electrónico, chat, redes sociales, etc.
Éstas permiten «compartir» recursos. Una extensión de este concepto es el término Networking, que significa «trabajo en red».
Pueden convivir diferentes sistemas operativos, tales como Linux, Novell, Windows.

2. Clasificación

- **Redes cableadas, inalámbricas, etc.**

Pueden clasificarse por su **tamaño**, es decir la extensión física en que se ubican sus componentes, o por el medio **utilizado para transmitir**, ya sea por un cable, o por señales de radiofrecuencia.
Dentro de las redes conectadas por **medios físicos discretos** (como un cable de cobre, por ejemplo, podemos encontrar básicamente tres tipos:

- Redes de Area Amplia o WAN
- Redes de Area Metropolitana o MAN
- Redes de Area Local o LAN

- **Redes de Area Amplia o WAN (Wide Area Network)**

Es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

Hoy en día Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente mientras que las VPN que utilizan cifrado y otras técnicas para hacer esa red dedicada aumentan continuamente.
Normalmente la WAN es una red punto a punto, es decir, red de paquete conmutado. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio. Fue la aparición de los portátiles y los PDA la que trajo el concepto de redes inalámbricas.
Una red de área amplia o WAN (Wide Area Network) se extiende sobre un área geográfica extensa, a veces un país o un continente, y su función fundamental está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí. Para ello cuentan con una infraestructura basada en poderosos nodos de conmutación que llevan a cabo la interconexión de dichos elementos, por los que además fluyen un volumen apreciable de información de manera continua. Por esta razón también se dice que las redes WAN tienen carácter público, pues el tráfico de información que por ellas circula proviene de diferentes lugares, siendo usada por numerosos usuarios de diferentes países del mundo para transmitir información de un lugar a otro. A diferencia de las redes LAN (siglas de "local area network", es decir, "red de área local"), la velocidad a la que circulan los datos por las redes WAN suele ser menor que la que se puede alcanzar en las redes LAN. Además, las redes LAN tienen carácter privado, pues su uso está restringido normalmente a los usuarios miembros de una empresa, o institución, para los cuales se diseñó la red.
La infraestructura de redes WAN la componen, además de los nodos de conmutación, líneas de transmisión de grandes prestaciones, caracterizadas por sus grandes velocidades y ancho de banda en la mayoría de los casos. Las líneas de transmisión (también llamadas "circuitos", "canales" o "troncales") mueven información entre los diferentes nodos que componen la red.
Los elementos de conmutación también son dispositivos de altas prestaciones, pues deben ser capaces de manejar la cantidad de tráfico que por ellos circula. De manera general, a estos dispositivos les llegan los datos por una línea de entrada, y este debe encargarse de escoger una línea de salida para reenviarlos. A continuación, en la Figura 1, se muestra un esquema general de los que podría ser la estructura de una WAN. En el mismo, cada host está conectada a una red LAN, que a su vez se conecta a uno de los nodos de conmutación de la red WAN. Este nodo debe encargarse de encaminar la información hacia el destino para la que está dirigida.

- **Redes de Area Metropolitana o MAN (Metropolitan Area Network)**

Es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado, la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes, ofrecen velocidades que van desde los 2Mbps y los 155Mbps.
El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.
Las redes de área metropolitana tienen muchas y variadas aplicaciones, las principales son:

- Interconexión de redes de área local (LAN)
- Despliegue de Zonas Wifi sin necesidad de utilizar Backhaul inalámbrico (liberando la totalidad de canales Wifi para acceso), esto en la práctica supone más del 60% de mejora en la conexión de usuarios wifi.
- Interconexión equipos entre si
- Transmisión de vídeo e imágenes (sistema de videovigilancia metropolitana)
- Puertas de enlace para redes de área extensa (WAN)

Los sistemas más utilizados en la actualidad son:

- SMDS (Servicio de Datos Conmutados Multimegabit)
- ATM (Asynchronous Transfer Mode)
- FDDI (Fiber Distributed Data Interface)

- **Redes de Area Local o LAN (Local Area Network)**

Una red local, es la interconexión de varios equipos y periféricos. (*LAN* es la abreviatura inglesa de *Local Area Network*, 'red de área local'). En las redes locales pequeñas o domésticas, lo más común, es que las computadoras se comuniquen mediante un cable que une a cada equipo; si fuera necesario conectar más de dos equipos se debe contar con algún dispositivo de enlace de datos que asegure la eficiencia en la red local; un ejemplo de este tipo de dispositivos es el conmutador switch).

Su aplicación más extendida es la interconexión de equipos personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

En épocas anteriores a los ordenadores personales, una empresa podía tener solamente un servidor, accediendo los usuarios a éste mediante terminales con un cable simple de baja velocidad. Las redes como SNA de IBM (Arquitectura de Red de Sistemas) fueron diseñadas para unir terminales o servidores a sitios remotos con líneas alquiladas. Las primeras LAN fueron creadas a finales de los años 1970 y se solían crear líneas de alta velocidad para conectar grandes servidores a un solo lugar. Muchos de los sistemas fiables creados en esta época, como Ethernet y ARCNET, fueron los más populares.

El crecimiento CP/M y DOS basados en computadoras personales significó que en un lugar físico existieran docenas o incluso cientos de equipos. La intención inicial de conectar estos equipos fue, generalmente, compartir espacio de disco e impresoras láser, pues eran muy caros en este tiempo.

Dentro de las que utilizan como medio físico para transmitir las señales de radio frecuencias podemos distinguir cuatro tipos:

- **Redes inalámbricas de área metropolitana (WMAN)**

También conocidas como **bucle local inalámbrico** (*WLL*, Wireless Local Loop). Se basan en el estándar *IEEE 802.16*. Los bucles locales inalámbricos ofrecen una velocidad total efectiva de 1 a 10 Mbps, con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones.

La mejor red inalámbrica de área metropolitana es WiMAX, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros.

- **Redes inalámbricas de área extensa (WWAN)**

Tienen el alcance más amplio de todas las redes inalámbricas. Por esta razón, todos los teléfonos móviles están conectados a una red inalámbrica de área extensa. Las tecnologías principales son:

- GSM (*Global System for Mobile Communication*)
- GPRS (*General Packet Radio Service*)
- UMTS (*Universal Mobile Telecommunication System*)

Si bien las denominaciones y los límites son similares entre los dos tipos de medios, la tecnología utilizada es totalmente diferente.

- **Redes de área local inalámbricas (WLAN)**

Es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí. Existen varios tipos de tecnologías:
Wifi (o IEEE 802.11) con el respaldo de WECA (Wireless Ethernet Compatibility Alliance) ofrece una velocidad máxima de 54 Mbps en una distancia de varios cientos de metros.
hiperLAN2 (*High Performance Radio LAN 2.0*), estándar europeo desarrollado por ETSI (*European Telecommunications Standards Institute*). HiperLAN 2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de cien metros, y transmite dentro del rango de frecuencias de 5150 y 5300 MHz.

- **Red Inalámbrica de Área Personal (WPAN)** (Wireless Personal Area Networks)

Es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella.

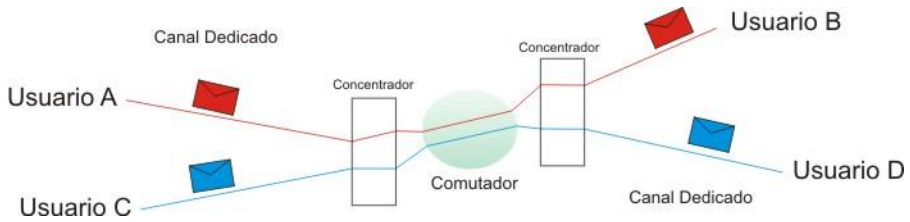
- **El paradigma PAN**

Las redes para espacios personales continúan desarrollándose hacia la tecnología del Bluetooth hacia el concepto de redes dinámicas, el cual nos permite una fácil comunicación con los dispositivos que van adheridos a nuestro cuerpo o a nuestra indumentaria, ya sea que estemos en movimiento o no, dentro del área de cobertura de nuestra red.

3. Conmutación

- **Conmutación de circuitos**

Los sistemas telefónicos existentes se llevan a cabo con un método muy confiable, pero ineficiente: la conmutación de circuitos.
La conmutación de circuitos es un concepto básico que ha sido utilizado en las redes telefónicas por más de 100 años. Mientras se hace una llamada, una porción de la capacidad del cable se mantiene reservada. Dado que estamos conectando dos puntos en ambas direcciones, la conexión se llama circuito. Este es el fundamento de lo que se denomina PSTN, sigla en inglés de ‘red telefónica pública y conmutada’.
Durante el transcurso de una llamada el circuito está continuamente abierto entre los dos teléfonos. Hasta 1960 cada llamada tenía una extensión de cable dedicada de un extremo al otro durante toda su duración. El costo de las llamadas de larga distancia era alto porque el usuario se apoderaba momentáneamente de cientos de kilómetros de cobre al hacerlas.
Hoy en día la voz es digitalizada, y se combinan miles de llamadas en un sólo cable de fibra óptica. Estas llamadas son transmitidas a una tasa fija de 64 Kbps en cada dirección, con lo que la tasa total de transmisión es de 128 Kbps. Esto equivale a 16 kilobytes por segundo. En conclusión, una conversación de 10 minutos ocupa aproximadamente 10 megabytes (9600 KB).

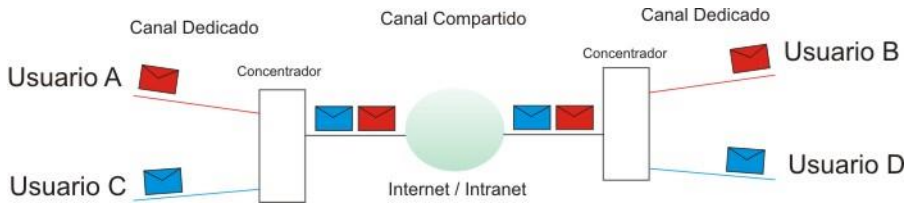


En este caso, en el momento de la comunicación se reserva un circuito de líneas de comunicación entre el nodo remitente (ej: Usuario A) y el nodo receptor (ej: UsuarioB) para que se puedan enviar datos a través de él. El circuito se vuelve a liberar cuando se completa la

transmisión. En este caso, en el momento de la comunicación se reserva un circuito de líneas de comunicación entre el nodo remitente y el nodo receptor para que se puedan enviar datos a través de él. El circuito se vuelve a liberar cuando se completa la transmisión.

- **Conmutación de paquetes**

En una llamada telefónica, cuando una persona está hablando, la otra escucha. Esto significa que en todo momento sólo se utiliza la mitad de una conexión. Entonces podríamos deducir que una llamada de 10 minutos ocuparía la mitad de la del ejemplo anterior: 4.7 MB.
Pero además una cantidad significante del tiempo en la mayoría de las conversaciones es silencio. Inclusive, hay pequeños momentos en los que ninguna de las dos partes habla. Si pudiéramos remover esos intervalos nuestro archivo imaginario sería aún menor. En vez de enviar un flujo continuo de bytes, tanto silenciosos como no, sólo estaríamos escogiendo los que contienen algún sonido. Estas son las posibilidades que abre una transmisión por paquetes.
Hoy en día las dos clases de conmutación coexisten. El punto fuerte de la de circuitos es la confiabilidad, mientras que la de paquetes se destaca por su eficiencia en el uso de los recursos de la red. La conmutación de paquetes es más reciente, moderna, pero la confiabilidad de los circuitos todavía les garantiza un buen lugar en el futuro.



Cuando se envían datos con **conmutación de paquetes**, los datos que se van a transmitir se dividen en paquetes de datos (esto se denomina **segmentación**) y se envían por separado a través de la red.
Los nodos de la red pueden determinar libremente la ruta de cada paquete de manera individual, según su tabla de enrutamiento. Los paquetes que se envían de esta manera pueden tomar diferentes rutas y se vuelven a montar una vez que llegan al nodo receptor.
En este caso, los paquetes pueden llegar en un orden distinto del que fueron enviados y se pueden perder. Por esta razón, ciertos mecanismos se arman en paquetes para que se puedan reorganizar de ser necesario o volver a enviar si los paquetes se pierden.

Principales Diferencias y Características de ambos

Conmutación de circuitos

- Se reservan recursos extremo-a-extremo para establecer la comunicación
- Ancho de banda, capacidad en los conmutadores
- Recursos dedicados: no se comparten aunque no se usen
- Garantías de calidad
- Requiere un establecimiento de la conexión

Conmutación de paquetes

- Cada extremo envía un flujo de datos divididos en paquetes
- Cada paquete contiene información para llegar al destino
- No se reservan recursos
- Cada paquete usa toda la capacidad del enlace pero puede tener que esperar a que se envíen otros antes

4. Topologías de red

Los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red. La disposición de los diferentes componentes de una red se conoce con el nombre de topología de la red. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que deseemos, etc.

Podemos distinguir tres aspectos diferentes a la hora de considerar una topología:

1. La topología física, que es la disposición real de las máquinas, dispositivos de red y cableado (los medios) en la red.

2. La topología lógica, que es la forma en que las máquinas se comunican a través del medio físico. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

3. La topología matemática, mapas de nodos y enlaces, a menudo formando patrones.
La topología de broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita. Esta es la forma en que funciona Ethernet.

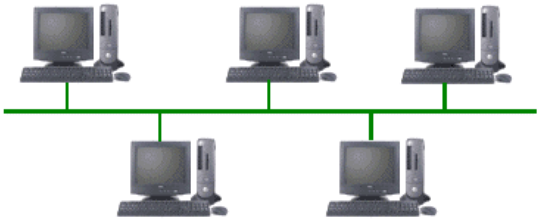
En cambio, la transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token significa que puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.

Modelos de topología

- Topología de bus
- Topología de anillo doble
- Topología en estrella
- Topología en estrella extendida
- Topología en árbol
- Topología en malla completa
- Topología irregular

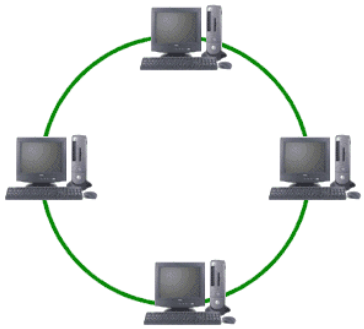
Topología de bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados.



La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común

que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes. Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.



Topología de anillo

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.

Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

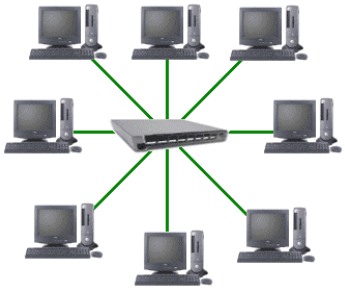
Topología de anillo doble

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos. La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

Topología en estrella

La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula por la red.

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.



Topología en estrella extendida

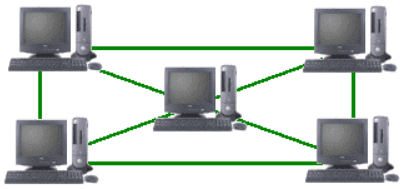
La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs. La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

Topología en árbol

La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

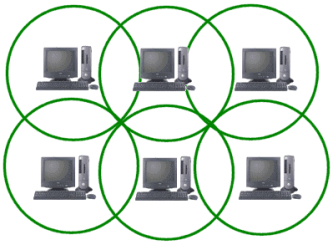
El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

Topología en malla completa
En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.



La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

Topología de red celular La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.



La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; sólo hay ondas electromagnéticas. La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad. Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

Topología irregular
En este tipo de topología no existe un patrón obvio de enlaces y nodos. El cableado no sigue un modelo determinado; de los nodos salen cantidades variables de cables. Las redes que se encuentran en las primeras etapas de construcción, o se encuentran mal planificadas, a menudo se conectan de esta manera. Las topologías LAN más comunes son:

Ethernet: topología de bus lógica y en estrella física o en estrella extendida.
Token Ring: topología de anillo lógica y una topología física en estrella.
FDDI: topología de anillo lógica y topología física de anillo doble.

5. Diferencias entre bit y bit rate

Es importante en este punto aclarar las cuestiones que tienen que ver con las unidades que vamos a utilizar a lo largo del curso y que obviamente son las utilizadas por los equipos informáticos.
Primero tenemos que hacer una gran diferenciación entre byte/bit y bits/s(bit rate). Un byte debe ser considerado como una secuencia de bits contiguos, cuyo tamaño depende del código de información o código de caracteres en que sea definido. La unidad **byte** se representa con el símbolo **B**.

Se usa comúnmente como unidad básica de almacenamiento de información en combinación con los prefijos de cantidad. Originalmente el byte fue elegido para ser un submúltiplo del tamaño de palabra de un ordenador, desde seis a nueve bits (un carácter codificado estaría adaptado a esta unidad). Son sus múltiplos más utilizados:

Unidad	Signo	Equivalencia
bit	b	0 ó 1
byte	B	8 bits
kilobit	kb (kbits)	1000 bits
Kilobyte (binario)	KB	1024 bytes
Kilobyte (decimal)	KB (ó kB)	1000 bytes
Megabit	Mb	1000 kilobits
Megabyte (binario)	MB	1024 Kilobytes
Megabyte (decimal)	MB (ó mB)	1000 Kilobytes
Gigabit	Gb	1000 Megabits
Gigabyte (binario)	GB	1024 Megabytes
Gigabyte (decimal)	GB (ó gB)	1000 Megabytes
Terabit	Tb	1000 Gigabits
Terabyte (binario)	TB	1024 Gigabytes
Terabyte (decimal)	TB (ó tB)	1000 Gigabytes
Petabit	Pb	1000 Terabits
Petabyte (binario)	PB	1024 Terabytes
Petabyte (decimal)	PB (ó pB)	1000 Terabytes
Exabit	Eb	1000 Petabits
Exabyte (binario)	EB	1024 Petabytes
Exabyte (decimal)	EB (ó eB)	1000 Petabytes

Por otro lado, en telecomunicación e informática, el término ***bit rate*** (en español velocidad binaria, cadencia, tasa o flujo de bits) define el número de bits que se transmiten por unidad de tiempo a través de un sistema de transmisión digital o entre dos dispositivos digitales. Así pues, el bit rate es la **velocidad de transferencia** de datos.
La unidad con que el SI (Sistema Internacional) expresa el bit rate es el bit por segundo (bit/s, b/s, bps). La *b* debe escribirse siempre en minúscula, para impedir la confusión con byte por segundo (B/s). Para convertir de bytes/s a bits/s, basta simplemente multiplicar por 8 y viceversa.

Que la unidad utilizada sea el bit/s, no implica que no puedan utilizarse múltiplos del mismo:

- kbit/s o kbps (kb/s, kilobit/s o mil bits por segundo)
- Mbit/s o Mbps(Mb/s, Megabit/s o un millón de bits por segundo)
- Gbit/s o Gbps (Gb/s, Gigabit, mil millones de bits)
- byte/s (B/s u 8 bits por segundo)
- kilobyte/s (kB/s, mil bytes u ocho mil bits por segundo)
- megabyte/s (MB/s, un millón de bytes u 8 millones de bit por segundo)
- gigabyte/s (GB/s, mil millones de bytes u 8 mil millones de bits)

Velocidades típicas de los accesos de conexión a Internet actuales - Ejemplos:
- Módem RTB: 56 kbps = 7 kB/s (7 kilobytes por segundo)
- ADSL: 1024 kbps (nominal 1 Mbps) = 128 kB/s (128 kilobytes por segundo)
- Cable: 2400 kbps = 300 kB/s (300 kilobytes por segundo)
- Telefonía móvil 3G: 384 kbps = 48 kB/s (48 kilobytes por segundo)

Los proveedores de internet hablan de velocidades de bajada de 64 kbps, 128 kbps, 256 kbps, 512 kbps, 1 mega (1024 kbps), 2 megas (2049 kbps) (o sea, lo expresan en bits por segundo). Pero tanto en Internet Explorer como en programas de descargas y en Internet en general, se habla en KB (que es, en definitiva, lo que ocupa un archivo) y en KB/s (kilobyte por segundo); por lo tanto, es interesante saber de cuánto es la velocidad de bajada expresada en KB por segundo. Esto puede traer confusión a los usuarios no expertos pues podrían pensar que bajarían 1 megabyte de información por segundo, pero en realidad bajan 1 megabit.

En principio es más conveniente saber la velocidad de descarga (y de subida) de la conexión en KB/s, pues es más fácil entenderlo. Si, por ejemplo, un archivo se está descargando a 25 KB/s, sabremos que se están descargando 25 mil caracteres del archivo por segundo (y más precisamente, 25600 caracteres)

Conversión entre bps y bytes/s.

Como en general no necesitamos demasiada precisión, tomaremos el camino más fácil, y la 'k' corresponderá a 1000 y no a 1024.

Supongamos que tenemos una conexión de 128 kbps o 128.000 bps, así se convierte.
8 bps ----------> 1 byte/s
128.000 bps ----> X bytes/s
X = (128.000 bps x 1 byte/s) / 8 bps = 16.000 bytes/s = 16 KB/s

Por lo tanto se estarán bajando unos 16 mil caracteres por segundo.

Conversiones más comunes:

kbps	28.8 kbps	57.6 kbps	64 kbps	128 kbps	256 kbps
Kbytes/s (KB/s)	3.6 KB/s	7.2 KB/s	8 KB/s	16 KB/s	32 KB/s

kbps	512 kbps	1024 kbps o 1 mega/s	2048 kbps o 2 megas/s
Kbytes/s (KB/s)	64 KB/s (kilobytes por segundo)	128 KB/s	256 KB/s

Existen dos sistemas de medir la velocidad
En el caso de la conexión a Internet, sin duda la mejor forma de medirla es por KB/s (kilobytes por segundo), pues estamos tratando siempre con archivos formados por caracteres (1 byte) y recordemos que un caracter está formado por 8 bits.
Hay casos en que la transmisión es serial (bit por bit) y la información no necesariamente está "empaquetada" en caracteres de 8 bits.
Muchas empresas se aprovechan de la confusión generada por los kbps y los KB/s para su beneficio.

Modelos de referencias de redes, protocolos y servicios

1. **Uso de las capas para analizar problemas en un flujo de materiales**

El concepto de *capas* le ayudará a comprender la acción que se produce durante el proceso de comunicación de un computador a otro. En la figura se plantean preguntas que involucran el movimiento de objetos físicos como por ejemplo, el tráfico de autopistas o los datos electrónicos. Este desplazamiento de objetos, sea este físico o lógico, se conoce como flujo. Existen muchas capas que ayudan a describir los detalles del proceso de flujo. Otros ejemplos de sistemas de flujo son el sistema de suministro de agua, el sistema de autopistas, el sistema postal y el sistema telefónico.

Comparación de redes

¿Red?	¿Qué fluye?	¿Diferentes formas?	¿Reglas?	¿Dónde?
Agua	Agua	Caliente; fría; potable; servida/cloaca	Reglas de acceso (abrir o cerrar grifos); descarga; no echar determinados elementos en las cañerías	Pipes
Autopistas	Vehículos	Camiones, automóviles, ciclos	Leyes de tránsito y reglas de cortesía	Roads and Highways
Servicio postal	Objetos	Cartas (información escrita);paquetes	Reglas para el empaquetado y franqueo	Cajas especiales de correo, oficinas, camiones, aviones, carteros
Teléfono	Información	Lenguajes hablados	Reglas de acceso al teléfono y reglas de cortesía	Sistema telefónico: cables, ondas electromagnéticas, etc.

Ahora, examine la figura el cuadro "Comparación de redes". ¿Qué red está examinando? ¿Qué fluye? ¿Cuáles son las distintas formas del objeto que fluye? ¿Cuáles son las normas para el flujo? ¿Dónde se produce el flujo? Las redes que aparecen en este esquema le ofrecen más analogías para ayudarlo a comprender las redes informáticas.

Otro ejemplo que describe cómo puede usar el concepto de capas para analizar un tema cotidiano es examinar una conversación entre dos personas. Cuando usted tiene una idea que desea comunicarle a otra persona, lo primero que hace es elegir (a menudo de modo subconsciente) cómo desea expresar esa idea, luego decide cómo comunicarla de forma adecuada y, por último, transmite esa idea.

Imagínese a un joven que está sentado en uno de los extremos de una mesa muy larga. En el otro extremo de la mesa, bastante lejos, está sentada su abuela. El joven habla en inglés. Su abuela prefiere hablar en español. En la mesa se ha servido una cena espléndida que ha preparado la abuela. Súbitamente, el joven grita lo más alto posible, en inglés: "Hey you! Give me the rice!" (¡Oye, tú! ¡Dame el arroz!) y extiende la mano sobre la mesa para agarrarlo. En la mayoría de los lugares, esta acción se considera bastante grosera. ¿Qué es lo que el joven debería haber hecho para comunicar sus deseos de forma aceptable?

Para ayudarlo a encontrar la respuesta a esta pregunta, analice el proceso de comunicación por capas. En primer lugar está la idea – el joven desea el arroz; luego está la representación de la idea– hablada en inglés (en lugar de español); a continuación, el método de entrega – "Oye tú"; y finalmente el medio – gritar (sonido) y extender la mano (acción física) sobre la mesa para tomar el arroz.

A partir de este grupo de cuatro *capas*, se puede observar que tres de estas capas impiden que el joven comunique su idea de forma adecuada/aceptable. La primera capa (la idea) es aceptable. La segunda capa (representación), hablando en inglés en lugar de español, y la tercera capa (entrega), exigiendo en lugar de solicitar con educación, definitivamente no obedecen a los protocolos sociales aceptados. La cuarta capa (medio), gritar y tomar las cosas de la mesa en vez de solicitar ayuda en forma educada a otra persona es un comportamiento inaceptable prácticamente en cualquier situación social.
Si analiza esta interacción desde el punto de vista de las capas podrá entender más claramente algunos de los problemas de la comunicación (entre las personas o entre los computadores) y cómo es posible resolver estos problemas.

2. Modelo OSI

A principios de la década de 1980 el desarrollo de redes sucedió con desorden en muchos sentidos. Se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnologías de conexión, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.
Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de conexión privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controla todo uso de la tecnología. Las tecnologías de conexión que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.
Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de conexión como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

2.1. **El modelo de referencia OSI**

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.
El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aun cuando el transmisor y el receptor tengan distintos tipos de medios de red.
En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.

- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

2.2. **Las siete capas del modelo de referencia OSI**

El problema de trasladar información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo. Las siete capas del modelo de referencia *OSI* son:

- ⇨ Capa 7: La capa de aplicación
- ⇨ Capa 6: La capa de presentación
- ⇨ Capa 5: La capa de sesión
- ⇨ Capa 4: La capa de transporte
- ⇨ Capa 3: La capa de red
- ⇨ Capa 2: La capa de enlace de datos
- ⇨ Capa 1: La capa física

Durante el transcurso de este semestre veremos las capas, comenzando por la Capa 1 y estudiando el modelo OSI capa por capa. Al estudiar una por una las capas del modelo de referencia OSI, comprenderá de qué manera los paquetes de datos viajan a través de una red y qué dispositivos operan en cada capa a medida que los paquetes de datos las atraviesan. Como resultado, comprenderá cómo diagnosticar las fallas cuando se presenten problemas de red, especialmente durante el flujo de paquetes de datos.

2.3. **Funciones de cada capa**

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. A continuación, presentamos una breve descripción de cada capa del modelo de referencia OSI tal como aparece en la figura.

Capa 7: La capa de aplicación La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas

debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos. Si desea recordar a la Capa 7 en la menor cantidad de palabras posible, piense en los navegadores de Web.

Capa 6: La capa de presentación La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común. Si desea recordar la Capa 6 en la menor cantidad de palabras posible, piense en un formato de datos común.

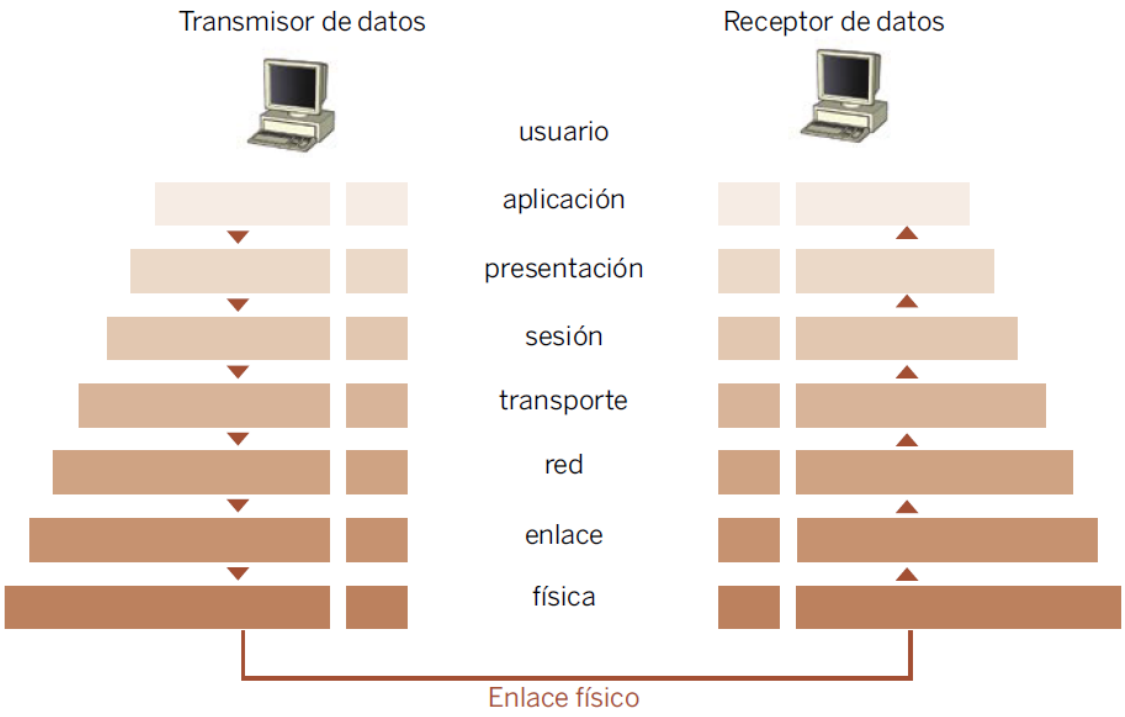
Capa 5: La capa de sesión Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación. Si desea recordar la Capa 5 en la menor cantidad de palabras posible, piense en diálogos y conversaciones.

Capa 4: La capa de transporte La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.
La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte. Si desea recordar a la Capa 4 en la menor cantidad de palabras posible, piense en calidad de servicio y confiabilidad.

Capa 3: La capa de red La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Si desea recordar la Capa 3 en la menor cantidad de palabras posible, piense en selección de ruta, direccionamiento y enrutamiento.

Capa 2: La capa de enlace de datos La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico) , la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Si desea recordar la Capa 2 en la menor cantidad de palabras posible, piense en tramas y control de acceso al medio.

Capa 1: La capa física La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física. Si desea recordar la Capa 1 en la menor cantidad de palabras posible, piense en señales y medios.



Funcionamiento del Modelo OSI

2.4. Las 7 capas del modelo OSI y sus funciones principales

Capa Física

- Transmisión de flujo de bits a través del medio. No existe estructura alguna.
- Maneja voltajes y pulsos eléctricos.
- Especifica cables, conectores y componentes de interfaz con el medio de transmisión.

Capa Enlace de Datos

- Estructura el flujo de bits bajo un formato predefinido llamado trama.
- Para formar una trama, el nivel de enlace agrega una secuencia especial de bits al principio y al final del flujo inicial de bits.
- Transfiere tramas de una forma confiable libre de errores (utiliza reconocimientos y retransmisión de tramas).
- Provee control de flujo.
- Utiliza la técnica de "piggybacking"

Capa de Red (Nivel de paquetes)

- Divide los mensajes de la capa de transporte en paquetes y los ensambla al final.
- Utiliza el nivel de enlace para el envío de paquetes: un paquete es encapsulado en una trama.
- Enrutamiento de paquetes.
- Envía los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Control de Congestión.

Capa de Transporte

- Establece conexiones punto a punto sin errores para el envío de mensajes.
- Permite multiplexar una conexión punto a punto entre diferentes procesos del usuario (puntos extremos de una conexión).
- Provee la función de difusión de mensajes (broadcast) a múltiples destinos.

- Control de Flujo.

Capa de Sesión

- Permite a usuarios en diferentes máquinas establecer una sesión.
- Una sesión puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas, etc.
- Controla el diálogo (quién habla, cuándo, cuánto tiempo, half duplex o full duplex).
- Función de sincronización.

Capa de Presentación

- Establece una sintaxis y semántica de la información transmitida.
- Se define la estructura de los datos a transmitir (v.g. define los campos de un registro: nombre, dirección, teléfono, etc).
- Define el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc).
- Compresión de datos.
- Criptografía.

Capa de Aplicación

- Transferencia de archivos (ftp).
- Login remoto (rlogin, telnet).
- Correo electrónico (mail).
- Acceso a bases de datos, etc.

3. El modelo TCP/IP

Aunque el modelo de referencia OSI sea universalmente reconocido, el estandar abierto de Internet desde el punto de vista histórico y técnico es el *Protocolo de control de transmisión/Protocolo Internet (TCP/IP).* El modelo de referencia *TCP/IP* y la *pila de protocolo TCP/IP* hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de la luz. El modelo TCP/IP tiene importancia histórica, al igual que las normas que permitieron el desarrollo de la industria telefónica, de energía eléctrica, el ferrocarril, la televisión y las industrias de vídeos.

3.1. **Las capas del modelo de referencia TCP/IP**

El Departamento de Defensa de EE.UU. (*DoD*) creó el modelo TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. Para brindar un ejemplo más amplio, supongamos que el mundo está en estado de guerra, atravesado en todas direcciones por distintos tipos de conexiones: cables, microondas, fibras ópticas y enlaces satelitales. Imaginemos entonces que se necesita que fluya la información o los datos (organizados en forma de paquetes), independientemente de la condición de cualquier nodo o red en particular de la internetwork (que en este caso podrían haber sido destruidos por la guerra). El DoD desea que sus paquetes lleguen a destino siempre, bajo cualquier condición, desde un punto determinado hasta cualquier otro. Este problema de diseño de difícil solución fue

lo que llevó a la creación del modelo TCP/IP, que desde entonces se transformó en el estándar a partir del cual se desarrolló Internet.
A medida que obtenga más información acerca de las capas, tenga en cuenta el propósito original de Internet; esto le ayudará a entender por qué motivo ciertas cosas son como son. El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la *capa de Internet*y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. No confunda las capas de los dos modelos, porque la capa de aplicación tiene diferentes funciones en cada modelo.

Capa de aplicación Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y garantiza que estos datos estén correctamente empaquetados para la siguiente capa.

Capa de transporte La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. TCP es un protocolo orientado a la conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a la conexión no significa que el circuito exista entre los computadores que se están comunicando (esto sería una conmutación de circuito). Significa que los segmentos de Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período. Esto se conoce como conmutación de paquetes.

Capa de Internet El propósito de la *capa de Internet* es enviar paquetes origen desde cualquier red en la internetwork y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Esto se puede comparar con el sistema postal. Cuando envía una carta por correo, usted no sabe cómo llega a destino (existen varias rutas posibles); lo que le interesa es que la carta llegue.

Capa de acceso de red El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas física y de enlace de datos del modelo OSI.

4. Protocolos

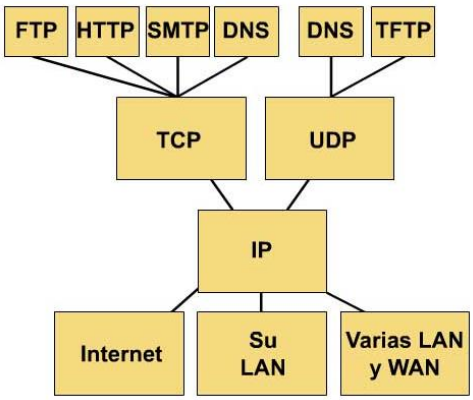
Un **protocolo** es un método establecido de intercambiar datos en Internet por el cual dos computadoras acuerdan comunicarse. Como seres humanos, utilizamos el lenguaje como protocolo, en este caso hemos acordado comunicarnos con la lengua española.

El protocolo determina lo siguiente:

- El tipo de comprobación de errores que se utilizará.
- El método de compresión de los datos, si lo hay.
- Cómo indicará el dispositivo que envía que ha acabado el enviar un mensaje.
- Cómo indicará el dispositivo que recibe que ha recibido un mensaje.

Desde el punto de vista de un usuario, el único aspecto interesante sobre protocolos es que tu ordenador o dispositivo debe soportar los protocolos adecuados si quieres comunicarte con otros ordenadores. El protocolo se puede implementar en hardware o en software.

Gráfico de protocolo TCP/IP



El diagrama que aparece en la siguiente figura se denomina gráfico de protocolo.
Este gráfico ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP. En la capa de aplicación, aparecen distintas tareas de red que probablemente usted no reconozca, pero como usuario de Internet, probablemente use todos los días. Estas aplicaciones incluyen las siguientes:

- FTP : File Transfer Protocol (Protocolo de transporte de archivos)
- HTTP: Hypertext Transfer protocol (Protocolo de transferencia de hipertexto)
- SMTP: Simple Mail transport protocol (Protocolo de transporte de correo simple)
- DNS: Domain Name Service (Servicio de nombre de dominio)
- TFTP: Trival File transport protocol (Protocolo de transporte de archivo trivial)

El modelo TCP/IP enfatiza la máxima flexibilidad, en la capa de aplicación, para los diseñadores de software. La capa de transporte involucra dos protocolos: el protocolo de control de transmisión (TCP) y el protocolo de datagrama (UDP). Estos protocolos se examinarán posteriormente con más detalle. La capa inferior, la capa de red, se relaciona con la tecnología LAN o WAN que se utiliza en particular.
En el modelo TCP/IP existe solamente un protocolo de red: el protocolo Internet, o IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento.

Capa Física

1. La placa de red (NIC)

Una tarjeta de interfaz de red o **N**etwork **I**nterface **C**ard (NIC) es una placa de circuito instalada en una PC que le permite conectarse a una red.

Para instalar en una PC, se debe considerar:

- La velocidad de su concentrador, conmutador, o servidor de impresora - Ethernet (10Mbps) o Fast Ethernet (100Mbps).
- El tipo de conexión que necesita - RJ-45 para par trenzado o BNC para cable coaxial.
- El tipo de conector NIC disponible dentro de su PC-ISA o PCI.

1.1. Velocidad de conexión

Debe utilizarse una NIC de Ethernet con un concentrador o conmutador Ethernet, y debe usarse una NIC de Fast Ethernet con un concentrador o conmutador Fast Ethernet.
En caso de una NIC 10/100, podrá conectarla al concentrador Ethernet de 10Mbps o al concentrador Fast Ethernet de 100Mbps. La NIC 10/100 ajustará su velocidad para que coincida con la velocidad más alta soportada por ambos extremos de la conexión.

1.2. .Tipo de conexión

Si está instalando una red que utiliza cables de par trenzado, necesitará una NIC con un conector RJ-45.
O bien la opción sin cables Wireless, tanto para slot PCI, PCMCIA, o usb.

1.3. Modems

Es un dispositivo que sirve para modular y desmodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada *portadora* mediante otra señal de entrada llamada *moduladora*. Se han usado modems desde los años 60 o antes del siglo XX, principalmente debido a que la transmisión directa de las señales electrónicas inteligibles, a largas distancias, no es eficiente. Por ejemplo, para transmitir señales de audio por el aire, se requerirían antenas de gran tamaño (del orden de cientos de metros) para su correcta recepción.
Este dispositivo permite conectar dos computadoras remotas utilizando por ejemplo la línea telefónica de forma que puedan intercambiar información entre sí. El módem es uno de los métodos más extendidos para la interconexión de computadoras por su sencillez y bajo costo.
La gran cobertura de la red telefónica convencional posibilita la casi inmediata conexión de dos ordenadores si se utiliza módems. El módem es por todas estas razones el método más popular de acceso a la Internet por parte de los usuarios privados y también de muchas empresas.
En la actualidad el uso de la red telefónica, (o par de cobre) no es el único método de conexión, se ha extendido a operadores de televisión por cable, señales satelitales por medio de antenas receptoras, o incluso el uso de tecnología celular.
Entre las principales tecnologías de conexión podemos destacar:

- *Módem Telefónico*
- *Módem ADSL*
- *Módem Cablemodem*
- *Módem Celulares*
- *Módem Redes Inalámbricas*

Módem Telefónico

Su uso más común y conocido es en transmisiones de datos por vía telefónica.
Las computadoras procesan datos de forma digital; sin embargo, las líneas telefónicas de la red básica sólo transmiten señales analógicas.
Los métodos de modulación y otras características de los módems telefónicos están estandarizados por el UIT-T (el antiguo CCITT) en la serie de Recomendaciones "V". Estas Recomendaciones también determinan la velocidad de transmisión.

Destacan:

- **V.32**. Transmisión a 9.600 bps.
- **V.32 bis**. Transmisión a 14.400 bps.
- **V.34**. Transmisión a 33.600 bps. Uso de técnicas de compresión de datos.
- **V.90**. Transmisión a 56'6 kbps de descarga y hasta 33.600 bps de subida.
- **V.92**. Mejora sobre V.90 con compresión de datos y llamada en espera. La velocidad de subida se incrementa, pero sigue sin igualar a la de descarga.

Módem ADSL

En contra de lo que se cree, no es una tecnología digital, sino tan analógica como el antiguo modem de 56 KBps. La diferencia estriba en un elemento definitivo: el oído humano no es capaz de oír todo el rango de frecuencias que produce la voz (el mismo principio empleado para poder comprimir música). De este modo, se aplica un filtro sofométrico que deja pasar sólo el rango de frecuencias audibles y descarta las restantes, tanto por encima como por debajo de este rango. Es la función que desempeña el microfiltro que se pone en los teléfonos en una línea ADSL.
El modem ADSL proporciona acceso a Internet a través de una línea ADSL, por lo que la interfaz que comunica con el exterior debe adaptarse a este medio. Por ello, este dispositivo lleva una interfaz RJ11 para conectar el cable telefónico. Además, debe de estar provisto de un modulador para adecuar las señales de datos a las frecuencias en las que trabaja la tecnología ADSL y de un demodulador para poder interpretar las señales que le llegan desde el exterior.

Modem Cablemodem

Es un tipo especial de módem diseñado para modular la señal de datos sobre una infraestructura de televisión por cable. El término *Internet por cable* (o simplemente cable) se refiere a la distribución de un servicio de conectividad a Internet sobre esta infraestructura de telecomunicaciones.
Se utilizan principalmente para distribuir el acceso a Internet de banda ancha, aprovechando el ancho de banda que no se utiliza en la red de TV por cable.
A menudo, la idea de una línea compartida se considera como un punto débil de la conexión a Internet por cable. Desde un punto de vista técnico, todas las redes, incluyendo los servicios DSL, comparten una cantidad fija de ancho de banda entre multitud de usuarios -- pero ya que las redes de cable tienden a abarcar áreas más grandes que los servicios DSL, se debe tener más cuidado para asegurar un buen rendimiento en la red.
Una debilidad más significativa de las redes de cable al usar una línea compartida es el riesgo de la pérdida de privacidad, especialmente considerando la disponibilidad de herramientas de *hacking* para cablemódems. De este problema se encarga el cifrado de datos y otras características de privacidad especificadas en el estándar **DOCSIS** ("**Data Over Cable Service Interface Specification**"), utilizado por la mayoría de cablemodems.

Modems "Celulares"

Con la aparición de la telefonía móvil digital, fue posible acceder a páginas de Internet especialmente diseñadas para móviles, conocidos como tecnología WAP.
Las primeras conexiones se efectuaban mediante una llamada telefónica a un número del operador a través de la cual se transmitían los datos de manera similar a como lo haría un módem de PC.

Posteriormente, nació el GPRS, que permitió acceder a internet a través del protocolo TCP/IP. Mediante el software adecuado es posible acceder, desde un terminal móvil, a servicios como FTP, Telnet, mensajería instantánea, correo electrónico, utilizando los mismos protocolos que un ordenador convencional. La velocidad del GPRS es de 54 kbit/s en condiciones óptimas, y se tarifa en función de la cantidad de información transmitida y recibida.
Otras tecnologías más recientes que permiten el acceso a Internet son EDGE, EvDO HSPA
Aprovechando la tecnología UMTS, que es una de las tecnologías usadas por los móviles de tercera generación (3G) comienzan a aparecer módems para PC que conectan a Internet utilizando la red de telefonía móvil, consiguiendo velocidades similares a las de la ADSL. Este sistema aún es caro ya que el sistema de tarificación no es una verdadera tarifa plana sino que establece limitaciones en cuanto a datos o velocidad.

Módem Redes Inalámbricas

Wireless Data Access (WDA) es la primer tecnología utilizada, para la cual se necesita una antena y un modem, es la tecnología aún utilizada por varios de los proveedores de internet (ISP) en el país.
Poco a poco esta tecnología se está reemplazando por la de WiMax que derivada de la tecnología WIFI, mejora notablemente las capacidades de las de tipo WDA.

1.4. Hub (concentrador)

Es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos. Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central. Llamado también repetidor multipuerto, existen 3 clases.

- **Pasivo:** Sirve sólo como punto de conexión física. No manipula o visualiza el tráfico que lo cruza. No amplifica o limpia la señal. Un hub pasivo se utiliza sólo para compartir los medios físicos. En sí, un hub pasivo no requiere energía eléctrica.

- **Activo:** Necesita alimentación para amplificar la señal entrante antes de pasarla a los otros puertos.

- **Inteligente:** A los hubs inteligentes a veces se los denomina "smart hubs". Estos dispositivos básicamente funcionan como hubs activos, pero también incluyen un chip microprocesador y capacidades diagnósticas. Los hubs inteligentes son más costosos que los hubs activos, pero resultan muy útiles en el diagnóstico de fallas.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.
Los concentradores fueron muy populares hasta que se abarataron los switch que tienen una función similar pero proporcionan más seguridad contra programas como los sniffer. La disponibilidad de switches ethernet de bajo precio ha dejado obsoletos, pero aún se pueden encontrar en instalaciones antiguas y en aplicaciones especializadas.

1.5. La alternativa WIFI el Access Point

Se trata de un dispositivo inalámbrico que mediante sistema de radio frecuencia se encarga de recibir información de diferentes estaciones móviles que pueden ser equipos de escritorio, notebooks, PDA wireless, USB Wifi, etc. . Este dispositivo "capta" la información de las estaciones y las transmite (esta vez, por medio de cables) a un servidor, que puede ser único o formar parte de una red, cableada, más extensa. Su alcance máximo aproximado es de 100 metros y llegan a velocidad de 108Mbps.
Esto soluciona muchos problemas. Al evitar estar "atados" a un cable permite movilidad, comodidad, estética, ahorros de instalaciones, etc. La desventaja en la práctica es que por la frecuencia utilizada se ve bastante afectado a interferencias producidas por medio.

Una posible topología podría ser:

Capa Enlace

1. Cableado Estructurado

En sus inicios se llamó teleproceso a la comunicación de datos, originalmente las terminales sólo eran simples traductores de datos e impulsos electrónicos y viceversa, tanto para ser enviados a que los procesara una computadora central como para interpretar, en el otro sentido, los resultados enviados por esa computadora. Al evolucionar el concepto de teleproceso, y sobre todo la tecnología de información, se cuenta con terminales con inteligencia y una serie de funciones adicionales a las primeras, de manera que son capaces de procesar independientemente a cierto nivel. También ha crecido la necesidad de interconectar las computadoras para poner al alcance del usuario un sin número de información.
En su evolución el teleproceso significa tecnología de la información en su más amplio sentido, ya no sólo significa proceso remoto sino que ahora se transfieren datos, imágenes, voz, música, etc. ya procesados o para procesar.
Estamos frente al concepto de “red”, para el que a su vez se puede hablar en términos muy generales en la interconexión lógica y física.
Un ambiente moderno de negocios debe estar dotado de una infraestructura flexible en la que todo el movimiento de información de la organización sea transportado a través de una plataforma universal.
En el mundo actual de las telecomunicaciones, se hace evidente la necesidad de transmitir más información a mayores distancias; para ello es fundamental que los equipos que procesan y transmiten esta información sean accesibles por el usuario en todo momento; el cableado estructurado es pieza clave en facilitar este proceso.

¿Qué es Cableado Estructurado?

En el clima actual de los negocios, el tener un sistema confiable de cableado para comunicaciones es tan importante como tener un suministro de energía eléctrica en el que se pueda confiar. Hace unos años, el único cable utilizado para el cableado de edificios era el cable regular para teléfono, instalado por las compañías que suministraban Conmutadores y teléfonos. Estas redes de cables eran capaces de manejar comunicaciones de voz pero, para poder apoyar las comunicaciones de datos, se tenía que instalar un segundo sistema privado de cables; por lo que las compañías suministradoras de computadoras tenían que realizar el cableado necesario para sus aplicaciones.
Un sistema de cableado estructurado consiste de una infraestructura flexible de cables que puede aceptar y soportar sistemas de computación y de teléfono múltiples, independientemente de quién fabricó los componentes del mismo. En este sistema, cada estación de trabajo se conecta a un punto central utilizando una topología tipo estrella, facilitando la interconexión y la administración del sistema. Esta disposición permite la comunicación con, virtualmente cualquier dispositivo, en cualquier lugar y en cualquier momento.

2. Dirección física (MAC)

En redes de computadoras la dirección MAC *(Medium Access Control address* o dirección de control de acceso al medio) es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (**los últimos 24 bits**) y el fabricante (**los primeros 24 bits**) utilizando el OUI.
No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma, las direcciones MAC son a veces llamadas *Las Direcciones Quemadas" (BIA, por las siglas de* Burned-in Address*).*
La dirección MAC es un número único de 48 bits asignado a cada tarjeta de red. Se conoce también como la dirección física en cuanto identificar dispositivos de red.
En la mayoría de los casos no es necesario conocer la dirección MAC, ni para montar una red doméstica, ni para configurar la conexión a internet. Pero si queremos configurar una red wifi y habilitar en el punto de acceso un sistema de filtrado basado en MAC (a veces denominado filtrado por hardware), el cual solo permitirá el acceso a la red a adaptadores de red concretos, identificados con su MAC, entonces si que necesitamos conocer dicha dirección.

3. Switch - Bridge

Podemos pensar al switch en una "mezcla de hub y bridge", hub por la capacidad multipuerto, y bridge por la capacidad de conmutación.
La conmutación es una tecnología que alivia la congestión, en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los switches, reemplazan en la actualidad a los hubs y funcionan con infraestructuras de cable existentes, de manera que su instalación puede realizarse con un mínimo de problemas en las redes existentes.
En la actualidad, en las comunicaciones de datos, todos los equipos de conmutación y de enrutamiento ejecutan dos operaciones básicas:

1) Conmutación de tramas de datos: Esta es una operación de "guardar y enviar" en la que una trama llega a un medio de entrada y se transmite a un medio de salida.
2) Mantenimiento de operaciones de conmutación: Los switches crean y mantienen tablas de conmutación y buscan loops.

Como en el caso de los Bridges (puentes), los switches conectan segmentos de la LAN, usan una tabla de direcciones MAC para determinar el segmento en el que es necesario transmitir un datagrama y reducen el tráfico. Los switches operan a velocidades mucho más altas que los puentes y pueden soportar nuevas funcionalidades como, por ejemplo, las LAN virtuales.
Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina *microsegmentación*. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host. Esto aumenta al máximo el ancho de banda disponible en el medio compartido. Otra de las ventajas es que desplazarse a un entorno de LAN conmutado es muy económico ya que el hardware y el cableado se pueden volver a utilizar y dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz.
Por último, los administradores de red tienen mayor flexibilidad para administrar la red a través de la potencia del switch y del software para configurar la LAN.
Resumiendo como ventajas del switch podemos destacar:

- Reducción de la cantidad de colisiones
- Múltiples comunicaciones simultáneas
- Respuesta de red mejorada

Son de aspecto similar a un hub.

Capa Red

1. El Protocolo IP

El protocolo de IP (Internet Protocol) es la base fundamental de la Internet. Porta datagramas de la fuente al destino. El nivel de transporte parte el flujo de datos en datagramas. Durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino. Las principales características de este protocolo son:

- Protocolo orientado a no conexión.
- Fragmenta paquetes si es necesario.
- Direccionamiento mediante direcciones lógicas IP de 32 bits.
- Si un paquete no es recibido, este permanecerá en la red durante un tiempo finito.
- Realiza el "mejor esfuerzo" para la distribución de paquetes.
- Tamaño máximo del paquete de 65635 bytes.
- Sólo ser realiza verificación por suma al encabezado del paquete, no a los datos éste que contiene.

El Protocolo Internet proporciona un servicio de distribución de paquetes de información orientado a no conexión de manera no fiable. La orientación a no conexión significa que los paquetes de información, que será emitido a la red, son tratados independientemente, pudiendo viajar por diferentes trayectorias para llegar a su destino. El término no fiable significa más que nada que no se garantiza la recepción del paquete.
La unidad de información intercambiada por IP es denominada datagrama. Tomando como analogía las tramas intercambiadas por una red física los datagramas contienen un encabezado y una área de datos. IP no especifica el contenido del área de datos, ésta será utilizada arbitrariamente por el protocolo de transporte.

2. Direcciones IP

Es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos equipos con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí.

Las direcciones IP se clasifican en:

- **Direcciones IP públicas**. Son visibles en todo Internet. Un host con una IP pública es accesible (visible) desde cualquier otro host conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- **Direcciones IP privadas (reservadas)**. Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los host con direcciones IP privadas pueden salir a Internet por medio de un router (o *proxy*) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- **Direcciones IP estáticas (fijas)**. Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.
- **Direcciones IP dinámicas**. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99.
Las direcciones IP también se pueden representar en hexadecimal, desde la 00.00.00.00 hasta la FF.FF.FF.FF o en binario, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.
Las tres direcciones siguientes representan a la misma máquina (podemos utilizar la calculadora científica para realizar las conversiones).

(decimal) 128.10.2.30
(hexadecimal) 80.0A.02.1E
(binario) 10000000.00001010.00000010.00011110

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: el *identificador de red* y el *identificador de host*.

3. **Router** (enrutador, ruteador o encaminador)

Es un dispositivo capa tres de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.
Cuando un usuario accede a una URL, el cliente web (navegador) consulta al servidor de nombre de dominio, el cual le indica la dirección IP del equipo deseado.
La estación de trabajo envía la solicitud al router más cercano, es decir, a la pasarela (gateway) predeterminada de la red en la que se encuentra. Este router determinará así el siguiente equipo al que se le enviarán los datos para poder escoger la mejor ruta posible.
Comúnmente los routers se implementan también como puertas de acceso a Internet (por ejemplo un enrutador ADSL), usándose normalmente en casas y oficinas pequeñas. Es correcto utilizar el término router en este caso, ya que estos dispositivos unen dos redes (una red de área local con Internet).

Ejemplos comunes en la actualidad:

3.1. Routers inalámbricos

A pesar de que tradicionalmente los routers solían tratar con redes fijas (Ethernet, ADSL, RDSI...), en los últimos tiempos han comenzado a aparecer los que permiten realizar una interfaz entre redes fijas y móviles (Wi-Fi, GPRS, Edge, UMTS,Fritz!Box, WiMAX)... Si bien comparte el mismo principio que un router tradicional, éste permite la conexión de dispositivos inalámbricos a las redes a las que el router está conectado mediante conexiones por cable. La diferencia existente entre este tipo de routers viene dada por la potencia que alcanzan, las frecuencias y los protocolos en los que trabajan.

3.2. Routers ADSL

Realmente se trata de varios componentes en uno. Realiza las funciones de:

- Puerta de enlace (gateway), ya que proporciona salida hacia el exterior a una red local.
- Router: cuando le llega un paquete procedente de Internet, lo dirige hacia la interfaz destino por el camino correspondiente, es decir, es capaz de rutear paquetes IP.
- Módem ADSL: modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL y demodula las señales recibidas por ésta para que los equipos de la LAN puedan interpretarlos. De hecho, existen configuraciones formadas por un módem ADSL y un router que hacen la misma función que un router ADSL.

- Punto de acceso wireless: algunos router ADSL permiten la comunicación vía Wireless (sin cables) con los equipos de la red local.

Como se puede ver, los avances tecnológicos han conseguido introducir la funcionalidad de cuatro equipos en uno sólo.

Cualquiera de estos routers pueden poseer entre sus características un proxy, firewalls, etc. como asi también múltiples salidas con lo que cumplen además la función de un switch o hub.

4. IPv6

El 6 de junio de 2012 fue el lanzamiento mundial de IPv6, el nuevo protocolo de Internet, que comenzará a funcionar de forma permanente. Se trata del mayor cambio hecho a la red desde sus inicios, y probablemente pasará desapercibido por la mayoría de los usuarios - lo que no lo hace menos relevante.
Desde 1981 se viene utilizando la versión 4 del protocolo (o IPv4), donde operan la mayoría de las comunicaciones de internet. IPv4 usa direcciones de 32 bit, que permite un total de 2^32 direcciones (o 4.294.967.296 direcciones en total). Eso era muchísimo en los 80′s, pero con el desarrollo de la web, las direcciones IPv4 ya se agotaron prácticamente.
La solución es IPv6, la siguiente evolución del protocolo, que usa direcciones de 128 bits y permite 2^128 series de números (como 340 sextillones de direcciones). La idea es que alcance no sólo computadores que se conecten a internet, sino también smartphones, tablets, y otros dispositivos inteligentes que pudieran aparecer. IPv6 se terminó de desarrollar en 1996, y las primeras redes ya se podían construir en 1999, sin embargo, la implementación del sistema ha tomado tiempo.

Si hoy comenzamos a usar IPv6, ¿se acaba IPv4?
Pese a que es el lanzamiento mundial, muchas empresas alrededor del mundo no han implementado IPv6 todavía y siguen usando direcciones IPv4. Esto es especialmente cierto en Latinoamérica, que es la región geográfica que más direcciones IPv4 tiene disponibles.
Asia ya las agotó, mientras que Norteamérica y Europa están a punto de terminárselas todas. América Latina y el Caribe todavía tienen reservas hasta 2014, lo que significa que probablemente nuestra región avance más lento que el resto en IPv6.

¿IPv6 crea una "internet separada"?
El problema de IPv6 es que **no tiene interoperabilidad con IPv4**, sino que funciona en paralelo, creando una Internet independiente a la que existe ahora. Por ejemplo, si una persona entra a un sitio en una dirección IPv6, y trata de comunicarse con otro (a través de un link por ejemplo) que funcione sobre IPv4, podría obtener un mensaje de error. A la inversa, habrá personas que no podrán entrar a sitios que sólo tengan dirección IPv6, si es que sus ISPs no dan soporte a este protocolo.

¿Qué sitios están operando en IPv6?
Aquí hay una lista completa con las webs que ya están operativas en IPv6. Universidades, organizaciones y empresas como Google, Facebook, Bing, Cisco y otros comenzarán a funcionar usando IPv6 desde ya.

¿Estamos listos para IPv6?
Casi todos los sistemas operativos modernos, incluyendo a Mac OS X de Apple, Windows de Microsoft, y gran parte de las distribuciones de Linux que existen tienen soporte para IPv6 integrado desde hace años.
Es necesario un Router que soporte IPv6 aunque hay que recordar que **si tu ISP (Proveedor de servicio de internet) no está entregando soporte al nuevo sistema, no servirá de nada.**

Capa Transporte

1. La capa de transporte y la calidad del servicio

La frase "calidad del servicio" (QoS, Quality of Service, en inglés) se usa a menudo para describir el propósito de la Capa 4, la capa de transporte. Sus funciones principales son transportar y regular el flujo de información desde el origen hasta el destino de manera confiable y precisa. El control de extremo a extremo, que suministran las ventanas deslizantes, y la confiabilidad proporcionada por el uso de números de secuencia y acuses de recibo son las funciones principales de la Capa 4.
Para comprender la confiabilidad y el control de flujo, piense en un estudiante que ha estudiado un idioma extranjero durante un año. Ahora imagine que este estudiante visita el país donde se habla ese idioma. Durante las conversaciones, deberá pedirle a la gente que repitan lo que han dicho (para confiabilidad) y que hablen despacio, para que pueda entender las palabras (control de flujo).

2. El Protocolo TCP (*Transmission Control Protocol*)

Este protocolo de control de transmisión está basado en IP que es no fiable y no orientado a conexión, y sin embargo es:
Orientado a conexión. Es necesario establecer una conexión previa entre las dos máquinas antes de poder transmitir ningún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.
Fiable. La información que envía el emisor llega de forma correcta al destino.

El protocolo TCP permite una comunicación fiable entre dos aplicaciones. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

El flujo de datos entre una aplicación y otra viajan por un *circuito virtual*. Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los routers que atraviesen, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logre la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro (algo así como una tubería entre el origen y el destino). Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados. La unidad de datos del protocolo es el *byte*, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes.

El protocolo TCP envía un *flujo de información no estructurado*. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra. Ambas aplicaciones deberán ponerse de acuerdo para comprender la información que se están enviando.
Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es *full-dúplex*.

3. Puertos TCP

TCP usa el concepto de *número de puerto* para identificar a las aplicaciones emisoras y receptoras. Cada lado de la conexión TCP tiene asociado un número de puerto (de 16 bits sin signo, con lo que existen 65536 puertos posibles) asignado por la aplicación emisora o receptora. Los puertos son clasificados en tres categorías: bien conocidos, registrados y dinámicos/privados. Los puertos bien conocidos son asignados por la Internet Assigned Numbers Authority (IANA), van del 0 al 1023 y son usados normalmente por el sistema o por procesos con privilegios. Las aplicaciones que usan este tipo de puertos son ejecutadas como servidores y se quedan a la escucha de conexiones. Algunos ejemplos son: FTP (21), SSH (22), Telnet (23), SMTP (25) y HTTP (80). Los puertos registrados son normalmente empleados por

las aplicaciones de usuario de forma temporal cuando conectan con los servidores, pero también pueden representar servicios que hayan sido registrados por un tercero (rango de puertos registrados: 1024 al 49151). Los puertos dinámicos/privados también pueden ser usados por las aplicaciones de usuario, pero este caso es menos común. Los puertos dinámicos/privados no tienen significado fuera de la conexión TCP en la que fueron usados (rango de puertos dinámicos/privados: 49152 al 65535, recordemos que el rango total de 2 elevado a la potencia 16, cubre 65536 números, del 0 al 65535)

Algunos de los puertos usados más comunes son:

Puerto	Descripción
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP -- Datos
21	FTP -- Control
22	SSH - Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	WhoIs
49	Login Host Protocol (Login)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Services
79	Finger
80	HTTP
103	X.400 Standard
108	SNA Gateway Access Server
109	POP2
110	POP3
115	Simple File Transfer Protocol (SFTP)

Puerto	Descripción
118	SQL Services
119	Newsgroup (NNTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
150	NetBIOS Session Service
156	SQL Server
161	SNMP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
194	Internet Relay Chat (IRC)
197	Directory Location Service (DLS)
389	Lightweight Directory Access Protocol (LDAP)
396	Novell Netware over IP
443	HTTPS
444	Simple Network Paging Protocol (SNPP)
445	Microsoft-DS
458	Apple QuickTime
546	DHCP Client
547	DHCP Server
563	SNEWS
569	MSN
1080	Socks

Capa Aplicación

1. Proxy

En el contexto de las redes informáticas, el término **proxy** hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de **servidor proxy**, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

- El uso más común es el de **servidor proxy**, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.
  - De ellos, el más famoso es el **servidor proxy de web** (comúnmente conocido solamente como «**proxy**»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.
  - También existen proxies para otros protocolos, como el **proxy de FTP**.
  - El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.

1.1. Proxy de web / Proxy cache de web

Se trata de un proxy para una aplicación específica; el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una cache para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Funcionamiento

1) El cliente realiza una petición (por ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
2) Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, devuelve el documento inmediatamente, si no es así, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda una copia en su caché para futuras peticiones.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").
Los proxies web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

1.2. Proxy NAT (Network Address Translation) / Enmascaramiento

Otro mecanismo para hacer de intermediario en una red es el NAT.
La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").
Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó.

Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x
Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.
Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.
La función de NAT reside en los Firewalls y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un router.

2. El protocolo HTTP (HyperText Transfer Protocol)
El Protocolo de Transferencia de HiperTexto es un protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP. La especificación completa del protocolo HTTP 1/0 está recogida en el RFC 1945. Fue propuesto por Tim Berners-Lee, atendiendo a las necesidades de un sistema global de distribución de información como el World Wide Web.
Desde el punto de vista de las comunicaciones, está soportado sobre los servicios de conexión TCP/IP.
Un proceso del servidor escucha en un puerto de comunicaciones TCP (por defecto, el 80), y espera las solicitudes de conexión de los clientes Web. Una vez que se establece la conexión, el protocolo TCP se encarga de mantener la comunicación y garantizar un intercambio de datos libre de errores.
HTTP se basa en sencillas operaciones de solicitud/respuesta. Un cliente establece una conexión con un servidor y envía un mensaje con los datos de la solicitud. El servidor responde con un mensaje similar, que contiene el estado de la operación y su posible resultado. Todas las operaciones pueden adjuntar un objeto o recurso sobre el que actúan; cada objeto Web (documento HTML, fichero multimedia o aplicación CGI) es conocido por su URL.
Etapas de una transacción HTTP.

3. **El protocolo FTP** (File Transfer Protocol)
Es un protocolo para transferir archivos.
La implementación del FTP se remonta a 1971 cuando se desarrolló un sistema de transferencia de archivos (descrito en RFC141) entre equipos del Instituto Tecnológico de Massachusetts (*MIT, Massachusetts Institute of Technology*). Desde entonces, diversos documentos de RFC (petición de comentarios) han mejorado el protocolo básico, pero las innovaciones más importantes se llevaron a cabo en julio de 1973.
El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP. U objetivo es:

- permitir que equipos remotos puedan compartir archivos
- permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor
- permitir una transferencia de datos eficaz

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor).

4. Protocolos de correo electrónico (SMTP, POP, IMAP)
Hoy día, el correo electrónico es entregado usando una arquitectura cliente/servidor. Un mensaje de correo electrónico es creado usando un programa de correo cliente. Este programa luego envía el mensaje a un servidor. El servidor luego lo redirige al servidor de correo del recipiente y allí se le suministra al cliente de correo del recipiente.

Para permitir todo este proceso, existe una variedad de protocolos de red estándar que permiten que diferentes máquinas, a menudo ejecutando sistemas operativos diferentes y usando diferentes programas de correo, envíen y reciban correo electrónico o email.
Los protocolos que se indican a continuación son los que más se utilizan para transferir correo electrónico.

5. Protocolos de transporte de correo

La entrega de correo desde una aplicación cliente a un servidor, y desde un servidor origen al servidor destino es manejada por el *Protocolo simple de transferencia de correo* (*Simple Mail Transfer Protocol* o *SMTP*).

5.1. SMTP

El objetivo principal del protocolo simple de transferencia de correo, SMTP, es transmitir correo entre servidores de correo. Sin embargo, es crítico para los clientes de correo también. Para poder enviar correo, el cliente envia el mensaje a un servidor de correo saliente, el cual luego contacta al servidor de correo de destino para la entrega. Por esta razón, es necesario especificar un servidor SMTP cuando se esté configurando un cliente de correo.
Un punto importante sobre el protocolo SMTP es que no requiere autenticación. Esto permite que cualquiera en la Internet puede enviar correo a cualquiera otra persona o a grandes grupos de personas. Esta característica de SMTP es lo que hace posible el correo basura o *spam*. Los servidores SMTP modernos intentan minimizar este comportamiento permitiendo que sólo los hosts conocidos accedan al servidor SMTP. Los servidores que no ponen tales restricciones son llamados servidores *open relay*.

5.2. Protocolos de acceso a correo

Hay dos protocolos principales usados por las aplicaciones de correo cliente para recuperar correo desde los servidores de correo: el *Post Office Protocol* (*POP*) y el *Internet Message Access Protocol* (*IMAP*).
A diferencia de SMTP, estos protocolos requieren autenticación de los clientes usando un nombre de usuario y una contraseña. Por defecto, las contraseñas para ambos protocolos son pasadas a través de la red sin encriptar.

POP

Cuando se utiliza POP, los mensajes de correo son descargados a través de las aplicaciones de correo cliente. Por defecto, la mayoría de los clientes de correo POP son configurados para borrar automáticamente el mensaje en el servidor de correo después que éste ha sido transferido exitósamente, sin embargo esta configuración se puede cambiar.
POP es completamente compatible con estándares importantes de mensajería de Internet, tales como *Multipurpose Internet Mail Extensions* (*MIME*), el cual permite los anexos de correo.
POP funciona mejor para usuarios que tienen un sistema en el cual leer correo. También funciona bien para usuarios que no tienen una conexión permanente a la Internet o a la red que contiene el servidor de correo. Desafortunadamente para aquellos con conexiones lentas, POP requiere que luego de la autenticación los programas cliente descarguen el contenido completo de cada mensaje. Esto puede tomar un buen tiempo si algún mensaje tiene anexos grandes.
La versión más reciente del protocolo estándar POP es POP3.
Para añadir seguridad, es posible utilizar la encriptación *Secure Socket Layer* (*SSL*) para la autenticación del cliente y las sesiones de transferencias de datos.

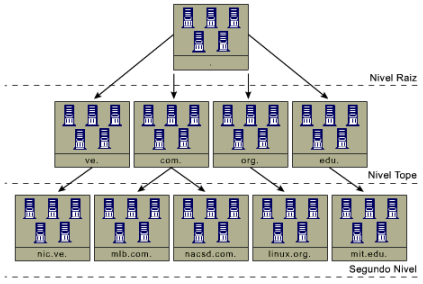
5.3. IMAP

En el caso de un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios pueden leerlos o borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo.
IMAP lo utilizan principalmente los usuarios que acceden a su correo desde varias máquinas. El protocolo es conveniente también para usuarios que se estén conectando al servidor de correo a través de una conexión lenta, porque sólo la información de la cabecera del correo es

descargada para los mensajes, hasta que son abiertos, ahorrando de esta forma ancho de banda. El usuario también tiene la habilidad de eliminar mensajes sin verlos o descargarlos.
Por conveniencia, las aplicaciones cliente IMAP son capaces de hacer caché de los mensajes localmente, para que el usuario pueda hojear los mensajes previamente leídos cuando no se esté conectado directamente al servidor IMAP.
IMAP, como POP, es completamente compatible con estándares de mensajería de Internet, tales como MIME, que permite los anexos de correo.
Para seguridad adicional, es posible utilizar la encriptación *SSL* para la autenticación de clientes y para las sesiones de transferencia de datos.

6. El protocolo DNS

En el grupo de protocolos TCP-IP se encuentran los protocolos de resolución de nombres por direcciones IP. Estos protocolos permiten a las aplicaciones tener acceso a los servicios de un servidor a través del uso de un nombre. Para ello debe existir un mecanismo que permita la resolución y asociación de una dirección IP por un nombre. El mecanismo de asociación consiste en una base de datos donde se encuentran las asociaciones de una dirección IP con su nombre respectivo. Y el mecanismo de resolución consiste en identificar cual es la dirección IP asociada a un nombre. De esta manera los host de la red pueden ser accesados a través de un nombre en vez de su dirección IP.
En los comienzos de la red Internet la resolución de nombres por números IP se realizaba a través de un archivo de texto llamado hosts. Este archivo de texto contenía todas las direcciones IP asociadas al nombre asignado a cada computador. A medida que la red Internet fue creciendo este método de resolución de nombre por números IP fue presentando problemas debido a que el archivo hosts era administrado por el administrador de cada red, de esta manera no se podía garantizar que un administrador no asignara el mismo nombre a máquinas distintas ubicadas en redes distintas. Esto trae como consecuencia la colisión de nombres e inconsistencia del archivo hosts a lo largo de una red en crecimiento.
Con el fin de resolver los problemas explicados anteriormente se desarrolló el protocolo de Sistema de nombres de dominios "DNS Domain Name System". Este protocolo es una base de datos distribuida que permite un control local sobre los segmentos de la base de datos en general, logrando que cada segmento esté disponible a lo largo de toda la red Internet. El sistema de nombres de dominios utiliza un esquema cliente servidor. El protocolo DNS está compuesto por dos programas uno llamado **servidor de nombres de dominios** y otro llamado **resolvers**. Los servidores de nombres de dominios contienen la base de datos de un segmento y dicha base de datos es accesada por los clientes a través de un programa conocido como resolvers. Los resolvers son rutinas utilizadas para tener acceso a la base de datos ubicada en los servidores de nombres de dominios con el fin de resolver la búsqueda de una dirección IP asociada a un nombre.
Un nombre de dominio es un índice dentro de la base de datos DNS. Los nombres indexados en un dominio son las rutas que conforman el espacio de nombres de dominio. El nombre completo asociado a una dirección IP es una secuencia de nombres de dominios asignados desde su nodo hasta el nodo raíz.
El espacio de dominio de la red Internet está dividido básicamente en tres niveles: Nivel Raíz, Nivel Tope y Nivel secundario. En la figura siguiente podemos observar el nivel jerárquico de cada uno de estos niveles.



- Com. Son dominios asignados a organizaciones comerciales. Ej. newdevices.com.
- Edu. Son dominios asignados a instituciones educativas. Ej. ucv.edu.
- Gov. Son dominios asignados a agencias gubernamentales.
- Net. Son dominios asignados a organizaciones relacionadas con la red Internet.
- Org. Son dominios asignados a organizaciones sin fines de lucro.

Además de estos nombres de dominio incluidos en el nivel tope se encuentran los nombres de dominio geográficos basados en la nomenclatura ISO3166. Cada uno de estos nombres de dominio son administrados por cada país. Este tipo de nombres de dominio son organizados por localidad y son útiles para organizaciones y negocios que deseen operar en dicha localidad geográfica.
Los servidores de nombres de dominio de nivel tope delegan la resolución de nombres por números IP a los servidores de nombres de dominio de nivel secundario. En este nivel se encuentran todos los nombres de dominio asignados a las computadoras que ofrecen servicios de Internet. Ejemplo: www.caida.org..

7. **El protocolo DHCP** (Dynamic Host Configuration Protocol)

Son las siglas que identifican a un protocolo empleado para que los hosts (clientes) en una red puedan obtener su configuración de forma dinámica a través de un servidor del protocolo. Los datos así obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de broadcast, las características del DNS, entre otros. El servicio DHCP permite acelerar y facilitar la configuración de muchos hosts en una red evitando en gran medida los posibles errores humanos.
Un servidor de DHCP puede identificar a cada cliente a través de dos formas fundamentales:
La dirección MAC (*Media Access Control*) de la tarjeta de red del cliente.
Un identificador que le indique el cliente.
Aunque la idea central del servicio DHCP es la dinamicidad de las direcciones IP asignadas no se excluye la posibilidad de utilizar direcciones fijas para algunos *hosts* que por sus características lo requieran, ejemplo de ello son las máquinas proveedoras de disímiles servicios como el correo electrónico o el DNS. Este tipo de *host* utilizaría las ventajas del servicio para obtener el resto de los datos que se pueden proveer mediante DHCP.

Las ventajas del uso de DHCP son:

a) solo se configura un servidor para entregar números IP para clientes de red
b) se entregan todos los parámetros básicos de TCP/IP
c) facilidad de configuración
d) Las desventajas del uso de DHCP son:
e) La seguridad
f) Al entregar números IP dentro de la red, habiendo un DNS, no hay un puente intermedio entre DNS y DHCP directo. Es decir, hay que agregar las máquinas "a mano" en el DNS
g) Mayor difusión de paquetes en la red, aunque hoy en día con la velocidad de las redes no parece demasiado problemático.

8. **Telnet vs SSH** (TELecommunication NETwork)

Es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.
Telnet sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. También se usaba para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc.
Aparte de estos usos, en general telnet se ha utilizado (y aún hoy se puede utilizar en su variante SSH) para abrir una sesión con una máquina UNIX, de modo que múltiples usuarios

con cuenta en la máquina, se conectan, abren sesión y pueden trabajar utilizando esa máquina. Es una forma muy usual de trabajar con sistemas UNIX.
Su mayor problema es de seguridad, por esta razón dejó de usarse, casi totalmente, hace unos años, cuando apareció y se popularizó el SSH, que puede describirse como una versión cifrada de telnet.

9. SSH (Secure SHell)

SSH o shell seguro fue desarrollado por Tatu Ylönen en Finlandia, como parte de una estrategia para remplazar TELNET, RCP, RSH; la estrategia principal de este sistemas es permitir conexiones seguras por medio de la la codificación de los mensajes entre el servidor y el cliente. Adicionalmente permite la compresión de la información que se envía de manera opcional, pudiendo utilizarse con otros sistemas de autenticación como kerberos, y S/KEY, para de esta manera proveer todo un marco de alta seguridad en entornos UNIX de conexión remota..
La primera versión del protocolo se conoce como SSH1, en un principio era gratuito, pero hoy día en su última versión es un protocolo que requiere licenciamiento si desea más información a este respecto la puede encontrar en: http://www.ssh.fi/.

¿Por qué y para que SSH?

El motivo principal por el que se utiliza este sistema es debido a la falta de seguridad de los sistemas de acceso remoto tipo telnet. Esta falta de seguridad radica en el envío de información en texto plano, es decir sin ningún tipo de codificación que evite el que la información sea leída por alguien indebido, además de esto los sistemas de log remoto anteriores no hacían verificación de ningún tipo sobre la máquina que estaba intentando conectarse con el servidor, abriendo la puerta a una serie de problemas informáticos relacionados con intrusos. O personas indeseables tratando de acceder al sistema. El esquema de seguridad usado por este sistema es el de llave publica/privada, de tipo RSA para de esta manera hacer el doble proceso de verificación y de codificación de la información.
Las características anteriores de la conexión permiten por tanto una protección mucho más elevada así:

- Captura de información por parte de hackers en la transmisión.
- Manipulación de la información a lo largo de la transmisión.
- Suplantación de direcciones IP
- Suplantación en el DNS
- Desvío de la información de una IP

Por estas razones es un esquema bastante seguro en entornos que requieren acceso remoto al sistema o al servidor, y que deseen proteger la integridad de la información.

Fuentes:

- http://www.une.edu.ve/~iramirez/telecom2/Osi/mcomunicacion.htm
- http://www.adslfaqs.com.ar/que-es-una-wan/
- http://docente.ucol.mx/al956659/public_html/cableados.html
- http://www.econ.uba.ar/www/departamentos/sistemas/plan97/tecn_informac/briano/seoane/tp/2002_1/redes.htm
- http://www.une.edu.ve/~iramirez/telecom2/Osi/osi.htm
- http://abc.gov.ar/lainstitucion/revistacomponents/otraspublicaciones/index.cfm?ISSN=0000-0000&CLASE=RECURSO

Autor: Prof. Daniela Casco

Cómo citar este texto:
Daniela Casco (2014), “Informática III – Redes”, Departamento de Tecnologías de la Información y las Comunicaciones, Escuela Superior de Comercio “Lib. Gral. San Martín” (UNR).