INTRODUCCIÓN A LAS REDES

SISTEMAS INFORMÁTICOS - 1º DAM

INTRODUCCIÓN A LAS REDES

RED (net)

Elementos interconectados para un fin común

RED DE COMUNICACIÓN

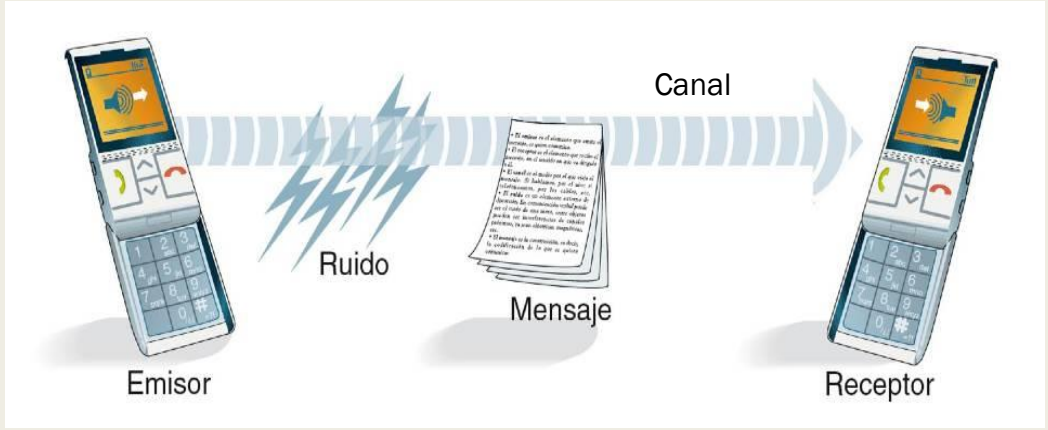
Red que permite transmitir información desde un punto a otro.

RED INFORMÁTICA

Conjunto de dispositivos informáticos conectados entre sí que se comunican y transmiten información.

COMPONENTES DE UNA RED DE COMUNICACIÓN

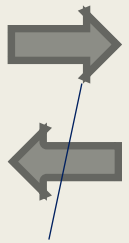
- ***EMISOR:*** *Elemento que envía la señal*
- ***RECEPTOR:*** *Elemento que recibe la señal*
- ***CANAL:*** *Medio por el que viaja el mensaje.*
- ***MENSAJE:*** *Codificación de lo que se quiere comunicar.*
- ***RUIDO:*** *Elemento externo de distorsión.*



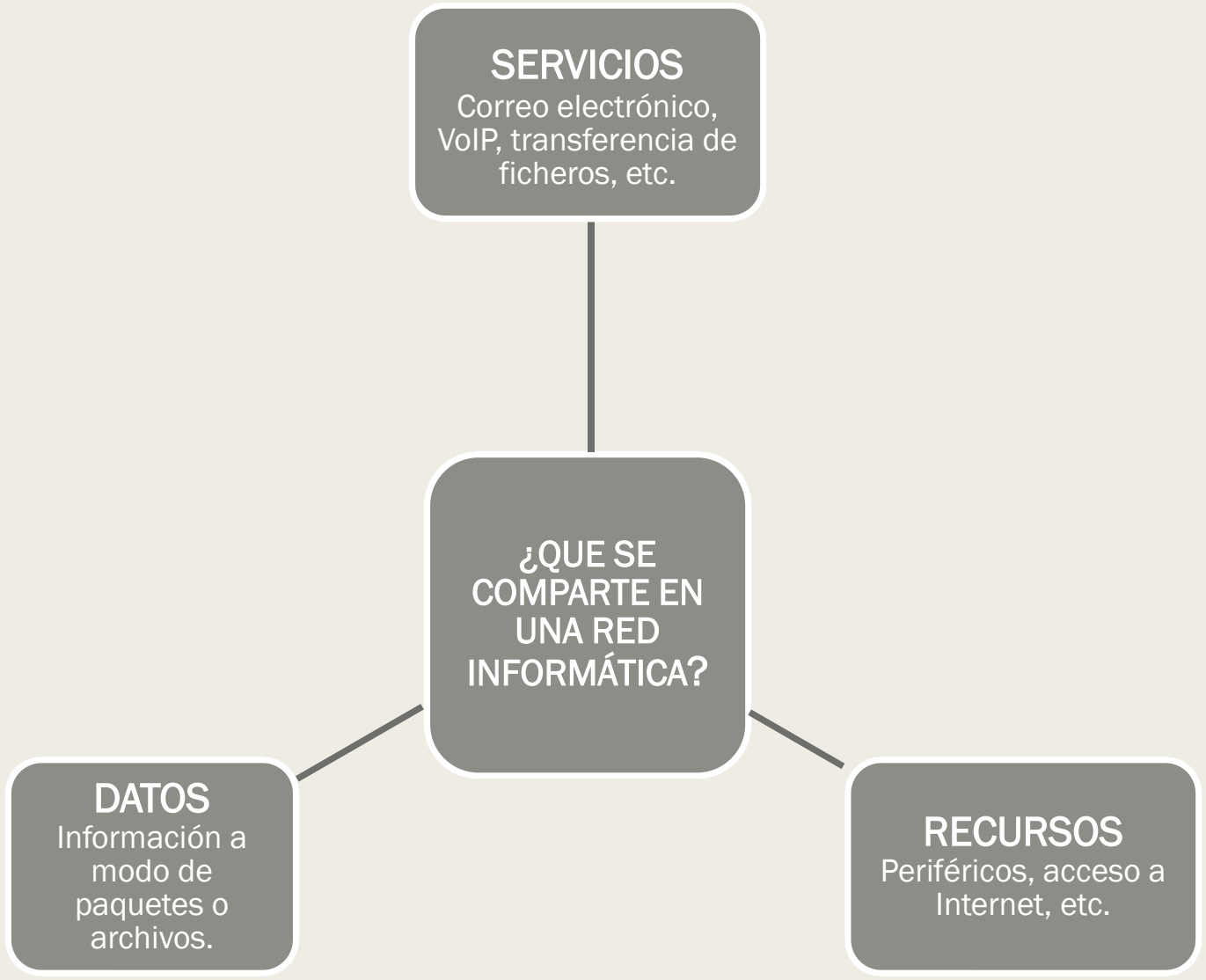
RED INFORMÁTICA

- *La **transmisión** proceso de transporte de la señal donde viajan los datos. La transmisión solo se encarga de transportar sin importarle la información.*
- *La **comunicación** es la transmisión de información. Aquí solo importan los datos, no la manera de transmitirlos.*

Comunicación



Transmisión



TRANSMISIÓN DE DATOS

La transmisión de datos puede ser de dos tipos:

- **Analógica:** la señal puede tomar cualquier valor
- **Digital:** la señal solo toma valores 0 y 1

TRANSMISIÓN DE SEÑALES ANALÓGICAS POR REDES DIGITALES

- La señal sale de la fuente.
- Pasa por un codificador de la señal Analógica a Digital.
- Pasa por el canal de transmisión.
- Llega al decodificador .
- Finalmente llega al equipo terminal.

TRANSMISIÓN DE SEÑALES DIGITALES POR REDES ANALÓGICAS

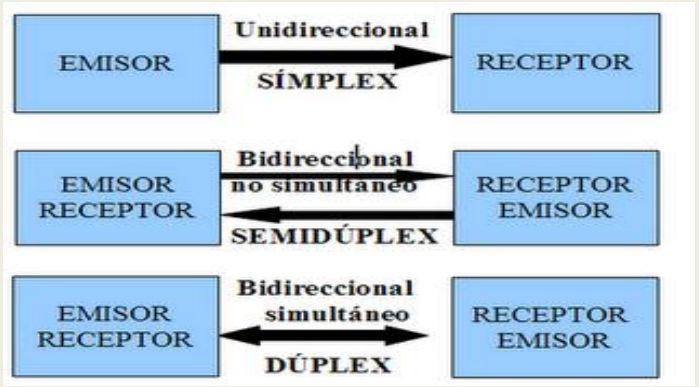
- La señal sale de la fuente.
- Pasa por el **mo**dulador (módem) que convierte la señal Digital a Analógica
- Pasa por el canal de transmisión.
- Llega al **dem**odulador (módem)
- Finalmente llega al equipo terminal.

Llamamos **información digitalizada** a aquella que está formada por series de bits.

MODOS DE TRANSMISIÓN DE DATOS

Según las direcciones que utiliza

- *SIMPLEX (SIMPLEX):* *Comunicación unidireccional de un emisor a un receptor sin cambio de papeles (la televisión, la cadena es el emisor y el televidente es el receptor.*
- *SEMI-DÚPLEX (HALF-DUPLEX):* *Comunicación bidireccional con sólo un sentido a la vez . El receptor y el emisor pueden cambiarse , pero no pueden ser emisor y receptor a la vez (los Walkie-Talkies)*
- *DÚPLEX (FULL-DUPLEX):* *Comunicación bidireccional en ambos sentidos a la vez (el teléfono donde ambos interlocutores pueden ser emisor y receptor)*



Según el nº de bits que puede enviar

- *SERIE:* *Envía los datos de uno en uno (de bit a bit).*
- *PARALELO:* *Envía los datos de byte en byte (ó múltiplos)*

Según su sincronización

- SÍNCRONA O SINCRÓNICA: El intercambio de información se realiza en tiempo real.
- ASÍNCRONA O ASINCRÓNICA: La transmisión es diferida. Existen bits de control que indican donde empieza y acaba la transmisión.

COMPONENTES DE UNA RED INFORMÁTICA

DISPOSITIVOS DE RED

- **Finales o hosts**: todos los dispositivos conectados a la red y que son origen o destino de un mensaje transmitido a través de ella (PC, portátil, móvil, impresora, teléfono IP, etc)
- **Intermediarios o de red:** dispositivos que conectan los hosts a la red y /o varias redes entre sí (router, switch, firewall, etc)

MEDIOS DE RED

Proporcionan el canal por el cual viaja el mensaje desde el origen hasta el destino.

- **Hilos metálicos dentro de cables:** los datos se codifican en impulsos eléctricos.
- **Fibras de vidrio o plástico (cable de fibra óptica):** los datos se codifican como pulsos de luz.
- **Transmisión inalámbrica:** los datos se codifican con longitudes de onda del espectro electromagnético.

SERVICIOS DE RED

Es la creación de una red de trabajo en un host que actúa como servidor de los clientes que se conectan a él (DHCP, DNS, correo, web, FTP, etc)

VENTAJAS	INCONVENIENTES
ECONOMÍA - Compartir recursos y servicios permite ahorrar en costes.	SEGURIDAD - La seguridad debe ser una cuestión importante, pues algunos usuarios pueden crear problemas voluntaria o involuntariamente.
MODULAR - Se pueden añadir nuevos dispositivos.	ADMINISTRACIÓN – Dependiendo del tamaño se puede complicar la administración de la red.
SEGURIDAD - Permite mejorar la seguridad y control de la información que se utiliza.	COMPATIBILIDAD - Las tecnologías evolucionan continuamente, esto puede hacer que dos aplicaciones iguales, en distintas versiones, no sean compatibles.
EFICIENCIA – Más recursos para conseguir realizar tareas en menos tiempo.	No se puede asegurar al 100% la fiabilidad, integridad y privacidad.
COMUNICACIÓN - Posibilita la comunicación entre elementos de la misma red y de otras redes.	
MOVILIDAD - Los elementos se pueden cambiar de lugar sin perder conexión.	

TIPOS DE REDES

SEGÚN LOS SERVICIOS QUE BRINDA

RED ENTRE IGUALES (P2P, red peer-to-peer)

- *Es el tipo de red más sencillo y barato.*
- *Es poco seguro.*
- *Todos los equipos pueden actuar como cliente y servidor a la vez.*
- *Todos los equipos están al mismo nivel.*

REDES CLIENTE-SERVIDOR

- *Los clientes son hosts que tienen instalado un software que les permite solicitar información al servidor y mostrar la información obtenida.*
- *Los servidores son host con software que les permite proporcionar información.*

POR SU EXTENSIÓN

PAN

(Personal Area Network)

- *Red de interconexión de dispositivos cercanos a una persona (PC, portátil, PDA, móvil, impresora, etc.).*
- *Configuración de acceso a la red sencilla, incluso a veces automática.*
- *El alcance de una PAN normalmente se extiende a 10 metros.*
- *Un cable PAN se construye generalmente con conexiones USB y Firewire.*
- ***WPAN (estándar IEEE 802.15):** red inalámbrica de área personal.*
  - **Bluetooth** (IEEE 802.15.1) estándar más conocido
  - **ZigBee** (IEEE 802.15.4)

LAN

(Local Area Network)

- *Red que suele situarse en el mismo edificio o en entornos de unos 200 m (1 km con repetidores) o a 450 m en versiones inalámbricas (en la práctica 100 o 200 m).*
- *Suele ser una red privada.*
- *La tasa de error debe ser muy baja.*
- *Su versión inalámbrica es la WLAN, que utiliza las ondas de radio para transmitir datos y conectar dispositivos a Internet,*
  - *El estándar más conocido es WiFi - IEEE 802.11 en sus múltiples versiones (802.11a, 802.11b, 802.11g, 802.11n y 802.11ac), aunque existen otras tecnologías.*
  - **LiFi** (IEEE 802.11.bb)??

POR SU EXTENSIÓN

CAN

(Campus Area Network)

- *Red cuya extensión es la de un campus universitario, una base militar, un polígono industrial o un grupo de grandes edificios en un área geográfica limitada.*
- *Las dimensiones suelen ser superiores a las de las redes locales, sin embargo, tienen la misma tecnología.*
- *Muchos la consideran como un subtipo de las redes MAN*

MAN

(Metropolitan Area Network)

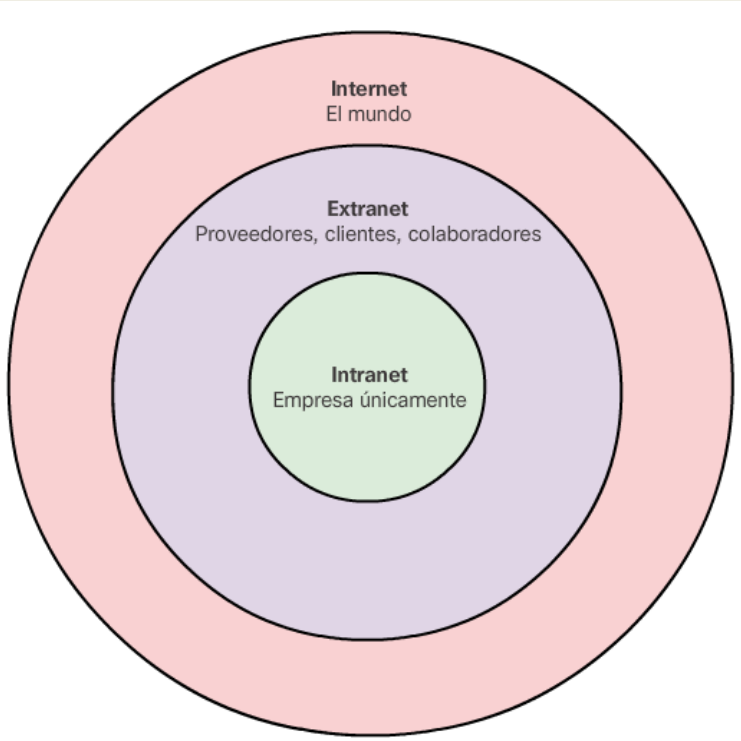
- *Red que se sitúa en una ciudad o municipio.*
- *Está compuesta por redes LAN interconectadas entre sí.*
- *Las tecnologías de este grupo se conocen como de **banda ancha.***
- *Se pueden conectar por cable (pares trenzados de cobre, fibra óptica) o por redes inalámbricas (**WiMax IEEE 802,16**)*

WAN

(Wide Area Network)

- *Es la red global (varios países, un continente o incluso mundial).*
- *Las tecnologías inalámbricas de este tipo como **vSAT** (conexiones satélite muy utilizadas en barrios de la periferia de las capitales, en el campo, etc.), **2G, 3G, 4G y 5G** (soluciones vía telefonía móvil pueden llegar a velocidades de cientos de megabits por segundo),*

SEGÚN EL GRADO DE DIFUSIÓN



- **Intranet:** conexión privada de LAN y/o WAN de una organización, diseñada para que accedan a ella personas autorizadas (miembros, empleados, etc.). También puede utilizar protocolos TCP/IP
- **Extranet:** proporciona acceso seguro a personas que no tienen acceso a la intranet pero necesitan datos de la organización.
- **Internet:** conjunto de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP funcionan como una red lógica única, de alcance mundial.

Nota: “internet” (con “i” minúscula) describe un conjunto de redes interconectadas. “Internet” (con “I” mayúscula) para hablar de la World Wide Web.

SEGÚN EL TIPO DE CONEXIÓN

Redes cableadas:

- Se utilizan diferentes tipos de cables para conectar los hosts.
- Permiten mayor velocidad y producen menos problemas de señal y alcance.
- Son más fáciles de implementar.

Redes inalámbricas:

- No necesitan cables para comunicarse.
- Son menos seguras ya que las señales viajan en el aire y pueden ser interceptadas
- Las redes inalámbricas usan las normas de seguridad, como WEP (Privaciada Equivalente al Cableado) y WPA (Wi-Fi con acceso protegido) para restringir el acceso no autorizado y proteger la privacidad.

ARQUITECTURA DE RED

ARQUITECTURA DE RED

La **arquitectura de red** define la forma de conexión de los nodos de red (software y hardware) y el proceso que deben seguir para comunicarse con otro host teniendo en cuenta el medio del que disponen. La mayoría están basadas en los **modelos OSI** y **TCP/IP**, ambos métodos operan con sistema de capas de protocolos.

La arquitectura de red viene definida por las siguientes características:

- *TOPOLOGÍA.*
- *MÉTODO DE ACCESO A LA RED.*
- *PROTOCOLOS.*

TOPOLOGÍA

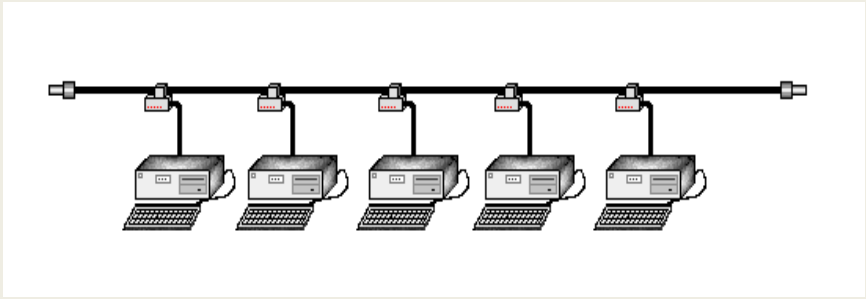
La topología es la forma en que se conectan los nodos de una red para poder comunicarse entre sí.

- ***Topología física:*** se refiere a las **conexiones físicas**, es decir, situación de los dispositivos y del cableado que constituyen la red
- ***Topología lógica:*** hace referencia a como los dispositivos "ven" el flujo y sentido de la comunicación.

La topología de red se suele utilizar en redes cableadas, pero en redes inalámbricas también se distinguen topologías como la **ad-hoc** en la que existe una comunicación punto a punto entre dos elementos de red.

TOPOLOGÍAS DE RED CABLEADA

- BUS
  - *Tiene una estructura lineal.*
  - *Un único bus (bus troncal o backbone) con múltiples accesos para que se conecten los diferentes dispositivos de la red.*
  - *En los extremos de este bus se colocan unos terminadores para evitar la producción de ECO.*
  - *Fácil implementación*
  - *Límite máximo de equipos conectados y de longitud del cable*
  - *Degradación de la señal.*

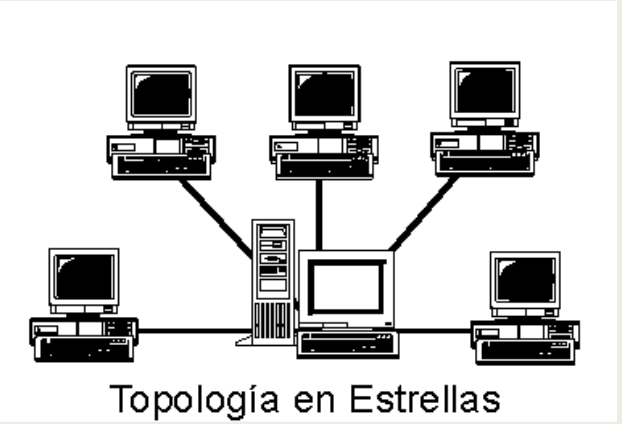


TOPOLOGÍA

- **ESTRELLA**

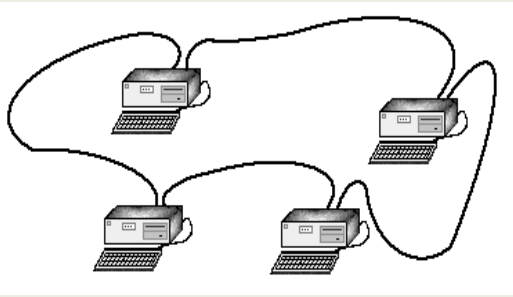
  Todas las estaciones están conectadas a un punto central y todas las comunicaciones se realizan a través de él.

  - Si un terminal falla, no influye en el resto de la red
  - Es fácil prevenir conflictos
  - Es bastante segura, el nodo central aísla los problemas
  - Cuello de botella
  - Requiere demasiado cableado
  - Mal funcionamiento del nodo central implica fallo en el resto


Topología en Estrellas

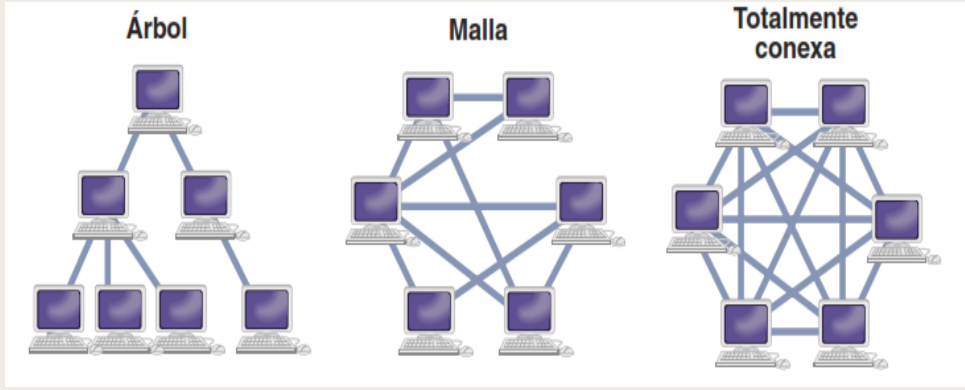
- **ANILLO**

  - *Cada nodo está conectado al siguiente y el último al primero.*
  - *Cada nodo tiene un receptor y un transmisor que hacen la función de repetidor hacia el siguiente nodo.*
  - *Esta topología tiene menos colisiones por los algoritmos de paso de testigo (o token).*
  - *La red local en anillo tradicional es la* ***Token ring*** *(topología física de estrella con todos los nodos conectados a MAU o MSAU y lógica de anillo)*
  - *Existe la* ***topología de doble anillo*** *para que la comunicación sea bidireccional, creando una gran tolerancia a fallos.*
  - *Tiene las mismas ventajas e inconvenientes que el tipo bus siendo el más preocupante el de su fragilidad (si falla un terminal, la red no funciona).*



TOPOLOGÍA

- ÁRBOL
  - *Tienen una estructura jerárquica.*
  - *Si un nodo falla, deja a un grupo de terminales sin conexión (los de sus niveles inferiores, hijos y descendientes).*
  - *Se usa mucho en redes de telefonía con centralitas locales, municipales, comarcales, regionales, estatales, etc.*
- MALLA
  - *Todos los nodos están conectados entre sí con varias conexiones a otros equipos.*
  - *Caro de cablear, pero muy tolerante a fallos.*
  - *Una malla totalmente conexa es un subtipo de malla donde todos los nodos están conectados entre sí, todos con todos.*
- MIXTA
  - *La topología mixta es la combinación de varias topologías.*



MÉTODO DE ACCESO A LA RED

- Es la forma de controlar el tráfico de mensajes por la red para que no se solapen distintas comunicaciones.
- Hay dos métodos de acceso generalizados en redes locales:
  - ***el acceso por contención o aleatorio.*** *Permite que cualquier usuario empiece a transmitir en cualquier momento siempre que el camino no esté ocupado.*

    El método más común el ***CSMA (acceso múltiple sensible a la portadora).*** *Se basa en el método de escuchar antes de enviar.*

    - **CSMA-CA** → escucha la red a ver si está libre → se transmite el dato → el receptor envía reconocimiento.
    - **CSMA-CD** igual que el anterior pero sin reconocimiento
  - ***el acceso determinístico****: El sistema determina que nodo puede transmitir en cada momento.*

    El método más utilizado es el ***Token Passing*** → El testigo se pasa de un nodo a otro → cuando uno quiere transmitir espera al testigo y lo guarda, envía el mensaje por la red hasta que vuelve a él → libera el testigo que pasa a otro nodo.

PROTOCOLOS DE RED

- **PROTOCOLO.** Conjunto de reglas normalizadas que los dispositivos deben cumplir para intercambiar mensajes.

  Existen protocolos para casi todo tipo de comunicación, (enviar correo, recibirlo, videoconferencia, etc.).

- **SUITE O FAMILIA DE PROTOCOLOS.** Grupo de protocolos que trabajan en forma conjunta para proporcionar servicios integrales de comunicación de red.

- **ESTANDAR.** Modelo que se propone a los distintos fabricantes para que lo sigan y fabriquen componentes compatibles entre sí.
  - *Existen normas o estándares legitimados por un organismo **(norma de iure)** y otras que no lo están (**norma de facto**).*

ORGANISMOS

- **IEEE** (Institute of Electrical and Electronics Engineers) es una asociación mundial de ingenieros dedicada a la normalización y el desarrollo en áreas técnicas.
- **ISO** (Organización Internacional de Estandarización) es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de normalización.
- **ANSI** (Instituto Nacional Estadounidense de Estándares) es una organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.
- Las normas españolas suelen llevar las siglas **UNE** (Unificación de Normativas españolas**).** Las europeas **EN** (Estándares Europeos, que son de la Unión Europea).
- Ambas son coordinadas por el **CEN** (Comité Europeo de Normalización), a excepción de las normas de telecomunicaciones que se encarga el **ETSI** (European Telecommunications Standards Intitute).
- Las normas de estos organismos se suelen nombrar de la siguiente forma **EN–CEN–802.**

CAPAS O NIVELES

- Una arquitectura de red se divide en **capas o niveles**.
- Las capas adyacentes transmiten información de una a otra mediante una interfaz.
- Una **pila de protocolos** es una colección ordenada de protocolos organizados en capas.

Existen dos tipos básicos de modelos de redes:

- **Modelo de protocolo.** Indica los protocolos que debemos utilizar en cada capa. **El modelo TCP/IP es un modelo de protocolo**
- **Modelo de referencia.** Describe qué es lo que se debe hacer en cada capa, pero no indica cómo. **El modelo OSI en un modelo de referencia**

MODELO DE PROTOCOLO TCP/IP

- Se llama **familia de protocolos de Internet** y contiene decenas de protocolos
- **TCP** es el **Protocolo de Control de Transmisión** (Transmisión Control Protocol)
- **IP** es el **Protocolo de Internet** (Internet Protocol).
- Fue desarrollado por el Departamento de Defensa de los Estados Unidos en 1972, ejecutándolo en la red militar ARPANET.
- Actualmente todos los sistemas operativos llevan este protocolo.
- Tiene 4 capas o niveles.

NIVELES DEL MODELO TCP/IP

APLICACIÓN

- Representa datos para el usuario.
- Controla la codificación y el diálogo.

SSH, SMTP, DHCP, FTP, DNS, SNMP, HTTP

TRANSPORTE

- Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores.

TCP, UDP

INTERNET

- Determina el mejor camino a través de una red

IP, ICMP

ACCESO A LA RED

- Controla los dispositivos del hardware y los medios que forman la red

ARP, ETHERNET

MODELO DE REFERENCIA OSI

- **OSI (Interconexión de sistemas abiertos)** es el modelo de referencia creado por la ISO.
- Es un modelo teórico a seguir para desarrollar protocolos para la conexión de diferentes tipos de redes.
- Proporciona una lista de funciones y servicios que se pueden presentar en cada capa.
- Describe la interacción de cada capa con las capas directamente por encima y por debajo de él.
- Tiene 7 capas o niveles.
- El nivel físico, el enlace de datos y el de red se relacionan con el hardware.
- EL nivel de sesión, el de presentación y el de aplicación con el software.

NIVELES DEL MODELO OSI

Capa 1, capa física. Se encarga de las conexiones físicas, incluyendo el cableado y los componentes necesarios para transmitir la señal.

Capa 2, capa de enlace de datos. Empaqueta los datos para transmitirlos a través de la capa física. Se define el direccionamiento físico mediante las direcciones MAC. Se encarga del acceso al medio, el control de enlace lógico y de la detección de errores de transmisión, entre otras cosas.

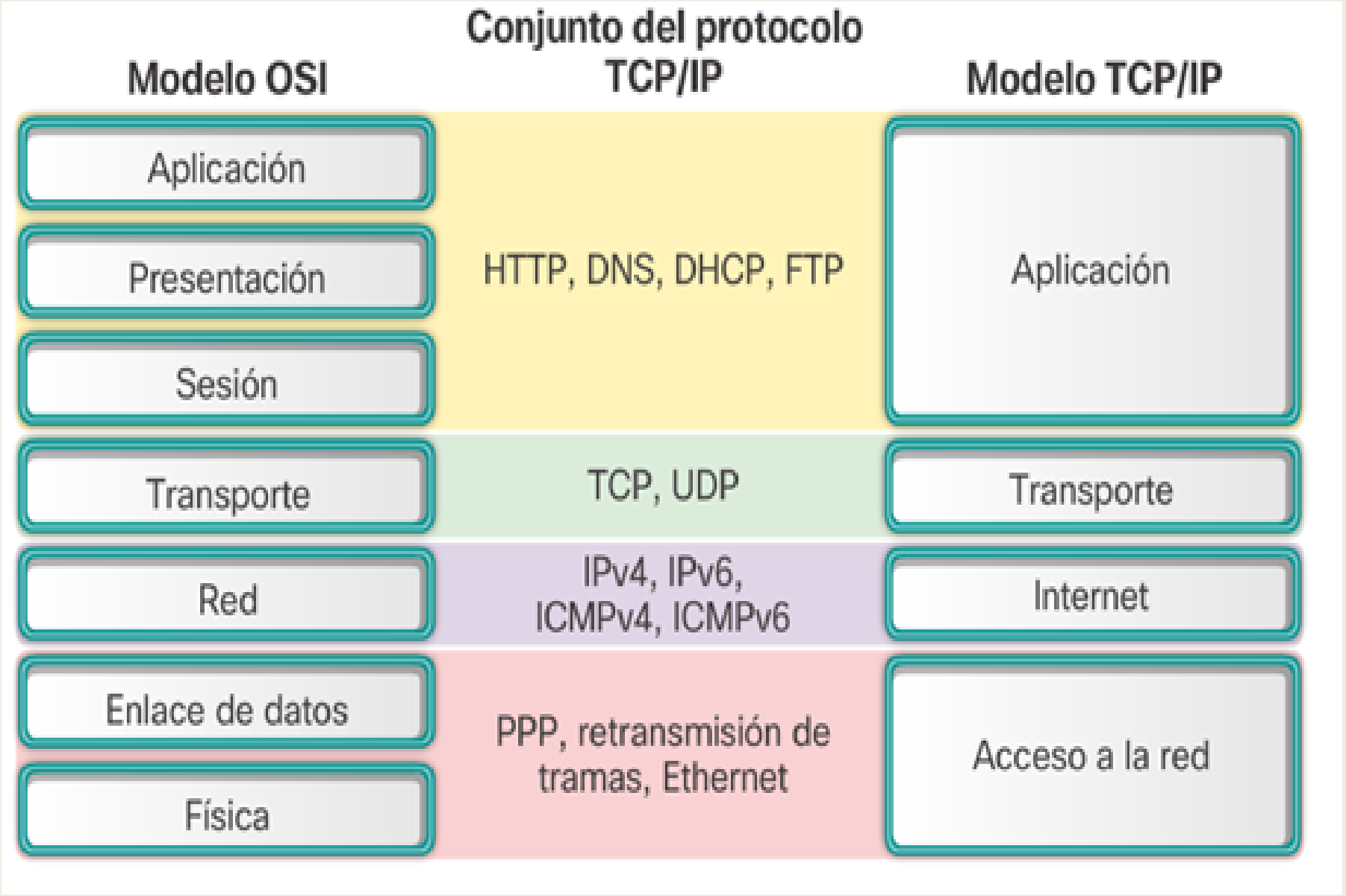
Capa 3, capa de red. Separa los datos en paquetes, determina la ruta que tomaran los datos y define el direccionamiento.

Capa 4, capa de transporte. Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores.

Capa 5, capa de sesión. Mantiene y controla el enlace entre los dos extremos de la comunicación.

Capa 6, capa de presentación. Determina el formato de las comunicaciones así como adapta la información al protocolo que se esté usando.

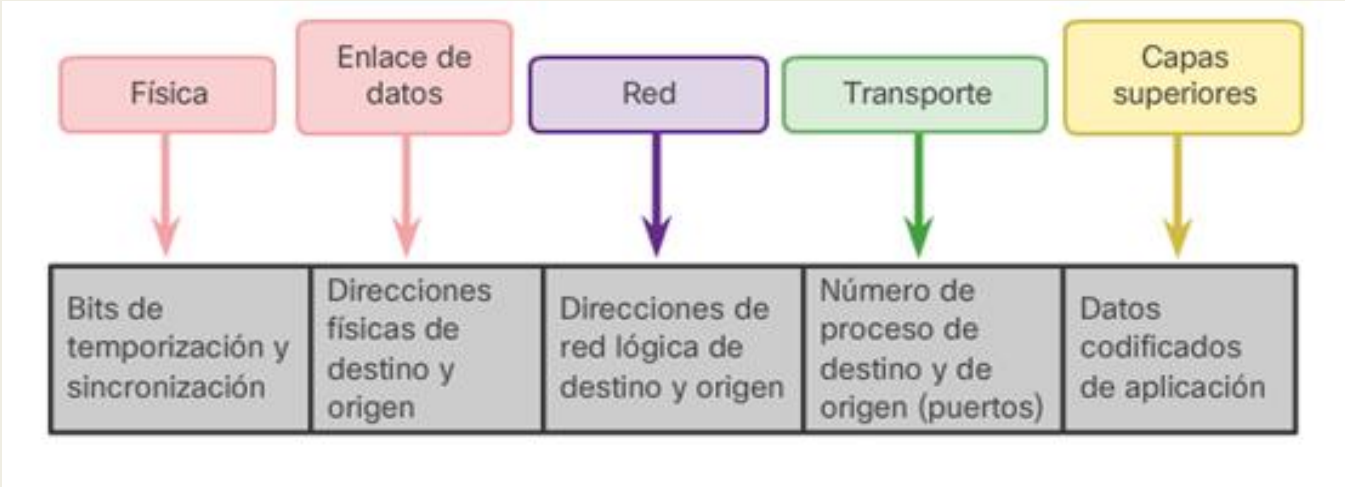
Capa 7, capa de aplicación. Define los protocolos que utilizan cada una de las aplicaciones para poder ser utilizadas en red.


Modelo OSI
Conjunto del protocolo TCP/IP
Modelo TCP/IP
Aplicación
Presentación
Sesión
HTTP, DNS, DHCP, FTP
Aplicación
Transporte
TCP, UDP
Transporte
Red
IPv4, IPv6, ICMPv4, ICMPv6
Internet
Enlace de datos
Física
PPP, retransmisión de tramas, Ethernet
Acceso a la red

UNIDADES DE DATOS DE PROTOCOLO

Encapsulamiento: Agregar información de protocolos en cada nivel según van bajando los datos hasta la capa física.
Unidad de datos del protocolo (PDU) es la forma que adopta una porción de datos en cualquier capa.

- BIT – capa física
- TRAMA – enlace de datos
- PAQUETE – capa de red
- SEGMENTO (TCP), DATAGRAMA (UDP) – capa de transporte
- DATOS – resto



MAC IP PUERTO

PROTOCOLOS TCP Y UDP

- **TCP y UDP** son dos protocolos de comunicación a través de Internet.
- Se sitúan en la **capa de transporte del modelo TCP/IP.**
- **El protocolo TCP (Protocolo de Control de Transmisión)** permite que las aplicaciones puedan comunicarse con garantías independientemente de las capas inferiores del modelo TCP/IP.
- **TCP da soporte a múltiples protocolos de la capa de aplicación**, (HTTP (web), HTTPS (web segura), POP3 (correo entrante) y SMTP (correo saliente) sus versiones seguras utilizando TLS, FTP, FTPES y SFTP para transferir archivos desde un origen a un destino, protocolo SSH para administrar equipos de forma local y remota de manera segura utiliza el protocolo TCP.)
- **El protocolo UDP (protocolo de datagramas de usuário)** es un protocolo sin conexión de la familia de protocolos de Internet que funciona en la capa de transporte.
- **El protocolo UDP funciona sin conexión.** Los datagramas respectivos se envían a la dirección IP preferida de la secuencia **especificando el puerto de destino.**
- **El protocolo UDP permite una comunicación rápida y sin retardos, pero no ofrece garantía de seguridad e integridad de los datos.**
- Se usa principalmente para consultas DNS, conexiones VPN y para el streaming de audio y vídeo.

IDENTIFICACION DE ELEMENTOS Y ESPACIOS

MEDIOS DE TRANSMISIÓN

- El **medio de transmisión** constituye el canal en la comunicación entre sistemas informáticos.
- Pertenecen al nivel FÍSICO del modelo OSI.
- Dependiendo de la forma de conducir la señal a través del medio puede ser:

MEDIOS FÍSICOS GUIADOS

- ✓ *Cable de par trenzado*
- ✓ *Cable coaxial*
- ✓ *Fibra óptica*

MEDIOS FÍSICOS NO GUIADOS

- ✓ *Ondas de radio*
- ✓ *Microondas Terrestres*
- ✓ *Infrarrojos/láser*

CARACTERISTICAS DE LOS MEDIOS DE TRANSMISIÓN

ANCHO DE BANDA

- Es la cantidad máxima de datos que podemos enviar o recibir utilizando una conexión de red que se mantiene constante, en un período de tiempo determinado.
- Se mide en bits por segundo (bps).

TASA DE TRANSFERENCIA o VELOCIDAD DE TRANSFERENCIA

- Es la rapidez con la que se pueden comunicar dos dispositivos digitales.
- Se mide en bits por segundo (bps).

LATENCIA

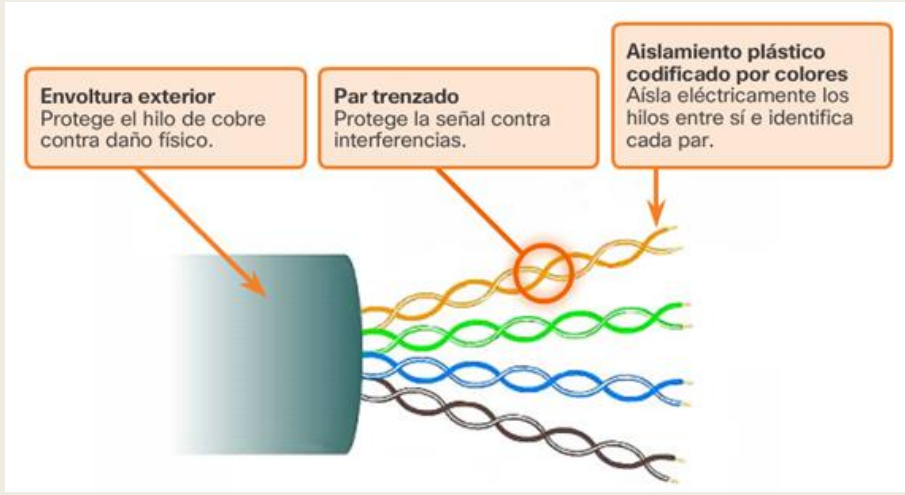
- tiempo total que transcurre desde que envía una información, hasta que la misma llega a un receptor. Su valor de medición se hace en milisegundos

RUIDO

- Es el conjunto de señales extrañas a la transmisión que se introducen en el medio de transmisión provocando alteraciones de amplitud del voltaje y variaciones de frecuencia

CABLE DE PAR TRENZADO

- Consta de 8 hilos (4 grupos de dos hilos llamados par) de un material conductor (cobre), que se trenzan de forma helicoidal. Esto aumenta la potencia y minimiza las interferencias y la diafonía (crosstalk Perturbación electromagnética producida en un canal de comunicación por el acoplamiento de este con otro u otros vecinos).
- La **tasa de trenzado** mide el número de vueltas por metro, a mayor tasa de trenzado, mayor será la atenuación de la diafonía.
- El cable está forrado por PVC. El recubrimiento de los hilos está coloreado, de forma normalizada.
- Para el cable de cuatro pares, que se utiliza en redes de ordenadores bajo el estándar IEEE 802.3 (Ethernet) se utiliza el siguiente código de colores:
  - *Par 1: Blanco-Azul/Azul*
  - *Par 2: Blanco-Naranja/Naranja*
  - *Par 3: Blanco-Verde/Verde*
  - *Par 4: Blanco-Marrón/Marrón*
- Tipos de cableado de par trenzado por su apantallamiento:
  - *Sin apantallar: Unshielded Twisted Pair (**UTP**)*
  - *Apantallado: Shielded Twisted Pair (**STP**)*
  - *Con pantalla global: Foiled twisted Pair (**FTP**)*



TIPOS DE CABLE DE PAR TRENZADO

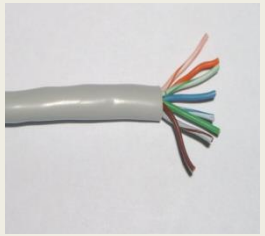
UTP

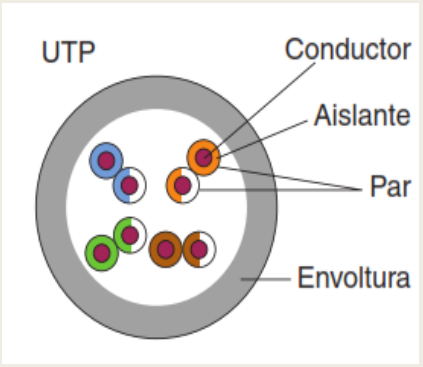
Par trenzado sin apantallar

Son de bajo costo y de fácil uso

Producen más errores que otros tipos de cable

Tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal.





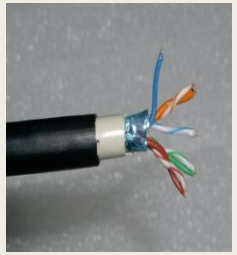
FTP

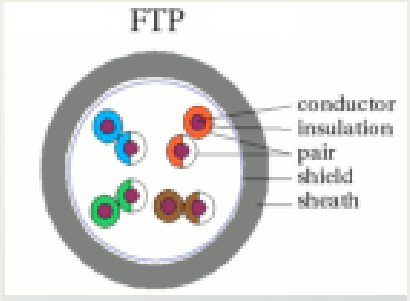
Par trenzado con blindaje global

Mejora la protección frente a interferencias

Tiene una rigidez intermedia.

También existe el SFTP con blindaje extra.





STP

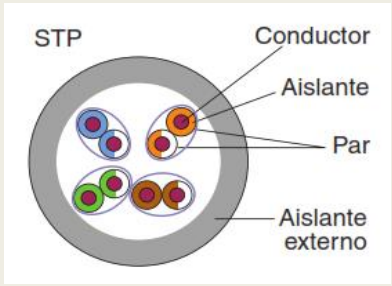
Par trenzado apantallado individualmente.

Cada par se envuelve en una malla conductora y otra general que recubre a todos los pares.

Poseen gran inmunidad al ruido,

Es el cable menos flexible.

También existe el SSTP con blindaje extra.



TIPOS DE CABLE DE PAR TRENZADO

CAT	USO	VELOCIDAD	ESTÁNDAR
1	Transmisión telefónica Suele tener 4 hilos de cobre		
2	Transmisión de datos (desfasado)	4 Mbits/s	
3	Transmisión de datos	10 Mbits/s	ETHERNET 10base-T
4	Transmisión de datos (poco común)	20 Mbits/s	
5	Transmisión de datos	100 Mbits/s	ETHERNET Fast ETHERNET
5e	Transmisión de datos	1 Gbits/s	Fast ETHERNET Gigabit ETHERNET
6	Transmisión de datos entre puntos bastante distanciados	1 Gbits/s	Fast ETHERNET Gigabit ETHERNET
6a y 7	Transmisión de datos a muy altas velocidades	10 Gbits/s	10 Gigabit ETHERNET

CONECTORES PARA CABLE DE PAR TRENZADO

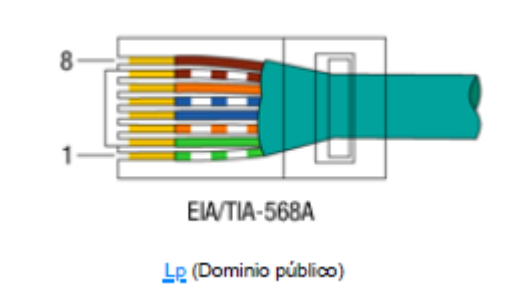
RJ11
Conector utilizado para líneas telefónicas.

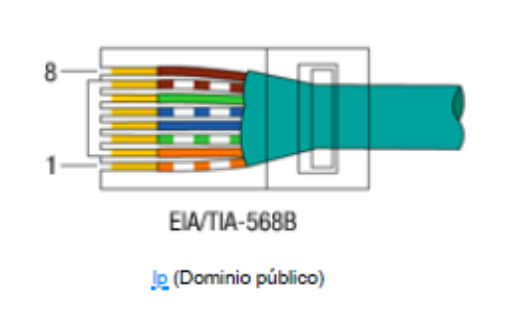
RJ45
Conector principal utilizado con tarjetas de red Ethernet.

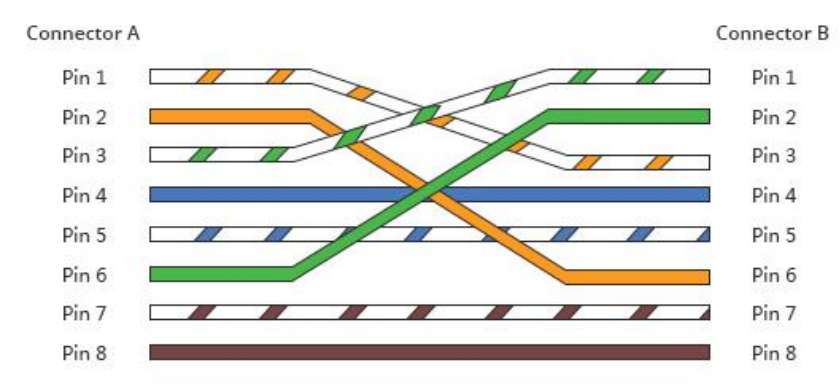
RJ49
Igual que el RJ45 pero recubierto con una capa metálica para que haga contacto con la que recubre el cable STP o FTP

ESTÁNDARES DE CONEXIÓN

- Para la conexión de los 8 hilos al conector RJ-45 se realiza según los **estándares** ANSI/EIA/TIA **568 A y B**.
- En las conexiones de dispositivos de distintas capas usaremos **cables directos, que significa que los dos extremos utilizarán el mismo estándar**, se recomienda usar la 568B.
- El **cable cruzado se utilizará en el caso de dispositivos de la misma capa, se usará la norma 568A en un extremo y la norma 568B en el otro**. En la actualidad la mayoría de dispositivos admite el cable directo y él se encarga de cruzarlo.

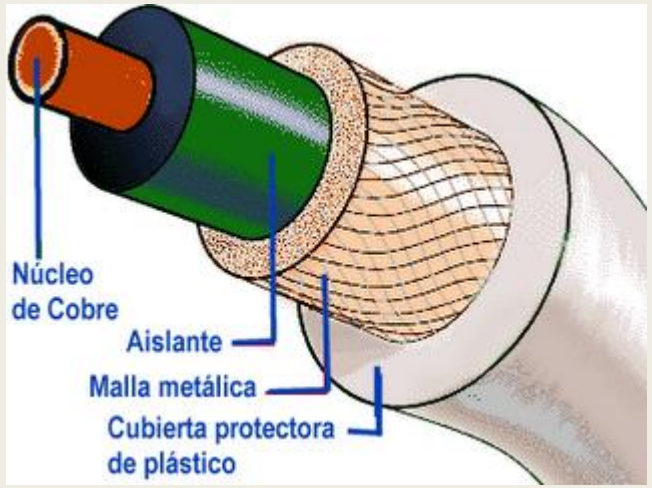






CABLE COAXIAL

- Es el cable de antena de televisión.
- Tiene dos conductores concéntricos: uno de cobre rígido (o hilos trenzados) que lleva la información, y otro exterior en forma de malla trenzada (o de tubo de cobre o aluminio) que sirve de referencia de tierra y retorno de corriente.
- La atenuación, disminuye según aumenta el grosor del hilo de cobre interior, de modo que se consigue un mayor alcance de la señal.
- Los tipos de cable coaxial para las redes de área local son:
- Ethernet grueso (**THICK**):
  - *Tiene un grosor de 1,27 cm*
  - *Transporta la señal a más de 500 m.*
  - *Cable bastante grueso*
- Ethernet fino (**THIN**):
  - *Tiene un grosor de 0,64 cm*
  - *Transportar una señal hasta 185 m.*
  - *Es un cable flexible y de fácil instalación (comparado con el cable coaxial grueso).*



ELEMENTOS NECESARIOS PARA LA CONEXIÓN

Pertenecen a la familia denominada **BNC.** Los principales son:

El conector de cable BNC

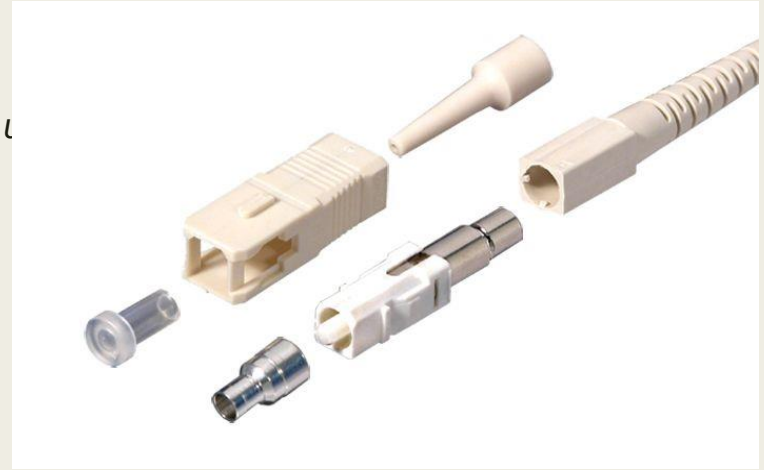
Conector BNC, en forma de T, conecta la tarjeta de red del ordenador con el cable de red.

Terminador, se trata de una resistencia de 50 ohmios que cierra el extremo del cable. Su finalidad es absorber las señales perdidas, y así evitar que reboten indefinidamente.

Conector acoplador, denominado **barrel**, utilizado para unir dos cables y así alargar su longitud.

FIBRA ÓPTICA

- Se basa en la utilización de ondas de luz para transmitir información binaria.
- Un sistema de transmisión óptico se compone de tres componentes:
  - *La fuente de luz: convencionalmente, un pulso de luz indica un bit 1 y la ausencia de luz u*
  - *El medio de transmisión: fibra de vidrio ultradelgada.*
  - *El detector: genera un impulso eléctrico cuando la luz incide sobre él.*
- Existen dos formas diferentes de transmisión de la luz:



Monomodo:

La fibra es tan delgada que la luz se transmite paralela al eje.
Permiten solo un modo de propagación.
Se usan para distancias largas
Más costoso
Permite mayor capacidad de transporte (

Multimodo:

La luz se propaga por el interior del núcleo incidiendo sobre su superficie interna, como si se tratara de un espejo.
Se puede llegar a tener más de mil modos en una misma fibra.
Su uso está extendido para distancias inferiores al kilómetro por ser más económico.
Al ser su núcleo más ancho, es más fácil de conectar y tiene más tolerancia a componentes de menor precisión.

CONECTORES FIBRA ÓPTICA

MEDIOS FÍSICOS NO GUIADOS

La información se envía mediante señales electromagnéticas.

Para que se produzca la transmisión de información deben existir antenas que se encargues de la emisión y recepción de las ondas.

Pueden ser:

- *Transmisión direccional*
- *Transmisión omnidireccional*

Son medios físicos no guiados:

- *Sistemas radio terrestres, radiotransmisión*
- *Sistemas de Microondas*
- *Sistemas de ondas infrarrojas, para dispositivos que no estén a mucha distancia.*

Conexiones a Internet domésticas y de oficinas pequeñas

Cable:

- *La señal de datos se transmite a través del mismo cable que la señal de televisión por cable.*
- *Conexión siempre activa y de un ancho de banda elevado.*

DSL: (línea de suscriptor digital)

- *Se transporta por la línea de teléfono.*
- *Conexión a Internet siempre activa y de un ancho de banda elevado.*
- *Generalmente se conectan mediante una línea de suscriptor digital asimétrica (ADSL), (velocidad de descarga mayor que la de carga).*

Red móvil:

- *En cualquier lugar donde tenga cobertura de telefonía móvil, puede tener acceso a Internet.*
- *Rendimiento limitado por las capacidades del dispositivo y la torre a la que se conecte.*

Conexiones a Internet domésticas y de oficinas pequeñas

Satelital:

- *Ventaja para las áreas que no tienen acceso a otro tipo de conectividad a Internet.*
- *Las antenas parabólicas requieren una línea de vista despejada al satélite.*

Telefonía por conexión conmutada:

- *Opción de bajo costo que funciona con cualquier línea telefónica y un módem.*
- *El ancho de banda que proporciona una conexión por módem bajo y no suele ser suficiente para trasferencias de datos masivas, pero si para acceso móvil durante viajes.*

Conexiones a Internet empresariales

Las empresas requieren un ancho de banda mayor y dedicado.

Líneas arrendadas dedicadas:

- *Circuitos reservados dentro de la red del proveedor (sp) que conectan oficinas separadas geográficamente para de comunicaciones por voz o redes de datos privados.*

WAN Ethernet:

- *Amplían la tecnología de acceso LAN a una WAN.*
- *Ethernet es una red LAN que ahora se extienden a las redes WAN.(metro Ethernet)*

DSL:

- *Similar al ADSL para usuario.*
- *La más utilizada es SDSL (línea de suscriptor digital simétrica), velocidad subida = descarga.*

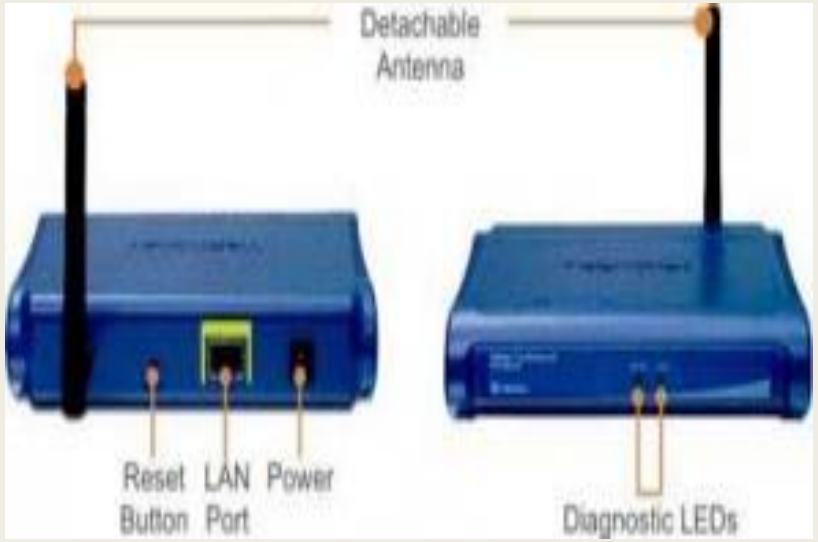
Satelital:

- *Similar al servicio para usuarios de oficinas en el hogar.*

DISPOSITIVOS DE CONEXIÓN

Los **dispositivos de conexión** son los diferentes dispositivos que utilizamos para poder ampliar una red aislada o interconectar redes individuales, con el propósito de compartir o unir los ordenadores y los recursos que contienen.

- **REPEATER (REPETIDOR):** Amplifica la señal de la red, permitiendo utilizar longitudes mayores de cable. Actúa en la capa 1 (física) del modelo OSI.



HUB (CONCENTRADOR)

Contiene diferentes puntos de conexión, denominados **puertos,** retransmitiendo cada paquete de datos recibidos por uno de los puertos a todos los demás.

Actúa en el nivel físico o capa 1 del modelo OSI.

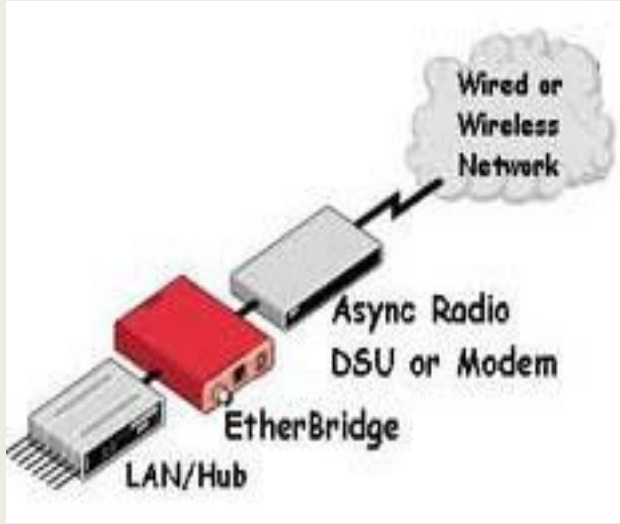
BRIDGE (PUENTE)

Une dos segmentos lógicos de la misma red

seleccionando el tráfico que pasa de un segmento a otro.

Los Bridge actúan a nivel físico y de enlace de datos del

modelo OSI.

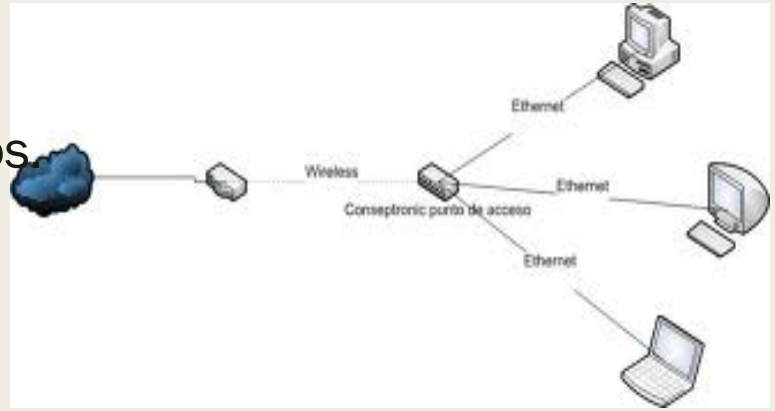


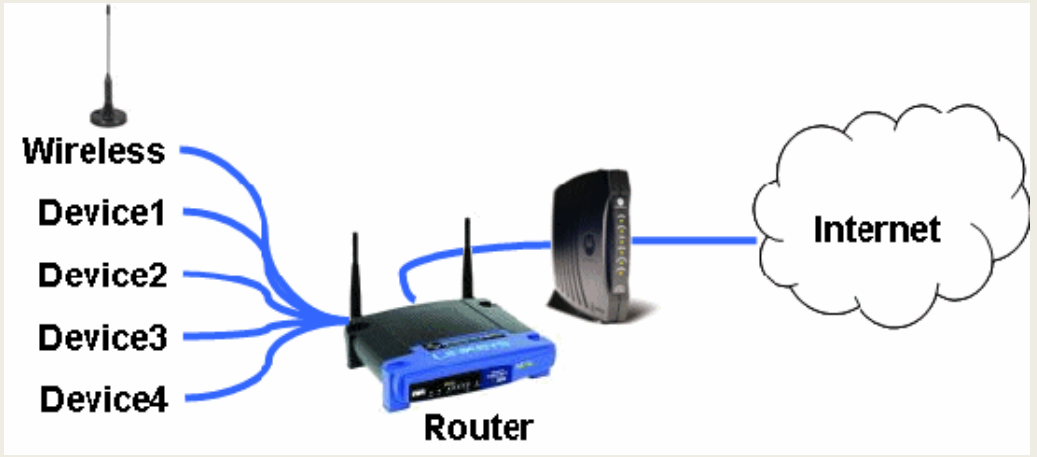
SWITCH (CONMUTADOR)

Interconecta dos o más segmentos de red, pasando segmentos de uno a otro de acuerdo con la dirección de control de acceso al medio (MAC). Actúa como filtro en la capa de enlace de datos (capa 2) del modelo OSI.

ACCESS POINT (punto de acceso inalámbrico, WAP o AP)

Es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. También puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.





- ROUTER (ENCAMINADOR)

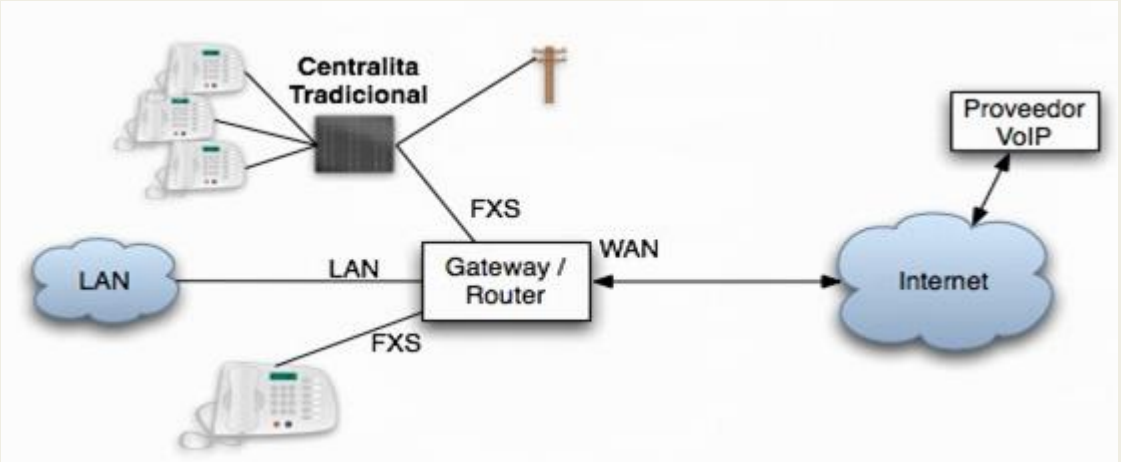
Operan entre redes aisladas que utilizan protocolos similares.

La primera función de un router, es saber si el destinatario de un paquete de información está en nuestra propia red o en una remota. Para ello utiliza la “máscara de red”.

Además encamina la información por la mejor ruta.

Los routers pueden estar conectados a dos o más redes a la vez, y realiza tareas a nivel de red del modelo OSI , aunque puede realizar tareas de los tres niveles inferiores del modelo OSI: físico, enlace de datos y red.

Existen routers que son también Switch y punto de acceso WIFI.

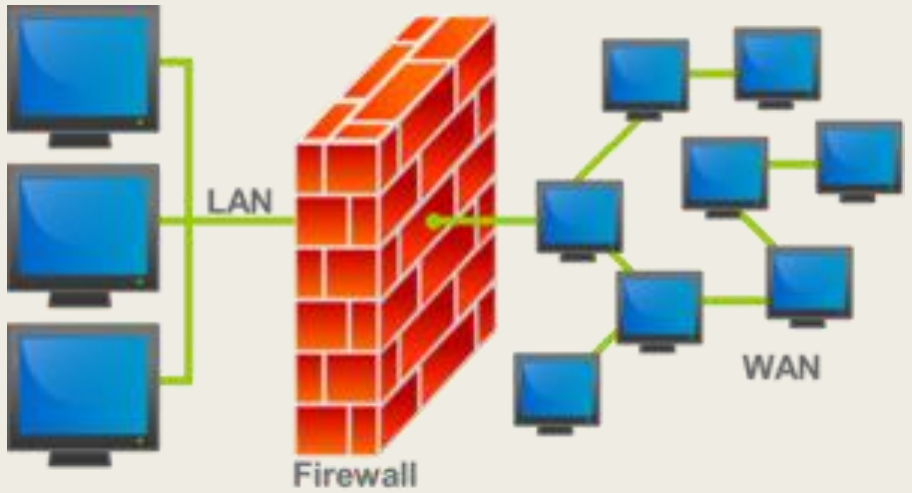


- **GATEWAY (PASARELA)**

  Son dispositivos que trabajan a nivel de transporte, sesión, presentación y aplicación, del modelo OSI, y que permiten interconectar redes que utilizan distintos protocolos: por ejemplo TCP/IP, SNA, Netware, VoIP.

  Los Gateway desensamblar las tramas y paquetes para obtener el mensaje original y después vuelven a reconfigurar los paquetes y las tramas de acuerdo con el protocolo de la red donde se encuentra la estación de destino.

  En la actualidad los Gateway son muy utilizados en voz sobre IP (VoIP).



- **FIREWALL (CORTAFUEGOS)**

  Componente hardware o software, o ambos que bloquea el acceso no autorizado y permite comunicaciones autorizadas.

  Todos el tráfico pasa a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. Si se necesitan servidores que permanezcan accesibles desde la red exterior, se conecta el cortafuegos a una red, llamada *zona desmilitarizada o* DMZ.

OTROS ELEMENTOS DE RED

PUERTOS

- Un puerto permite identificar los procesos de nivel de aplicación que forman parte de la comunicación.
- Se implementa por el nivel de transporte.
- El campo de puerto tiene una longitud de 16 bits, por lo que el rango de valores válidos va de 0 a 65.535.
- El puerto 0 está reservado, pero es un valor permitido como puerto origen si el proceso emisor no espera recibir mensajes como respuesta.
  - *Puertos "bien conocidos": 1 a 1023*
  - *Los puertos 1024 a 49.151 son puertos registrados y se utilizan para aplicaciones no estándar.*
  - *Los puertos 49.152 a 65.535 son puertos efímeros y son utilizados como puertos temporales, sobre todo por los clientes al comunicarse con los servidores.*

SERVIDOR PROXY

- Un servidor hace de proxy cuando oculta los nodos a los que está dando el servicio.

- **Ejemplo:** Si en una red el PC1 se quiere conectar al PC3 a través del proxy PC2, el PC3 no sabrá que los paquetes que le llegan son originariamente de PC1, ya que pensará que toda la información proviene del PC2

ISP (proveedor de servicios de Internet)

- Un ISP es un servidor que ofrece conexión a Internet a otros equipos de la red.

- Los ISP se dividen en tres niveles:
  - *Nivel 1: enlaces troncales de Internet*
  - *Nivel 2: Usuarios de los ISP nivel 1. Tienen cobertura regional o nacional.*
  - *Nivel 3: sirve conexión al usuario final*

- NAP (network Access point) son el punto de interconexión entre los ISP del mismo nivel.
- POP (point of presence) routers encargados de conectar unos ISP a otros (puede que de distinto nivel)

REDES LOCALES VIRTUALES (VLAN)

- Una VLAN es un método que crea una red lógica dentro de una red física.
- Con esto conseguimos que la información que se genera dentro de las redes virtuales solo sea recibida por hosts de la propia red lógica y no por toda la red física.
- Estas redes se configuran mediante conmutadores (switches) VLAN.
- Existen dos formas de configurar las redes virtuales:
  - ***Estáticas:*** *Se definen los puertos de cada conmutador que pertenecen a una VLAN*
  - ***Dinámicas:*** *Los puertos se asignan automáticamente en función de algún parámetro de la red (MAC, nombre de usuario, etc)*

¿Qué es un servidor DHCP?

- **DHCP** es el protocolo de servicio TCP/IP que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Entre estos parámetros se encuentran las direcciones IP.
- Las estaciones de trabajo "piden" su dirección IP (y demás configuraciones para este protocolo) al servidor, y éste les va asignando direcciones del rango que sirve, de entre aquellas que le quedan libres.
- Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:
- **manualmente**, cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC (código que identifica a la tarjeta de red) con direcciones IP, creada manualmente por el administrador de la red. Sólo clientes con una dirección MAC válida recibirán una dirección IP del servidor.
- **automáticamente**, donde el servidor DHCP asigna permanentemente una dirección IP libre, tomada de un rango prefijado por el administrador, a cualquier cliente que solicite una.
- **dinámicamente**, el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

¿Qué es un servidor DNS?

- El Sistema de Nombres de Dominio o DNS resuelve las peticiones de asignación de nombres.
- Cada vez que un usuario registra un dominio, se crea una entrada WHOIS en el registro correspondiente y queda almacenada en la base de datos del correspondiente DNS.
- La creación del DNS en 1983 sustituyó al procedimiento basado en un archivo local de hosts (***hosts.txt) en*** UNIX lo encontramos en el directorio *etc/* y, en Windows, en *%SystemRoot%\system32\drivers\etc*.
- Actualmente, este archivo se usa para la clasificación de direcciones IP en redes locales. Y para bloquear servidores web desviando automáticamente su dirección hacia el alojamiento local (local host).

Nuevas tendencias

BYOD (Bring Your Own Device)

- "cualquier dispositivo, a cualquier contenido, de cualquier forma"
- Permite a los usuarios finales sus propias herramientas para acceder a información y comunicarse a través de una red.

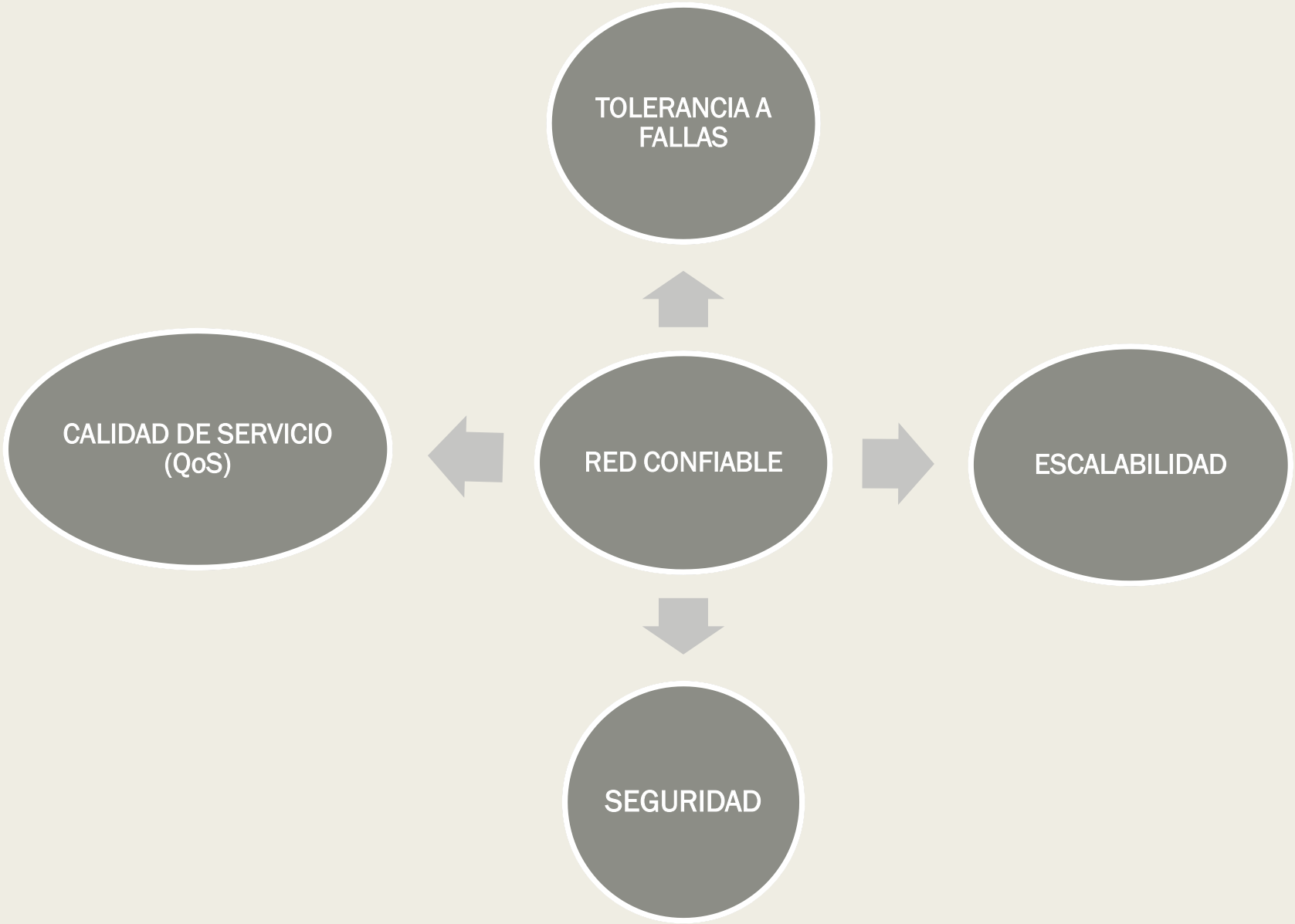
Redes por línea eléctrica

- Mediante un adaptador de línea eléctrica, los dispositivos pueden conectarse a la LAN.

Banda ancha inalámbrica

- *Utiliza la misma tecnología de red móvil*

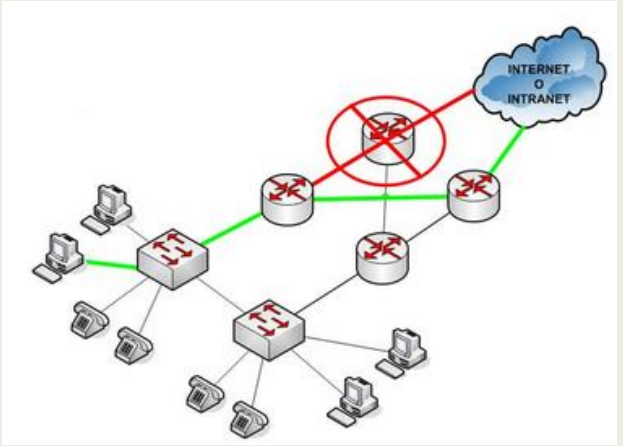
SEGURIDAD


TOLERANCIA A FALLAS
CALIDAD DE SERVICIO (QoS)
RED CONFIABLE
ESCALABILIDAD
SEGURIDAD

Tolerancia a fallas

*Una **red con tolerancia a fallas** es la que limita el impacto de las fallas.*

- *Afecte a la menor cantidad de dispositivos.*
- *Se recupera rápidamente.*



***Las redes de conmutación de circuitos** establecen un circuito dedicado entre el origen y el destino antes de que los usuarios se puedan comunicar.*

***Las redes de conmutación por paquetes** divide el tráfico en paquetes que se enrutan a través de una red compartida. Es decir que los paquetes de un mismo mensaje pueden tomar distintas rutas para llegar al destino. Esto proporciona **redundancia** a las redes confiables.*

Escalabilidad
Calidad de servicio

Escalabilidad

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales.

Calidad de servicio (QoS Quality of Service)

Se da prioridad a unos datos antes que

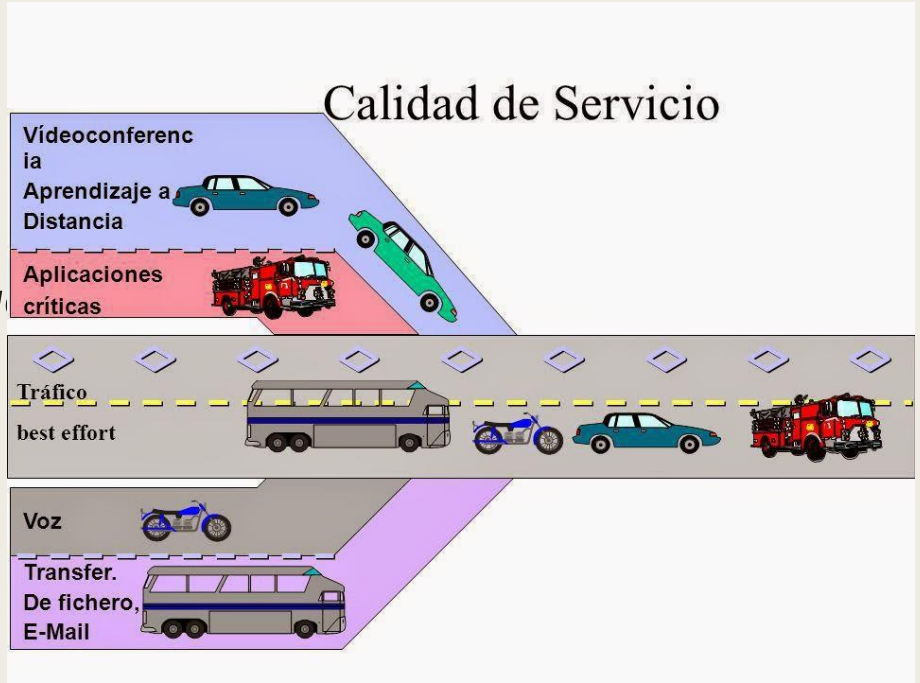
a otros.

El ancho de banda de la red es la cantidad de bits qu
segundo (bps).

Cuando el volumen de tráfico es mayor de lo que

se puede transportar, los dispositivos colocan los

paquetes en cola en la memoria.



Seguridad

Existen dos tipos de problemas de seguridad de red:

- ***La seguridad de la infraestructura de red****: asegurar físicamente los dispositivos que proporcionan conectividad y evitar el acceso no autorizado.*
- ***La seguridad de la información****: proteger la información que contienen los paquetes que se transmiten por la red y la información almacenada.*

Para que una red tenga seguridad debe cumplir:

- **Confidencialidad:** solamente los destinatarios deseados y autorizados pueden acceder a los datos y leerlos.
- **Integridad:** la información no se va a alterar en la transmisión, del origen al destino.
- **Disponibilidad:** acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizado.