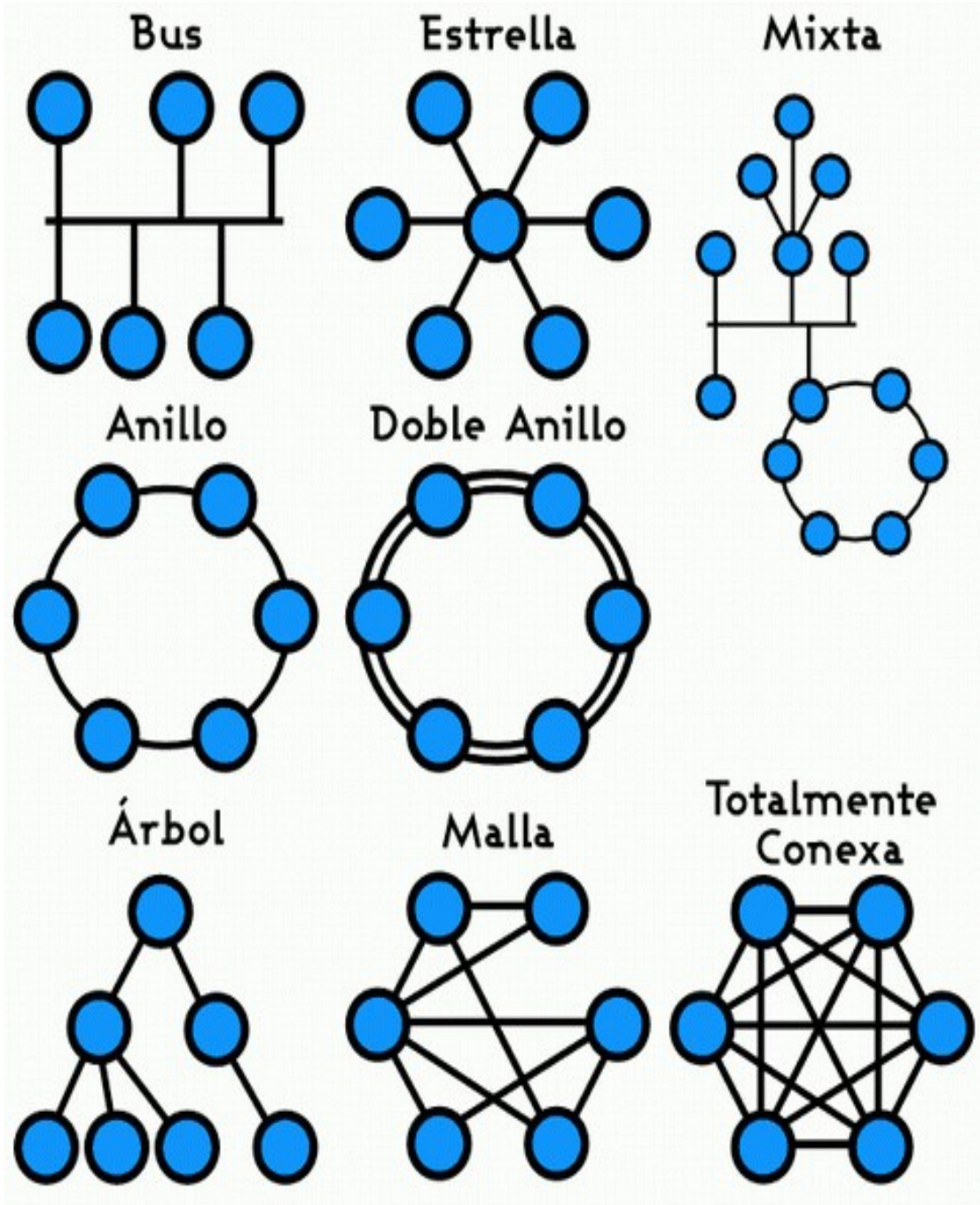
TOPOLOGIAS DE RED



Definición

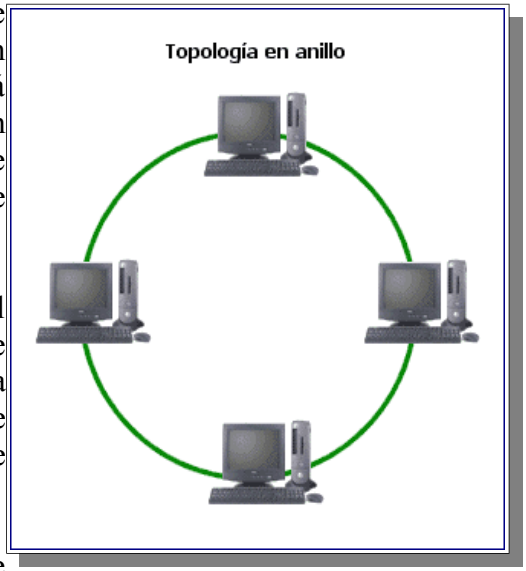
La **topología de red** es la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se la llama mixta.

> **Definición de Nodo** : El término nodo se refiere a un punto de intersección en el que confluyen dos o más elementos de una red de comunicaciones. De esta manera, si nos referimos a una red de computadoras, cada una de las máquinas constituye un nodo. Y si a lo que hacemos referencia es a una red de Internet, cada uno de los servidores también es considerado un nodo, y tienen un nombre propio de dominio y una dirección. También un nodo puede ser los routers, los switchers, etc.
>
> Para entenderlo mejor, no hay que pensar en un nodo como un elemento constituido solamente por una parte física, sino más bien considerarlo como una unidad funcional en donde tiene que haber tanto hardware como software.
>
> Por otra parte, al ser el punto de conexión de dos o más elementos, el nodo por lo general tiene la capacidad de recibir información, procesarla y enrutarla a otro u otros nodos. De esta manera, un nodo puede ser el punto de conexión para transmitir los datos, el punto desde el cual se redistribuye los datos hacia otros nodos y el punto final al que se transmiten los datos.

Topologías más comunes

Red en anillo

Topología de red en la que las estaciones se conectan formando un anillo. Cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación del anillo.



En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evita perdida de información debido a colisiones.

Cabe mencionar que si algún nodo de la red se cae (termino informático para decir que esta en mal funcionamiento o no funciona para nada) la comunicación en todo el anillo se pierde.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos). Evita las colisiones.

Ventajas

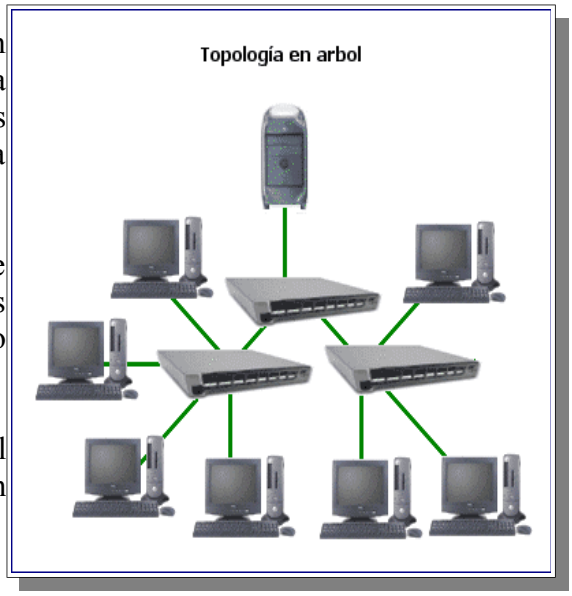
- Simplicidad de arquitectura.
- Facilidad de configuración.
- Facilidad de fluidez de datos

Desventajas

- Longitudes de canales
- El canal usualmente se degradará a medida que la red crece.
- Difícil de diagnosticar y reparar los problemas.
- Si una estación o el canal falla, las restantes quedan incomunicadas.

Red en árbol

Topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas.



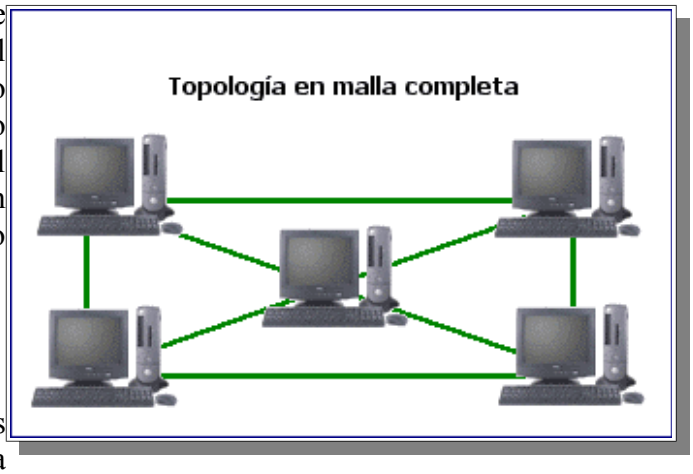
Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

Cuenta con un cable principal (*backbone*) al que hay conectadas redes individuales en bus.

Red en malla

La Red en malla es una topología de red en la que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos.

Si la red de malla está completamente conectada no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.



Esta topología, a diferencia de otras (como la topología en árbol y la topología en estrella), no requiere de un servidor o nodo central, con lo que se reduce el mantenimiento (un error en un nodo, sea importante o no, no implica la caída de toda la red).

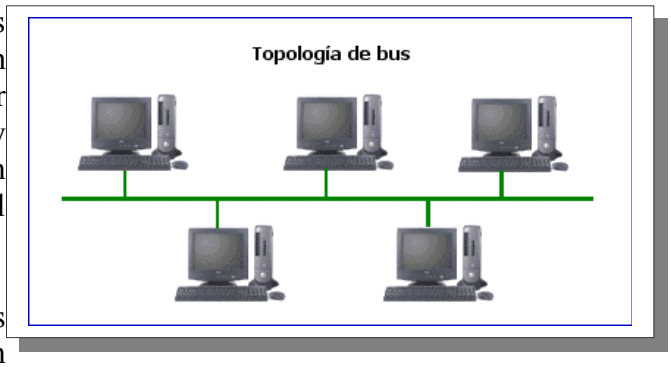
Ventajas

- Es posible llevar los mensajes de un nodo a otro por diferentes caminos.
- No puede existir absolutamente ninguna interrupción en las comunicaciones.
- Cada servidor tiene sus propias comunicaciones con todos los demás servidores.
- Si falla un cable el otro se hará cargo del trafico.
- No requiere un nodo o servidor central lo que reduce el mantenimiento.
- Si un nodo desaparece o falla no afecta en absoluto a los demás nodos.
- Si desaparece no afecta tanto a los nodos de redes.
- Las redes de malla son auto ruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.

Desventajas

El costo de la red puede aumentar en los casos en los que se implemente de forma alámbrica, la topología de red y las características de la misma implican el uso de más recursos.

Red en bus



Topología de red en la que todas las estaciones están conectadas a un único canal de comunicaciones por medio de unidades interfaz y derivadores. Las estaciones utilizan este canal para comunicarse con el resto.

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

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes. Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

Ventajas

- Facilidad en la conexión de nuevas estaciones a la red.
- A diferencia de la topología en estrella, en la que el nodo central es el receptor y emisor, en la topología en bus la información viaja libremente a través del canal de transmisión, pudiendo utilizarse toda la capacidad de transmisión de que se dispone.

Desventajas

- Dado que la información viaja por un único canal, a veces pueden producirse interferencias entre unas emisiones y otras.
- Las estaciones conectadas deben ser inteligentes o en su defecto, necesitan una interfase de conexión que lo sea.
- Normalmente la longitud del canal de transmisión no sobrepasa los 1500-2000 metros.

Características del Cable

- 10-BASE-5 Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo de 500 metros. Distancia entre nodos: 2.5 m. Terminadores: 50 ohm.
- 10-BASE-2 Cable coaxial fino (Ethernet fino). Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo de 185 metros. Distancia entre nodos: 1 m. Terminadores: 50 ohm.

Red en estrella

Red en la cual las estaciones están conectadas directamente al servidor u ordenador y todas las comunicaciones se han de hacer necesariamente a través de él. Todas las estaciones están conectadas por separado a un centro de comunicaciones, concentrador o nodo central, pero no están conectadas entre sí. Esta red crea una mayor facilidad de supervisión y control de información ya que para pasar los

mensajes deben pasar por el hub o concentrador, el cual gestiona la redistribución de la información a los demás nodos. La fiabilidad de este tipo de red es que el malfuncionamiento de un ordenador no afecta en nada a la red entera, puesto que cada ordenar se conecta independientemente del hub, el costo del cableado puede llegar a ser muy alto. Su punto débil consta en el hub ya que es el que sostiene la red en uno.

Características del Cable

- Tipo de cable usado 10 BASE T Tipo de conector RJ-45 Velocidad 10 Mbits/s Máxima longitud entre la estación y el concentrador 90 m Máxima longitud entre concentradores 100 m Máximo de dispositivos conectados por segmento 512

Red Inalámbrica Wi-Fi

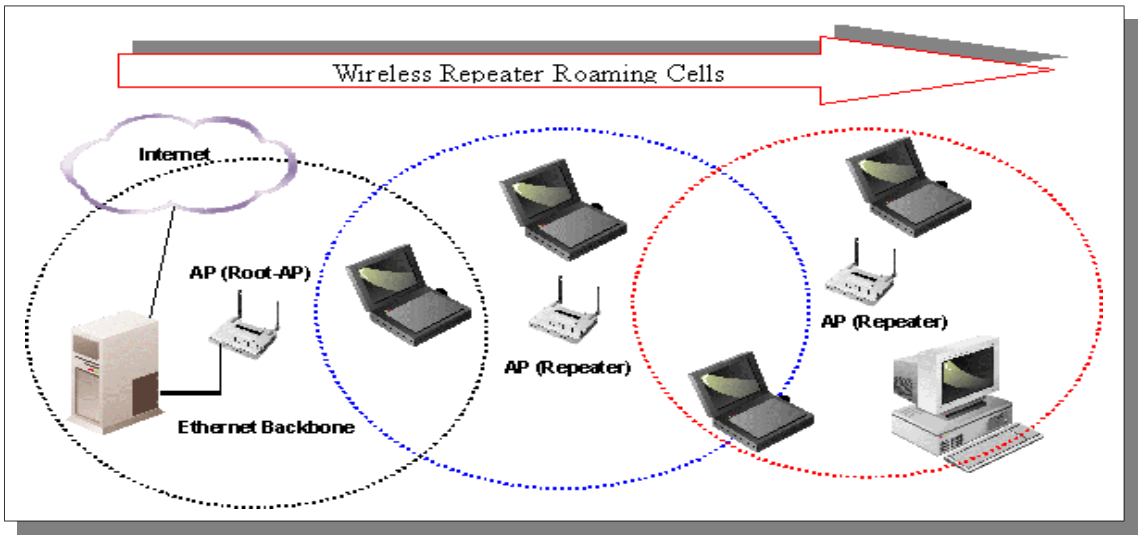
Wi-Fi es una marca de la *Wi-Fi Alliance* (anteriormente la *Wireless Ethernet Compatibility Alliance*), la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x.

Las nuevas redes sin cables hacen posible que se pueda conectar a una red local cualquier dispositivo sin necesidad de instalación, lo que permite que nos podamos pasear libremente por la oficina con nuestro ordenador portátil conectado a la red o conectar sin cables cámaras de vigilancia en los lugares más inaccesibles. También se puede instalar en locales públicos y dar el servicio de acceso a Internet sin cables.

La norma IEEE 802.11b dio carácter universal a esta tecnología que permite la conexión de cualquier equipo informático a una red de datos Ethernet sin necesidad de cableado, que actualmente se puede integrar también con los equipos de acceso ADSL para Internet.

Seguridad

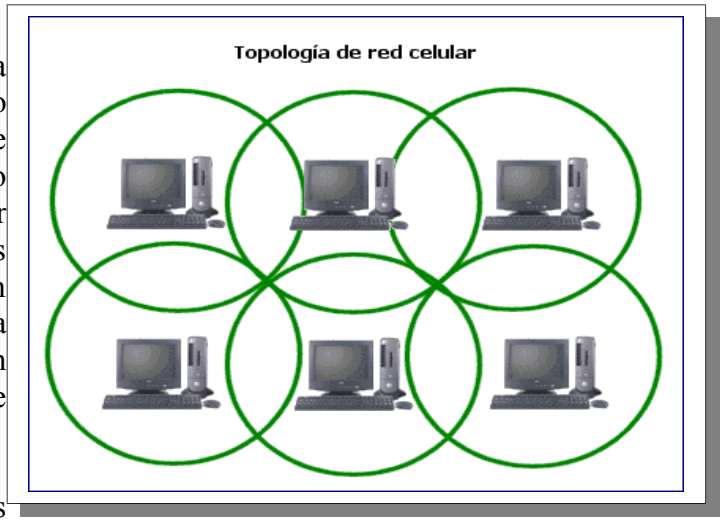
Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes se han instalado por administradores de sistemas o de redes por su simplicidad de implementación, sin tener en consideración la seguridad y por tanto han convertido sus redes en redes abiertas, sin proteger el acceso a la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes, las más comunes son la utilización de protocolos de encriptación de datos como el WEP y el WPA, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) y 802.1x, proporcionados por o mediando otros dispositivos de la red de datos.



Red celular

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

La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica. En esta tecnología no existen enlaces físicos; solo hay ondas electromagnéticas.



La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios y violaciones de seguridad.

Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

Red en Bus: 802.3 "Ethernet"

Norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionada para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla de versiones futuras de 40 Gbps y 100 Gbps. En sus versiones de hasta 1 Gbps utiliza el protocolo de acceso al medio CSMA/CD (Carrier Sense Multiple Access / Collision Detect - Acceso múltiple con detección de

portadora y detección de colisiones). Actualmente Ethernet es el estándar más utilizado en redes locales/LANs.

Ethernet fue creado por Robert Metcalfe y otros en Xerox Parc, centro de investigación de Xerox para interconectar computadoras. El diseño original funcionaba a 1 Mbps sobre cable coaxial grueso con conexiones vampiro (que "muerden" el cable). Para la norma de 10 Mbps se añadieron las conexiones en coaxial fino (10Base2, también de 50 ohmios, pero más flexible), con tramos conectados entre si mediante conectores BNC; par trenzado categoría 3 (10BaseT) con conectores RJ45, mediante el empleo de hubs y con una configuración física en estrella; e incluso una conexión de fibra óptica (10BaseF).

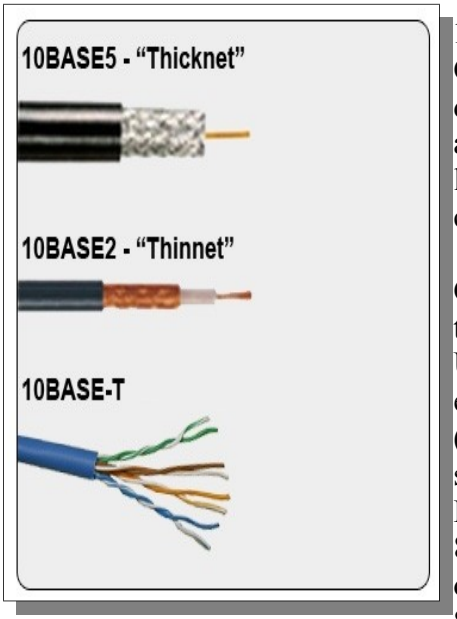
Los estándares sucesivos (100 Mbps o Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet) abandonaron los coaxiales dejando únicamente los cables de par trenzado sin apantallar (UTP - Unshielded Twisted Pair), de categorías 5 y superiores y la Fibra óptica.

Hardware comúnmente utilizado en una red Ethernet

- **NIC,** o **adaptador de red Ethernet**: Permite el acceso de una computadora a una red. Cada adaptador posee una dirección MAC que la identifica en la red y es única. Una computadora conectada a una red se denomina nodo.
- **Repetidor** o **repeater**: Aumenta el alcance de una conexión física, disminuyendo la degradación de la señal eléctrica en el medio físico
- **Concentrador** o **hub**: Funciona como un repetidor, pero permite la interconexión de múltiples nodos, además cada mensaje que es enviado por un nodo, es repetido en cada boca el hub.
- **Puente** o **bridge**: Interconectan segmentos de red, haciendo el cambio de frames entre las redes de acuerdo con una tabla de direcciones que dice en que segmento está ubicada una dirección MAC.
- **Conmutador** o **switch**: Funciona como el bridge, pero permite la interconexión de múltiples segmentos de red, funciona en velocidades más rápidas y es más sofisticado. Los switches pueden tener otras funcionalidades, como redes virtuales y permiten su configuración a través de la propia red.
- **Enrutador** o **router**: Funciona en una capa de red más alta que los anteriores -- el nivel de red, como en el protocolo IP, por ejemplo -- haciendo el enrutamiento de paquetes entre las redes interconectadas. A través de tablas y algoritmos de enrutamiento, un enrutador decide el mejor camino que debe tomar un paquete para llegar a una determinada dirección de destino.

Estándares utilizados en Ethernet

Los principales estándares utilizados en Ethernet son los siguientes:



10Base5

Conocido como Ethernet de cable grueso. 10 Mbps, de banda base. Puede ser identificado por su cable amarillo. Utiliza cable coaxial grueso; el 5 viene de la longitud máxima del segmento que son 500 m. El cable debe estar unido a tierra en un solo punto.

Cada estación está unida al cable mediante un tranceptor denominado MAU ("Medium Attachment Unit") y un cable de derivación. El conector usado en los adaptadores 10Base5 se denomina AUI ("Attachment Unit Interface"). Tiene un aspecto similar al de un puerto serie con 15 patillas (DB15). Los transceptores no deben estar situados a menos de 8.2 piés (2.5 metros) entre sí, y el cable de derivación no debe exceder de 165 piés (50 metros). Si se utiliza un cable de derivación de alta flexibilidad esta longitud deben ser reducida a 41 piés (12.5 metros).

10Base2

Conocido como Ethernet de cable fino cuya designación comercial es RG-58. 10 Mbps, banda base; utiliza conectores BNC ("Bayonet Nut connector"). Su distancia máxima por segmento es de 606 pies (185 m), aunque pueden utilizarse repetidores para aumentar esta distancia siempre que los datos no pasen por más de dos repetidores antes de alcanzar su destino.

El número de DTEs en cada segmento no debe ser mayor de 30, y deben estar separados por un mínimo de 1.6 pies (0.5 metros).

Utiliza cable coaxial de 50 Ohm apantallado que debe estar terminado por adaptadores resistivos de 50 Ohmios y estar conectado a tierra en un punto. El cable no debe estar conectado consigo mismo formando un anillo, y debe estar conectado al DTE mediante un adaptador "T", sin que esté permitido añadir un prolongador a dicho adaptador ni conectar directamente con el DTE eliminando el adaptador "T". Su mejor atractivo es su precio, del orden del 15% del cable grueso.

10Base-T

En Septiembre de 1990, el IEEE aprobó un añadido a la especificación 802.3i, conocida generalmente como 10BaseT. Estas líneas son mucho más económicas que las anteriores de cable coaxial, pueden ser instaladas sobre los cableados telefónicos UTP ("Unshielded Twister Pairs") existentes [3], y utilizar los conectores telefónicos estándar RJ-45 (ISO 8877), lo que reduce enormemente el costo de instalación (H12.4.2).

Estos cables se conectan a una serie de "hubs", también conocidos como repetidores multipuerto, que pueden estar conectados entre sí en cadena o formando una topología arborescente, pero el camino de la señal entre dos DTEs no debe incluir más de cinco segmentos, cuatro repetidores (incluyendo AUIs opcionales), dos tranceptores (MAUs) y dos AUIs.

10 Mbps, banda base, cable telefónico UTP de 2 pares de categoría 3, 4 o 5, con una impedancia característica de 100 +/-15 ohms a 10 Mhz [4]; no debe exceder de 328 pies (100 m).

Cuando una red contenga cinco segmentos y cuatro repetidores, el número de segmentos coaxiales no debe ser mayor que tres, el resto deben ser de enlace con DTEs (es lo que se conoce como regla 5-4-3). Dicho de otra forma: Entre cualquier par de estaciones no debe haber más de 5 segmentos, 4 repetidores y 3 conexiones hub-hub. Si se utilizan segmentos de fibra óptica, no deben exceder de 1640 pies (500 metros).

Cuando una red contenga cuatro segmentos y tres repetidores utilizando enlaces de fibra óptica, los segmentos no deben exceder de 3280 pies (1000 metros).

10Base-F
10 Mbps, banda base, cable de fibra óptica. Longitud máxima del segmento: 2000 metros.

100Base-FX
Fast Ethernet a 100 Mbps que utiliza fibra óptica. Longitud máxima del segmento: 2000 metros.

100Base-T4
Fast Ethernet a 100 Mbps, banda base, que utiliza par trenzado de 4 pares de categoría 3, 4 o 5. Distancia máxima: 100 metros.

100Base-TX
Fast Ethernet a 100 Mbps, banda base, utiliza par trenzado de 2 pares de categoría 5.

> **Nota**: Como puede verse, los distintos estándares Ethernet tienen una denominación que responde a la fórmula general **xBaseZ**. La designación **Base** se refiere a "Baseband modulation", que es el método de modulación empleado. El primer número **X**, indica la velocidad en Megabits por segundo sobre el canal (que es distinta de la velocidad disponible para datos, ya que junto a estos se incluyen los "envoltorios"). La última cifra (o letra) **Z**, señala la longitud máxima del cable en centenares de metros, o el tipo de tecnología. Por ejemplo, **T** significa "Twisted (pairs)", **F** "Fiber", etc.

Distancia máxima: 100 metros.

Componentes básicos de una red

Los componentes básicos para poder montar una red local son:

Servidor

Es una computadora utilizada para gestionar el sistema de archivos de la red, da servicio a las impresoras, controla las comunicaciones y realiza otras funciones. Puede ser dedicado o no dedicado.

El sistema operativo de la red está cargado en el disco fijo del servidor, junto con las herramientas de administración del sistema y las utilidades del usuario.

La tarea de un servidor dedicado es procesar las peticiones realizadas por la estación de trabajo. Estas peticiones pueden ser de acceso a disco, a colas de impresión o de comunicaciones con otros dispositivos. La recepción, gestión y realización de estas peticiones puede requerir un tiempo considerable, que se incrementa de forma paralela al número de estaciones de trabajo activas en la red. Como el servidor gestiona las peticiones de todas las estaciones de trabajo, su carga puede ser muy pesada.

Se puede entonces llegar a una congestión, el tráfico puede ser tan elevado que podría impedir la recepción de algunas peticiones enviadas.

Cuanto mayor es la red, resulta más importante tener un servidor con elevadas prestaciones. Se necesitan grandes cantidades de memoria RAM para optimizar los accesos a disco y mantener las colas de impresión. El rendimiento de un procesador es una combinación de varios factores, incluyendo el tipo de procesador, la velocidad, el factor de estados de espera, el tamaño del canal, el tamaño del bus, la memoria caché así como de otros factores.

Estaciones de Trabajo

Se pueden conectar a través de la placa de conexión de red y el cableado correspondiente. Los terminales “tontos” utilizados con las grandes computadoras y mini computadoras son también utilizadas en las redes, y no poseen capacidad propia de procesamiento.

Sin embargo las estaciones de trabajo son, generalmente, sistemas inteligentes. Los terminales inteligentes son los que se encargan de sus propias tareas de procesamiento, así que cuanto mayor y más rápido sea el equipo, mejor.

Los terminales tontos en cambio, utilizan el espacio de almacenamiento así como los recursos disponibles en el servidor.

Tarjetas de Conexión de Red (Interface Cards)

Permiten conectar el cableado entre servidores y estaciones de trabajo. En la actualidad existen numerosos tipos de placas que soportan distintos tipos de cables y topologías de red.

Las placas contienen los protocolos y órdenes necesarios para soportar el tipo de red al que está destinada. Muchas tienen memoria adicional para almacenar temporalmente los paquetes de datos enviados y recibidos, mejorando el rendimiento de la red.

La compatibilidad a nivel físico y lógico se convierte en una cuestión relevante cuando se considera el uso de cualquier placa de red. Hay que asegurarse que la placa pueda funcionar en la estación deseada, y de que existen programas controladores que permitan al sistema operativo enlazarlo con sus protocolos y características a nivel físico.

Cableado

Una vez que tenemos las estaciones de trabajo, el servidor y las placas de red, requerimos interconectar todo el conjunto. El tipo de cable utilizado depende de muchos factores, que se mencionarán a continuación:

Los tipos de cableado de red más populares son: par trenzado, cable coaxial y fibra óptica.
Además se pueden realizar conexiones a través de radio o microondas.

Cada tipo de cable o método tiene sus ventajas. y desventajas. Algunos son propensos a interferencias, mientras otros no pueden usarse por razones de seguridad.

La velocidad y longitud del tendido son otros factores a tener en cuenta el tipo de cable a utilizar.

Par Trenzado: Consiste en dos hilos de cobre trenzado, aislados de forma independiente y trenzados entre sí. El par está cubierto por una capa aislante externa. Entre sus principales ventajas tenemos:

- Es una tecnología bien estudiada
- No requiere una habilidad especial para instalación
- La instalación es rápida y fácil
- La emisión de señales al exterior es mínima.
- Ofrece alguna inmunidad frente a interferencias, modulación cruzada y corrosión.

Cable Coaxial: Se compone de un hilo conductor de cobre envuelto por una malla trenzada plana que hace las funciones de tierra. Entre el hilo conductor y la malla hay una capa gruesa de material aislante, y todo el conjunto está protegido por una cobertura externa.
El cable está disponible en dos espesores: grueso y fino.

El cable grueso soporta largas distancias, pero es más caro. El cable fino puede ser más práctico para conectar puntos cercanos.

El cable coaxial ofrece las siguientes ventajas:

- Soporta comunicaciones en banda ancha y en banda base (Banda base es la señal de una sola transmisión en un canal, banda ancha significa que lleva más de una

señal y cada una de ellas se transmite en diferentes canales, hasta su número máximo de canal).
- Es útil para varias señales, incluyendo voz, video y datos.
- Es una tecnología bien estudiada.

Conexión fibra óptica: Esta conexión es cara, pero permite transmitir la información a gran velocidad e impide la intervención de las líneas. Como la señal es transmitida a través de luz, existen muy pocas posibilidades de interferencias eléctricas o emisión de señal. El cable consta de dos núcleos ópticos, uno interno y otro externo, que refractan la luz de forma distinta. La fibra está encapsulada en un cable protector.

Ofrece las siguientes ventajas:
- Alta velocidad de transmisión
- No emite señales eléctricas o magnéticas, lo cual redunda en la seguridad
- Inmunidad frente a interferencias y modulación cruzada.
- Mayor economía que el cable coaxial en algunas instalaciones.
- Soporta mayores distancias

	Par Trenzado	**Par Trenzado Blindado**	**Coaxial**	**Fibra Óptica**
Tecnología ampliamente probada	Si	Si	Si	Si
Ancho de banda	Medio	Medio	Alto	Muy Alto
Hasta 1 Mhz	Si	Si	Si	Si
Hasta 10 Mhz	Si	Si	Si	Si
Hasta 20 Mhz	Si	Si	Si	Si
Hasta 100 Mhz	Si (*)	Si	Si	Si
27 Canales video	No	No	Si	Si
Canal Full Duplex	Si	Si	Si	Si
Distancias medias	100 m 65 Mhz	100 m 67 Mhz	500 (Ethernet)	2 km(Multi.) 100km(Mono.)
Inmunidad Electromagnética	Limitada	Media	Media	Alta
Seguridad	Baja	Baja	Media	Alta
Coste	Bajo	Medio	Medio	Alto

Redes Virtuales (vLANs)

Un nuevo concepto en Redes Computacionales

Muy pocos conceptos en el mundo de la interconexión actual son tan confusos como Redes Virtuales. Las Redes Virtuales son muy nuevas, y su uso a nivel mundial esta sólo comenzando. Muchos fabricantes, en el intento de tomar ventaja en el interés que se ha despertado en ellas, han tergiversado el concepto de lo que realmente es una Red Virtual. Existen diferentes maneras de implementar redes virtuales a través de productos conmutados (Switches), cada una con diferentes capacidades y limitaciones.

La cantidad de datos que es transportada mediante las redes de área local (LAN) ha crecido firme y rápidamente. Esto se debe básicamente al crecimiento de las aplicaciones existentes, hoy en día casi todas las personas tienen un Computador en su escritorio, y casi todos están conectados en red. Esto difiere mucho de la situación presentada hace unos pocos años, inclusive en redes extensas. Pero dos nuevas tendencias, en hardware y software, han acelerado e incrementado el uso de la red.

Los primeros PC's y Macintosh revolucionaron tanto la computación como la interconexión en redes. Actualmente, en vez de que cada usuario utilice un terminal "tonto", conectado a un "inteligente" minicomputador o mainframe, se tienen computadores de escritorio que comparten la inteligencia de los sistemas. Las redes anteriormente transportaban imágenes desde los computadores grandes hacia los terminales, y señales de mandatos o instrucciones desde los terminales hacia el Computador central. Esto cambio radicalmente con la estaciones de trabajo inteligentes. Ahora, existe necesidad de mover archivos, y los antiguos enlaces de 9.6 Kbps ya no son lo suficientemente rápidos. Ethernet y Token Ring fueron presionadas a prestar servicio para mover archivos de programas, archivos de impresión y compartición de recursos.

Pero esas antiguas estaciones de trabajo estaban limitadas en el procesamiento y manejo de información debido a su poca capacidad y rendimiento (capacidad de disco, memoria, MIPS, flujo de la red, etc.). Las computadoras de escritorio de hoy en día son 100 veces más poderosas. Como resultado, cada máquina es capaz de colocar una carga mayor en la red a la cual esta conectada.

Inclusive hasta después de la "Revolución de los PC's" que remplazó los terminales por computadores de escritorio, la naturaleza esencial de los datos permanecía sin cambio. Excepto por algunas aplicaciones científicas y de diseño, la gran mayoría de la información que se transportaba a través de la red era textual. Esto limitaba severamente la cantidad de información que necesitaba ser movida.

Las aplicaciones de hoy transfieren grandes cantidades de información gráfica. Las operaciones de manufactura utilizan gráficos para guiar a los trabajadores interactivamente en nuevos procesos. Las firmas de abogados y compañías de seguro están digitalizando grandes volúmenes de documentos, utilizando en muchos casos bitmaps para preservar documentos hechos a mano. Una amplia variedad de procesos médicos también usan imágenes para guiar a radiólogos, cirujanos y otros especialistas

en sus diagnósticos y procedimientos. Eventualmente, se incluye video a través de la LAN, aplicación que requiere aún anchos de banda mayores.

Los Switches LAN hacen posible transmitir cantidades mayores de data de lo que es posible transmitir con concentradores y Routers. Segmentos Ethernet y Token Ring pueden ser dedicados a dispositivos individuales, ó a pequeños grupos de dispositivos.

Pero los Switches LAN alcanzan sus niveles de alto performance utilizando procesos simplificados. Son básicamente Bridges, no ruteadores. Ellos conmutan o "switchean" a través de la segunda capa las direcciones de destino/origen ("MAC"), que es mucho más simple que rutear. Los Routers deben manejar una variedad de protocolos (selección de rutas, resolución de direcciones, transferencia de paquetes Internet, control de mensajes Internet, etc.) sólo para mover información en una sola "stack" de protocolo, como TCP/IP por ejemplo. Muchas redes combinan una variedad de stacks, y cada una de ellas necesitan un completo set de protocolos.

No hay nada nuevo en el uso de Bridges para construir redes locales. Las primeras LANs fueron creadas con Bridges sencillos. La diferencia radica en que hoy por hoy el hardware a avanzado significativamente, y enormes volúmenes de tramas pueden ser manejadas en un simple Switch.

Todas las redes "puenteadas", o interconectadas a través de Bridges, tienen una limitación básica: los Bridges, dado que ellos no participan en los protocolos de la capa tres (modelo OSI), la cual usa MAC broadcast (ó envío de paquetes a direcciones específicas), sino que envía paquetes a todos los puertos ó direcciones. Aunque el tráfico es aislado para los puertos específicos que envían y reciben esos paquetes, deben ser enviados a todas partes.

En la mayoría de las redes de mediano tamaño, este "flujo" no tiene mayor impacto en los otros tráficos, no hay más que unos cuantos "broadcasts" y las direcciones MAC se aprenden rápidamente, pero en una red bastante grande ó en una que exista niveles inusuales de broadcasts, es posible que este flujo impacte en el trafico punto a punto de las estaciones. Cuando esto pasa es importante mantener estos broadcast aislados en lo que se llama "Dominios de Broadcast".

Muchas de las redes locales en estos últimos diez años han estado basadas en concentradores y Routers. Las Estaciones de Trabajos, Servidores y otros dispositivos están conectados a los concentradores, los concentradores están interconectados con los Routers. En este tipo de Red Local los dominios de Broadcast se implementan de una forma muy simple y automática, cada concentrador (concentrador segmentado o anillo) es un dominio de broadcast.

Los Routers son esencialmente dispositivos para interconectar dominios de broadcast. Pero con redes basadas en Switches vamos a necesitar proveer esta función de otra forma.

Las Redes Virtuales sobrepasan limitaciones

Que es lo que hacen las redes virtuales (vLANs)?. Una red virtual es un dominio de broadcast. Como en un concentrador, todos los dispositivos en una red virtual ve todos los broadcast así como también todas las tramas con dirección de destino desconocida, sólo que los broadcast y tramas desconocidas son originadas dentro de esta red virtual.

Esto no es nada nuevo, es exactamente la misma técnica usada en las redes LAN basadas en concentradores y Routers. Con los concentradores y Routers, las tramas son regeneradas dentro del concentrador y enrutadas entre los concentradores. Con las redes virtuales, las tramas son swichadas (puenteadas: "bridged") dentro de una red virtual y enrutada entre redes virtuales. De manera tal que una red virtual no es más que una mejor y más flexible versión de las prácticas de Networking.

Lo nuevo de este tipo de dominio de broadcast es que no está restringido a que la misma localidad física de la red. Esto es importante, ya que es importante recordar que el Switching en mas simple que el enrutamiento, y por lo tanto más rápido. Para la extender el tráfico en la red local puede ser en base a switcheo entre dispositivos en vez de enrutamiento, y por lo tanto puede moverse mucho más rápidamente. Desafortunadamente para redes basadas en concentradores/enrutadores todos los dispositivos de red necesitan estar conectados y a veces todo el día y a menudo en diferentes partes del edificio, o en otro edificio en el Campus o en una red metropolitana reduciendo y desperdiciando ancho de banda. Las redes virtuales resuelven este problema. Un dominio de broadcast en una buena implementación de red virtual puede desplegarse a un edificio, Campus o ciudad. De tal manera que la necesidad de enrutamiento sea minimizada y el tráfico en la red se mueva mucho más rápidamente.

Beneficios adicionales que brindan las redes virtuales

Los Routers utilizan la capa tres del modelo OSI para mover tráfico en la red local (LAN). Cada capa contiene campos los cuales identifica el dominio de broadcast en el cual el destino puede ser encontrado (Dirección de red: 'Network Address'). Esas direcciones están asignadas por un administrador de red, y son generalmente registrada dentro de los archivos de configuración de las estaciones de red. En una red basada en concentradores y enrutadores la dirección de red identifica un segmento de red (Ethernet o Token Ring).

Desafortunadamente, si el dispositivo o estación de red es movida de un concentrador a otro, la dirección de red ya no es válida y alguien de grupo de redes debe ir a la estación de trabajo y corregir los archivos de configuración. Esto no es demasiado trabajo si pasa pocas veces, pero en una red de gran tamaño con un alto porcentaje de estaciones moviéndose cada año el proceso puede comer una gran cantidad de tiempo, y hasta que la actualización no se realice, la estación de trabajo no puede comunicarse.

Una característica de una buena red Virtual elimina este problema. Una estación de trabajo o servidor permanece en la misma red virtual automáticamente y no importa donde y en que parte de la red esté conectada(o).

Teóricamente, las direcciones de redes pueden ser asignadas en cualquier forma que el administrador seleccione. Desafortunadamente esa no es una práctica en muchas redes hoy en día. La razón es Internet. En orden de mezclar una red privada con Internet, es necesario restringir los números de red a aquellos los que hallan sido asignados por las autoridades que se encargan de administrar los números IP. El explosivo crecimiento de esta red mundial ha agotado un largo porcentaje de los posibles números de red, y por ende las organizaciones están restringidas de ellos.

Hasta la extensión de la implementacion de la próxima generación de IP, las redes virtuales puede ayudar bastante en reducir el desperdicio de números de redes clase B y C. Las redes virtuales hacen posible el uso limitado de direcciones de redes muy eficientemente. En una esquema concentrador/Router, cada segmento o anillo tiene su propio numero de subred, de tal forma que el Router puede mover tráfico entre cada una de ellas. En una red virtual cualquier numero de segmentos o anillos pueden ser combinados en una sola red virtual de tal forma que ninguna dirección sea desperdiciada.