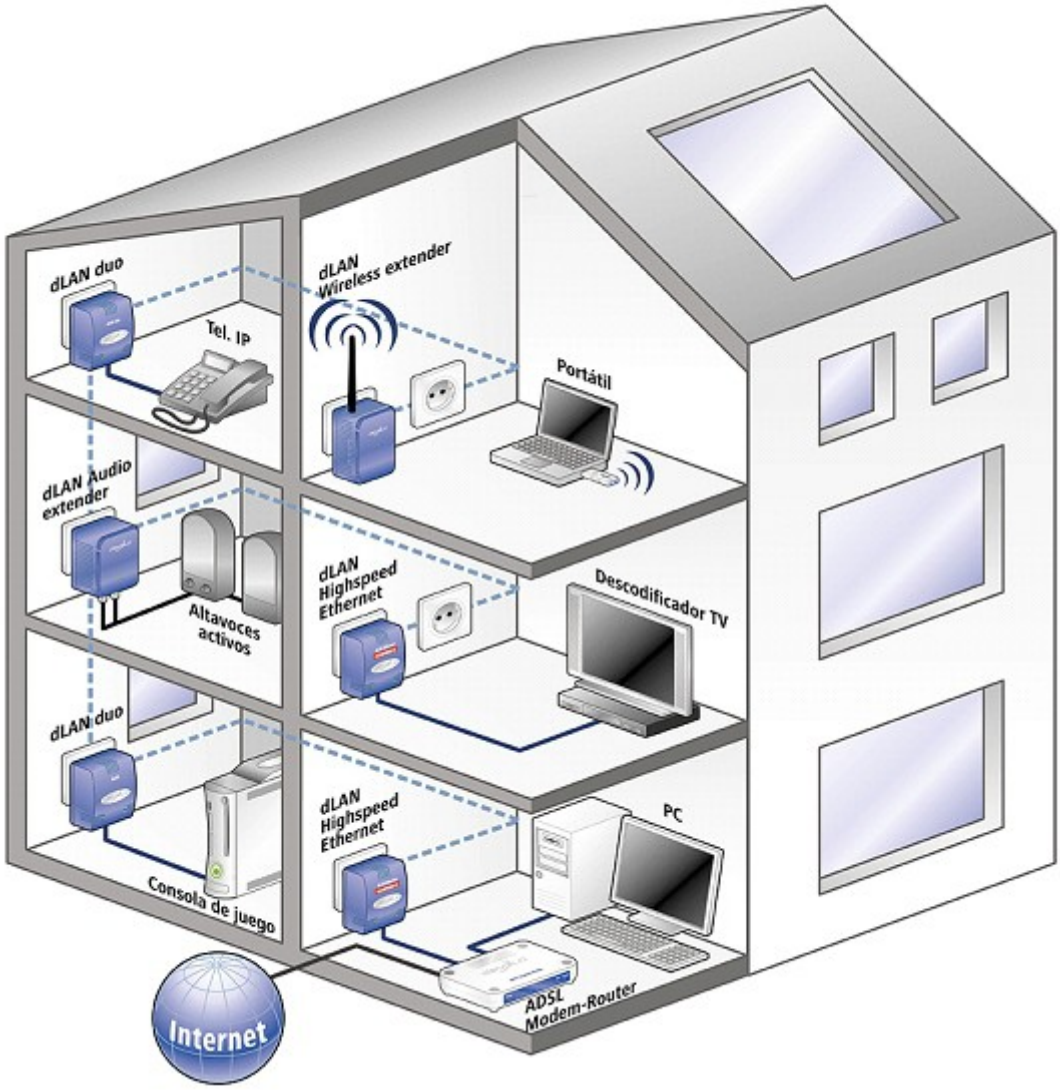
Redes y servicios de Internet



1. ¿Qué es una red informática?

Se define una red informática como un conjunto de equipos conectados entre sí con la finalidad de compartir información y recursos de forma segura. La finalidad de una red es que los usuarios de los sistemas informáticos puedan hacer un mejor uso de los recursos. Las redes mejoran aspectos como:

- Mayor facilidad de comunicación.
- Realizar copias de seguridad centralizadas.
- Ahorro económico al compartir recursos.
- Mejoras en la administración de los programas.
- Gestionar eficazmente la seguridad de los equipos.

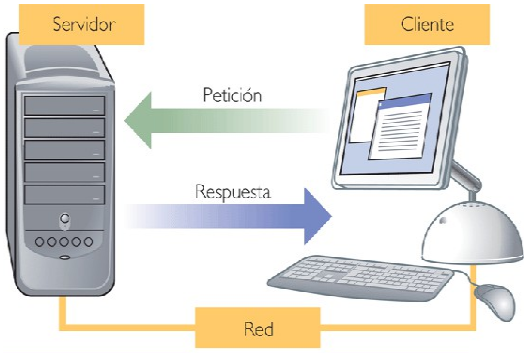
Para la creación de una red se hace necesario unos medios de comunicación, así como un sistema operativo que maneje estos medios. Un sistema operativo de red es un conjunto de programas que permiten y controlan el uso de dispositivos de red para múltiples usuarios. Éste gestiona las peticiones (de acceso, de impresión, de comunicación, etc) consultando a los servidores si se permite dicha operación. Según la forma de interacción de los programas en la red, existen dos formas de arquitectura lógica:

a) Cliente-servidor

En este modelo, al menos un equipo realiza las funciones de controlador de red (puede haber varios), los demás equipos solicitarán al servidor permiso para realizar cualquier operación de red, normalmente la concesión de estos permisos se realiza mediante una autentificación de usuario y contraseña.

Las ventajas de este modelo incluyen:

- Control o reducción de costos al compartir recursos.
- Facilidad de administración, al concentrarse el trabajo en los servidores.
- Facilidad de adaptación.
- Facilidad en el acceso a los recursos.

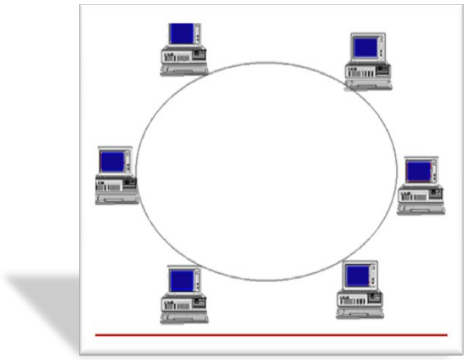


b) Redes de pares (peer-to-peer).

Este modelo permite la comunicación entre usuarios (hosts) directamente sin que ninguno de ellos tenga el rol de servidor. Cada usuario que desee acceder a un recurso compartido tendrá que autenticarse en el equipo dueño de dicho recurso (tantas veces como recursos haya en equipos distintos). Las principales ventajas de este modelo son:

- Todos los hosts pueden ser cliente y servidores.

•No existe dependencia de un servidor. En una red cliente servidor, si el servidor falla, la red se "cae" completamente.



2. Clasificación De Redes

Se pueden clasificar las redes en base a los siguientes criterios:

a) Según la tecnología de transmisión:

•Multidifusión. Un solo canal de comunicación compartido por todas las máquinas. Un "*paquete*" mandado por alguna máquina es recibido por todas las otras. Por ejemplo las redes wifi

•Point-to-point. Conexiones dedicadas entre máquinas.

b) Según el medio físico utilizado:

•Alámbricas: se utilizan cables para transmitir los datos.

•Inalámbricas: se usan ondas electromagnéticas para enviar y recibir datos.

•Mixtas: en unas zonas se comunican por cables y en otras de forma inalámbrica.

c)Por el tamaño:

•PAN (Personal Area Network): Pocos metros (oficina)

•LAN (Local Area Network): Varios metros (edificio)

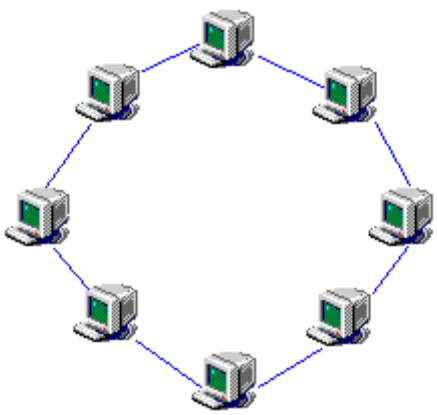
•MAN (Metropolitan Area Network): 5 - 100 km (localidad)

•WAN (Wide Area Network): 100 km a 10.000 km (paises)

d) Por la topología:

La topología o forma lógica de una red es la forma en que se construye el cableado que comunica a cada computador con el servidor, esto puede ser en:

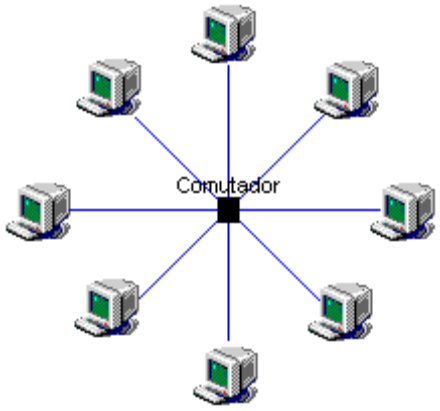
- Anillo.
- Estrella.
- Bus.
- Árbol.
- Malla.



Anillo

Es una de las principales topologías de red. Las estaciones están unidas una con otra formando un círculo por medio de un cable común. Las señales circulan en un solo sentido alrededor del círculo,

regenerándose en cada nodo. Si un ordenador falla, se pierde la red. Una variante es la de doble anillo.



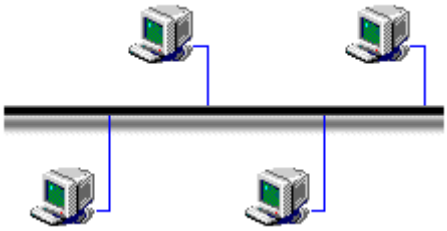
Estrella

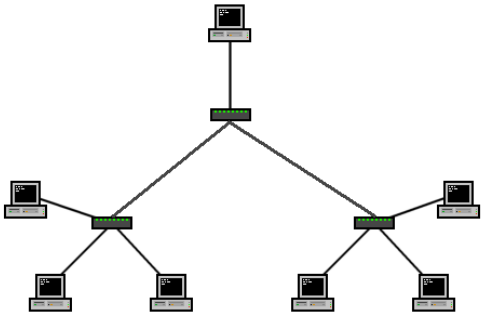
La red se une en un único punto, normalmente con control centralizado, como un concentrador de cableado (switch). Cada nodo tiene un funcionamiento independiente, lo cual es una ventaja.

Esta tecnología es la más usada en las redes de área local.

Bus o Lineal

Las estaciones están conectadas por un único segmento de cable. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo y además puede existir acumulación de tráfico.



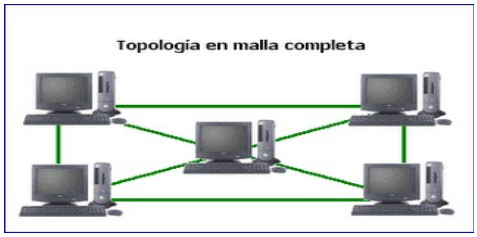


Árbol

Cuando la redes de área local aumenta en número de hosts o elementos con direcciones de red, se necesitan elementos concentradores (switch), estos se conectan entre sí de forma jerárquica formando la figura.

Malla

Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de redes locales (Lan). Los nodos están conectados cada uno con todos los demás.Es segura pero compleja de diseñar.



3. Dispositivos físicos de una red

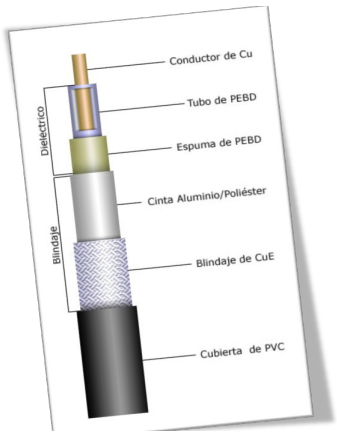
a) Tarjeta de red

Es el dispositivo encargado de enviar y recibir información al resto de los ordenadores. Se conecta a la placa base mediante un bus PCI, pudiendo estar integrada en la misma. Cada tarjeta se identifica en la red mediante un código llamado dirección Mac, que está formado por seis pares de dígitos en hexadecimal. Cumplen con el estándar **Ethernet**, que garantiza la compatibilidad física de los equipos en red.Las tarjetas de red funcionan del siguiente modo: cuando un equipo quiere transmitir, escucha lo que pasa en la red, y si no hay ninguna otra señal transmitida, permite el envío de los datos. Si la señal emitida choca con otra distinta, deja de enviar datos y espera un tiempo para volver a intentarlo.

b) Medio físico

El medio físico es el medio sobre el que se envían las señales eléctricas para realizar la transmisión de la información. Los *cables de cobre* utilizados para transmisión son conductores clásicos que en ocasiones no son de este metal, sino aleaciones que mejoran las características eléctricas del cable. Los más utilizados son:

Coaxial

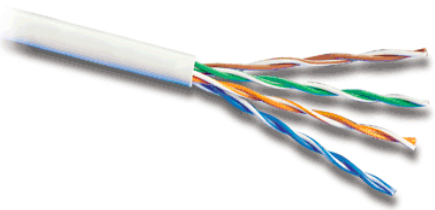


El término *coaxial* quiere decir eje común ya que un cable coaxial está formado por un conductor central rodeado de una capa de material aislante o *dieléctrico*, rodeada a su vez por una malla de hilos conductores cubierta por una funda de material aislante y protector. Actualmente es usado por las empresas de televisión por cable en algunas zonas de la red cableada.

Par trenzado apantallado (STP, Shielded Twisted Pair).

Este tipo de cable está formado por grupos de dos conductores cada uno con su propio aislante trenzados entre sí y rodeados de una pantalla de material conductor, recubierta a su vez por un aislante. Cada grupo se trenza con los demás que forman el cable y, el conjunto total se rodea de una malla conductora y una capa de aislante protector. Esta disposición reduce las interferencias externas.

Par trenzado sin pantalla (UTP, Unshielded Twisted Pair).



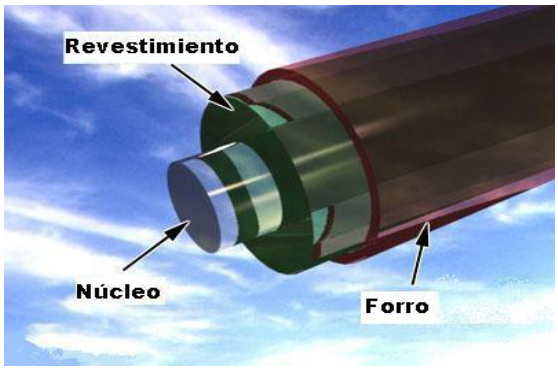
En este tipo de cable, los conductores aislados se trenzan entre sí en pares y todos los pares del cable a su vez. Esto reduce las interferencias entre pares y la emisión de señales.

Estos cables se utilizan, sobre todo, para los sistemas de cableado, combinando telefonía y redes de transmisión de datos.

Fibra óptica

Una fibra óptica es un filamento delgado y largo de un material dieléctrico transparente, usualmente vidrio o plástico de un diámetro aproximadamente igual al de un cabello (entre 50 a 125 micras) al cual se le hace un revestimiento especial. Un cable de fibra óptica está compuesto de las siguientes partes.

- **Núcleo:** Es propiamente la fibra óptica, la hebra delgada de vidrio por donde viaja la luz.
- **Revestimiento:** Es una o más capas que rodean a la fibra óptica y están hechas de un material con un índice de refracción menor al de la fibra óptica, de tal forma que los rayos de luz se reflejen por el principio de reflexión total interna hacia el núcleo y permite que no se pierda la luz.
- **Forro:** Es un revestimiento de plástico que protege a la fibra y la capa media de la humedad y los maltratos.



El peso del cable de fibras ópticas es muy inferior al de los cables metálicos, redundando en su facilidad de instalación. La mayoría de las fibras ópticas se hacen de arena o sílice, materia prima abundante en comparación con el cobre. Con unos kilogramos de vidrio pueden fabricarse aproximadamente 43 kilómetros de fibra óptica. Presenta un funcionamiento uniforme desde -550 C a +125C. Es el medio físico que predominará en las redes de telecomunicaciones en los próximos años.

Ondas de radio (WIFI): Wireless Fidelity

Usa el aire como medio de comunicación, desde su aparición y comercialización, ha tenido una gran aceptación y expansión tanto en las LAN como en las ADSL caseras. La eliminación de cables y conexiones físicas, así como sus buenas características tanto de velocidad como de seguridad, hacen que hoy día sea la más extendida. Se conecta por radiofrecuencia en la banda de 2,4 – 5 Ghz.

4. Interconexión de redes: router, hub y switch

Para realizar la conexión de dos redes, es posible utilizar distintos dispositivos. El uso de uno u otro vendrá dada, en una primera instancia, por el tipo de redes que se necesite interconectar. De forma básica, se puede decir que, cuanto mayores sean las similitudes (cableado, protocolo, etc.) de las redes a interconectar, menor será la complicación para el o los dispositivos responsables de la interconexión. Así mismo, su sofisticación aumentará cuanta mayor seguridad y/o grado de optimización se requiera.

Concentrador (hub)

Es un dispositivo de interconexión que centraliza las conexiones de los nodos. Actúa a nivel físico y conforma topologías de red en estrella. También denominados *repetidores multipuestos*. En vez de distribuir la señal de estación a estación, el concentrador reúne todas las conexiones, de modo que el fallo de una de ellas no afecta al funcionamiento general de toda la red. Este tipo de conexionado conforma una topología en estrella. Resulta evidente que, ante un fallo del repetidor, la red caerá. Como punto positivo, este tipo de errores en estas redes tienen un solo punto de origen, fácilmente localizable: el hub.

Conmutador (switch)

El **conmutador** o **switch** es otro de los dispositivos dedicados a la interconexión de redes. Permite conmutar o seleccionar el puesto al que da prioridad de informacion en cada momento. Además, el rendimiento del conmutador, al tener funciones más específicas, es mayor que el hub; ya que sólo envía los paquetes de información a su destinatario. De hecho, comercialmente, los conmutadores se ofrecen habitualmente con posibilidad de ser apilados, facilitando la estabilidad. Si se desea obtener alto rendimiento en estas situaciones, existen en el mercado posibilidades de conectar mediante un bus especial de alta velocidad los distintos módulos.

Enrutador (router)

El **enrutador, encaminador** o **router** es el responsable de adaptar los paquetes de información, a nivel de red, cuando las máquinas origen y destino se encuentran en distintas redes.

Los enrutadores son dispositivos (software o hardware) configurables para encaminar paquetes entre sus puertos de red. Para ello, se puede utilizar la dirección lógica (no la dirección MAC - *Media Access Control* – de la tarjeta de red) de Internet, por ejemplo, la dirección IP

5. Internet

Existen multitud de definiciones para internet, dos frases que son mas frecuentemente usadas y que dan una idea más global de ella son:

- Red de Redes
- Autopista de la información

Red de Redes, nos transmite la idea de que Internet se compone de múltiples redes LAN, MAN, WAN, interconectadas físicamente. Esto da idea de una única red extendida por todo el mundo.
Autopista de la información, Con esta frase se intenta transmitir la idea de los millones de bytes que circulan por segundo por todo internet. Se estima en cerca de 2000 millones de personas que tienen acceso a Internet por todo el mundo.
Uno de los grandes logros de Internet es la posibilidad de acceder a cualquier ordenador del mundo que desee ofrecernos información, incluso poder ver en directo que está ocurriendo en cualquier lugar.

Arquitectura de Internet (TCP/IP)

El primer problema que se tuvo que afrontar al intentar conectar redes heterogéneas (distintos medios y forma de comunicación), fue la creación de una serie de protocolos que unificarán la forma de conexión e intercambio de datos entre todas las redes que de forma emergente surgían.

La Familia de Protocolos de Internet fue el resultado del trabajo llevado a cabo por la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA) a principio de 1970 y siguiente años (años finales de la guerra fría).
Tras múltiples pruebas y mejoras en el año 1983 surgió TCP/IP V4 que aún se usa en la actualidad. En 1985 se creó el primer Taller informático que mostraba al mundo esta arquitectura.

La familia de protocolos de Internet es un conjunto de protocolos de red, que permiten la transmisión de datos entre redes de computadoras. Se le denomina conjunto de protocolos **TCP/IP**, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (**TCP**) y Protocolo de Internet (**IP**), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular **HTTP** (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el **ARP** (Address Resolution Protocol) para la resolución de direcciones, el **FTP** (File Transfer Protocol) para transferencia de archivos, y el **SMTP** (Simple Mail Transfer Protocol) y el **POP** (Post Office Protocol) para correo electrónico, **TELNET** para acceder a equipos remotos, entre otros.

6. Seguridad informática

Es el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, condifencialidad y disponibilidad.
Un sistema es íntegro si impide la modificación de la información a cualquier usuario que no haya sido autorizado con anterioridad.

Un sistema es confidencial si impide la visualización de datos a los usuarios que no tengan privilegios en el sistema.

6.1. Seguridad activa y pasiva

Existe dos tipos de herramientas relacionadas con la seguridad:
- Técnicas de seguridad activa: pretenden evitar daños a los sistemas informáticos.

1. Usar cotraseñas adecuadas.
2. Encriptación de datos.
3. Uso de software de seguridad informática.

- Técnicas de seguridad pasiva: cuyo fin es minimizar los daños causados por distintos factores como un accidente o un malware.
1. Uso de un hardware adecuado frente a accidentes y averías.
2. Realizar copias de seguridad de los datos y del sistema operativo en distintos soportes físicos.

6.2. Amenazas para los sistemas informáticos

Todo equipo informático está expuesto a una serie de programas maliciosos y dañinos que puede introducirse en el pc por medio de correos electrónicos, navegar por páginas webs falsas o infectadas, transmisión de archivos contaminados desde otros soportes, etc. Se pueden clasificar en:

a) Virus: programas que se introducen en los ordenadores sin conocimiento del usuario y se caracterizan porque al ejecutarse realizan acciones molestas o incluso dañinas para el pc.

b) Gusano: son similares a los virus pero su acción se limita a hacerse copias de si mismo a tal velocidad que colapsan la red y ralentizan los equipos.

c)Troyano: estos son también similares a los virus, pero al ejecutarse se instala lo que se llama una puerta trasera a traves de la cual se puede controlar el PC infectado por otro usuario.

d) Espía: estos programas recogen datos de hábitos del uso de Internet de los users y los envía a empresas de publicidad sin el consentimiento de los usuarios.

e) Spam: se trata del envío indiscriminado de mensajes de correo no solicitados, generalmente publicitarios; se la conoce como correo basura.

Para combatir todas estas amenazas podemos utilizar las siguientes herramientas:

1.Los antivirus son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos, gusanos, espías y troyanos.

2.Los cortafuegos (firewalls) son programas cuya finalidad es permitir o prohibir la comunicación entre las aplicaciones del equipo y la red, así como evitar ataques intrusos.

3.El antispam es un programa que detecta el correo basura mediante filtros.ç

4.El antiespía es un programa que compara los archivos de nuestro equipo con una base de datos de archivos espía y puede prevenir,detectar e incluso eliminar estos archivos indeseados.