# Conceptos Básicos de Redes

**By DrinShot**

**Índice General**



**By DrinShot**

## 1. Conceptos básicos [ Importantes ]

**Internet:** Una red interna específica, consiste en una interconexión mundial de las redes gubernamentales, académicas, públicas, y privadas basadas sobre el Advanced Research Projects Agency Network (ARPANET) desarrollado por ARPA del departamento de los EE.UU. de la defensa también a casa al World Wide Web (WWW) y designado el "Internet" con un capital "I" para distinguirlo de otros internetworks genéricos.

**Intranet:** Una red o una red interna que se limitan en alcance a una sola organización o entidad y que utilicen el TCP/ip Protocol Suite, el HTTP, el ftp, y los otros protocolos y software de red de uso general en el Internet. Nota: Intranets se puede también categorizar como el LAN, CAN, MAN, WAN, o el otro tipo de red.

**Extranet:** Una red o una red interna que se limitan en alcance a una sola organización o entidad pero que también han limitado conexiones a las redes de una o más generalmente, pero no necesariamente, organizaciones confiadas o entidades (e.g., los clientes de una compañía pueden tener acceso proporcionado a una cierta parte de su Intranet thusly que crea un extranet mientras que al mismo tiempo los clientes pueden no ser considerados "confiados en" de un punto de vista de la seguridad). Nota: Técnico, un extranet se puede también categorizar como CAN, MAN, WAN, u otro tipo de red, aunque, por la definición, un extranet no puede consistir en un solo LAN, porque un extranet debe tener por lo menos una conexión con una red exterior. Intranets y los extranets pueden o no pueden tener conexiones al Internet. Si está conectado con el Internet, el Intranet o el extranet se protege normalmente contra ser alcanzado del Internet sin la autorización apropiada. El Internet en sí mismo no se considera ser una parte del Intranet o del extranet, aunque el Internet puede servir como portal para el acceso a las porciones de un extranet.

**Puente de red:** Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete.

Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red.

Funciona a través de una tabla de direcciones MAC detectadas en cada segmento a que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.

La principal diferencia entre un bridge y un hub es que el segundo pasa cualquier trama con cualquier destino para todos los otros nodos conectados, en cambio el primero sólo pasa las tramas pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico inútil.

Para hacer el bridging o interconexión de más de 2 redes, se utilizan los switches.

**Switch:** Un switch (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

**Router:** En español, enrutador o encaminador. Dispositivo de hardware para interconexión de redes de las computadoras que opera en la capa tres.

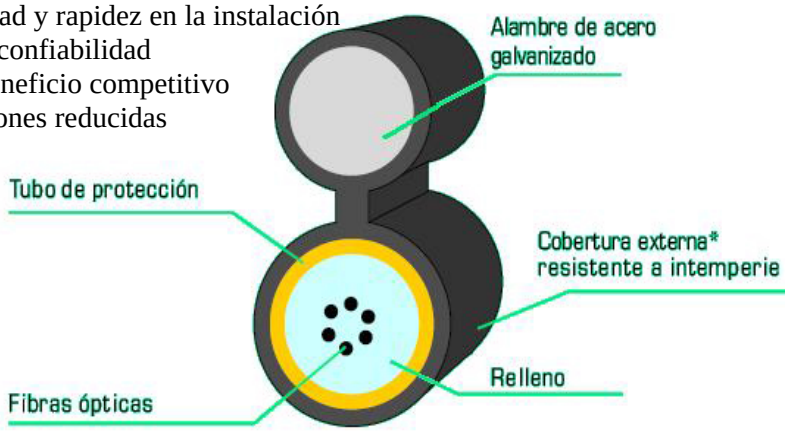
**Cable Drop Óptico:** Es un tipo de cable que es recomendado como cable de acceso al usuario en Operadoras de Telecomunicaciones.

Este cable también es apropiado en cooperativas de electrificación rural y agropecuaria con interés en desarrollar redes propias de transmisión de datos y telefonía para su comunidad.

Su construcción, le ofrece gran facilidad de instalación y confiabilidad de red, sumado al bajo costo de instalación y mantenimiento.

**Características**

- Cable óptico auto-sustentado de alta resistencia mecánica
- Bajo peso
- Practicidad y rapidez en la instalación
- Elevada confiabilidad
- Costo-beneficio competitivo
- Dimensiones reducidas




**Transceiver:** (Transductor) Dispositivo que recibe la potencia de un sistema mecánico, electromagnético o acústico y lo transmite a otro, generalmente en forma distinta. El micrófono y el altavoz son ejemplos de transductores. En comunicaciones (informática) es un transmisor/receptor de señales de radio frecuencia (RF), sirve para conectar aparatos por vía inalámbrica.

**Repetidores:** Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

En una red de comunicaciones, los repetidores son utilizados para regenerar la información que circula por el medio, dándole potencia y la vuelve a dejar en el medio para ser transportada hasta el ordenador destino.

**Direcciones físicas:** son aquellas que referencian alguna posición en la memoria física.

**Direcciones lógicas:** son las direcciones utilizadas por los procesos. Sufren una serie de transformaciones, realizadas por el procesador (la MMU), antes de convertirse en direcciones físicas.

**Módem:** Dispositivo que permite al ordenador transmitir y recibir información a través de la línea telefónica. Este sirve para conectar tu PC a Internet

## 2. ¿Qué son las redes?

Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de computadoras y/o dispositivos conectados por enlaces, a través de medios físicos (medios guiados) ó inalámbricos (medios no guiados) y que comparten información (**archivos**), recursos (**CD-ROM, impresoras, etc**.) y servicios (**e-mail, chat, juegos**), etc.

## 3. Componentes de una red

Dentro de lo que son componentes de una red vamos a distinguir entre equipos de red, cableados y conectores a la misma; y, dentro de los equipos de red, también vamos a hacer una subdivisión en equipos que interconectan redes y equipos conectados a un segmento de las mismas.

**Equipos que interconectan redes. Repetidores.**

Los repetidores son equipos que trabajan a nivel 1 de la pila OSI, es decir, repiten todas las señales de un segmento a otro a nivel eléctrico.

Se utilizan para resolver los problemas de longitudes máximas de los segmentos de red (su función es extender una red Ethernet más allá de un segmento). No obstante, hay que tener en cuenta que, al retransmitir todas las señales de un segmento a otro, también retransmitirán las colisiones. Estos equipos sólo aíslan entre los segmentos los problemas eléctricos que pudieran existir en algunos de ellos.

El número máximo de repetidores en cascada es de cuatro, pero con la condición de que los segmentos 2 y 4 sean IRL, es decir, que no tengan ningún equipo conectado que no sean los repetidores. En caso contrario, el número máximo es de 2, interconectando 3 segmentos de red.

El repetidor tiene dos puertas que conectan dos segmentos Ethernet por medio de transceivers (instalando diferentes transceivers es posible interconectar dos segmentos de diferentes medios físicos) y cables drop.

El repetidor tiene como mínimo una salida Ethernet y otra para teléfono.

Con un repetidor modular se pude centralizar y estructurar todo el cableado de un edificio, con diferentes medios, adecuados según el entorno, y las conexiones al exterior.

Un Concentrador es un equipo igual a un multiport repeater pero con salida RJ-45.

Los repetidores con buffers son aquellos que trabajan a nivel de paquetes de datos. En lugar de pasar la información contenida en la señal, almacena paquetes enteros de una red en un buffer interno y, luego, lo retransmite a la otra red, por lo que no deja pasar las colisiones. Debido a que los fenómenos de bajo nivel, como las colisiones, no son repetidos.

**Puentes o Bridges.**

Estos equipos se utilizan asimismo para interconectar segmentos de red, (amplía una red que ha llegado a su máximo, ya sea por distancia o por el número de equipos) y se utilizan cuando el tráfico no es excesivamente alto en las redes pero interesa aislar las colisiones que se produzcan en los segmentos interconectados entre sí.

Los bridges trabajan en el nivel 2 de OSI, con direcciones físicas, por lo que filtra tráfico de un segmento a otro.

Esto lo hace de la siguiente forma: Escucha los paquetes que pasan por la red y va configurando una tabla de direcciones físicas de equipos que tiene a un lado y otro (generalmente tienen una tabla dinámica), de tal forma que cuando escucha en un segmento un paquete de información que va dirigido a ese mismo segmento no lo pasa al otro, y viceversa.

No filtra los broadcasts, que son paquetes genéricos que lanzan los equipos a la red para que algún otro les responda, aunque puede impedir el paso de determinados tipos de broadcast. Esto es típico para solicitar las cargas de software, por ejemplo. Por tanto, al interconectar segmentos de red con bridges, podemos tener problemas de tormentas de broadcasts, de saturación del puente por sobrecarga de tráfico, etc.

El número máximo de puentes en cascada es de siete; no pueden existir bucles o lazos activos, es decir, si hay caminos redundantes para ir de un equipo a otro, sólo uno de ellos debe estar activo, mientras que el redundante debe ser de backup. Para esto, cuando se está haciendo bridging en las redes, se usa el algoritmo de spanning-tree, mediante el cual se deshacen los bucles de los caminos redundantes.

Las posibles colisiones no se transmiten de un lado a otro de la red. El bridge sólo deja pasar los datos que van a un equipo que él conoce.

El bridge generalmente tiene una tabla dinámica, aíslan las colisiones, **pero no filtran protocolos**.

El bridge trabaja en el nivel 2 de OSI y aísla las colisiones

La primera vez que llega un paquete al bridge lo transmitirá, pero aprende (ya que, si el paquete no lo coge nadie, significa que no está).

El peligro de los bridges es cuando hay exceso de broadcast y se colapsa la red. A esto se le llama tormenta de broadcast, y se produce porque un equipo está pidiendo ayuda (falla).

## 4. ¿Qué es TCP/IP?

Cuando se habla de TCP/IP, se relaciona automáticamente como el protocolo sobre el que funciona la red Internet. Esto, en cierta forma es cierto, ya que se le llama TCP/IP, a la familia de protocolos que nos permite estar conectados a la red Internet. Este nombre viene dado por los dos protocolos estrella de esta familia:

- El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.

- El protocolo IP, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras maquinas.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre ordenadores, además de los que proporciona los protocolos TCP e IP.

**Arquitectura de protocolos TCP/IP**

Para poder solucionar los problemas que van ligados a la comunicación de ordenadores dentro de la red Internet, se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada TCP/IP:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación (módem, tarjeta de red...)

- La comunicación no esta orientada a la conexión de dos maquinas, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos maquinas.

- La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.

- El uso de la red no impone ninguna topología en especial (distribución de los distintos ordenadores).

De esta forma, podremos decir, que dos redes están interconectadas, si hay una maquina común que pase información de una red a otra. Además, también podremos decir que una red Internet virtual realizara conexiones entre redes, que ha cambio de pertenecer a la gran red, colaboraran en el trafico de información procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las maquinas que implementen estas funciones, y de los sistemas operativos que estas utilicen.

**Descomposición en niveles de TCP/IP.**

Toda arquitectura de protocolos se descompone en una serie de niveles, usando como referencia el modelo OSI. Esto se hace para poder dividir el problema global en subproblemas de más fácil solución.

Al diferencia de OSI, formado por una torre de siete niveles, TCP/IP se descompone en cinco niveles, cuatro niveles software y un nivel hardware. A continuación pasaremos a describir los niveles software, los cuales tienen cierto paralelismo con el modelo OSI.

**Nivel de aplicación**

Constituye el nivel mas alto de la torre tcp/ip. A diferencia del modelo OSI, se trata de un nivel simple en el que se encuentran las aplicaciones que acceden a servicios disponibles a través de Internet. Estos servicios están sustentados por una serie de protocolos que los proporcionan.

Por ejemplo, tenemos el protocolo FTP (File Transfer Protocol), que proporciona los servicios necesarios para la transferencia de ficheros entre dos ordenadores.

Otro servicio, sin el cual no se concibe Internet, es el de correo electrónico, sustentado por el protocolo SMTP (Simple Mail Transfer Protocol).

**Nivel de transporte**

Este nivel proporciona una comunicación extremo a extremo entre programas de aplicación. La maquina remota recibe exactamente lo mismo que le envió la maquina origen.

En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de flujo y control de errores, y se los pasa al nivel de red junto con la dirección de destino.

En el receptor este nivel se encarga de ordenar y unir las tramas para generar de nuevo la información original.

Para implementar el nivel de transporte se utilizan dos protocolos:

- **UDP:** proporciona un nivel de transporte no fiable de data gramas, ya que apenas añade información al paquete que envía al nivel inferior, solo la necesaria para la comunicación extremo a extremo. Lo utilizan aplicaciones como NFS y RPC, pero sobre todo se emplea en tareas de control.

- **TCP (Transport Control Protocolo):** es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. Esta pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de aplicaciones de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, perdidas de paquete, orden en que llegan los paquetes, duplicados de paquetes, ...) que gestiona el propio protocolo. Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes a enviar. Debido a que los paquetes a enviar tienen un tamaño máximo, como mas información añada el protocolo para su gestión, menos información que proviene de la aplicación podrá contener ese paquete. Por eso, cuando es mas importante la velocidad que la fiabilidad, se utiliza UDP, en cambio TCP asegura la recepción en destino de la información a transmitir.

**Nivel de red**

También recibe el nombre de **nivel Internet**. Coloca la información que le pasa el nivel de transporte en data gramas IP, le añade cabeceras necesaria para su nivel y lo envía al nivel inferior. Es en este nivel donde se emplea el algoritmo de encaminamiento, al recibir un data grama del nivel inferior decide, en función de su dirección, si debe procesarlo y pasarlo al nivel superior, o bien encaminarlo hacia otra maquina. Para implementar este nivel se utilizan los siguientes protocolos:

- **IP (Internet Protocol):** es un protocolo no orientado a la conexión, con mensajes de un tamaño máximo. Cada data grama se gestiona de forma independiente, por lo que dos data gramas pueden utilizar diferentes caminos para llegar al mismo destino, provocando que lleguen en diferente orden o bien duplicados. Es un protocolo no fiable, eso quiere decir que no corrige los anteriores problemas, ni tampoco informa de ellos. Este protocolo recibe información del nivel superior y le añade la información necesaria para su gestión (direcciones IP, checksum)

- **ICMP (Internet Control Message Protocol):** proporciona un mecanismo de comunicación de información de control y de errores entre maquinas intermedias por las que viajaran los paquetes de datos. Esto data gramas los suelen emplear las maquinas (gateways, host, ...) para informarse de condiciones especiales en la red, como la existencia de una congestión , la existencia de errores y las posibles peticiones de cambios de ruta. Los mensajes de ICMP están encapsulados en data gramas IP.

- **IGMP (Internet Group Management Protocol):** este protocolo esta íntimamente ligado a IP. Se emplea en maquinas que emplean IP multicast. El IP multicast es una variante de IP que permite emplear data gramas con múltiples destinatarios.

También en este nivel tenemos una serie de protocolos que se encargan de la resolución de direcciones:

- **ARP (Address Resolution Protocol):** cuando una maquina desea ponerse en contacto con otra conoce su dirección IP, entonces necesita un mecanismo dinámico que permite conocer su dirección física. Entonces envía una petición ARP por broadcast ( o sea a todas las maquinas ). El protocolo establece que solo contestara a la petición, si esta lleva su dirección IP. Por lo tanto solo contestara la maquina que corresponde a la dirección IP buscada, con un mensaje que incluya la dirección física. El software de comunicaciones debe mantener una cache con los pares IP-dirección física. De este modo la siguiente vez que hay que hacer una transmisión a es dirección IP, ya conoceremos la dirección física.

- **RARP (Reverse Address Resolution Protocol):** a veces el problema es al revés, o sea, una máquina solo conoce su dirección física, y desea conocer su dirección lógica. Esto ocurre, por ejemplo, cuando se accede a Internet con una dirección diferente, en el caso de PC que acceden por módem a Internet, y se le asigna una dirección diferente de las que tiene el proveedor sin utilizar. Para solucionar esto se envía por broadcast una petición RARP con su dirección física, para que un servidor pueda darle su correspondencia IP.

- **BOOTP (Bootstrap Protocol):** el protocolo RARP resuelve el problema de la resolución inversa de direcciones, pero para que pueda ser mas eficiente, enviando más información que meramente la dirección IP, se ha creado el protocolo BOOTP. Este además de la dirección IP del solicitante , proporciona información adicional, facilitando la movilidad y el mantenimiento de las maquinas.

**Nivel de enlace**

Este nivel se limita a recibir data gramas del nivel superior (nivel de red) y transmitirlo al hardware de la red. Pueden usarse diversos protocolos: DLC(IEEE 802.2), Frame Relay, X.25, etc.

La interconexión de diferentes redes genera una red virtual en la que las maquinas se identifican mediante una dirección de red lógica. Sin embargo a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas. Un diseño eficiente implica que una dirección lógica sea independiente de una dirección física, por lo tanto es necesario un mecanismo que relacione las direcciones lógicas con las direcciones físicas. De esta forma podremos cambiar nuestra dirección lógica IP conservando el mismo hardware, del mismo modo podremos cambiar una tarjeta de red, la cual contiene una dirección física, sin tener que cambiar nuestra dirección lógica IP.

## 5. Señales y Protocolos

**Señales:**

Los equipos se comunican sobre una red de muchas formas y por muchas razones, pero mucho de lo que ocurre en la conexión no esta relaciona con la naturaleza de los datos que pasan por la red. En el momento en que los datos generados por el equipo transmisor alcanzan el cable o el medio, se han reducido a señales que son nativas para ese medio de transmisión. Estas pueden ser:

- Señales eléctricas para un cable de cobre
- Pulsos de luz por fibra óptica u ondas infrarrojas.

Estas señales forman un código que la interfaz de red en cada equipo que recibe los datos convierte en datos binarios comprensibles para el Software. Luego, el equipo traduce el código binario en información que puede ser usada de muchas formas.

**Protocolos:**

Un protocolo de red puede ser relativamente simple o muy complejo. En algunos casos, un protocolo es un código simple, como ser un patrón de voltajes eléctricos, que define el valor binario de un bit de datos: **0** y **1**.

El concepto es similar al del código Morse, en el cual un patrón de puntos y rayas representa una letra del alfabeto. Los Protocolos más complicados de red pueden proporcionar una diversidad de servicios, incluyendo los siguientes:

- **Recepción de Paquetes:** La transmisión de un mensaje emitido por el destinatario para confirmar la recepción de un paquete o paquetes. Un paquete es la unidad Fundamental de datos transmitidos a través de una LAN.

- **Segmentación:** La división de una transmisión de datos extensa en segmentos lo suficientemente pequeños para su transporte en forma de paquetes.

- **Control de Flujo:** La generación de mensajes en el sistema receptor, que instruyen al sistema emisor que aumente o disminuya la velocidad de la transmisión.

- **Detección de Errores:** La inclusión de códigos especiales en un paquete que utiliza el sistema receptor para verificar que el contenido de los paquetes no se dañó durante la transmisión.

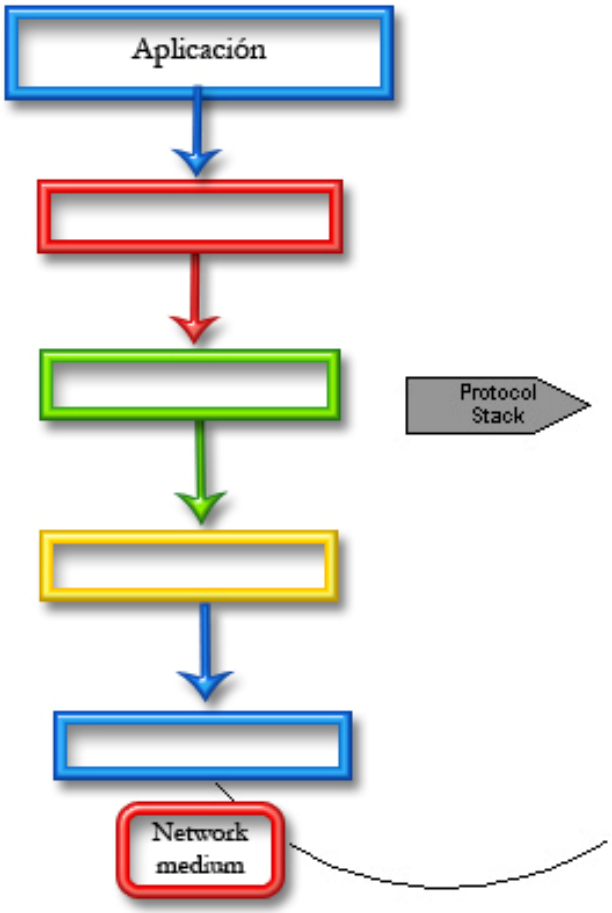
- **Corrección de Errores:** La generación de mensajes en el sistema receptor, que informan al emisor de paquetes específicos que se dañaron y deben ser retransmitidos.

- **Comprensión de Datos:** Mecanismo para la reducción de la cantidad de datos transmitidos en la red eliminando información redundante.

- **Cifrado de Datos:** Mecanismo para la protección de datos transmitidos en la red cifrándoos con una llave o clave conocida por el receptor.

6. **Interacción de Protocolos**

Los Protocolos que operan en varias capas OSI se conocen a menudo como una pila de Protocolos. Los protocolos que operan en un equipo en red trabajan para proporcionar los servicios necesarios para una Aplicación en particular. En términos generales, los servicios proporcionados por los protocolos no son redundantes. Por ejemplo, un protocolo en una capa proporciona un servicio en particular, los protocolos en otras capas no proporcionan exactamente el mismo servicio. Los protocolos en capas adyacentes en la pila proporcionan servicios para cada una de las capas, dependiendo de la dirección en que se transmiten los datos.




Como se muestra en la imagen anterior, los datos en el sistema transmisor se originan en una aplicación en la parte superior de la pila de protocolos y fluyen hacia abajo a trabes de las capas. Cada protocolo proporciona un servicio a un protocolo operando en la capa inferior. Al final de la pila de protocolos está el medio de red, que lleva los datos hacia otro equipo en la red.

## 7. Redes de Área Local y Redes de Área Amplia

Una LAN es un grupo de equipos localizados en un área relativamente pequeña conectados por un medio de transmisión común. Cada uno de los equipos y dispositivos de comunicación en una LAN se denomina nodo. Una LAN se caracteriza por tres atributos primarios: su topología, su medio de transmisión y sus protocolos. La topología es el patrón que se utiliza pata conectar los equipos. Con una topología de bus, el cable de red conecta un equipo con el siguiente, formando una cadena. Cada uno de los equipos está conectado a un nexo central llamado hub o switch. Una topología anillo es esencialmente una topología bus con los dos extremos unidos.

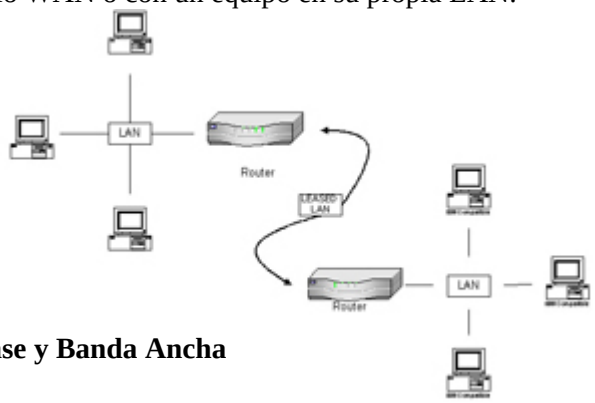
El medio de transmisión es la conexión física entre equipos. La topología y el medio de

transmisión usados en un equipo en particular, están determinados por el protocolo que esta operando en la capa enlace de datos del modelo OSI, como pueden ser Ethernet o Token Ring.

Ethernet, por ejemplo, admite muchas topologías y medios de transmisión para una LAN, como ser cable UTP en una topología estrella, se debe usar (en la mayoría de los casos) la misma topología y medio de transmisión para todos los equipos en la LAN. Existe hardware que permite la conexión de tecnologías estrechamente relacionadas. No es posible, por ejemplo, conectar un equipo en una red bus Ethernet y hacer que ambos equipos participen en la misma LAN.

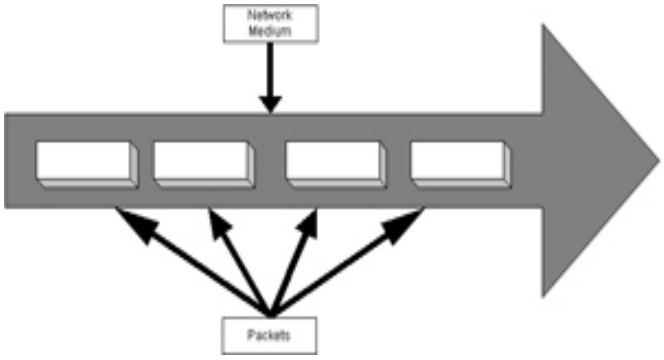
En la mayoría de los casos, una LAN esta confinada a una sola área, piso, o edificio. Para expandir la red fuera de esos limites, se pueden conectar múltiples LANs con dispositivos denominados Routers. Permite formar una red interconectada o internet, que es esencialmente, una red de redes. Un equipo en una LAN puede comunicarse con sistemas en otra LAN debido a ese tipo de interconexión. Con la conexión de LANs es posible construir una red interconectada del tamaño que se necesite. Muchas fuentes usan el término red cuando describen una LAN, pero también usan el mismo termino cuando se refieren a una red interconectada.

En muchos casos, una red interconectada está compuesta de LANs en ubicaciones remotas. Para conectar LANs de forma remota, se utiliza un tipo de conexión de red distinta: una conexión WAN. Las conexiones WAN usan líneas telefónicas, ondas de radio o cualquiera de muchas otras tecnologías. Las conexiones WAN normalmente son conexiones punto a punto, lo que significa que la conexión existe entre dos sistemas. Son diferentes de las LANs, en que todos los sistemas están interconectados. Un ejemplo de una conexión WAN podría ser una compañía con dos oficinas en ciudades distantes, cada una con su propia red LAN y conectadas por la línea telefónica. Cada extremo esta conectado a un Router y los Routers están conectados a LANs individuales. Cualquier equipo en una LAN se puede comunicar con cualquier equipo en el otro extremo del vínculo WAN o con un equipo en su propia LAN.




## 8. Banda Base y Banda Ancha

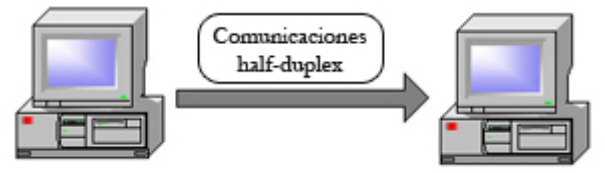
En muchos casos, las redes LAN usan un medio de transmisión compartido. El cable que conecta los equipos lleva una señal a la vez, y todos los sistemas se turnan para usarlo. Este tipo de red se denomina red en Banda Base. Para que una red en banda base sea practica para varios equipos, los datos transmitidos por cada sistema se subdividen en unidades llamadas paquetes. Si se pudiera observar un cable de transmisión en banda base y examinar la forma en que viajan las señales, se vería una sucesión de paquetes generados por varios sistemas y destinados a otros sistemas. Cuando un equipo transmite un mensaje de correo electrónico, por ejemplo, este mensaje se puede dividir en varios paquetes y el equipo transmite cada paquete por separado. Si cuando todos los paquetes que constituyen una transmisión en particular, alcanzan su destino, los equipos receptores unen las piezas para formar el mensaje de correo electrónico original. Esta es la base de una conmutación de paquetes.




La alternativa a una red de conmutación de paquetes es una red de conmutación de circuitos, en al que dos sistemas que necesitan comunicarse establecen una ruta a través de la red que los conecta (denominada circuito) antes de transmitir la información. Para hacer que la conmutación de circuitos sea practica, las compañías de teléfono usan redes de banda ancha. Al contrario de una banda base, la banda ancha lleva múltiples señales simultáneamente en un solo cable. Puede ser la que utiliza una compañía de T.V por cable. El servicio de televisión por cable instala un solo cable dentro del hogar del usuario, pero ese único cable transporta señales para docenas de canales simultáneamente, y proporciona también en algunos casos accesos a internet. Si se tiene mas de un TV en el hogar, el hecho de poder ver un programa de televisión distinto en cada TV, demuestra que el cable transporta múltiples señales a la vez . Las tecnologías de banda ancha casi no se utilizan en las redes de área local, pero son cada vez más utilizadas como solución en redes de área amplia.

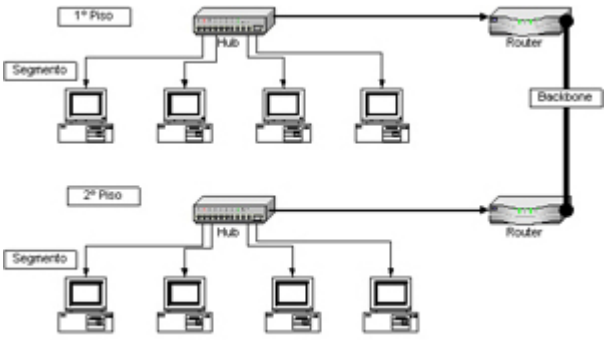
## 9. Comunicaciones Half-Duplex y Full duplex

Cuando dos equipos se comunican en una LAN, la información viaja normalmente en una sola dirección a la vez, dado que las redes en banda base usadas por las redes LAN admiten solo una señal. Esto de denomina comunicación **half-duplex**. En cambio dos sistemas que se pueden comunicar simultáneamente en dos direcciones están operando en modo **full-duplex**. El ejemplo más común de una red **full-duplex** es, una vez mas, el sistema telefónico. Ambas parte pueden hablar simultáneamente durante una llamada telefónica y cada parte puede oír a la otra a la vez. Un ejemplo de un sistema de comunicación **half-duplex** es la radio, como ser los radiotransmisores, en los que solo una parte puede transmitir a la vez, y cada parte debe decir "cambio", para indicar que ha terminado de transmitir y está pasando de modo transmisión a modo recepción.




## 10. Segmentos y Backbone

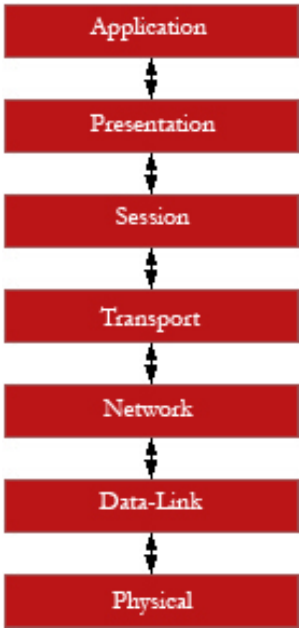
Cuando una red pequeña comienza a crecer, es posible conectar redes LAN de forma temporal. Sin embargo, la construcción de una gran red empresarial conectando varias redes LAN es un proyecto complejo que requiere de una planificación cuidadosa. Una de los diseños más comunes para redes de este tipo es una serie de segmentos LAN conectadas por medio de un Backbone o eje troncal. El término segmento a veces se utiliza como sinónimo de LAN o red para referirse a un conjunto de equipos conectados en red, pero en este contexto se refiere a una LAN compuesta de estaciones de trabajo y de otros dispositivos de usuario final, como ser las impresoras. Una red empresarial esta compuesta de muchas redes LAN, conectadas a otra LAN denominadas Backbone. El Backbone existe principalmente como un conducto que permite a los segmentos comunicarse entre si. Una configuración para un edificio de muchos pisos necesita de un segmento horizontal que conecte todas las estaciones de trabajo en cada piso y un Backbone en forma vertical desde la parte superior del edificio hasta la planta baja que conecte todos los segmentos.




Este tipo de configuración incrementa la eficiencia de la red usando la red troncal para llevar todo el tráfico de una red a otra. Con esa configuración los paquetes no deben atravesar más de tres LANs. En cambio, si se conecta cada uno de los segmentos horizontales a un segmento adyacente, en un enlace tipo cadena, la mayoría de los paquetes transmitidos entre redes tendrían que viajar a través de muchos más segmentos para alcanzar su destino, sobrecargando los segmentos intermedios con tráfico innecesario.

## 11. Introducción al Modelo OSI

En 1983, Organización Internacional para la Estandarización (**ISO**), publicaron un documento denominado "El modelo básico de referencia para Interconexión de Sistemas Abiertos". El modelo descrito en ese documento divide las funciones de red de un equipo en siete capaz, como se muestra en la siguiente figura. Originalmente, esta estructura de siete capas estaba diseñada para ser el modelo de una nueva pila de protocolos, pero esto no se materializó de forma comercial. En lugar de eso el modelo OSI se utiliza con los protocolos de red existentes como una herramienta de enseñanza y referencia.



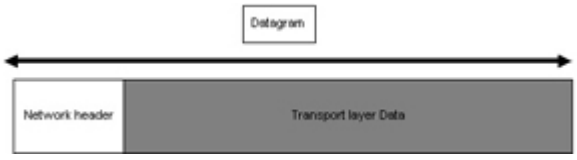

La mayoría de los protocolos más utilizados son anteriores al modelo OSI, por lo que no tienen la estructura de siete capas. En muchos casos, los protocolos combinan las funciones de dos o más de las capas en el modelo, y los límites entre los protocolos a menudo no se adaptan a los límites de las capas del modelo. Sin embargo, el modelo continúa siendo una excelente herramienta para el estudio de la comunicación en red, y los profesionales frecuentemente hacen referencia a funciones y protocolos asociados con capas específicas.

## 12. La Capa Red

A primera vista la capa red parece duplicar algunas funciones de la capa enlace de datos. Sin embargo, esto no es así, dado que los protocolos de la capa red son responsables de las comunicaciones fin a fin, mientras que los protocolos de capa enlace de datos funcionan solo en LAN local. Decir que los protocolos de la capa red son responsables por las comunicaciones fin a fin significa el protocolo de la capa red es responsable por el viaje de un paquete desde el sistema que lo creó hasta su destino final. Dependiendo de la naturaleza de la red, los sistemas de origen y destino pueden estar en la misma LAN o separados a miles de kilómetros de distancia, por Ejemplo, cuando se conecta un servidor a internet, los paquetes que crea el equipo pueden pasar por docenas de redes antes de llegar a su destino.

El protocolo de la capa Enlace de Datos puede cambiar muchas veces para adaptarse a docenas de redes, pero el protocolo de la capa red permanece intacto en todo el viaje.

La unidad de datos creada por un protocolo de capa red, está compuesta por los datos de la capa transporte además del encabezado de red y se denomina "data grama".



## 13. La Capa Transporte

Los protocolos de la capa transporte proporcionan servicios que complementan aquellos proporcionados por la capa red. Los protocolos de la capa red y transporte que se usan para transmitir los datos se consideran frecuentemente un solo componente, como en el caso del TCP/IP. Estos protocolos incluyen TCP, que operan en la capa transporte, además de IP, que corre en la capa red. La mayoría de las suites de protocolos proporcionan dos o más protocolos en la capa transporte, los mismos que proporcionan diferentes niveles de servicios. La alternativa a TCP es el User Datagram Protocol (UDP). El protocolo IPX también ofrece alternativas entre protocolos de la capa transporte, incluyendo el Netware Core Protocol (NCP) y el Sequenced Packet Exchange (SPX).

## 14. La Capa Sesión

La Capa sesión es el punto en el que los protocolos que se utilizan, actualmente empiezan a diferir sustancialmente el modelo OSI. No existe protocolos específicos para la capa sesión como existen en las capas inferiores. Más bien las funciones de la capa sesión están integradas dentro de otros protocolos que también incluyen funciones de las capas presentación y Aplicación. Las capas transporte, red, enlace de datos y física, están destinadas a la transmisión apropiada de los datos por la red, pero los protocolos en la capa sesión y superior no están involucrados en esa parte del proceso de comunicaciones. La capa sesión proporciona 22 servicios, muchos de los cuales están relacionados con las formas en que los sistemas en red intercambian la información. Los servicios más importantes son el control de diálogo y la separación de dialogo.

El intercambio de información entre dos sistemas en la red es llamado diálogo, y el control de diálogo es la selección de un modo que los sistemas usaran para el intercambio de mensajes. Cuando el diálogo se inicia, los sistemas pueden elegir uno de dos modos, modo alterno de dos vías (**TWA**) o modo simultáneo de dos vías (**TWS**), los dos sistemas intercambian una señal de datos "menor/actividad", y solo al equipo que posee esta señal se le permite la transmisión de datos. Esto elimina los problemas generados por mensajes que se cruzan en transito. El modo **TWS** es más complejo, debido a que ambos sistemas pueden transmitir al mismo tiempo, incluso simultáneamente.

## 15. La Capa Presentación

Existe solo una función de la capa Presentación: La traducción de las sintaxis entre sistemas distintos. En algunos casos los equipos que se comunican a través de una red usan diferentes sintaxis, y la capa presentación les permite negociar una sintaxis común para las comunicaciones. Cuando los sistemas establecen una conexión en la capa de presentación, intercambian mensajes que contiene información acerca de las sintaxis que tienen en común, y juntos eligen la sintaxis que usaran durante la sesión. Ambos sistemas envueltos en una conexión tiene una sintaxis abstracta, que es su forma nativa de comunicación. Los equipos que operan en diferentes plataformas pueden tener diferentes sintaxis abstractas. Durante el proceso de negociación, los sistemas escogen una sintaxis de transferencia, que es una sintaxis alternativa que ambos tienen en común.

El sistema transmisor convierte su sintaxis abstracta a la sintaxis de transferencia, y luego de la transmisión, el sistema receptor convierte la sintaxis de transferencia a su propia sintaxis abstracta. Cuando es necesario, los sistemas pueden seleccionar una sintaxis de transferencia que proporciona servicios adicionales, como ser la comprensión de datos o el cifrado.

Algunos estándares de conversión y formato de texto, audio, video e imagen, son: **ASCII, EBCDIC, Cifrado, conversión MIDI, MPEG, Quick Time, AVI, GIF, JPEG, PICT, TIFF.**

## 16. La Capa Aplicación

La capa Aplicación es el punto de entrada que utilizan los programas para acceder al modelo OSI y utilizar los recursos de red. Verifican la disponibilidad de los recursos necesarios para iniciar una sesión, vinculan la aplicación al servicio o protocolo correcto y sincronizan la transmisión de datos entre la aplicación y si protocolo. La mayoría de los protocolos en la capa aplicación proporcionan servicios que utilizan los programas para acceder a la red, como ser **Simple Mail Transfer Protocol** (**SMTP**),usado por muchos programas de correo electrónico para enviar mensajes de correo. En algunos casos, como en el caso del **File Transfer Protocol** (**FTP**), el protocolo de la capa aplicación es un programa en si mismo. Los protocolos de la capa aplicación frecuentemente incluyen las funciones de las capas sesión y presentación. Por lo tanto, una pila de protocolos típica, está compuesta de cuatro protocolos distintos que corren en la capa de aplicación, transporte, red y enlace de datos.