Introducción

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los ordenadores (computadores), asi como a la puesta en orbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información.

Las redes en general, consisten en "compartir recursos", y uno de sus objetivo es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la

presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Los ordenadores pequeños tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario, con los datos guardados una o más máquinas que funcionan como servidor de archivo compartido.

A continuación se dará a conocer todo lo relacionado a redes de computadoras, definiciones, topologías, medios de comunicación, tipos de señales……

REDES DE COMPUTADORAS

QUE ES UNA RED:

Existen varias definiciones acerca de que es una red, algunas de las cuales son:

- Conjunto de operaciones centralizadas o distribuidas, con el fin de compartir recursos "hardware y software".
- Sistema de transmisión de datos que permite el intercambio de información entre ordenadores.
- Conjunto de nodos "computador" conectados entre sí.

En todo caso podemos decir que es un **Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras**.

Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otros ordenadores.

Una red tiene tres niveles de componentes:

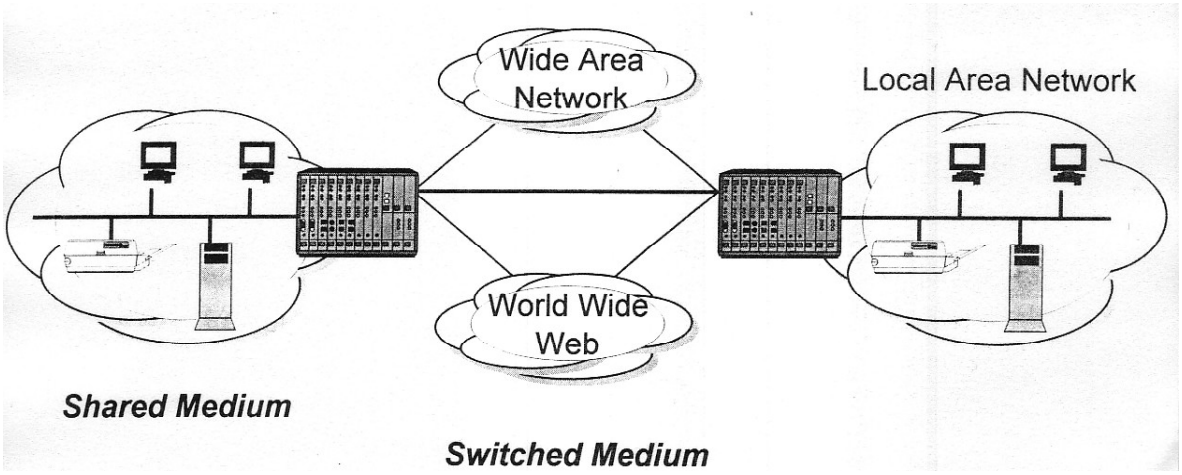
- Software de aplicaciones
- Software de red
- Hardware de red.

El software de aplicaciones: está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información (como archivos de bases de datos, de documentos, gráficos o vídeos) y recursos (como impresoras o unidades de disco). Un tipo de software de aplicaciones se denomina cliente-servidor. Las computadoras cliente envían peticiones de información o de uso de recursos a otras computadoras, llamadas servidores, que controlan el flujo de datos y la ejecución de las aplicaciones a través de la red. Otro tipo de software de aplicación se conoce como "de igual a igual" (peer to peer). En una red de este tipo, los ordenadores se envían entre sí mensajes y peticiones directamente sin utilizar un servidor como intermediario. Estas redes son más restringidas en sus capacidades de seguridad, auditoría y control, y normalmente se utilizan en ámbitos de trabajo con pocos ordenadores y en los que no se precisa un control tan estricto del uso de aplicaciones y privilegios para el acceso y modificación de datos; se utilizan, por ejemplo, en redes domésticas o en grupos de trabajo dentro de una red corporativa más amplia.

El software de red: consiste en programas informáticos que establecen protocolos, o normas, para que las computadoras se comuniquen entre sí. Estos

protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente.

El hardware de red: está formado por los componentes materiales que unen las computadoras. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables estándar o de fibra óptica, aunque también hay redes sin cables que realizan la transmisión por infrarrojos o por radiofrecuencias) y el adaptador de red, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios, o bits (unos y ceros), que pueden ser procesados por los circuitos electrónicos de los ordenadores.



Tipos de Redes

Existen varios tipos de redes, los cuales se clasifican de acuerdo a su tamaño y distribución lógica.

Clasificación según su tamaño

Las redes PAN (red de administración personal) son redes pequeñas, las cuales están conformadas por no más de 8 equipos, por ejemplo: café Internet.

CAN: Campus Area Network, Red de Area Campus. Una CAN es una colección de LANs dispersadas geográficamente dentro de un campus (universitario, oficinas de gobierno, maquilas o industrias) pertenecientes a una misma entidad en una área delimitada en kilometros. Una CAN utiliza comúnmente tecnologías tales como FDDI y Gigabit Ethernet para conectividad a través de medios de comunicación tales como fibra óptica y espectro disperso.

Redes de* Área *Local (LAN)

Una LAN (*Local Area Network*) es un sistema de interconexión de equipos de equipos informáticos basado en líneas de alta velocidad (decenas o cientos de megabits por segundo) y que suele abarcar, como mucho, un edificio.

Estas redes son las que todos conocemos, es decir, aquellas que se utilizan en nuestra empresa. Son redes pequeñas, entendiendo como pequeñas las redes de una oficina, de un edificio. Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto. Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce. Además, simplifica la administración de la red.

Suelen emplear tecnología de difusión mediante un cable sencillo (coaxial o UTP) al que están conectadas todas las máquinas. Operan a velocidades entre 10 y 100 Mbps.

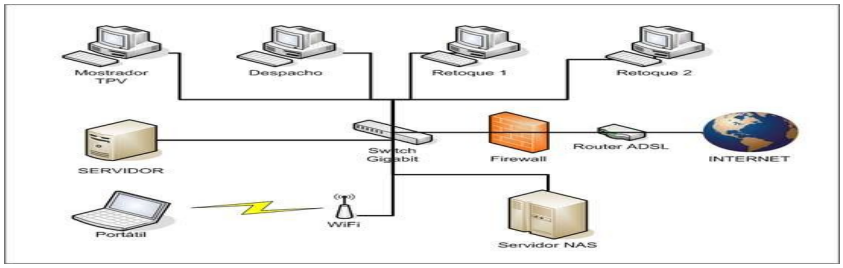
Características preponderantes:

- Los canales son propios de los usuarios o empresas.
- Los enlaces son líneas de alta velocidad.
- Las estaciones están cercas entre sí.
- Incrementan la eficiencia y productividad de los trabajos de oficinas al poder compartir información.
- Las tasas de error son menores que en las redes WAN.

La arquitectura permite compartir recursos.

Las principales tecnologías usadas en una LAN son: Ethernet, Token ring, ARCNET y FDDI .

Un caso típico de LAN es en la que existe un equipo servidor de LAN desde el que los usuarios cargan las aplicaciones que se ejecutarán en sus estaciones de trabajo. Los usuarios pueden también solicitar tareas de impresión y otros servicios que están disponibles mediante aplicaciones que se ejecutan en el servidor. Además pueden compartir ficheros con otros usuarios en el servidor. Los accesos a estos ficheros están controlados por un administrador de la LAN.



ELEMENTOS DE UNA RED DE AREA LOCAL

En una LAN existen elementos de *hardware y software* entre los cuales se pueden destacar:

- **El servidor:** es el elemento principal de procesamiento, contiene el sistema operativo de red y se encarga de administrar todos los procesos dentro de ella, controla también el acceso a los recursos comunes como son las impresoras y las unidades de almacenamiento.
- **Las estaciones de trabajo:** en ocasiones llamadas nodos, pueden ser computadoras personales o cualquier terminal conectada a la red. De esta manera trabaja con sus propios programas o aprovecha las aplicaciones existentes en el servidor.
- **El sistema operativo de red:** es el programa(*software)* que permite el control de la red y reside en el servidor. Ejemplos de estos sistemas operativos de red son: NetWare, LAN Manager, OS/2, LANtastic y Appletalk y Windows Server
- **Los protocolos de comunicación:** son un conjunto de normas que regulan la transmisión y recepción de datos dentro de la red.
- **La tarjeta de interface de red:** proporciona la conectividad de la terminal o usuario de la red física, ya que maneja los protocolos de comunicación de cada topología especifica

Redes de Área Metropolitana (MAN)

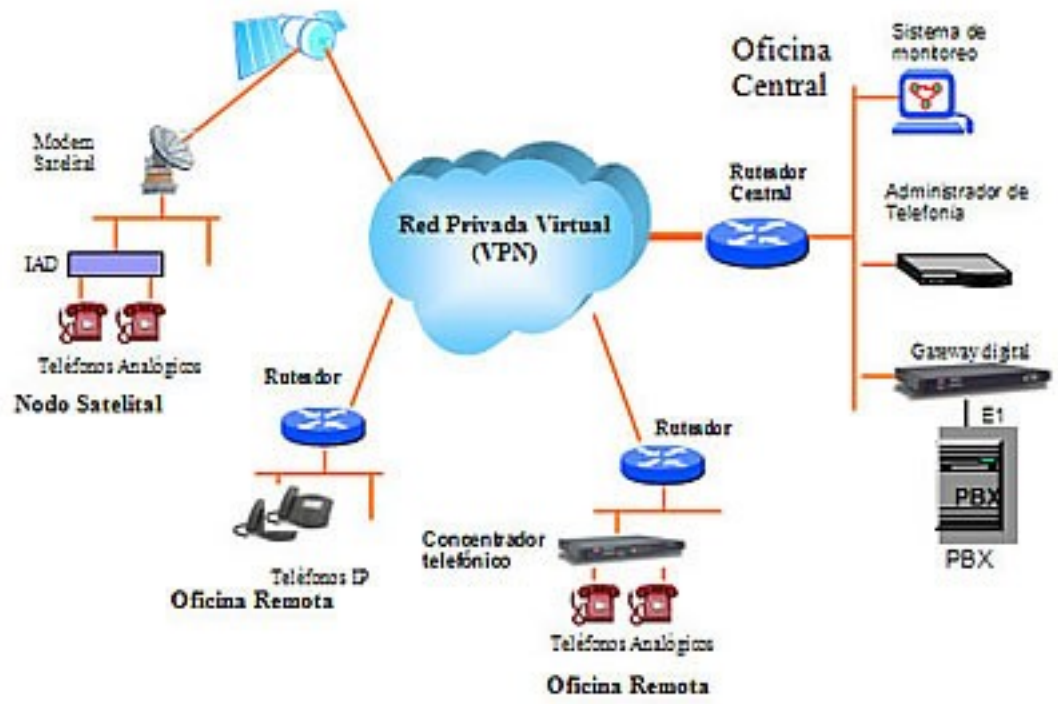
Una MAN (*Metropolitan Area Network*) es un sistema de interconexión de equipos informáticos distribuidos en una zona que abarca diversos edificios, por medios pertenecientes a la misma organización propietaria de los equipos. Este tipo de redes se utiliza normalmente para interconectar redes de área local.

Comprenden una ubicación geográfica determinada "ciudad, municipio", y su distancia de cobertura es mayor de 4 Kmts. Son redes con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos. Es básicamente una gran versión de LAN y usa una tecnología similar. Puede cubrir un grupo de oficinas de una misma corporación o ciudad, esta puede ser pública o privada. El mecanismo para la resolución de conflictos en la transmisión de datos que usan las MANs, es DQDB.

DQDB consiste en dos buses unidireccionales, en los cuales todas las estaciones están conectadas, cada bus tiene una cabecera y un fin. Cuando una computadora quiere transmitir a otra, si esta está ubicada a la izquierda usa el bus de arriba, caso contrario el de abajo.

Redes Punto a Punto. En una red punto a punto cada computadora puede actuar como cliente y como servidor. Las redes punto a punto hacen que el compartir datos y periféricos sea fácil para un pequeño grupo de gente. En una ambiente punto a punto, la seguridad es difícil, porque la administración no está centralizada.

Redes Basadas en servidor. Las redes basadas en servidor son mejores para compartir gran cantidad de recursos y datos. Un administrador supervisa la operación de la red, y vela que la seguridad sea mantenida. Este tipo de red puede tener uno o mas servidores, dependiendo del volumen de tráfico, número de periféricos etc. Por ejemplo, puede haber un servidor de impresión, un servidor de comunicaciones, y un servidor de base de datos, todos en una misma red.



Redes de Área Extensa (WAN)

Estas redes son punto a punto que interconectan países y continentes. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos. El alcance es una gran área geográfica, como por ejemplo: una ciudad o un continente. Está formada por una vasta cantidad de computadoras interconectadas (llamadas hosts), por medio de subredes de comunicación o subredes pequeñas, con el fin de ejecutar aplicaciones, programas, etc.

Una red de área extensa WAN es un sistema de interconexión de equipos informáticos geográficamente dispersos, incluso en continentes distintos. Las líneas utilizadas para realizar esta interconexión suelen ser parte de las redes públicas de transmisión de datos.

Las redes LAN comúnmente, se conectan a redes WAN, con el objetivo de tener acceso a mejores servicios, como por ejemplo a Internet. Las redes WAN son mucho más complejas, porque deben enrutar correctamente toda la información proveniente de las redes conectadas a ésta.

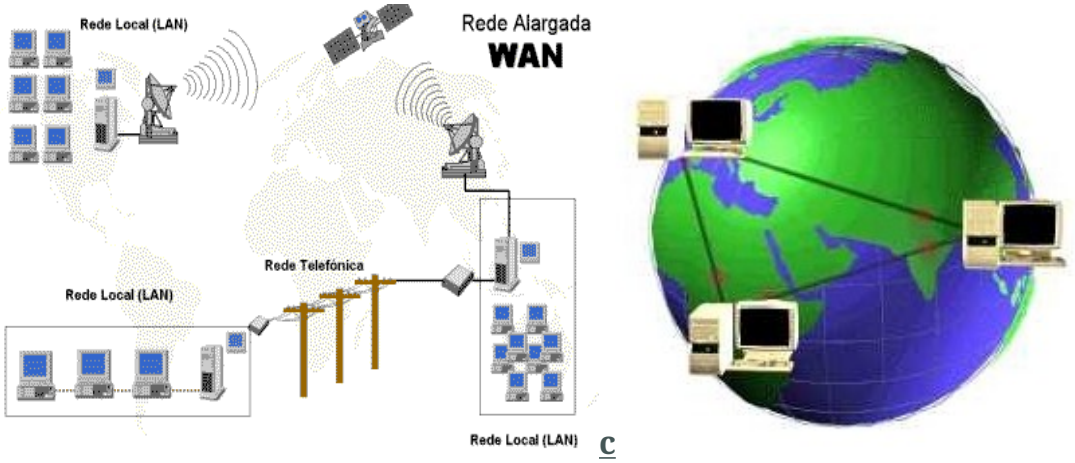
Una subred está formada por dos componentes:

Líneas de transmisión: quienes son las encargadas de llevar los bits entre los hosts.

Elementos interruptores (routers): son computadoras especializadas usadas por dos o más líneas de transmisión. Para que un paquete llegue de un router a otro, generalmente debe pasar por routers intermedios, cada uno de estos lo recibe por una línea de entrada, lo almacena y cuando una línea de salida está libre, lo retransmite.

INTERNET WORKS: Es una colección de redes interconectadas, cada una de ellas puede estar desallorrada sobre diferentes software y hardware. Una forma típica de Internet Works es un grupo de redes LANs conectadas con WANs. Si una subred le sumamos los host obtenemos una red.

El conjunto de redes mundiales es lo que conocemos como Internet.



c

Clasificación según su distribución lógica

Todos los ordenadores tienen un lado cliente y otro servidor: una máquina puede ser servidora de un determinado servicio pero cliente de otro servicio.

Servidor. Máquina que ofrece información o servicios al resto de los puestos de la red. La clase de información o servicios que ofrezca determina el tipo de servidor que es: servidor de impresión, de archivos, de páginas web, de correo, de usuarios, de IRC (charlas en Internet), de base de datos...

Cliente. Máquina que accede a la información de los servidores o utiliza sus servicios. Ejemplos: Cada vez que estamos viendo una página web (almacenada

en un servidor remoto) nos estamos comportando como clientes. También seremos clientes si utilizamos el servicio de impresión de un ordenador remoto en la red (el servidor que tiene la impresora conectada).

Todas estas redes deben de cumplir con las siguientes características:

- Confiabilidad "transportar datos".
- Transportabilidad "dispositivos".
- Gran procesamiento de información.

y de acuerdo estas, tienen diferentes usos, dependiendo de la necesidad del usuario, como son:

- Compañías - centralizar datos.
- Compartir recursos "periféricos, archivos, etc".
- Confiabilidad "transporte de datos".
- aumentar la disponibilidad de la información.
- Comunicación entre personal de las mismas áreas.
- Ahorro de dinero.
- Home Banking.

Aportes a la investigación "vídeo demanda,line T.V,Game Interactive".

Topologías de Red

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.

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.

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.

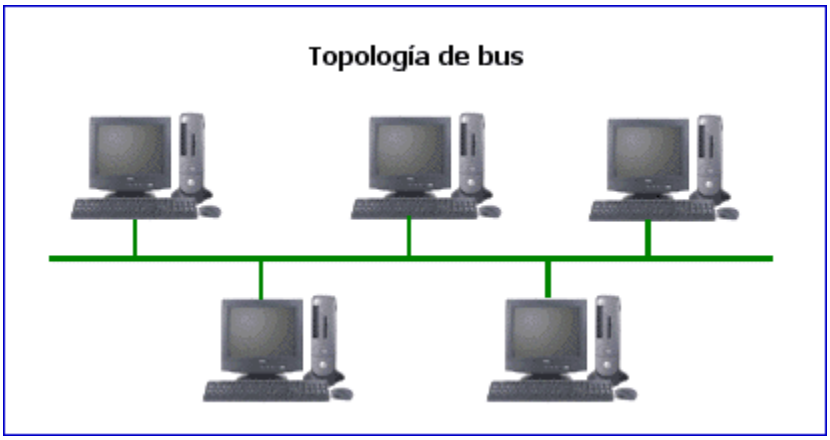
Si la red de malla está completamente conectada no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

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:

- Esta topología permite aumentar o disminuir el número de estaciones sin dificultad.
- La velocidad dependerá del flujo de información, cuantas mas estaciones intenten hacer uso de la red mas lento será el flujo de información.

Desventajas:

- Una falla en cualquier parte deja bloqueada a toda la red.

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.

Ventajas:

- Presenta buena flexibilidad para incrementar el numero de equipos conectados a la red.
- Si alguna de las computadoras falla el comportamiento de la red sigue sin problemas, sin embargo, si el problema se presenta en el controlador central se afecta toda la red.
- El diagnóstico de problemas es simple, debido a que todos los equipos están conectados a un controlador central.

Desventajas:

- No es adecuada para grandes instalaciones, debido a la cantidad de cable que deben agruparse en el controlador central.
- Esta configuración es rápida para las comunicaciones entre las estaciones o nodos y el controlador, pero las comunicaciones entre estaciones es lenta.

Red Inalámbrica Wi-Fi

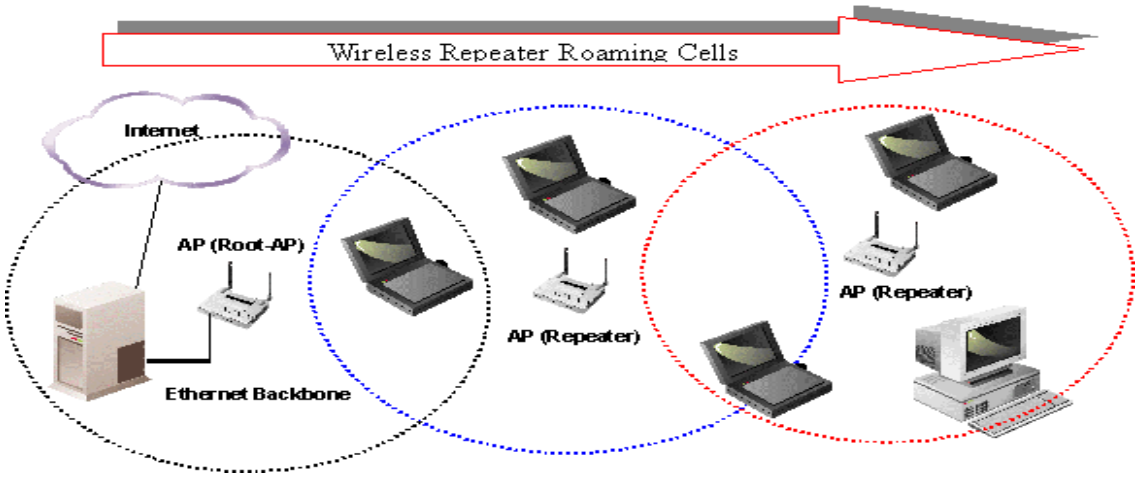
Wi-Fi es una marca de la *Wi-Fi Alliance* (anteriormente la *Wireless Ethernet Compatibility Alliance*), la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x.

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.



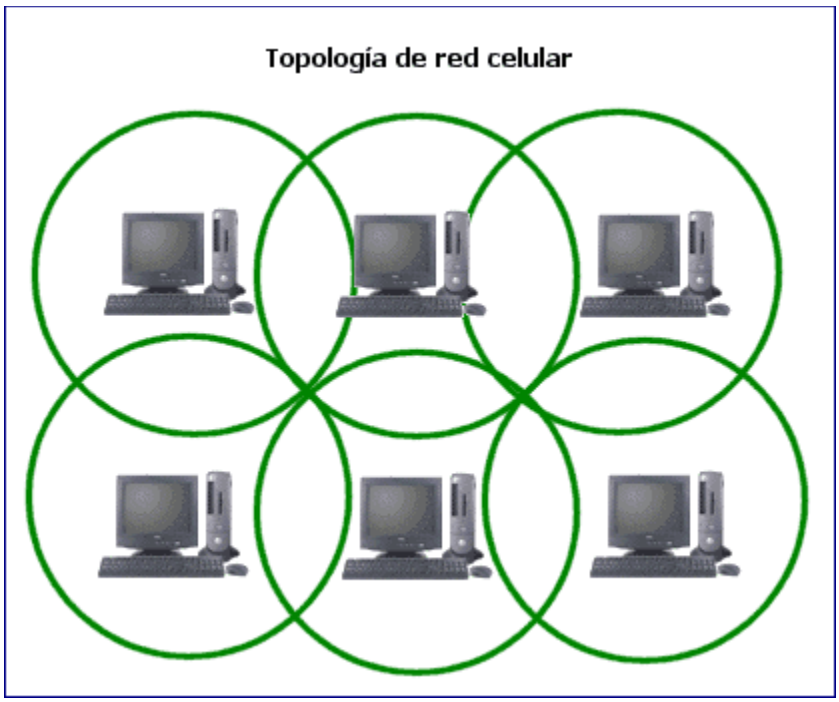
Topología Red celular:

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; silo 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 Alto. 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.

RED PRIVADA VIRTUAL

La **Red Privada Virtual** (**RPV**), en inglés *Virtual Private Network* (**VPN**), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Los ejemplos más comunes es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo esto utilizando la infraestructura de Internet

Por qué VPN

Las VPNs son una salida al costo que puede significar el pagar una conexión de alto costo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red.

Los datos son codificados o cifrados y recién enviados a través de la conexión, para de esa manera asegurar la información y el password que se esté enviando.

Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Mas aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red

La tecnología de túneles esta basado en estándares. Esta tecnología permite transmitir datos entre dos redes similares. A esto también se llama "encapsulación", es decir, a la tecnología que coloca algún tipo de paquetes dentro de otro protocolo (TCP). Aparte de todo esto, también se añade otra información necesaria para poder descifrar la información que se encuentra codificada. Estos paquetes llegan a su destino después de haber atravesado Internet, pero para verificar que ha llegado al destino correcto se realiza un proceso de autentificación.

Las VPNs son una gran solución a distintos problemas, pero solo en el campo de la economía de los usuarios porque por ejemplo en el caso de que se realice una conexión entre dos sedes de empresas, una en Japón y la otra en Perú, sería muy costoso el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más económica porque solo se hace uso de Internet que es un conjunto de redes conectadas entre si.

Pero observándolo desde el punto de vista de los usuarios particulares de Internet, como son los estudiantes o investigadores que utilizan el Internet como un medio de comunicación, de compartimiento de información, este tipo de redes perjudican este desarrollo, debido a varios factores como son, el consumo de ancho de banda, el consumo de direcciones IP, limitando así el normal desarrollo de la investigación a través de Internet.

Costo

La principal motivación del uso y difusión de esta tecnología es la reducción de los costos de comunicaciones directos, tanto en líneas *dial-up* como en vínculos WAN dedicados. Los costos se reducen drásticamente en estos casos:

En el caso de accesos remotos, llamadas locales a los ISP (Internet Service Provider) en vez de llamadas de larga distancia a los servidores de acceso remoto de la organización. O también mediante servicios de banda ancha.

En el caso de conexiones punto a punto, utilizando servicios de banda ancha para acceder a Internet, y desde Internet llegar al servidor VPN de la organización. Todo esto a un costo sensiblemente inferior al de los vínculos WAN dedicados.

Ancho de banda

Podemos encontrar otra motivación en el deseo de mejorar el ancho de banda utilizado en conexiones *dial-up*. Las conexiones VPN de banda ancha mejoran notablemente la capacidad del vínculo, pero los costos son más altos..

Zona desmilitarizada

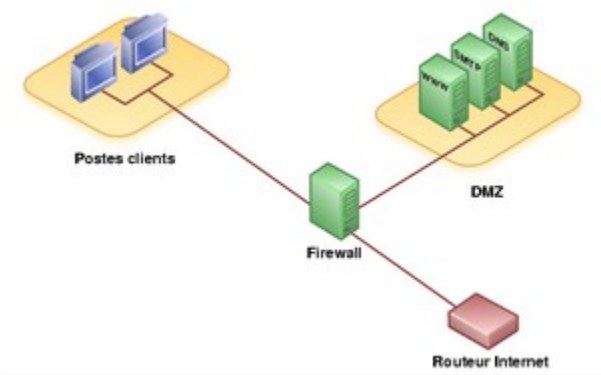


Diagrama de una red típica que usa una DMZ con un cortafuegos de tres patas (three-legged)

Una **DMZ** (del inglés *Demilitarized zone*) o Zona DesMilitarizada. En seguridad informática, una **zona desmilitarizada** (DMZ) o **red perimetral** es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

Una DMZ se crea a menudo a través **de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste - esta configuración se llama cortafuegos en trípode (three-legged firewall). Un planteamiento más seguro es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).**

Obsérvese que los router domésticos son llamados "DMZ host", aunque no es una definición correcta de zona desmilitarizada.

Origen del término

El término **zona desmilitarizada** es tomado de la franja de terreno neutral que separa a ambas Coreas, y que es una reminiscencia de la Guerra de Corea, aún vigente y en tregua desde 1953. Paradójicamente, a pesar de que esta zona desmilitarizada es terreno neutral, es una de las más peligrosas del planeta, y por ello da nombre al sistema **DMZ**.

Cortafuegos (informática)

Un **cortafuegos** (o ***firewall*** en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar al cortafuegos una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Tipos de cortafuegos

Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (nivel 4)

como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC.

Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (nivel 7) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder. Un cortafuegos a nivel 7 de tráfico HTTP es normalmente denominado Proxy y permite que los computadores de una organización entren a internet de una forma controlada.

Cortafuegos personal

Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

Ventajas de un cortafuegos

Protege de intrusiones. El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

Protección de información privada. Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

Optimización de acceso.- Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Limitaciones de un cortafuegos

Un cortafuegos no puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación.

El cortafuegos no puede proteger de las amenazas a que esta sometido por traidores o usuarios inconscientes. El cortafuegos no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y sustraigan éstas del edificio.

El cortafuegos no puede proteger contra los ataques de Ingeniería social

El cortafuegos no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real esta en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

El cortafuegos no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a Internet.

Políticas del cortafuegos

Hay dos políticas básicas en la configuración de un cortafuegos y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

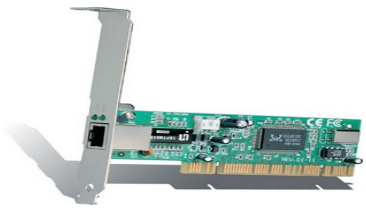
Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

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.

Un **repetidor** es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable.

El término repetidor se creó con la telegrafía y se refería a un dispositivo electromecánico utilizado para regenerar las señales telegráficas. El uso del término ha continuado en telefonía y transmisión de datos.

En telecomunicación el término repetidor tiene los siguientes significados normalizados:

1. Un dispositivo analógico que amplifica una señal de entrada, independientemente de su naturaleza (analógica o digital).
2. Un dispositivo digital que amplifica, conforma, retemporiza o lleva a cabo una combinación de cualquiera de estas funciones sobre una señal digital de entrada para su retransmisión.

En el modelo de referencia OSI el repetidor opera en el nivel físico.

En el caso de señales digitales el repetidor se suele denominar **regenerador** ya que, de hecho, la señal de salida es una señal *regenerada* a partir de la de entrada.

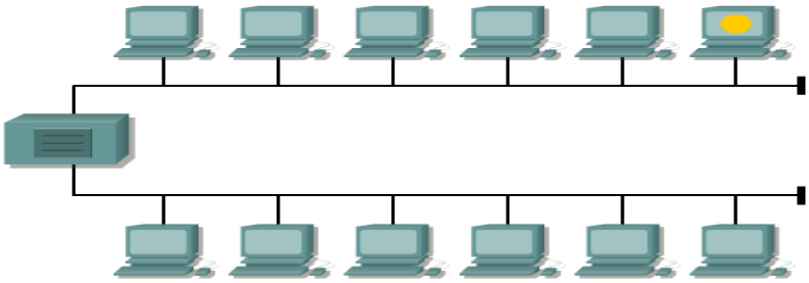
Los repetidores se utilizan a menudo en los cables transcontinentales y transoceánicos ya que la atenuación (pérdida de señal) en tales distancias sería completamente inaceptable sin ellos. Los repetidores se utilizan tanto en cables de cobre portadores de señales eléctricas como en cables de fibra óptica portadores de luz.

Los repetidores se utilizan también en los servicios de radiocomunicación. Un subgrupo de estos son los repetidores usados por los radioaficionados.

Asimismo, se utilizan repetidores en los enlaces de telecomunicación punto a punto mediante radioenlaces que funcionan en el rango de las microondas, como los utilizados para distribuir las señales de televisión entre los centros de producción y los distintos emisores o los utilizados en redes de telecomunicación para la transmisión de telefonía.

En comunicaciones ópticas el término repetidor se utiliza para describir un elemento del equipo que recibe una señal óptica, la convierte en eléctrica, la regenera y la retransmite de nuevo como señal óptica. Dado que estos dispositivos convierten la señal óptica en eléctrica y nuevamente en óptica, estos dispositivos se conocen a menudo como repetidores electroópticos.

Los repetidores telefónicos consistentes en un receptor (auricular) acoplado mecánicamente a un micrófono de carbón fueron utilizados antes de la invención de los amplificadores electrónicos dotados de tubos de vacío.



- **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.

Un **concentrador** es un dispositivo que permite centralizar el cableado de una red. También conocido con el nombre de *hub*.

Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma

que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central. Llamado también repetidor multipuerto, existen 3 clases.

Pasivo: No necesita energía eléctrica.

Activo: Necesita alimentación.

Inteligente: También llamados *smart hubs* son *hubs* activos que incluyen microprocesador.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.

Visto lo anterior podemos sacar las siguientes conclusiones:

1. El concentrador envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el concentrador envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.
2. Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea con otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.
3. Un concentrador funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el concentrador no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 megabit/segundo le trasmitiera a otro de 10 megabit/segundo algo se perdería del mensaje. En el caso del ADSL los routers suelen funcionar a 10 megabit/segundo, si lo conectamos a nuestra red casera, toda la red funcionará a 10 megabit/segundo, aunque nuestras tarjetas sean 10/100 megabit/segundo .
4. Un concentrador es un dispositivo simple, esto influye en dos características. El precio es barato. Un concentrador casi no añade ningún retardo a los mensajes.

Los concentradores fueron muy populares hasta que se abarataron los switch que tienen una función similar pero proporcionan más seguridad contra programas como los sniffer. La disponibilidad de switches ethernet de

bajo precio ha dejado obsoletos, pero aún se pueden encontrar en instalaciones antiguas y en aplicaciones especializadas.

- **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.

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

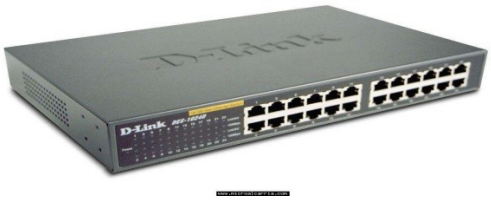
Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red.

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

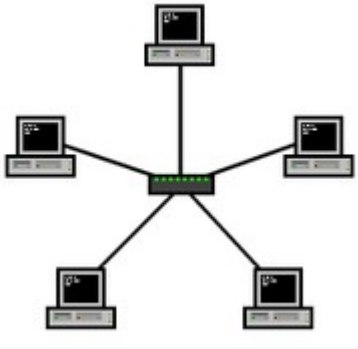
La principal diferencia entre un bridge y un hub es que el segundo pasa cualquier trama con cualquier destino para todos los otros nodos conectados, en cambio el primero sólo pasa las tramas pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico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

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

- **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.



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



Un conmutador en el centro de una red en estrella.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un *filtro* en la red, mejoran el rendimiento y la seguridad de las LANs (*Local Area Network*- Red de Área Local).

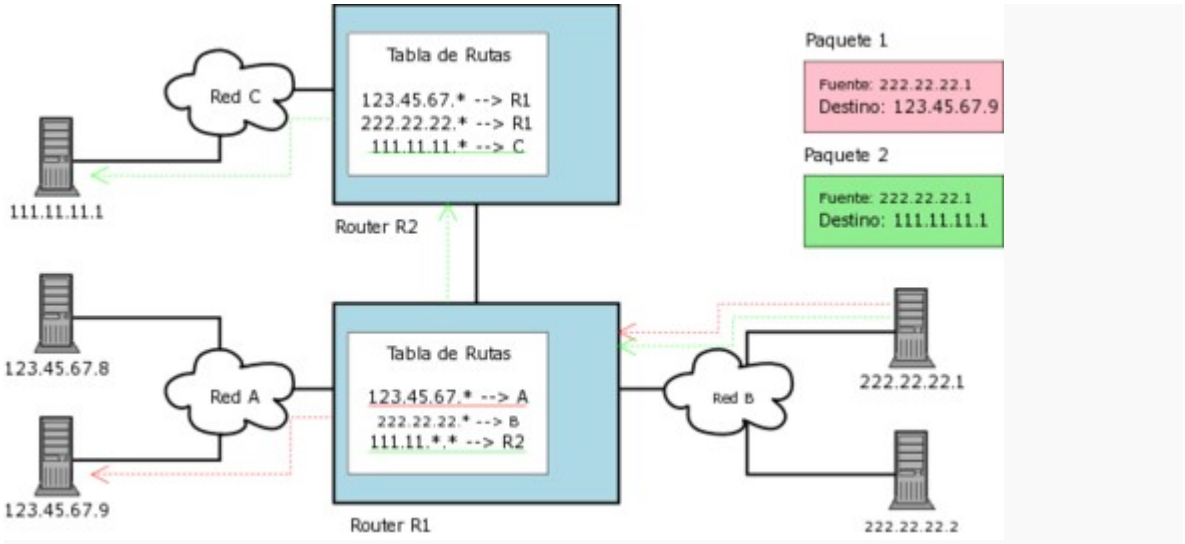
Cual es la diferencia entre un "Switch" y un "Hub" ?

El "Hub" básicamente extiende la funcionalidad de la red (LAN) para que el cableado pueda ser extendido a mayor distancia, es por esto que un "Hub" puede ser considerado como una repetidora. El problema es que el "Hub" transmite estos *"Broadcasts"* a todos los puertos que contenga, esto es, si el "Hub" contiene 8 puertos ("ports"), todas las computadoras que estén

conectadas al "Hub" recibirán la misma información, y como se mencionó anteriormente , en ocasiones resulta innecesario y excesivo
Un "Switch" es considerado un "Hub" inteligente, cuando es inicializado el "Switch", éste empieza a reconocer las direcciones "MAC" que generalmente son enviadas por cada puerto, en otras palabras, cuando llega información al "Switch" éste tiene mayor conocimiento sobre que puerto de salida es el *más apropiado*, y por lo tanto ahorra una carga ("bandwidth") a los demás puertos del "Switch", esta es una de la principales razones por la cuales en Redes por donde viaja Vídeo o CAD, se procura utilizar "Switches" para de esta forma garantizar que el cable no sea sobrecargado con información que eventualmente sería descartada por las computadoras finales,en el proceso, otorgando el mayor ancho de banda ("bandwidth") posible a los Vídeos o aplicaciones CAD.

- **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.

En español, enrutador o encaminador. Dispositivo de **hardware** para interconexión de redes de las computadoras que opera en la capa tres (nivel de red)



En el ejemplo del diagrama, se muestran 3 redes IP interconectadas por 2 routers. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1 A través de sus tablas de enrutamiento configurados previamente, los routers pasan los paquetes para la red o router con el rango de direcciones que corresponde al destino del paquete. Nota: el contenido de las tablas de rutas está simplificado por motivos didácticos. En realidad se utilizan máscaras de red para definir las subredes interconectadas.

Balance de carga

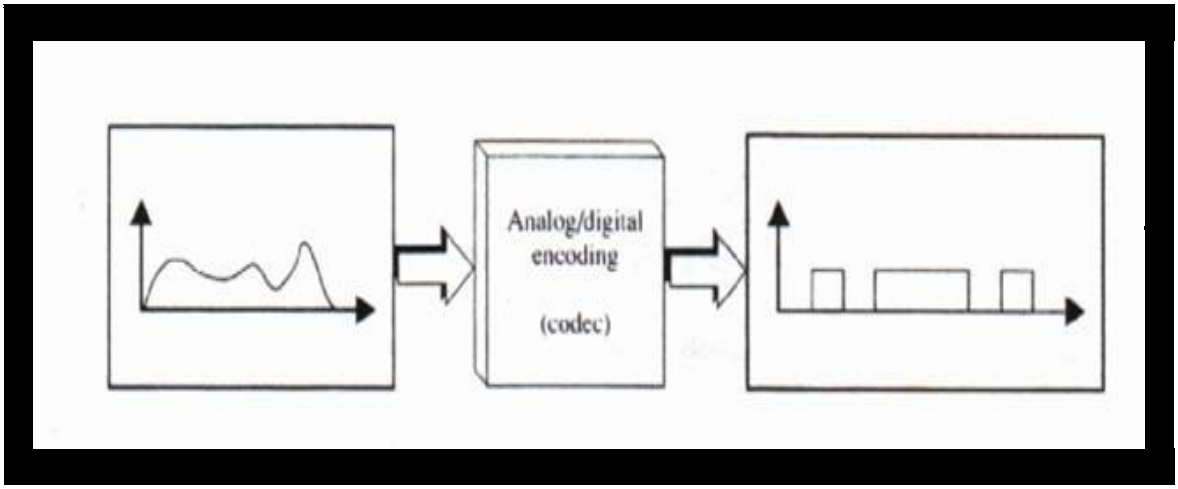
El balance o balanceo de carga es un concepto usado en **informática** que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado a los sistemas de **multiprocesamiento**, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles. ?? El *balance de carga* se mantiene gracias a un *algoritmo* que divide de la manera más equitativa posible el trabajo, para evitar los así denominados *cuellos de botella* que es el objetivo del multiprocesamiento

TIPOS DE SEÑALES

Señal Analógica

Es una forma de onda continua que pasa a tráves de un medio de

comunicaciones; se utiliza para comunicaciones de voz.



Señal digital

Es una forma de onda discreta que transmite datos codificados en estados discretos como bits 1 y 0 , los cuales se representan como el encendido y apagado de los pulsos eléctricos : se usa para comunicaciones de datos.

Modos De Transmision :

Los distintos tipos de transmisión de un canal de comunicaciones pueden ser de tres clases: 1. Símplex. 2. Semidúplex. 3. Dúplex.

Método Símplex.

Es aquel en el que una estación siempre actúa como fuente y la otra siempre como colector. este método permite la transmisión de información en un único sentido.

Método Semidúplex.

Es aquel en el que una estación A en un momento de tiempo, actúa como fuente y otra estación corresponsal B actúa como colector, y en el momento siguiente, la estación B actuará como fuente y la A como colector. Permite la transmisión en ambas direcciones, aunque en momentos diferentes. Un ejemplo es la conversación entre dos radioaficionados, pero donde uno espera que el otro termine de hablar para continuar el diálogo.

Método Dúplex.

En el que dos estaciones A y B, actúan como fuente y colector, transmitiendo y recibiendo información simultáneamente. permite la transmisión en ambas direcciones y de forma simultánea. Por ejemplo una conversación telefónica.

Medios de Transmisión

Con el pasar del tiempo, algunos tipos de cables se han quedado atrás por diversos factores tales como costos de producción, precio al consumidor, eficiencia, comodidad de manejo e instalación entre otros. No necesariamente todos estos tipos de cables se han vuelto obsoletos, tal es el caso del cable coaxial, el cual no se estandarizó la categoría a la que pertenece sin embargo posee un ancho de banda de 100MHz, y que por su geometría posee mayor capacidad de aislamiento que el mismo UTP, sin embargo la tecnología decidió darle a este último mayor énfasis pues es más barato y manipulable, aparte que la conectorización del UTP es mucho más simple que la del coaxial.

El cable coaxial 10Base 2 y 5 se utilizaba anteriormente en los enlaces de "columna vertebral" en las redes, sin embargo llegó a ser desplazado por la fibra óptica, la cual por estar compuesta netamente por materiales dieléctricos no presenta problemas de EMI e RFI. Esto no quiere decir que la fibra óptica como tal no se vea afectada por ningún tipo de ruido, ya que por ejemplo podemos citar el Ruido Láser, sin embargo y por la complejidad de dicho tema, será analizado en otra ocasión.

Por otro lado tenemos el cable Token Ring tipo 1, o cable STP, éste por su parte era un cable forrado, grueso, que a su vez fue el estándar inicial de IBM, es bastante inmune al ruido ya que en sus forros posee unas mallas y blindajes metálicos.

Aún en la actualidad existen redes que trabajan bajo esta arquitectura. En sí, este es un cable muy difícil de manipular por sus características físicas, y de un alto costo económico. Por sus características de aislamiento representa una opción bastante viable para ambientes industriales, y es catalogado e categoría 4.

Hasta hace poco tiempo se tenía la problemática de que no existía un cable de la línea del UTP capaz de trabajar con alto rendimiento en ambientes industriales, tal y como si lo podía hacer el Token Ring tipo 1 (STP), a menos que el mismo UTP

se colocara dentro de tuberías metálicas. En respuesta a esta necesidad surge el ScTP que posee las mismas características de protección contra el ruido que el STP (malla metálica y forro de aluminio), al igual que sus conectores y módulos debidamente blindados. Este tipo de cable pertenece a la categoría 5 y es de un costo económico bastante bajo en comparación con el STP.

Pares de Cable o Cable de par Trenzado

Constituyen el modo más simple y económico de todos los medios de transmisión. Sin embargo, presentan una serie de inconvenientes. En todo conductor, la resistencia eléctrica aumenta al disminuir la sección del conductor, por lo que hay que llegar a un compromiso entre volumen y peso, y la resistencia eléctrica del cable. Esta última está afectada directamente por la longitud máxima. Cuando se sobrepasan ciertas longitudes hay que recurrir al uso de repetidores para restablecer el nivel eléctrico de la señal.

Tanto la transmisión como la recepción utilizan un par de conductores que, si no están apantallados, son muy sensibles a interferencias y diafonías producidas por la inducción electromagnética de unos conductores en otros (motivo por el que en ocasiones percibimos conversaciones teléfonicas ajenas a nuestro teléfono). Un cable apantallado es aquel que está protegido de las interferencias eléctricas externas, normalmente a través de un conductor eléctrico externo al cable, por ejemplo una malla.

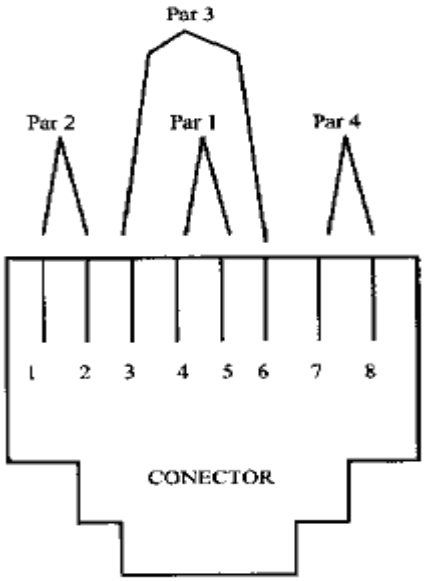
Un modo de subsanar estas interferencias consiste en trenzar los pares de modo que las intensidades de transmisión y recepción anulen las perturbaciones electromagnéticas sobre otros conductores próximos. Esta es la razón por la que este tipo de cables se llaman de pares trenzados. Con este tipo de cables es posible alcanzar velocidades de transmisión comprendidas entre 2 Mbps y 100 Mbps en el caso de señales digitales.

Es el cable más utilizado en telefonía y télex. Existen dos tipos fundamentalmente:

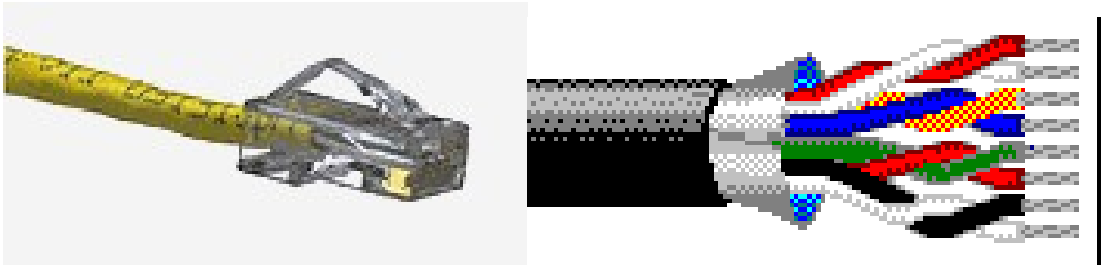
- *Cable UTP***.** UTP son las siglas de *Unshielded Twisted Pair*. Es un cable de pares trenzados y sin recubrimiento metálico externo, de modo que es sensible a las interferencias; sin embargo, al estar trenzado compensa las inducciones electromagnéticas producidas por las líneas del mismo cable. Es importante guardar la numeración de los pares, ya que de lo contrario el efecto del trenzado no será eficaz, disminuyendo sensiblemente, o incluso impidiendo, la capacidad de transmisión. Es un cable barato, flexible y sencillo de instalar. La impedancia de un cable UTP es de 100 ohmios. En la figura siguiente se pueden observar los distintos pares de un cable UTP.

- *Cable STP***.** STP son las siglas de *Shielded Twisted Pair*. Este cable es semejante al UTP pero se le añade un recubrimiento metálico para evitar las

interferencias externas. Por tanto, es un cable más protegido, pero menos flexible que el primero. el sistema de trenzado es idéntico al del cable UTP. La resistencia de un cable STP es de 150 ohmios.



Estos cables de pares tienen aplicación en muchos campos. El cable de cuatro pares está siendo utilizado como la forma de cableado general en muchas empresas, como conductores para la transmisión telefónica de voz, transporte de datos, etc. RDSI utiliza también este medio de transmisión.



Estructura de cables para un cable UTP en una red Ethernet o para una conexión RDSI, dependiendo de la elección de los pares

En los cable de pares hay que distinguir dos clasificaciones:

1. **La Categorías**: Cada categoría especifica unas características eléctricas para el cable: atenuación, capacidad de la línea e impedancia.
2. **Las Clases**: Cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de estas características.

CLASES	Clase A	Clase B	Clase C	Clase D
Ancho de banda	100 kHz	1 MHz	20 MHz	100 MHz
En categoría 3	2 km	500 m	100 m	no existe
En categoría 4	3 km	600 m	150 m	no existe
En categoría 5	3 km	700 m	160 m	100 m

Características de longitudes posibles y anchos de banda para las clases y categorías de pares trenzados.

Dado que el UTP de categoría 5 es barato y fácil de instalar, se está incrementando su utilización en las instalaciones de redes de área local con topología en estrella, mediante el uso de conmutadores y concentradores. Las aplicaciones típicas de la categoría 3 son transmisiones de datos hasta 10 Mbps (por ejemplo, la especificación 10baseT); para la categoría 4, 16 Mbps, y para la categoría 5 (por ejemplo, la especificación 100BaseT), 100 Mbps. En concreto, este cable UTP de categoría 5 viene especificado por las características de la Tabla siguiente (especificaciones TSB-36) referidas a un cable estándar de 100 metros de longitud.

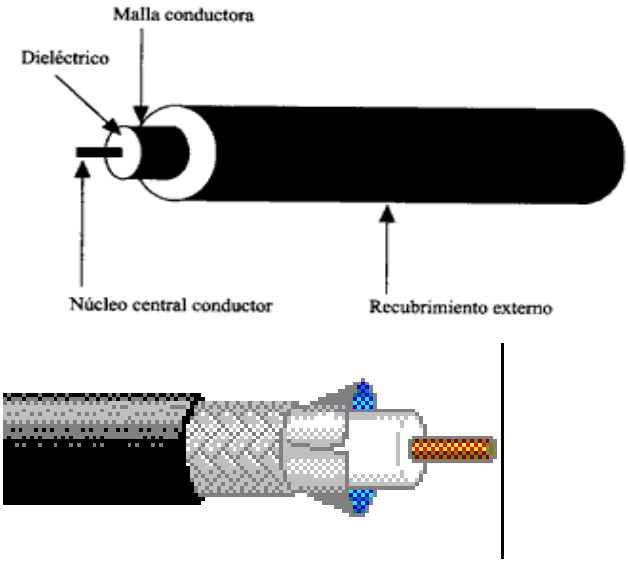
Velocidad de transmisión de datos	Nivel de atenuación
4 Mbps	13 dB
10 Mbps	20 dB
16 Mbps	25 dB
100 Mbps	67 dB

Nivel de atenuación permitido según la velocidad de transmisión para un cable UTP.

Es posible utilizar la lógica de las redes FDDI (*Fiber Distributed Data Interface*) utilizando como soporte cable UTP de categoría 5 en la clase D, ya que la velocidad de transmisión es de 100 Mbps como en FDDI. Por esta razón se le suele llamar TPDDI, *Twisted Pair Distributed Data Interface.*

El Cable Coaxial

Presenta propiedades mucho más favorables frente a interferencias y a la longitud de la línea de datos, de modo que el ancho de banda puede ser mayor. Esto permite una mayor concentración de las transmisiones analógicas o más capacidad de las transmisiones digitales.



Sección de un cable coaxial.

Su estructura es la de un cable formado por un conductor central macizo o compuesto por múltiples fibras al que rodea un aislante dieléctrico de mayor diámetro Figura siguiente. Una malla exterior aisla de interferencias al conductor central. Por último, utiliza un material aislante para recubrir y proteger todo el conjunto. Presenta condiciones eléctricas más favorables. En redes de área local se utilizan dos tipos de cable coaxial: fino y grueso.

Es capaz de llegar a anchos de banda comprendidos entre los 80 Mhz y los 400 Mhz (dependiendo de si es fino o grueso). Esto quiere decir que en transmisión de señal analógica seríamos capaces de tener, como mínimo. del orden de 10.000 circuitos de voz.

Originalmente fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en Declive

.

Su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos.

TIPOS DE CABLE COAXIAL

THICK (grueso). Este cable se conoce normalmente como "**cable amarillo**", fue el cable coaxial utilizado en la mayoría de las redes. Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Este cable es empleado en las redes de área local conformando con la norma 10 Base 2.

THIN (fino). Este cable se empezó a utilizar para reducir el coste de cableado de la redes. Su limitación está en la distancia máxima que puede alcanzar un tramo de red sin regeneración de la señal. Sin embargo el cable es mucho más barato y fino que el *thick* y, por lo tanto, solventa algunas de las desventajas del cable grueso.

Este cable es empleado en las redes de área local conformando con la norma 10 Base 5.

El cable coaxial en general solo se puede utilizar en conexiones Punto a Punto o dentro de los racks.

MODELOS DE CABLE COAXIAL

· Cable estándar Ethernet, de tipo especial conforme a las normas IEEE 802.3 10 BASE 5. Se denomina también cable coaxial "grueso", y tiene una impedancia de 50 Ohmios. El conector que utiliza es del tipo "N".

· Cable coaxial Ethernet delgado, denominado también RG 58, con una impedancia de 50 Ohmios. El conector utilizado es del tipo BNC.

· Cable coaxial del tipo RG 62, con una impedancia de 93 Ohmios. Es el cable estándar utilizado en la gama de equipos 3270 de IBM, y tambien en la red ARCNET. Usa un conector BNC.

· Cable coaxial del tipo RG 59, con una impedancia de 75 Ohmios. Este tipo de cable lo utiliza, en versión doble, la red WANGNET, y dispone de conectores DNC y TNC.

También están los llamados "TWINAXIAL" que en realidad son 2 hilos de cobre por un solo conducto.

Fibra Optica

La fibra óptica permite la transmisión de señales luminosas y es insensible a interferencias electromagnéticas externas. Cuando la señal supera frecuencias de 10^{10} Hz hablamos de frecuencias ópticas. Los medios conductores metálicos son incapaces de soportar estas frecuencias tan elevadas y son necesarios medios de transmisión ópticos.
Por otra parte, la luz ambiental es una mezcla de señales de muchas frecuencias distintas, por lo que no es una buena fuente para ser utilizada en las transmisión de datos. Son necesarias fuentes especializadas:

- Fuentes láser. a partir de la década de los sesenta se descubre el láser, una fuente luminosa de alta coherencia, es decir, que produce luz de una única frecuencia y toda la emisión se produce en fase.
- Diodos láser. es una fuente semiconductora de emisión de láser de bajo precio.

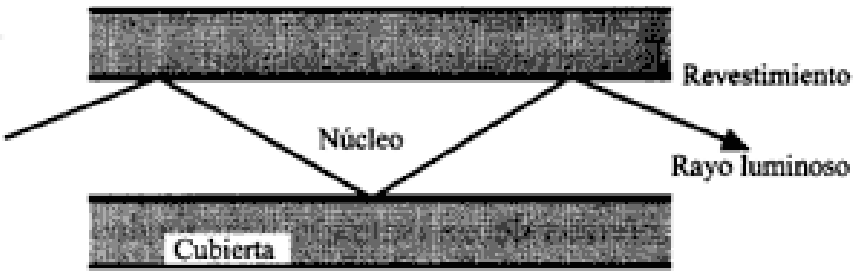
- Diodos LED. Son semiconductores que producen luz cuando son excitados eléctricamente.

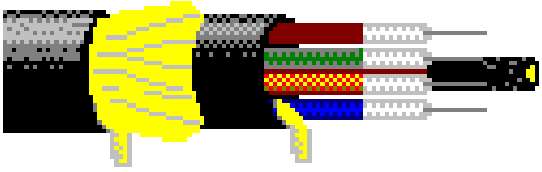
La composión del cable de fibra óptica consta de un núcleo, un revestimiento y una cubierta externa protectora Figura siguiente. El núcleo es el conductor de la señal luminosa y su atenuación es despreciable. La señal es conducida por el interior de éste núcleo fibroso, sin poder escapar de él debido a las reflexiones internas y totales que se producen, impidiendo tanto el escape de energía hacia el exterio como la adicción de nuevas señales externas.

Actualmente se utilizan tres tipos de fibras ópticas para la transmisión de datos:

1. Fibra monomodo. Permite la transmisión de señales con ancho de banda hasta 2 GHz.
2. Fibra multimodo de índice gradual. Permite transmisiones de hasta 500 MHz.
3. Fibra multimodo de índice escalonado. Permite transmisiones de hasta 35 MHz.

Se han llegado a efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra, debido a su gran ancho de banda. Otra ventaja es la gran fiabilidad, su tasa de error es mínima. Su peso y diámetro la hacen ideal frente a cables de pares o coaxiales. Normalmente se encuentra instalada en grupos, en forma de mangueras, con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas.
Su principal incoveniente es la dificultad de realizar una buena conexión de distintas fibras con el fin de evitar reflexiones de la señal, así como su fragilidad.





Sección longitudinal de una fibra óptica.

Topología de Cables

Cable RG-58, Coaxial ó BNC

Estas formas de denominación se refieren a la misma tecnología de cableado. La primera hace referencia a la normativa del cable propiamente dicho, la segunda a su nombre y la tercera al nombre técnico que utilizan los conectores usados en este tipo de cableado.

Es un cable compuesto, de fuera a dentro, de una funda plástica, habitualmente de color negro, tras la cual se encuentra una malla entrelazada de hilos de cobre que cubren a una protección plástica con un hilo de cobre central.

Su implantación es bastante sencilla, sólo necesitaremos un cable que una los distintos equipos de una red, denominándose topología en bus lineal.

La distancia máxima utilizada en este tipo de cable es de 150 metros y 15 nodos (normativa estándar) ó 300m. y 30 nodos (normativa extendida). Entendiendo por nodo un corte realizado a dicho cable.

Cable RJ-45, Par Trenzado ó UTP

Estas formas de denominación se refieren a la misma tecnología de cableado. La primera hace referencia a la normativa del cable propiamente dicho, la segunda a su nombre y la tercera al nombre técnico que utilizan los conectores usados en este tipo de cableado.

Cuando nos referimos a este cable y utilizamos "el apellido" Tipo 5, nos referimos a que dicho cable se compone de 8 hilos conductores de cobre. Existen otros Tipos, como el 3 compuesto de 4 hilos ó el Tipo 1, pero que con la incorporación de nuevas tecnologías han caído en desuso.

Es un cable compuesto, de fuera a dentro, de una funda de plástico, habitualmente de color gris, tras la cual se encuentran 8 hilos de cobre cubiertos de una funda plástica y entrelazados en pares dando dos vueltas y media por pulgada. (De ahí su nombre Par Trenzado).

Para la utilización de este tipo de cableado es necesario instalar un concentrador para que haga la función de repartidor de señales, por eso se denomina topología en estrella.

La distancia máxima utilizada en este tipo de cable es de 105 metros entre la tarjeta de red y el concentrador.

Cable STP, FTP ó RJ-49

No es mas que una derivación de la anterior estructura de cableado, incluyendo una platina de metal de separación entre la capa plástica de protección del cable y de los hilos.

No es ni mejor ni peor que el anterior cable, simplemente su utilización será recomendada en determinados entornos en detrimento del RJ-45 ó UTP.

Cable de Fibra Óptica

Cada vez mas utilizado este tipo de cableado, por su flexibilidad, manejabilidad y distancias que soporta. Se compone de dos hilos conductores, transmisión y recepción, de señal óptica. La distancia máxima que soporta es de 2 Km.

Todavía es una filosofía de cableado cara y costosa de grimpar, pues un error en el grimpaje del conector y habría que tirar el latiguillo de cable, pero se va imponiendo con mayor fuerza.

Conectores

Conector BNC

Es el conector utilizado cuando se utiliza cable coaxial. Como ya hemos dicho, la malla de cable coaxial y el hilo central están separados, así que es muy importante que a la hora de grimpar este conector al cable dichos hilos se hallen separados.

Conector RJ-45

Se utiliza con el cable UTP. Está compuesto de 8 vías con 8 "muelas" que a la hora de grimpar el conector pincharán el cable y harán posible la transmisión de datos. Por eso será muy importante que todas la muelas queden al ras del conector.

Conector RJ-49

Igual que el anterior, pero recubierto con una platina metálica para que haga contacto con la que recubre el cable STP.

Estándares de Telecomunicaciones

El Instituto Americano Nacional de Estándares, la Asociación de Industrias de Telecomunicaciones y la Asociación de Industrias Electrónicas (ANSI/TIA/EIA) publican conjuntamente estándares para la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico.

Cinco de éstos estándares de ANSI/TIA/EIA definen cableado de Telecomunicaciones en edificios.

Cada estándar cubre un parte específica del cableado del edificio. Los estándares establecen el cable, hardware, equipo, diseño y prácticas de instalación requeridas.

Cada estándar ANSI/TIA/EIA menciona estándares relacionados y otros materiales de referencia.

La mayoría de los estándares incluyen secciones que definen términos importantes, acrónimos y símbolos.

Documentos adicionales:

ANSI/TIA/EIA TSB-36.
Especificaciones Adicionales para Cables de Par Trenzado sin Blindaje. Esta especificación se define por aparte de ANSI/TIA/EIA-568 pero se incluye en el ANSI/TIA/EIA-568A

ANSI/TIA/EIA TSB-40.
Especificaciones Adicionales de Transmisión para Hardware de Conexión de Cables de Par Trenzado sin Blindaje. Esta especificación se define por aparte de ANSI/TIA/EIA-568 pero se incluye en ANSI/TIA/EIA-568A.

ANSI/TIA/EIA TSB-67.
Especificación para la Prueba en el Campo del Rendimiento de Transmisión de Sistemas de Cableado de Par Trenzado sin Blindaje

ANSI/TIA/EIA TSB-72. Guía para el Cableado de Fibra Optica Centralizada

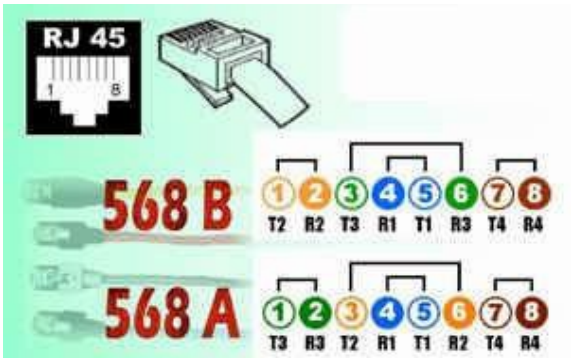
ANSI/TIA/EIA-568-A
La norma ANSI/TIA/EIA-568-A publicada en Octubre de 1995 amplio el uso de Cable de Par Trenzado (UTP) y elementos de conexión para aplicaciones en Redes de Area Local (LAN) de alto rendimiento.

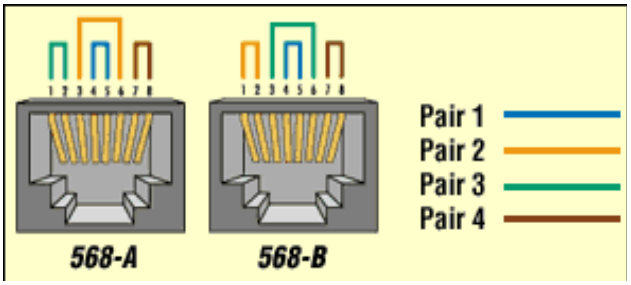
Para un cable UTP de 4 pares, el color primario es siempre blanco y los colores secundarios son azul, naranja, verde y marrón.

La secuencia es definida como el orden en el cual los pares que entran son conectados en los pines del conector modular.

Cada par es designado como un conductor de "punta" (tip) y un conductor de "llamada" (ring). El par número 1 es por lo tanto el designado como **T1** y **R1**.

La secuencia define que pines del encapsulado modular son definidos como T1, R1, T2, R2, etc





La secuencia EIA **568B** (258A) ha pasado a ser la secuencia más ampliamente especificada a nivel mundial para instalaciones de datos nuevas por la influencia de la compañía AT&T.

Es también la secuencia especificada por RDSI y un subgrupo especificado por la norma IEEE 802.3 10BaseT Ethernet sobre pares trenzados.

EIA **568A** es la más reciente de las opciones de secuencia según lo publicado en el "Borrador 9" de la EIA como la secuencia preferida para la conectorización de cableados de datos sobre par trenzado UTP.

Es similar a la secuencia 568B excepto que los pares 2 y 3 están invertidos.

Protocolos de Red

La función de los protocolos

Los protocolos son reglas y procedimientos para la comunicación. El término «protocolo» se utiliza en distintos contextos. Por ejemplo, los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma forma se aplican las reglas del protocolo al entorno informático. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.

Cuando piense en protocolos de red recuerde estos tres puntos:

- **Existen muchos protocolos.** A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza

distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.

- **Algunos protocolos sólo trabajan en ciertos niveles OSI.** El nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red (NIC) y salgan al cable de la red.

- **Los protocolos también puede trabajar juntos en una jerarquía o conjunto de protocolos.** Al igual que una red incorpora funciones a cada uno de los niveles del modelo OSI, distintos protocolos también trabajan juntos a distintos niveles en la jerarquía de protocolos. Los niveles de la jerarquía de protocolos se corresponden con los niveles del modelo OSI. Por ejemplo, el nivel de aplicación del protocolo TCP/IP se corresponde con el nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

Cómo funcionan los protocolos

La operación técnica en la que los datos son transmitidos a través de la red se puede dividir en dos pasos: discretos, sistemáticos. A cada paso se realizan ciertas acciones que no se pueden realizar en otro paso. Cada paso incluye sus propias reglas y procedimientos, o protocolo.

Los pasos del protocolo se tienen que llevar a cabo en un orden apropiado y que sea el mismo en cada uno de los equipos de la red. En el equipo origen, estos pasos se tienen que llevar a cabo de arriba hacia abajo. En el equipo de destino, estos pasos se tienen que llevar a cabo de abajo hacia arriba.

El equipo origen

Los protocolos en el equipo origen:

1. Se dividen en secciones más pequeñas, denominadas paquetes.
2. Se añade a los paquetes información sobre la dirección, de forma que el equipo de destino pueda determinar si los datos le pertenecen.

3. Prepara los datos para transmitirlos a través de la NIC y enviarlos a través del cable de la red.

El equipo de destino

Los protocolos en el equipo de destino constan de la misma serie de pasos, pero en sentido inverso.

1. Toma los paquetes de datos del cable y los introduce en el equipo a través de la NIC.

2. Extrae de los paquetes de datos toda la información transmitida eliminando la información añadida por el equipo origen.

3. Copia los datos de los paquetes en un búfer para reorganizarlos enviarlos a la aplicación.

Los equipos origen y destino necesitan realizar cada paso de la misma forma para que los datos tengan la misma estructura al recibirse que cuando se enviaron.

Protocolos encaminables

Hasta mediados de los ochenta, la mayoría de las redes de área local (LAN) estaban aisladas. Una LAN servía a un departamento o a una compañía y rara vez se conectaba a entornos más grandes. Sin embargo, a medida que maduraba la tecnología LAN, y la comunicación de los datos necesitaba la expansión de los negocios, las LAN evolucionaron, haciéndose componentes de redes de comunicaciones más grandes en las que las LAN podían hablar entre sí.

Los datos se envían de una LAN a otra a lo largo de varios caminos disponibles, es decir, *se encaminan.* A los protocolos que permiten la comunicación LAN a LAN se les conoce como *protocolos encaminables.* Debido a que los protocolos encaminables se pueden utilizar para unir varias LAN y crear entornos de red de área extensa, han tomado gran importancia.

Protocolos en una arquitectura multinivel

En una red, tienen que trabajar juntos varios protocolos. Al trabajar juntos, aseguran que los datos se preparan correctamente, se transfieran al destino correspondiente y se reciban de forma apropiada.

El trabajo de los distintos protocolos tiene que estar coordinado de forma que no se produzcan conflictos o se realicen tareas incompletas. Los resultados de esta coordinación se conocen como *trabajo en niveles.*

Jerarquías de protocolos

Una jerarquía de protocolos es una combinación de protocolos. Cada nivel de la jerarquía especifica un protocolo diferente para la gestión de una función o de un subsistema del proceso de comunicación. Cada nivel tiene su propio conjunto de reglas. Los protocolos definen las reglas para cada nivel en el modelo OSI:

Nivel de aplicación	Inicia o acepta una petición
Nivel de	Añade información de formato, presentación y

presentación	cifrado al paquete de datos
Nivel de sesión	Añade información del flujo de tráfico para determinar cuándo se envía el paquete
Nivel de transporte	Añade información para el control de errores
Nivel de red	Se añade información de dirección y secuencia al paquete
Nivel de enlace de datos	Añade información de comprobación de envío y prepara los datos para que vayan a la conexión física
Nivel físico	El paquete se envía como una secuencia de bits

Los niveles inferiores en el modelo OSI especifican cómo pueden conectar los fabricantes sus productos a los productos de otros fabricantes, por ejemplo, utilizando NIC de varios fabricantes en la misma LAN. Cuando utilicen los mismos protocolos, pueden enviar y recibir datos entre sí. Los niveles superiores especifican las reglas para dirigir las sesiones de comunicación (el tiempo en el que dos equipos mantienen una conexión) y la interpretación de aplicaciones. A medida que aumenta el nivel de la jerarquía, aumenta la sofisticación de las tareas asociadas a los protocolos.

El proceso de ligadura

El *proceso de ligadura (binding process),* el proceso con el que se conectan los protocolos entre sí y con la NIC, permite una gran flexibilidad a la hora de configurar una red. Se pueden mezclar y combinar los protocolos y las NIC según las necesidades. Por ejemplo, se pueden ligar dos jerarquías de protocolos a una NIC, como Intercambio de paquetes entre redes e Intercambio de paquetes en secuencia (IPX/SPX). Si hay más de una NIC en el equipo, cada jerarquía de protocolos puede estar en una NIC o en ambas.

El orden de ligadura determina la secuencia en la que el sistema operativo ejecuta el protocolo. Cuando se ligan varios protocolos a una NIC, el orden de ligadura es la secuencia en que se utilizarán los protocolos para intentar una comunicación correcta. Normalmente, el proceso de ligadura se inicia cuando se instala o se inicia el sistema operativo o el protocolo. Por ejemplo, si el primer protocolo ligado es TCP/IP, el sistema operativo de red intentará la conexión con TCP/IP antes de utilizar otro protocolo. Si falla esta conexión, el equipo tratará de realizar una conexión utilizando el siguiente protocolo en el orden de ligadura.

El proceso de ligadura consiste en asociar más de una jerarquía de protocolos a la NIC. Las jerarquías de protocolos tienen que estar ligadas o asociadas con los componentes en un orden para que los datos puedan moverse adecuadamente por la jerarquía durante la ejecución. Por ejemplo, se puede ligar TCP/IP al nivel de sesión del Sistema básico de entrada/salida en red (NetBIOS), así como al controlador de la NIC. El controlador de la NIC también está ligado a la NIC.

Jerarquías estándar

La industria informática ha diseñado varios tipos de protocolos como modelos estándar de protocolo. Los fabricantes de hardware y software pueden desarrollar sus productos para ajustarse a cada una de las combinaciones de estos protocolos. Los modelos más importantes incluyen:

- La familia de protocolos ISO/OSI.
- La arquitectura de sistemas en red de IBM (SNA).
- Digital DECnet.
- Novell NetWare.
- Apple Talk de Apple.
- El conjunto de protocolos de Internet, TCP/IP.

Los protocolos existen en cada nivel de estas jerarquías, realizando las tareas especificadas por el nivel. Sin embargo, las tareas de comunicación que tienen que realizar las redes se agrupan en un tipo de protocolo entre tres. Cada tipo está compuesto por uno o más niveles del modelo OSI.

Antes del modelo de referencia OSI se escribieron muchos protocolos. Por tanto, no es extraño encontrar jerarquías de protocolos que no se correspondan directamente con el modelo OSI.

Protocolos de aplicación

Los protocolos de aplicación trabajan en el nivel superior del modelo de referencia OSI y proporcionan interacción entre aplicaciones e intercambio de datos.

- **APPC (Comunicación avanzada entre programas):** Protocolo SNA *Trabajo en Grupo* de IBM, mayormente utilizado en equipos AS/400. APPC se define como un protocolo de aplicación porque trabaja en el nivel de presentación del modelo OSI. Sin embargo, también se considera un protocolo de transporte porque APPC utiliza el protocolo LU 6.2 que trabaja en los niveles de transporte y de sesión del modelo OSI.

- **FTAM (Acceso y gestión de la transferencia de archivos):** Un protocolo OSI de acceso a archivos

- **X.400:** Un protocolo CCITT para las transmisiones internacionales de correo electrónico.

- **X.500:** Un protocolo CCITT para servicios de archivos y directorio entre sistemas.

- **SMTP (Protocolo básico para la transferencia de correo):** Un protocolo Internet para las transferencias de correo electrónico.

- **FTP (Protocolo de transferencia de archivos):** Un protocolo para la transferencia de archivos en Internet.

- **SNMP (Protocolo básico de gestión de red):** Un protocolo Internet para el control de redes y componentes.

- **Telnet:** Un protocolo Internet para la conexión a máquinas remotas y procesar los datos localmente.

- **SMBs (Bloques de mensajes del servidor) de Microsoft y clientes o redirectores:** Un protocolo cliente/servidor de respuesta a peticiones.

- **NCP (Protocolo básico de NetWare) *y* clientes o redirectores:** Un conjunto de protocolos de servicio.

- **AppleTalk *y* AppleShare:** Conjunto de protocolos de red de Apple.

- **AFP (Protocolo de archivos AppleTalk):** Protocolo de Apple para el acceso a archivos remotos.

- **DAP (Protocolo de acceso a datos):** Un protocolo de DECnet para el acceso a archivos.

Protocolos de transporte

Los protocolos de transporte facilitan las sesiones de comunicación entre equipos y aseguran que los datos se pueden mover con seguridad entre equipos.

- **TCP:** El protocolo de TCP/IP para la entrega garantizada de datos en forma de paquetes secuenciados.
- **SPX:** Parte del conjunto de protocolos IPX/SPX de Novell para datos en forma de paquetes secuenciados.

- **NWLink:** La implementación de Microsoft del protocolo IPX/SPX.

- **NetBEUI (Interfaz de usuario ampliada NetBIOS):** Establece sesiones de comunicación entre equipos (NetBIOS) y proporciona los servicios de transporte de datos subyacentes (NetBEUI).

- **ATP (Protocolo de transacciones Apple Talk) y NBP (Protocolo de asignación de nombres):** Protocolos de Apple de sesión de comunicación y de transporte de datos.

Protocolos de red

Los protocolos de red proporcionan lo que se denominan «servicios de enlace». Estos protocolos gestionan información sobre direccionamiento y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es Ethernet o Token Ring.

- **IP:** El protocolo de TCP/IP para el encaminamiento de paquetes.
- **IPX:** El protocolo de Novell para el encaminamiento de paquetes.

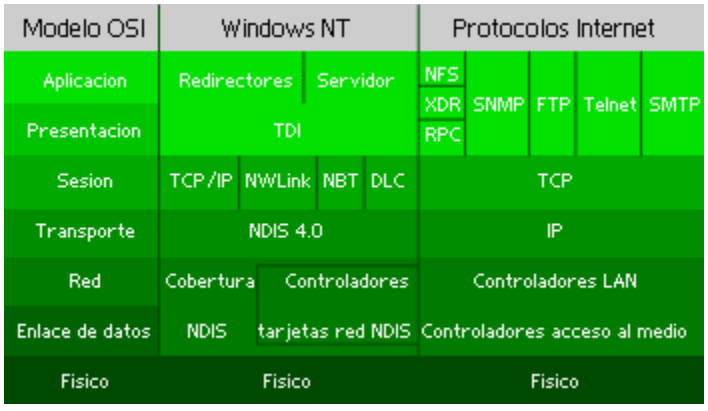
- **NWLink:** La implementación de Microsoft del protocolo IPX/SPX.

- **NetBEUI:** Un protocolo de transporte que proporciona servicios de transporte de datos para sesiones y aplicaciones NetBIOS.

- **DDP (Protocolo de entrega de datagramas):** Un protocolo de Apple Talk para el transporte de datos.

Estándares de protocolo

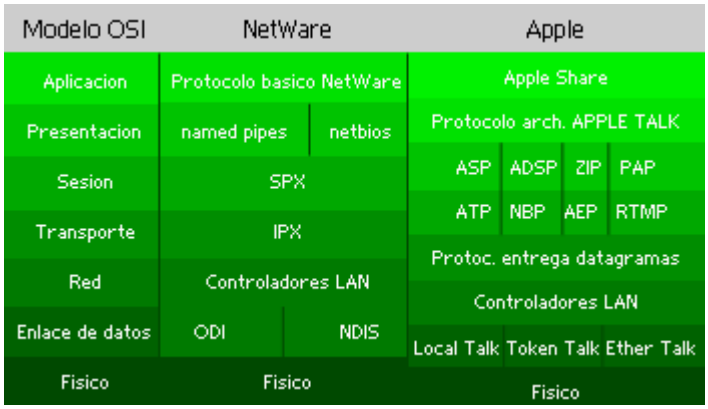
El modelo OSI se utiliza para definir los protocolos que se tienen que utilizar en cada nivel. Los productos de distintos fabricantes que se ajustan a este modelo se pueden comunicar entre sí.



La ISO, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), ANSI (Instituto de Estandarización Nacional Americano), CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía), ahora llamado ITU (Unión Internacional de Telecomunicaciones) y otros organismos de estandarización han desarrollado protocolos que se correspondan con algunos de los niveles del modelo OSI.

Los protocolos de IEEE a nivel físico son:

- **802.3 (Ethernet)**. Es una red lógica en bus que puede transmitir datos a 10 Mbps. Los datos se transmiten en la red a todos los equipos. Sólo los equipos que tenían que recibir los datos informan de la transmisión. El protocolo de acceso de múltiple con detección de portadora con detección de colisiones (CSMA/CD) regula el tráfico de la red permitiendo la transmisión sólo cuando la red esté despejada y no haya otro equipo transmitiendo.



- **802.4 (Token Bus)**. Es una red en bus que utiliza un esquema de paso de testigo. Cada equipo recibe todos los datos, pero sólo los equipos en los que coincida la dirección responderán. Un testigo que viaja por la red determina quién es el equipo que tiene que informar.

- **802.5 (Token Ring)**. Es un anillo lógico que transmite a 4 ó a 16 Mbps. Aunque se le llama en anillo, está montada como una estrella ya que cada equipo está conectado a un hub. Realmente, el anillo está dentro del hub. Un token a través del anillo determina qué equipo puede enviar datos.

El IEEE definió estos protocolos para facilitar la comunicación en el subnivel de Control de acceso al medio (MAC).

Un controlador MAC está situado en el subnivel de Control de acceso al medio; este controlador de dispositivo es conocido como controlador de la NIC. Proporciona acceso a bajo nivel a los adaptadores de red para proporcionar soporte en la transmisión de datos y algunas funciones básicas de control del adaptador.

Subniveles LLC y MAC del proyecto 802

Un protocolo MAC determina qué equipo puede utilizar el cable de red cuando varios equipos intenten utilizarlo simultáneamente. CSMA/CD, el protocolo 802.3, permite a los equipos transmitir datos cuando no hay otro equipo transmitiendo. Si dos máquinas transmiten simultáneamente se produce una colisión. El protocolo detecta la colisión y detiene toda transmisión hasta que se libera el cable.

Entonces, cada equipo puede volver a tratar de transmitir después de esperar un período de tiempo aleatorio.

TCP/IP

El Protocolo de control de transmisión/Protocolo Internet (TCP/IP) es un conjunto de Protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo (formado por elementos diferentes). Además, TCP/IP proporciona un protocolo de red encaminable y permite acceder a Internet y a sus recursos. Debido a su popularidad, TCP/IP se ha convertido en el estándar de hecho en lo que se conoce como *interconexión de redes,* la intercomunicación en una red que está formada por redes más pequeñas.

TCP/IP se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos. La interoperabilidad es la principal ventaja de TCP/IP. La mayoría de las redes permiten TCP/IP como protocolo. TCP/IP también permite el encaminamiento y se suele utilizar como un protocolo de interconexión de redes.

Entre otros protocolos escritos específicamente para el conjunto TCP/IP se incluyen:

- **SMTP** (Protocolo básico de transferencia de correo). Correo electrónico.
- **FTP** (Protocolo de transferencia de archivos). Para la interconexión de archivos entre equipos que ejecutan TCP/IP.

- **SNMP** (Protocolo básico de gestión de red). Para la gestión de redes.

Diseñado para ser encaminable, robusto y funcionalmente eficiente, TCP/IP fue desarrollado por el Departamento de Defensa de Estados Unidos como un conjunto de protocolos para redes de área extensa (WAN). Su propósito era el de mantener enlaces de comunicación entre sitios en el caso de una guerra nuclear. Actualmente, la responsabilidad del desarrollo de TCP/IP reside en la propia comunidad de Internet. La utilización de TCP/IP ofrece varias ventajas:

Es un estándar en la industria. Como un estándar de la industria, es un protocolo abierto. Esto quiere decir que no está controlado por una única compañía, y está menos sujeto a cuestiones de compatibilidad. Es el protocolo, de hecho, de Internet.

Contiene un conjunto de utilidades para la conexión de sistemas operativos diferentes. La conectividad entre un equipo y otro no depende del sistema operativo de red que esté utilizando cada equipo.

Utiliza una arquitectura escalable, cliente/servidor. TCP/IP puede ampliarse (o reducirse) para ajustarse a las necesidades y circunstancias

futuras. Utiliza sockets para hacer que el sistema operativo sea algo transparente.

Un socket es un identificador para un servicio concreto en un nodo concreto de la red. El socket consta de una dirección de nodo y de un número de puerto que identifica al servicio.

Históricamente, TCP/IP ha tenido dos grandes inconvenientes: su tamaño y su velocidad. TCP/IP es una jerarquía de protocolos relativamente grandes que puede causar problemas en clientes basados en MS-DOS. En cambio, debido a los requerimientos del sistema (velocidad de procesador y memoria) que imponen los sistemas operativos con interfaz gráfica de usuario (GUI), como Windows NT o Windows 95 y 98, el tamaño no es un problema.

Estándares TCP/IP

Los estándares de TCP/IP se publican en una serie de documentos denominados *Requests for comment* (RFC); Solicitudes de comentarios. Su objeto principal es proporcionar información o describir el estado de desarrollo. Aunque no se crearon para servir de estándar, muchas RFC han sido aceptadas como estándares.

El desarrollo Internet está basado en el concepto de estándares abiertos. Es decir, cualquiera que lo desee, puede utilizar o participar en el desarrollo de estándares para Internet. La Plataforma de arquitectura Internet (IAB) es el comité responsable para la gestión y publicación de las RFC. La IAB permite a cualquier persona o a cualquier compañía que envíe o que evalúe una RFC. Esto permite que cualquier sugerencia sea tenida en cuenta para cambiar o crear estándares. Transcurrido un tiempo razonable para permitir la discusión, se crea un nuevo borrador que se convertirá o no en un estándar.

TCP/IP y el modelo OSI

El protocolo TCP/IP no se corresponde exactamente con el modelo OSI. En vez de tener siete niveles, sólo utiliza cuatro. Normalmente conocido como *Conjunto de protocolos de Internet*, TCP/IP se divide en estos cuatro niveles:

Nivel de interfaz de red.
Nivel Internet.

Nivel de transporte.

Nivel de aplicación.

Cada uno de estos niveles se corresponde con uno o más niveles del modelo OSI.

Nivel de interfaz de red

El *nivel de interfaz de red,* que se corresponde con los niveles físico y de enlace de datos del modelo OSI se comunica directamente con la red. Proporciona la interfaz entre la arquitectura de red (como Token Ring, Ethernet) y el nivel Internet.

Nivel Internet

El *nivel internet,* que se corresponde con el nivel de red del modelo OSI, utiliza varios protocolos para encaminar y entregar los paquetes. Los routers son dependientes del protocolo. Funcionan a este nivel del modelo y se utilizan para enviar paquetes de una red a otra o de un segmento a otro. En el nivel de red trabajan varios protocolos.

Protocolo Internet (IP)

El Protocolo Internet (IP) es un protocolo de conmutación de paquetes que realiza direccionamiento y encaminamiento. Cuando se transmite un paquete, este protocolo añade una cabecera al paquete, de forma que pueda enviarse a través de la red utilizando las tablas de encaminamiento dinámico. IP es un protocolo no orientado a la conexión y envía paquetes sin esperar la señal de confirmación por parte del receptor. Además, IP es el responsable del empaquetado y división de los paquetes requerido por los niveles físico y de enlace de datos del modelo OSI. Cada paquete IP está compuesto por una dirección de origen y una de destino, un identificador de protocolo, un checksum (un valor calculado) y un TTL (tiempo de vida, del inglés *time to live).* El TTL indica a cada uno de los routers de la red entre el origen y el destino cuánto tiempo le queda al paquete por estar en la red. Funciona como un contador o reloj de cuenta atrás. Cuando el paquete pasa por el router, éste reduce el valor en una unidad (un segundo) o el tiempo que llevaba esperando para ser entregado. Por ejemplo, si un paquete tiene un TTL de 128, puede estar en la red durante 128 segundos o 128 saltos (cada parada, o router, en la red), o una combinación de los dos. El propósito del TTL es prevenir que los paquetes perdidos o dañados (como correos electrónicos con una dirección equivocada) estén vagando en la red. Cuando la cuenta TTL llega a cero, se retira al paquete de la red.

Otro método utilizado por IP para incrementar la velocidad de transmisión es el conocido como «ANDing». La idea del ANDing es determinar si la dirección es de un sitio local o remoto. Si la dirección es local, IP preguntará al Protocolo de resolución de direcciones (ARP) por la dirección hardware de la máquina de destino. Si la dirección es remota, el IP comprueba su tabla de encaminamiento

local para encaminarlo al destino. Si existe un camino, el paquete se envía por ahí. Si no existe el camino, el paquete se envía a través del gateway a su destino.

Un AND es una operación lógica que combina los valores de dos bits (0, 1) o dos valores lógicos (verdadero, falso) y devuelve un 1 (verdadero) si los valores de ambas entradas son 1 (verdadero) y devuelve 0 (falso) en caso contrario.

Protocolo de resolución de direcciones (ARP)

Antes de enviar un paquete IP a otro host se tiene que conocer la dirección hardware de la máquina receptora. El ARP determina la dirección hardware (dirección MAC) que corresponde a una dirección IP. Si ARP no contiene la dirección en su propia caché, envía una petición por toda la red solicitando la dirección. Todos los hosts de la red procesan la petición y, si contienen un valor para esa dirección, lo devuelven al solicitante. A continuación se envía el paquete a su destino y se guarda la información de la nueva dirección en la caché del router.

Protocolo inverso de resolución de direcciones (RARP)

Un servidor RARP mantiene una base de datos de números de máquina en la forma de una tabla (o caché) ARP que está creada por el administrador del sistema. A diferencia de ARP, el protocolo RARP proporciona una dirección IP a una petición con dirección de hardware. Cuando el servidor RARP recibe una petición de un número IP desde un nodo de la red, responde comprobando su tabla de encaminamiento para el número de máquina del nodo que realiza la petición y devuelve la dirección IP al nodo que realizó la petición.

Protocolo de mensajes de control de Internet (ICMP)

El ICMP es utilizado por los protocolos IP y superiores para enviar y recibir informes de estado sobre la información que se está transmitiendo. Los routers suelen utilizar ICMP para controlar el flujo, o velocidad, de datos entre ellos. Si el flujo de datos es demasiado rápido para un router, pide a los otros routers que reduzcan la velocidad de transmisión.

Los dos tipos básicos de mensajes ICMP son el de informar de errores y el de enviar preguntas.

Nivel de transporte

El *nivel de transporte,* que se corresponde con el nivel de transporte del modelo OSI, es el responsable de establecer y mantener una comunicación entre dos hosts. El nivel de transporte proporciona notificación de la recepción, control de flujo y secuenciación de paquetes. También gestiona las retransmisiones de

paquetes. El nivel de transporte puede utilizar los protocolos TCP o el Protocolo de datagramas de usuario (UDP) en función de los requerimientos de la transmisión.

Protocolo de control de transmisión (TCP)

El TCP es el responsable de la transmisión fiable de datos desde un nodo a otro. Es un protocolo orientado a la conexión y establece una conexión (también conocida como una sesión, circuito virtual o enlace) entre dos máquinas antes de transferir ningún dato. Para establecer una conexión fiable, TCP utiliza lo que se conoce como «acuerdo en tres pasos». Establece el número de puerto y los números de secuencia de inicio desde ambos lados de la transmisión. El acuerdo consta de tres pasos:

1. El solicitante envía al servidor un paquete especificando el número de puerto que él planea utilizar y el número de secuencia inicial (ISN).
2. El servidor responde con su ISN, que consiste en el ISN del solicitante más uno.

3. El solicitante responde a la respuesta del servidor con el ISN del servidor más uno.

En orden a mantener una conexión fiable, cada paquete tiene que contener:

Un número de puerto TCP origen y destino.
Un número de secuencia para mensajes que tienen que dividirse en partes más pequeñas.

Un checksum que asegura que la información se ha recibido sin error.

Un número de confirmación que indica a la máquina origen qué partes de la información han llegado.

Ventanas deslizantes *(Sliding Windows)* TCP.

Puertos, sockets y ventanas deslizantes *(sliding windows)*

Los números de puerto del protocolo se utilizan para hacer referencia a la localización de una aplicación o proceso en particular en cada máquina (en el nivel de aplicación). Al igual que una dirección IP identifica la dirección de un host de la red, el número de puerto identifica la aplicación a nivel de transporte, por lo que proporciona una conexión completa de una aplicación de un host a una aplicación de otro host. Las aplicaciones y servicios (como servicios de archivos e impresión o telnet) pueden configurar hasta 65.536 puertos. Las aplicaciones y servicios TCP/IP suele utilizar los primeros 1.023 puertos. La Internet Assigned Numbers Authority (IANA) los ha asignado como estándar, o puertos por omisión. Cualquier

aplicación cliente puede asignar números de puerto dinámicamente cuando sea necesario. Un puerto y una dirección de nodo forman un socket.

Los servicios y las aplicaciones utilizan sockets para establecer conexiones con otro host. Si las aplicaciones necesitan garantizar la entrega de datos, el socket elige el servicio orientado a conexión (TCP). Si la aplicación no necesita garantizar la entrega de los datos, el socket elige el servicio no orientado a la conexión (UDP).

TCP utiliza una ventana deslizante para transferir datos entre hosts. Regula cuánta información puede pasarse a través de una conexión IP antes de que el host de destino envíe una confirmación. Cada equipo tiene una ventana de envío y de recepción que utiliza a modo de búfer para guardar los datos y hacer más eficiente el proceso de comunicación. Una ventana deslizante permite al equipo origen transmitir una serie de paquetes sin tener que esperar a que le sea confirmada la llegada de cada paquete. Esto permite al equipo de destino que pueda recibir los paquetes en otro orden al enviado, y si no se recibe una confirmación en un período de tiempo, se reenvían los paquetes.

Protocolo de datagramas de usuario (UDP)

UDP es un protocolo no orientado a la conexión y es el responsable de la comunicación de datos extremo a extremo. En cambio, a diferencia de TCP, UDP no establece una conexión. Intenta enviar los datos e intenta comprobar que el host de destino recibe los datos. UDP se utiliza para enviar pequeñas cantidades de datos que no necesitan una entrega garantizada. Aunque UDP utiliza puertos, son distintos de los puertos TCP; así pues, pueden utilizar los mismos números sin interferirse.

Nivel de aplicación

El *nivel de aplicación* se corresponde con los niveles de sesión, presentación y aplicación del modelo OSI, y conecta las aplicaciones a la red. Dos interfaces de programación de aplicaciones (API) proporcionan acceso a los protocolos de transporte TCP/IP, los sockets de Windows y NetBIOS.

Interfaz de sockets de Windows

Los sockets de Windows (WinSock) son una API de red diseñada para facilitar la comunicación entre aplicaciones y jerarquías de protocolos TCP/IP diferentes. Se definió para que las aplicaciones que utilizasen TCP/IP pudiesen escribir en una interfaz estándar. WinSock se deriva de los sockets originales que creó la API para el sistema operativo Unix BSD. WinSock proporciona una interfaz común para las aplicaciones y protocolos que existen cerca de la cima del modelo de referencia TCP/IP. Cualquier programa o aplicación escrito utilizando la API de WinSock se puede comunicar con cualquier protocolo TCP/IP, y viceversa.

Protocolos NetWare

Al igual que TCP/IP, Novell proporciona un conjunto de protocolos desarrollados específicamente para NetWare. Los cinco protocolos principales utilizados por NetWare son:

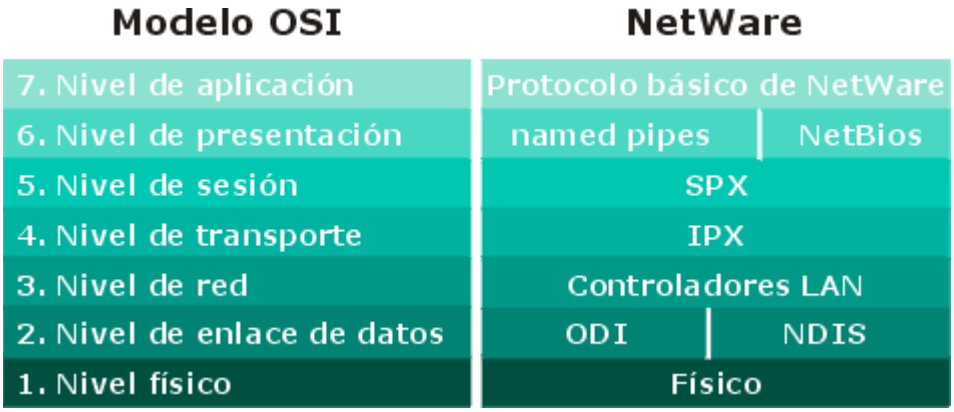
Protocolo de acceso al medio.
Intercambio de paquetes entre redes/Intercambio de paquetes en secuencia (IPX/SPX).

Protocolo de información de encaminamiento (RIP).

Protocolo de notificación de servicios (SAP).

Protocolo básico de NetWare (NCP).

Debido a que estos protocolos se definieron antes de la finalización del modelo OSI, no se ajustan exactamente al modelo OSI. Actualmente, no existe una correlación directa entre los límites de los niveles de las dos arquitecturas. Estos protocolos siguen un patrón de recubrimiento. Concretamente, los protocolos de nivel superior (NCP, SAP y RIP) están recubiertos por IPX/SPX. Luego, una cabecera y un final del Protocolo de acceso al medio recubre a IPX/SPX.



Protocolos de acceso al medio

Los protocolos de acceso al medio definen el direccionamiento que permite diferenciar a los nodos de una red NetWare. El direccionamiento está implementado en el hardware o en la NIC. Las implementaciones más conocidas son:

802.5 Token Ring.

802.3 Ethernet.

Ethernet 2.0.

El protocolo es responsable de colocar la cabecera al paquete. Cada cabecera incluye el código del origen y del destino. Una vez que se haya transmitido el paquete y que está en el medio, cada tarjeta de red comprueba la dirección; si la dirección coincide con la dirección del destino del paquete, o si el paquete es un mensaje de difusión, la NIC copia el paquete y lo envía a la jerarquía de protocolos.

Además del direccionamiento, este protocolo proporciona un control de errores a nivel de bit como una comprobación de redundancia cíclica (CRC). Una vez que se le añade la CRC al paquete, supuestamente los paquetes estaban libres de errores.

La comprobación de errores CRC utiliza un cálculo complejo para generar un número basado en los datos transmitidos. El dispositivo que realiza el envío hace el cálculo antes de realizar la transmisión y lo incluye en el paquete que se envía al dispositivo de destino. El dispositivo de destino vuelve a hacer este cálculo después de la transmisión. Si ambos dispositivos obtienen el mismo resultado, se supone que no se han producido errores en la transmisión. A este procedimiento se le conoce como comprobación de redundancia, porque cada transmisión incluye no sólo los datos, sino que además incluye valores de comprobación extras (redundantes).

Intercambio de paquetes entre redes/Intercambio de paquetes en secuencia (IPX/SPX, *Internetwork Packet Exchange/Sequenced Packet Exchange)*

El Intercambio de paquetes entre redes (IPX) define los esquemas de direccionamiento utilizados en una red NetWare, e Intercambio de paquetes en secuencia (SPX) proporciona la seguridad y fiabilidad al protocolo IPX. IPX es un protocolo a nivel de red basado en datagramas, no orientado a la conexión y no fiable, equivalente a IP. No requiere confirmación por cada paquete enviado. Cualquier control de confirmación o control de conexión tiene que ser proporcionado por los protocolos superiores a IPX. SPX proporciona servicios orientados a la conexión y fiables a nivel de transporte.

Novell adoptó el protocolo IPX utilizando el Protocolo de datagramas Internet del Sistema de red de Xerox (XNS). IPX define dos tipos de direccionamiento:

Direccionamiento a nivel de red. La dirección de un segmento de la red, identificado por el número de red asignado durante la instalación.

Direccionamiento a nivel de nodo. La dirección de un proceso en un nodo que está identificado por un número de socket.

Los protocolos IPX sólo se utilizan en redes con servidores NetWare y se suelen instalar con otro conjunto de protocolos como TCP/IP. Incluso NetWare está empezando a utilizar TCP/IP como un estándar.

Protocolo de información de encaminamiento (RIP, *Routing Information Protocol)*

RIP, al igual que IPX, facilita el intercambio de información de encaminamiento en una red NetWare y fue desarrollado desde XNS. Sin embargo, en RIP se ha añadido al paquete un campo de datos extra para mejorar el criterio de decisión para seleccionar la ruta más rápida hasta un destino. El hecho de realizar una difusión de un paquete RIP permite que ocurran ciertas cosas:

Las estaciones de trabajo pueden localizar el camino más rápido a un número de red.

Los routers pueden solicitar información de encaminamiento a otros routers para actualizar sus propias tablas internas.

Los routers pueden responder a peticiones de encaminamiento de otras estaciones de trabajo o de otros routers.

Los routers pueden asegurarse de si otros routers conocen la configuración de la red.

Los routers pueden detectar un cambio en la configuración de la red.

Protocolo de notificación de servicios (SAP, *Service Advertising Protocol)*

El Protocolo de notificación de servicios (SAP) permite a los nodos que proporcionan servicios (incluyen a los servidores de archivos, servidores de impresión, servidores gateway y servidores de aplicación) informar de sus servicios y direcciones. Los clientes de la red son capaces de obtener la dirección de la red de los servidores a los que pueden acceder. Con SAP, la incorporación y la eliminación de servicios en la red se vuelve dinámica. Por omisión, un servidor SAP informa de su presencia cada 60 segundos. Un paquete SAP contiene:

Información operativa. Especifica la operación que está realizando el paquete.

Tipo de servicio. Especifica el tipo de servicio ofrecido por el servidor.

Nombre del servidor. Especifica el nombre del servidor que difunde los servicios.

Dirección de red. Especifica el número de red del servidor que difunde los servicios.

Dirección de nodo. Especifica el número de nodo del servidor que difunde los servicios.

Dirección de socket. Especifica el número de socket del servidor que difunde los servicios.

Total de saltos hasta el servidor. Especifica el número de saltos que hay hasta el servidor que difunde los servicios.

Campo de operación. Especifica el tipo de petición.

Información adicional. Uno o más conjuntos de campos que pueden seguir al campo de operación con más información sobre uno o más servidores.

Protocolo básico de NetWare (NCP, *NetWare Core Protocol)*

El Protocolo básico de NetWare (NCP) define el control de la conexión y la codificación de la petición de servicio que hace posible que puedan interactuar los clientes y los servidores. Éste es el protocolo que proporciona los servicios de transporte y de sesión. La seguridad de NetWare también está proporcionada dentro de este protocolo.

Otros protocolos habituales

Sistema básico de Entrada/Salida en red (NetBIOS, *Network Basic Input/Output System)*

La mayoría de los servicios y aplicaciones que se ejecutan en el sistema operativo Windows utilizan la interfaz NetBIOS o la *Comunicación entre procesos (IPC).* NetBIOS se desarrolló sobre LAN y se ha convertido en una interfaz estándar para que las aplicaciones puedan acceder a los protocolos de red en el nivel de transporte con comunicaciones orientadas y no orientadas a la conexión. Existen interfaces NetBIOS para NetBEUI, NWLink y TCP/IP. Las interfaces NetBIOS necesitan una dirección IP y un nombre NetBIOS para identificar de forma única a un equipo.

NetBIOS realiza cuatro funciones importantes:

Resolución de nombres NetBIOS. Cada estación de trabajo de una red tienen uno o más nombres. NetBIOS mantiene una tabla con los nombres y algunos sinónimos. El primer nombre en la tabla es el nombre único de la NIC. Se pueden añadir nombres de usuario opcionales para proporcionar un sistema de identificación expresivo.

Servicio de datagramas NetBIOS. Esta función permite enviar un mensaje a un nombre, a un grupo de nombres, o a todos los usuarios de la

red. Sin embargo, debido a que no utiliza conexiones punto a punto, no se garantiza que el mensaje llegue a su destino.

Servicio de sesión NetBIOS. Este servicio abre una conexión punto a punto entre dos estaciones de trabajo de una red. Una estación inicia una llamada a otra y abre la conexión. Debido a que ambas estaciones son iguales, pueden enviar y recibir datos concurrentemente.

Estado de la sesión/NIC NetBIOS. Esta función ofrece información sobre la NIC local, otras NIC y las sesiones activas disponibles a cualquier aplicación que utilice NetBIOS.

Originalmente, IBM ofrecía NetBIOS como un producto separado, implementado como un programa residente (TSR). Actualmente, este programa TSR es obsoleto; si se encuentra uno de estos sistemas, debería sustituirlo con la interfaz NetBIOS de Windows.

NetBEUI

NetBEUI es el acrónimo de Interfaz de usuario ampliada NetBIOS. Originalmente, NetBIOS y NetBEUI estaban casi unidos y se les consideraba como un protocolo. Sin embargo, varios fabricantes separaron NetBIOS, el protocolo a nivel de sesión, de forma que pudiera utilizarse con otros protocolos de transporte encaminables. NetBIOS (Sistema básico de entrada/salida de la red) es una interfaz para LAN a nivel de sesión de IBM que actúa como una interfaz de aplicación para la red. NetBIOS proporciona a un programa las herramientas para que establezca en la red una sesión con otro programa, y debido a que muchos programas de aplicación lo soportan, es muy popular.

NetBEUI es un protocolo pequeño, rápido y eficiente a nivel de transporte proporcionado con todos los productos de red de Microsoft. Está disponible desde mediados de los ochenta y se suministró con el primer producto de red de Microsoft: MS-NET.

Entre las ventajas de NetBEUI se incluyen su pequeño tamaño (importante para los equipos que ejecuten MS-DOS), su velocidad de transferencia de datos en el medio y su compatibilidad con todas las redes Microsoft.

El principal inconveniente de NetBEUI es que no soporta el encaminamiento. También está limitado a redes Microsoft. NetBEUI es una buena solución económica para una red *Trabajo en Grupo* donde todas las estaciones utilizan sistemas operativos Microsoft.

Conmutación de paquetes X.25

X.25 es un conjunto de protocolos WAN para redes de conmutación de paquetes y está formado por servicios de conmutación. Los servicios de conmutación se crearon originalmente para conectar terminales remotos a sistemas mainframe. La red dividía cada transmisión en varios paquetes y los colocaba en la red. El camino entre los nodos era un circuito virtual, que los niveles superiores trataban como si se tratase de una conexión lógica continua. Cada paquete puede tomar distintos caminos entre el origen y el destino. Una vez que llegan los paquetes, se reorganizan como los datos del mensaje original.

Un paquete típico está formado por 128 bytes de datos; sin embargo, el origen y el destino, una vez establecida la conexión virtual, pueden negociar tamaños de paquete diferentes. El protocolo X.25 puede soportar en el nivel físico un máximo teórico de 4.095 circuitos virtuales concurrentes entre un nodo y una red X.25. La velocidad típica de transmisión de X.25 es de 64 Kbps.

El protocolo X.25 trabaja en los niveles físico, de enlace de datos y de red del modelo OSI. Se conoce desde mediados de los setenta y se ha depurado muy bien, por lo que proporciona un entorno de red muy estable. Sin embargo, tiene dos inconvenientes:

El mecanismo de guardar y enviar causa retardos. Normalmente, el retardo es de 6 décimas de segundos y no tiene efecto en bloques de datos grandes. En cambio, en un tipo de transmisión «flip-flop», el retraso puede ser considerable.

Un «flip-flop» es un circuito que alterna entre dos estados posibles cuando se recibe un pulso en la entrada. Por ejemplo, si la salida de un flip-flop es un valor alto y se recibe un pulso en la entrada, la salida cambia a un valor bajo; un segundo pulso en la entrada vuelve a colocar en la salida un valor alto, y así sucesivamente.

Para soportar la transferencia de guardar y enviar se requiere una gran cantidad de trabajo con el búfer.

X.25 y TCP/IP son similares en la medida en que utilizan protocolos de conmutación de paquetes. Sin embargo, existen algunas diferencias entre ellos:

TCP/IP sólo tiene comprobación de errores y control de flujo extremo a extremo; X.25 tienen control de errores nodo a nodo.

Para compensar el hecho de que una red TCP/IP sea completamente pasiva, TCP/IP tiene un control de flujo y un mecanismo de ventana más complicado que el de X.25.

X.25 tiene unos niveles de enlace y eléctricos muy concretos; TCP/IP está diseñado para trabajar con distintos tipos de medios, y con servicios de enlace muy variados.

Sistema de red de Xerox (XNS, *Xerox Network System)*

Xerox desarrolló el Sistema de red de Xerox (XNS) para sus LAN Ethernet. XNS se utilizaba mucho en los ochenta, pero ha sido lentamente sustituido por TCP/IP. Es un protocolo de gran tamaño, lento, ya que genera muchos envíos a todos los dispositivos, aumentando el tráfico de la red.

Comunicación avanzada entre programas (APPC, *Advanced Program-to-Program Communication)*

La Comunicación avanzada entre programas es un protocolo de transporte de IBM desarrollado como parte de su Arquitectura de sistemas en red (SNA). Se diseñó para permitir que los programas de aplicación que se estuviesen ejecutando en distintos equipos se pudiesen comunicar e intercambiar datos directamente.

Apple Talk

Apple Talk es la jerarquía de protocolos de Apple Computer para permitir que los equipos Apple Macintosh compartan archivos e impresoras en un entorno de red. Se introdujo en 1984 como una tecnología LAN autoconfigurable. Apple Talk también está disponible en muchos sistemas UNIX que utilizan paquetes comerciales y de libre distribución. El conjunto de protocolos AppleTalk permite compartir archivos a alto nivel utilizando AppleShare, los servicios de impresión y gestores de impresión de LaserWriter, junto con la secuencia de datos de bajo nivel y la entrega de datagramas básicos.

Protocolos AppleTalk

AppleTalk: Una colección de protocolos que se corresponde con el modelo OSI. Soporta LocalTalk, EtherTalk y TokenTalk.

LocalTalk: Describe el cable par trenzado apantallado utilizado para conectar equipos Macintosh con otros Macintosh o impresoras. Un segmento LocalTalk permite hasta un máximo de 32 dispositivos y opera a una velocidad de 230 Kbps.

Ether Talk: AppleTalk sobre Ethernet. Opera a una velocidad de 10 Mbps. Fast Ethernet opera a una velocidad de 100 Mbps.

Token Talk: AppleTalk sobre Token Ring. Dependiendo de su hardware, TokenTalk opera a 4 o a 16 Mbps.

Conjuntos de protocolos OSI

El conjunto de protocolos OSI es una jerarquía completa de protocolos. Cada protocolo se corresponde directamente con un único nivel del modelo OSI. El conjunto de protocolos OSI incluye protocolos de encaminamiento y transporte, la serie de protocolos IEEE 802, un protocolo a nivel de sesión, un protocolo a nivel de presentación y varios protocolos a nivel de aplicación diseñados para proporcionar una funcionalidad de red, incluyendo el acceso a archivos, impresión y emulación de terminal.

Modelo de Referencia OSI

Tecnologías y protocolos de red*	
Nivel de aplicación	DNS, FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, Telnet, SIP...
Nivel de presentación	ASN.1, MIME, SSL/TLS, XML...
Nivel de sesión	NetBIOS...
Nivel de transporte	SCTP, SPX, TCP, UDP...
Nivel de red	AppleTalk, IP, IPX, NetBEUI, X.25...
Nivel de enlace	ATM, Ethernet, Frame Relay, HDLC, PPP, Token Ring, Wi-Fi, STP...
Nivel físico	Cable coaxial, fibra óptica, par trenzado, microondas, radio, RS-232...

Modelo OSI

(Open Systems Interconnection - Interconexión de Sistemas Abiertos) Norma universal para protocolos de comunicación lanzado en 1984. Fue propuesto por ISO y divide las tareas de la red en siete niveles.

Proporciona a los fabricantes estándares que aseguran mayor compatibilidad e interoperatibilidad entre distintas tecnologías de red producidas a mundialmente.

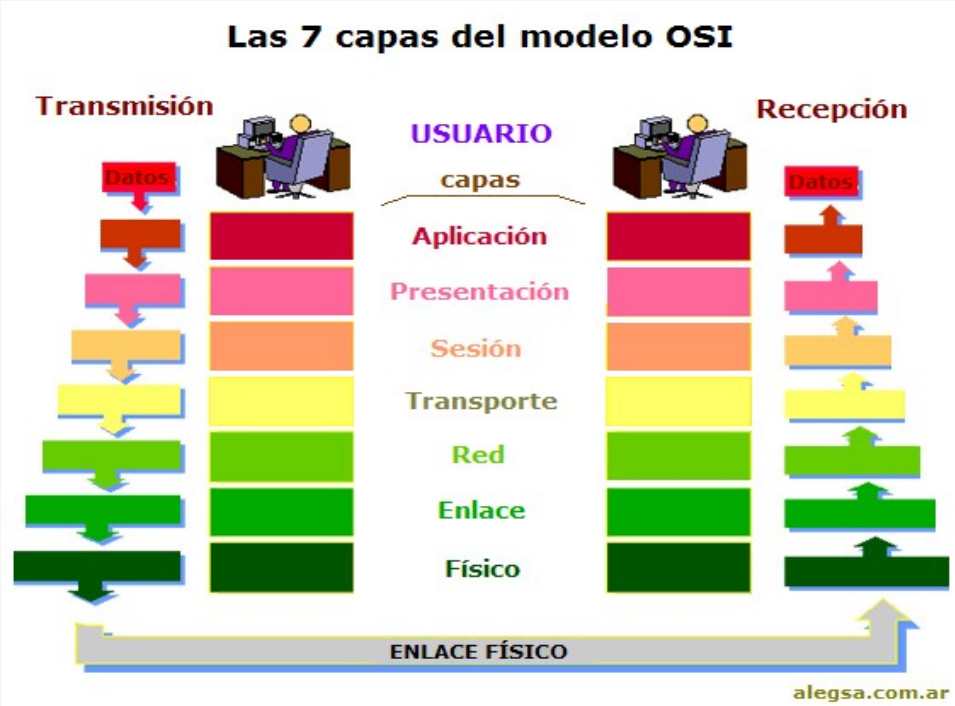
A principios de la década de 1980 hubo un gran crecimiento en cantidad y tamaño de redes, especialmente por parte de empresas. A mediados de la década se comenzaron a notar los inconvenientes de este gran crecimiento. Las redes tenían problemas para comunicarse entre sí por las diferentes implementaciones que tenía cada empresa desarrolladora de tecnologías de red.

Para resolver este problema de incompatibilidades entre redes, la ISO produjo un conjunto de reglas y normas aplicables en forma general a todas las redes. El resultado fue un modelo de red que ayuda a fabricantes y empresas a crear redes compatibles entre sí.

Este esquema fue utilizado para crear numerosos protocolos. Con el tiempo comenzaron a llegar protocolos más flexibles, donde cada capa no estaba tan diferenciada y por lo tanto no estaba claro el nivel OSI al que correspondían. Esto hizo que este esquema se ponga en segundo plano. Sin embargo sigue siendo muy utilizado en la enseñanza en universidades y cursos de redes, especialmente para mostrar cómo pueden estructurarse los protocolos de comunicaciones en forma de pila, aunque no se corresponda demasiado con la realidad.

El modelo, como puede observarse a la derecha, tiene siete niveles o capas:

1. Capa física
2. Capa de enlace de datos.
3. Capa de red.
4. Capa de transporte.
5. Capa de sesión.
6. Capa de presentación.
7. Capa de aplicación.



CAPAS DEL MODELO OSI

Capa Física.- Esta capa se ocupa de la transmisión de bits .en forma continua a lo largo de un canal de comunicación.

Capa de Enlace .-Realiza detección y posiblemente corrección de errores. La capa de enlace transmite los bits en grupos denominados tramas.

Capa de Red .-La capa de red se ocupa del control de la subred , pues es la que tiene el conocimiento de la topología de la red, y decide porque ruta va ha ser enviada la información para evitar la congestión. En esta capa maneja los bits agrupados por paquetes.

Capa de Transporte .-La capa de transporte es la encargada de fragmentar de forma adecuada los datos recibidos de la capa superior para transferirlos a la capa de red, asegurando la llegada y correcta recomposición de los fragmentos en su destino.

Capa de Sesión .-Es la primera capa accesible al usuario y en un sistema multiusuario.

Capa de sesión .- se ocupa de comunicar los hosts.

Capa de Presentación .-Se encarga de la preservación del significado de la información recibida y su trabajo consiste en codificar los datos de la máquina transmisora a un flujo de bits adecuados para la transmisión y luego decodificarlos , para presentarlos en el formato del destinatario.

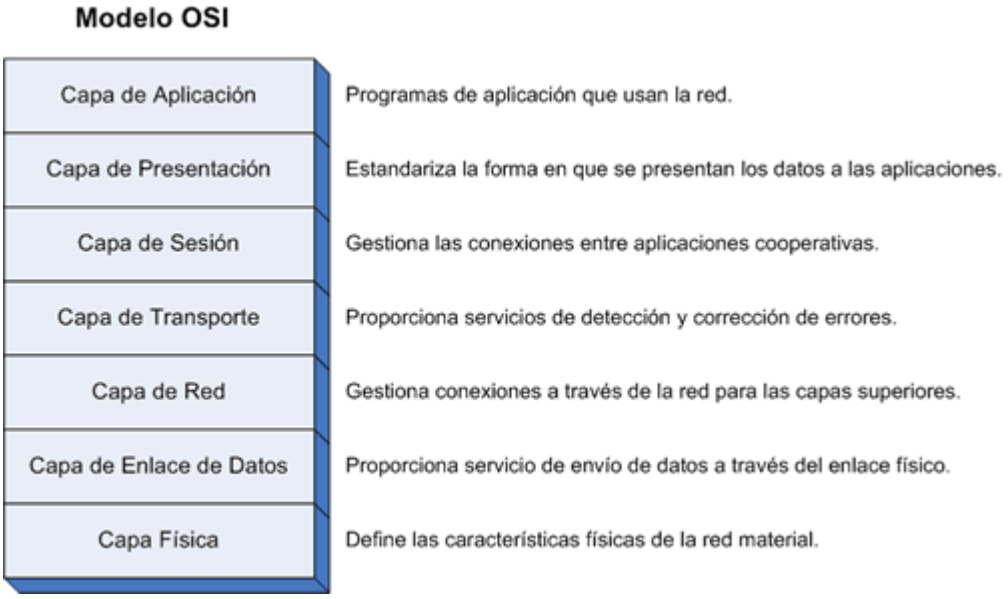
Capa de Aplicación .-La capa de aplicación contiene los programas del usuario , además que contiene los protocolos que se necesitan frecuentemente.

TCP/IP y el modelo OSI

El modelo de referencia OSI

A la hora de describir la estructura y función de los protocolos de comunicaciones se suele recurrir a un modelo de arquitectura desarrollado por la ISO (International Standards Organization). Este modelo se denomina Modelo de Referencia OSI (Open Systems Interconnect).

El modelo OSI está constituido por 7 capas que definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia.



Esta representación en forma de pila, en la que cada capa reposa sobre la anterior suele llamarse pila de protocolos o simplemente pila.

En una capa no se define un único protocolo sino una función de comunicación de datos que puede ser realizada por varios protocolos. Así, por ejemplo, un protocolo de transferencia de ficheros y otro de correo electrónico facilitan, ambos, servicios de usuario y son ambos parte de la capa de aplicación.

Cada protocolo se comunica con su igual en la capa equivalente de un sistema remoto. Cada protocolo solo ha de ocuparse de la comunicación con su gemelo, sin preocuparse de las capas superior o inferior. Sin embargo, también debe haber acuerdo en como pasan los datos de capa en capa dentro de un mismo sistema, pues cada capa está implicada en el envío de datos.

Las capas superiores delegan en las inferiores para la transmisión de los datos a través de la red subyacente. Los datos descienden por la pila, de capa en capa, hasta que son transmitidos a través de la red por los protocolos de la capa física. En el sistema remoto, irán ascendiendo por la pila hasta la aplicación correspondiente.

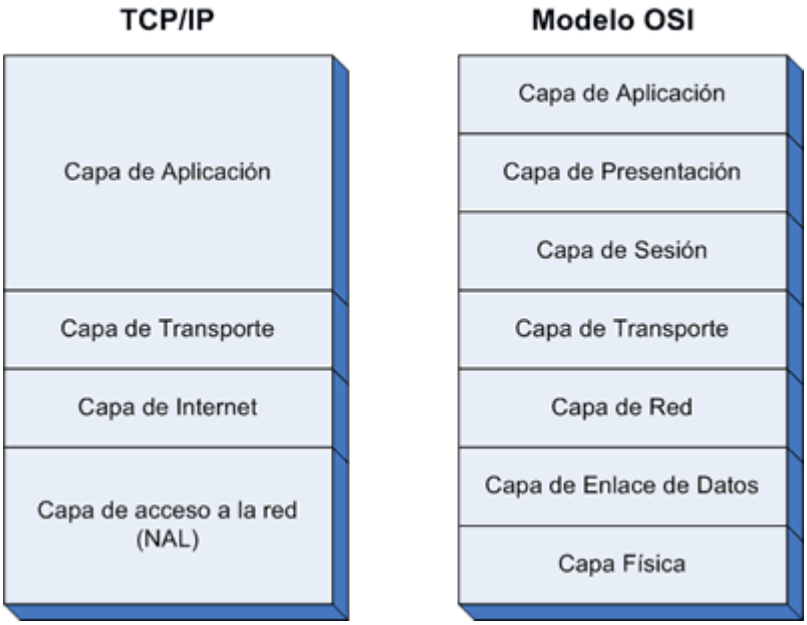
La ventaja de esta arquitectura es que, al aislar las funciones de comunicación de la red en capas, minimizamos el impacto de cambios tecnológicos en el juego de protocolos, es decir, podemos añadir nuevas aplicaciones sin cambios en la red física y también podemos añadir nuevo hardware a la red sin tener que reescribir el software de aplicación.

Aproximación al modelo de arquitectura de los protocolos TCP/IP

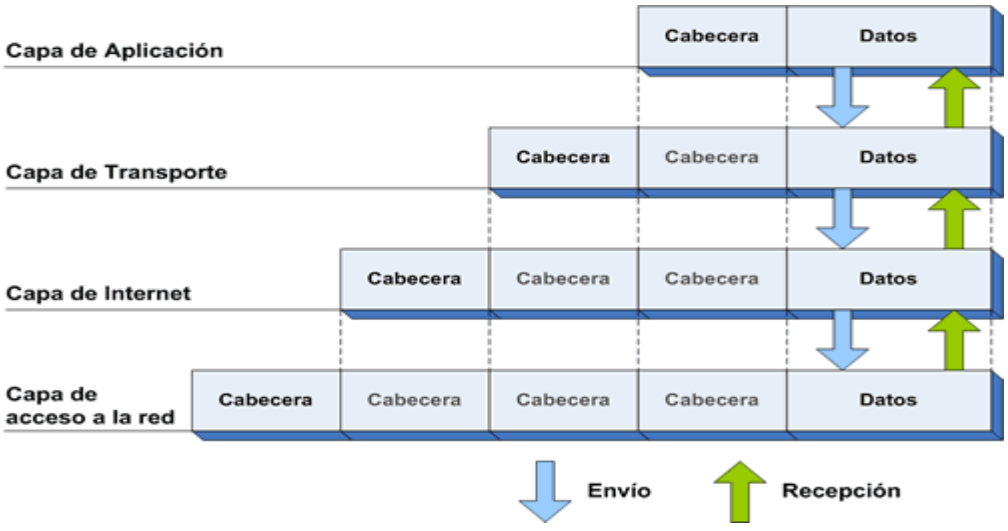
El modelo de arquitectura de estos protocolos es más simple que el modelo OSI, como resultado de la agrupación de diversas capas en una sola o bien por no usar alguna de las capas propuestas en dicho modelo de referencia.

Así, por ejemplo, la capa de presentación desaparece pues las funciones a definir en ellas se incluyen en las propias aplicaciones. Lo mismo sucede con la capa de sesión, cuyas funciones son incorporadas a la capa de transporte en los protocolos TCP/IP. Finalmente la capa de enlace de datos no suele usarse en dicho paquete de protocolos.

De esta forma nos quedamos con una modelo en cuatro capas, tal y como se ve en la siguiente figura:



Al igual que en el modelo OSI, los datos descienden por la pila de protocolos en el sistema emisor y la escalan en el extremo receptor. Cada capa de la pila añade a los datos a enviar a la capa inferior, información de control para que el envío sea correcto. Esta información de control se denomina cabecera, pues se coloca precediendo a los datos. A la adición de esta información en cada capa se le denomina encapsulación. Cuando los datos se reciben tiene lugar el proceso inverso, es decir, según los datos ascienden por la pila, se van eliminando las cabeceras correspondientes.



Cada capa de la pila tiene su propia forma de entender los datos y, normalmente, una denominación especifica que podemos ver en la tabla siguiente. Sin embargo, todos son

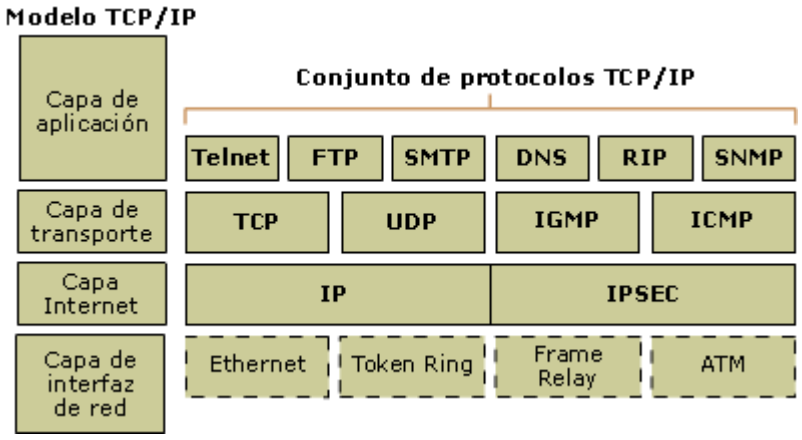
datos a transmitir, y los términos solo nos indican la interpretación que cada capa hace de los datos.

	TCP	UDP
Capa de Aplicación	Flujo	Mensaje
Capa de Transporte	Segmento	Paquete
Capa de Internet	Datagrama	Datagrama
Capa de Acceso a la Red	Trama	Trama

El modelo TCP/IP

TCP/IP está basado en un modelo de referencia de cuatro niveles. Todos los protocolos que pertenecen al conjunto de protocolos TCP/IP se encuentran en los tres niveles superiores de este modelo.

Tal como se muestra en la siguiente ilustración, cada nivel del modelo TCP/IP corresponde a uno o más niveles del modelo de referencia Interconexión de sistemas abiertos (OSI, *Open Systems Interconnection*) de siete niveles, propuesto por la Organización internacional de normalización (ISO, *International Organization for Standardization*).

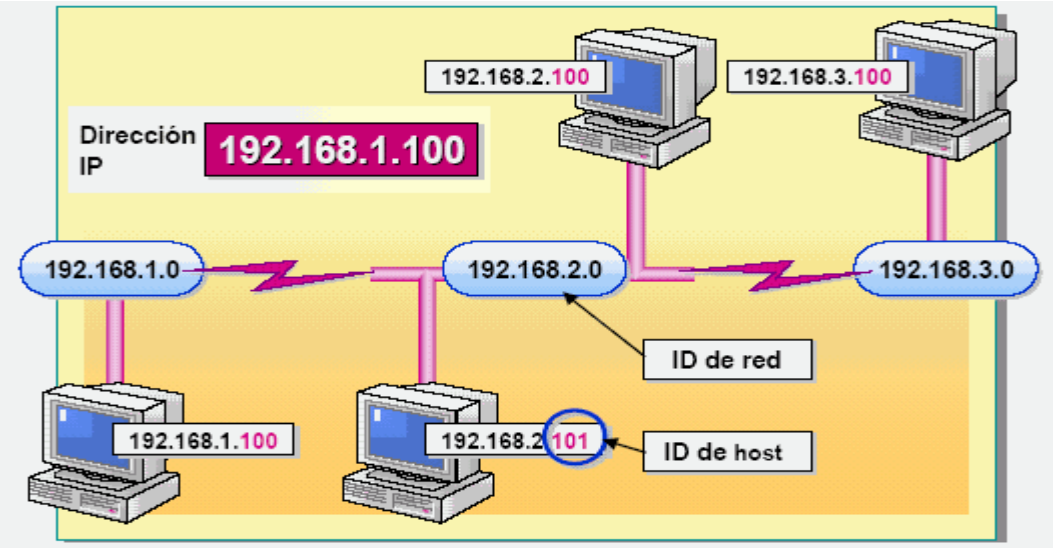


Los tipos de servicios realizados y los protocolos utilizados en cada nivel del modelo TCP/IP se describen con más detalle en la siguiente tabla.

Nivel	Descripción	Protocolos
Aplicación	Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows y otros protocolos de aplicación
Transporte	Permite administrar las sesiones de comunicación entre equipos host. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos.	TCP, UDP, RTP
Internet	Empaqueta los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre hosts y a través de redes. Realiza el enrutamiento de los datagramas IP.	IP, ICMP, ARP, RARP
Interfaz de red	Especifica información detallada de cómo se envían físicamente los datos a través de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

DIRECCIONAMIENTO IP

Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, existen tres clases de dirección que se utilizan para asignar direcciones IP a los equipos. El tamaño y tipo de la red determinará la clase de dirección IP que aplicaremos cuando proporcionemos direcciones IP a los equipos y otros hosts de nuestra red.



La dirección IP es el único identificador que diferencia un equipo de otro en una red y ayuda a localizar dónde reside ese equipo. Se necesita una dirección IP para cada equipo y componente de red, como un router, que se comunique mediante TCP/IP.

La dirección IP identifica la ubicación de un equipo en la red, al igual que el número de la dirección identifica una casa en una ciudad. Al igual que sucede con la dirección de una casa específica, que es exclusiva pero sigue ciertas convenciones, una dirección IP debe ser exclusiva pero conforme a un formato estándar. Una dirección IP está formada por un conjunto de cuatro números, cada uno de los cuales puede oscilar entre 0 y 255.

Componentes de una dirección IP

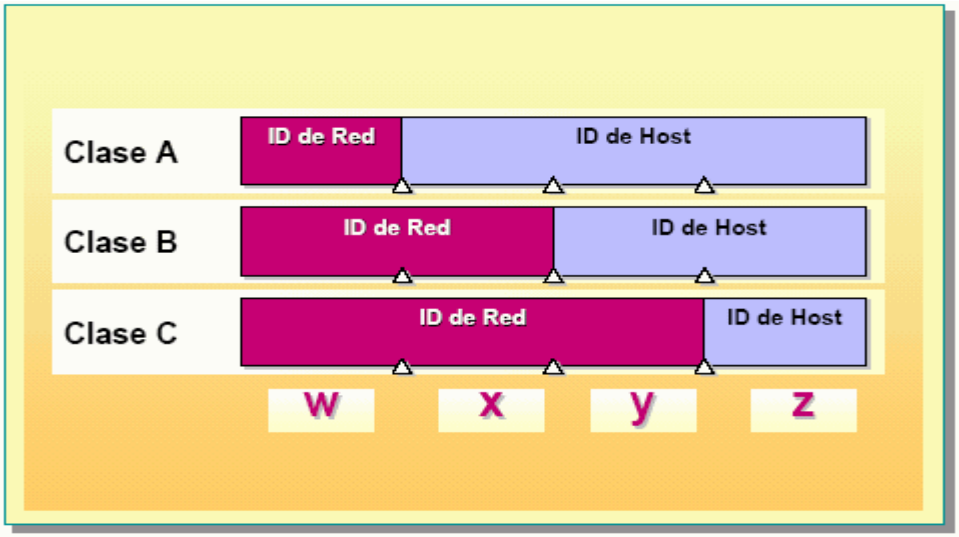
Al igual que la dirección de una casa tiene dos partes (una calle y un código postal), una dirección IP también está formada por dos partes: el ID de host y el ID de red. **ID de red** La primera parte de una dirección IP es el ID de red, que identifica el segmento de red en el que está ubicado el equipo.

Todos los equipos del mismo segmento deben tener el mismo ID de red, al igual que las casas de una zona determinada tienen el mismo código postal. **ID de host**

La segunda parte de una dirección IP es el ID de host, que identifica un equipo, un router u otro dispositivo de un segmento.

El ID de cada host debe ser exclusivo en el ID de red, al igual que la dirección de una casa es exclusiva dentro de la zona del código postal.

Es importante observar que al igual que dos zonas de código postal distinto pueden tener direcciones iguales, dos equipos con diferentes IDs de red pueden tener el mismo ID de host. Sin embargo, la combinación del ID de red y el ID de host debe ser exclusivo para todos los equipos que se comuniquen entre sí.



Las clases de direcciones se utilizan para asignar IDs de red a organizaciones para que los equipos de sus redes puedan comunicarse en Internet. Las clases de direcciones también se utilizan para definir el punto de división entre el ID de red y el ID de host.

Se asigna a una organización un bloque de direcciones IP, que tienen como referencia el ID de red de las direcciones y que dependen del tamaño de la organización. Por ejemplo, se asignará un ID de red de clase C a una organización con 200 hosts, y un ID de red de clase B a una organización con 20.000 hosts.

Clase A

Las direcciones de clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer número para el ID de red. Los tres números restantes se utilizan para el ID de host, permitiendo 16.777.214 hosts por red.

Clase B

Las direcciones de clase B se asignan a redes de tamaño mediano a grande. Esta clase permite 16.384 redes, utilizando los dos primeros números para el ID de red. Los dos números restantes se utilizan para el ID de host, permitiendo 65.534 hosts por red.

Clase C

Las direcciones de clase C se utilizan para redes de área local (LANs) pequeñas. Esta clase permite aproximadamente 2.097.152 redes utilizando los tres primeros números para el ID de red. El número restante se utiliza para el ID de host, permitiendo 254 hosts por red.

Clases D y E

Las clases D y E no se asignan a hosts. Las direcciones de clase D se utilizan para la multidifusión, y las direcciones de clase E se reservan para uso futuro.

Determinación de la clase de dirección

El direccionamiento IP en clases se basa en la estructura de la dirección IP y proporciona una forma sistemática de diferenciar IDs de red de IDs de host. Existen cuatro segmentos numéricos de una dirección IP. Una dirección IP puede estar representada como *w.x.y.z*, siendo *w*, *x*, *y* y *z* números con valores que oscilan entre 0 y 255. Dependiendo del valor del primer número, *w* en la representación numérica, las direcciones IP se clasifican en cinco clases de direcciones como se muestra en la siguiente tabla:

Clase de dirección IP	Dirección IP	ID de red	Valores de *w*
A	*w.x.y.z*	*w*.0.0.0	1 - 126*
B	*w.x.y.z*	*w.x*.0.0	128 – 191
C	*w.x.y.z*	*w.x.y*.0	192 – 223
D	*w.x.y.z*	No disponible	224 – 239
E	*w.x.y.z*	No disponible	240 - 255

*El ID de red 127.0.0.0 está reservado para las pruebas de conectividad.

Determinación de los ID de red y de host

En las direcciones IP de clase A, el ID de red es el primer número de la dirección IP. En la clase B, el ID de red son los dos primeros números; y en la clase C, el ID de red son los tres primeros números de la dirección IP. Los números restantes identifican el ID de host.

El ID de red tiene una estructura de cuatro números al igual que la dirección IP. Por tanto, si el primer número, *w*, de una dirección IP representa el ID de red, la estructura del ID de red es *w*.0.0.0, siendo 0 los tres números restantes. La estructura del ID de host es *x.y.z*. Observe que el host no va precedido de un 0.

Por ejemplo, la dirección IP 172.16.53.46 sería una dirección de clase B ya que *w*=172 y está entre 128 y 191. El ID de red sería 172.16.0.0 y el ID de host 53.46 (sin punto al final).

SUBDIVISION DE UNA RED

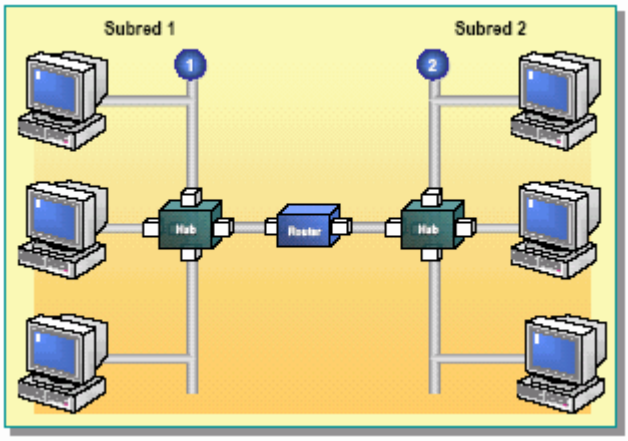
Podemos ampliar una red utilizando dispositivos físicos, como routers y puentes, para añadir segmentos de red. También podemos utilizar dispositivos físicos para dividir una red en segmentos más pequeños para incrementar la eficacia de la red.

Los segmentos de red separados por routers se denominan *subredes*. Cuando creamos subredes, debemos dividir el ID de red para los hosts de las subredes. La división del ID de red utilizado para comunicarse en Internet en IDs de red más pequeños (en función del número de direcciones IP identificadas) para una subred se denomina *subdivisión* de una red.

Para identificar el nuevo ID de red de cada subred, debemos utilizar una máscara de subred para especificar qué parte de la dirección IP va a ser utilizada por el nuevo ID de red de la subred. Podemos localizar un host en una red analizado su ID de red.

Los IDs de red coincidentes muestran qué hosts se encuentran en la misma subred. Si los IDs de red no son los mismos, sabremos que están en distintas subredes y que necesitaremos un router para establecer comunicación entre ellos.

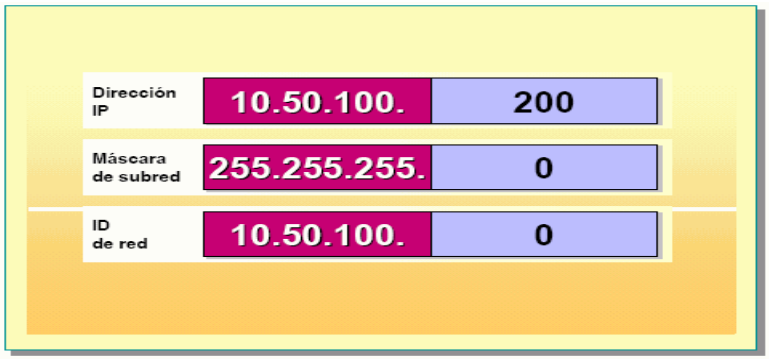
SUBREDES



A medida que crece el número de equipos y el volumen de tráfico en una red Ethernet, se produce un crecimiento de la colisión de datos y se reduce el rendimiento de la red. Para solucionar este problema, los equipos de una red Ethernet se agrupan juntos en divisiones físicas, denominadas segmentos, separadas por un dispositivo físico, como un router o un puente.

En un entorno TCP/IP, los segmentos separados por routers se denominan subredes. Todos los equipos que pertenecen a una subred tienen el mismo ID de red en sus direcciones IP. Cada subred debe tener un ID de red distinto para comunicarse con otras subredes. Basándose en el ID de red, las subredes definen las divisiones lógicas de una red. Los equipos que se encuentran en distintas subredes necesitan comunicarse a través de routers.

MÁSCARAS DE SUBRED



En el método de direccionamiento en clases, el número de redes y hosts disponibles para una clase de dirección específica está predeterminado. En consecuencia, una organización que tenga asignado un ID de red tiene un único ID de red fijo y un número de hosts específico determinado por la clase de dirección a la que pertenezca la dirección IP.

Con el ID de red único, la organización sólo puede tener una red conectándose a su número asignado de hosts. Si el número de hosts es grande, la red única no podrá funcionar eficazmente. Para solucionar este problema, se introdujo el concepto de subredes.

Las subredes permiten que un único ID de red de una clase se divida en IDs de red de menor tamaño (definido por el número de direcciones IP identificadas). Con el uso de estos múltiples IDs de red de menor tamaño, la red puede segmentarse en subredes, cada una con un ID de red distinto, también denominado ID de subred.

Estructura de las máscaras de subred

Para dividir un ID de red, utilizamos una máscara de subred. Una máscara de subred es una pantalla que diferencia el ID de red de un ID de host en una dirección IP pero no está restringido por las mismas normas que el método de clases anterior. Una máscara de subred está formada por un conjunto de cuatro números, similar a una dirección IP.

El valor de estos números oscila entre 0 y 255.

En el método de clases, cada uno de los cuatro números sólo puede asumir el valor máximo 255 o el valor mínimo 0. Los cuatro números están organizados como valores máximos contiguos seguidos de valores mínimos contiguos. Los valores máximos representan el ID de red y los valores mínimos representan el ID de host. Por ejemplo, 255.255.0.0 es una máscara de subred válida, pero 255.0.255.0 no lo es. La máscara de subred 255.255.0.0 identifica el ID de red como los dos primeros números de la dirección IP.

Máscaras de subred predeterminadas

En el método de clases, cada clase de dirección tiene una máscara de subred predeterminada. La siguiente tabla lista las máscaras de subred predeterminadas para cada clase de dirección.

Clase de dirección IP	Dirección IP	Máscara de subred	ID de red	ID de host
A	*w.x.y.z*	255.0.0.0	*w.0.0.0*	*x.y.z*
B	*w.x.y.z*	255.255.0.0	*w.x.0.0*	*x.y*
C	*w.x.y.z*	255.255.255.0	*w.x.y.0*	*z*

Máscaras de subred personalizadas

Cuando dividimos un ID de red existente para crear subredes adicionales, podemos utilizar cualquiera de las máscaras de subred anteriores con cualquier dirección IP o ID de red. Así, la dirección IP 172.16.2.200 podría tener la máscara de subred 255.255.255.0 y el ID de red 172.16.2.0 o la máscara de subred predeterminada 255.255.0.0 con el ID de red 172.16.0.0. Esto permite a una organización dividir en subredes un ID de red de clase B existente 172.16.0.0 en IDs de red más pequeños para que coincida con la configuración real de la red.

DETERMINACIÓN DE HOSTS LOCALES Y REMOTOS

Después de que el ID de red de un host ha sido identificado, es fácil determinar si otro host es local o remoto respecto a él. Para ello, comparamos los IDs de red de ambos hosts. Si coinciden, los dos hosts se encuentran en la misma subred. Si no coinciden, significa que los hosts se encuentran en distintas subredes y es necesario un router para transmitir datos entre ellos.

Ejemplo 1

Supongamos los dos equipos A y B con las direcciones IP 192.168.1.100 y 192.168.2.100 y una máscara de subred 255.255.0.0. Como se muestra en la siguiente tabla, los IDs de red de sus direcciones IP coinciden. Por tanto, los equipos A y B son locales.

	Equipo A	Equipo B
Dirección IP	192.168.1.100	192.168.2.100
Máscara de subred	255.255.0.0	255.255.0.0
ID de red	**192.168.0.0**	**192.168.0.0**

Ejemplo 2

Otro ejemplo serían los equipos A y D con las direcciones IP 192.168.1.100 y 192.168.2.100 y una máscara de subred 255.255.255.0. Los IDs de red de estas direcciones IP no coinciden, como muestra la siguiente tabla. Por tanto, el equipo A es remoto respecto al equipo D.

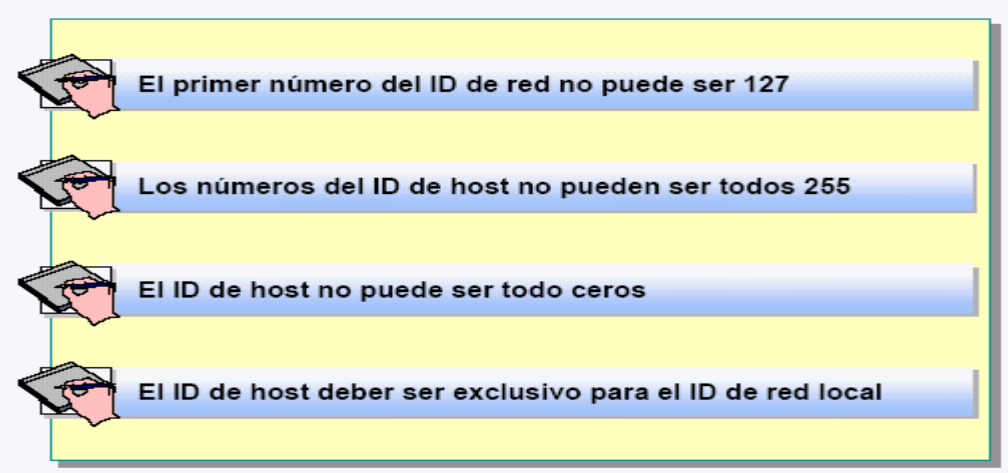
	Equipo A	Equipo D
Dirección IP	192.168.1.100	192.168.2.100
Máscara de subred	255.255.255.0	255.255.255.0
ID de red	**192.168.1.0**	**192.168.2.0**

PLANIFICACIÓN DEL DIRECCIONAMIENTO IP

Una vez establecida una red, todos los equipos que se encuentran en ella necesitan una dirección IP; parecido a las viviendas de un edificio, que necesitan direcciones asignadas a ellas. Sin una dirección IP, un equipo no recibe los datos que van dirigidos a él. Y al igual que las direcciones de una vivienda, el formato de la dirección IP debe seguir ciertas directrices para garantizar que los datos se transmiten al equipo correcto.

Esta sección explica las directrices para asignar IDs de red y de host.

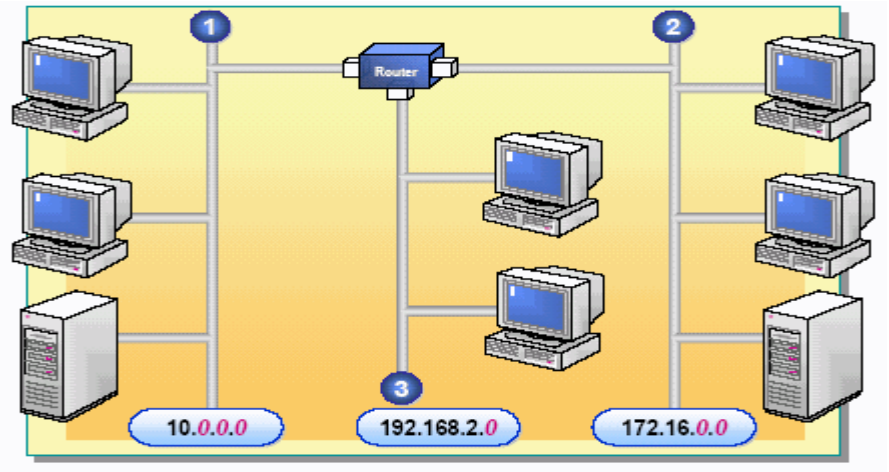
DIRECTRICES DE DIRECCIONAMIENTO



Debemos tener en cuenta algunas directrices sobre los números utilizados para el ID de red y el ID de host cuando asignemos una dirección IP utilizando clases. Estas directrices son las siguientes:

- El primer número del ID de red no puede ser 127. Este número de ID está reservado para pruebas de conexión, como realizar un bucle local.
- Los números del ID de host no pueden ser todos 255, ya que esta dirección se utiliza como dirección de difusión IP.
- El ID de host no puede ser todo ceros (0s), ya que esta dirección se utiliza para indicar un ID de red.
- El ID de host deber ser exclusivo para el ID de red local.

ASIGNACIÓN DE IDs DE RED



El ID de red identifica los hosts TCP/IP ubicados en la misma subred física. Todos los hosts de la misma subred deben tener asignado el mismo ID de red para que puedan comunicarse entre sí.

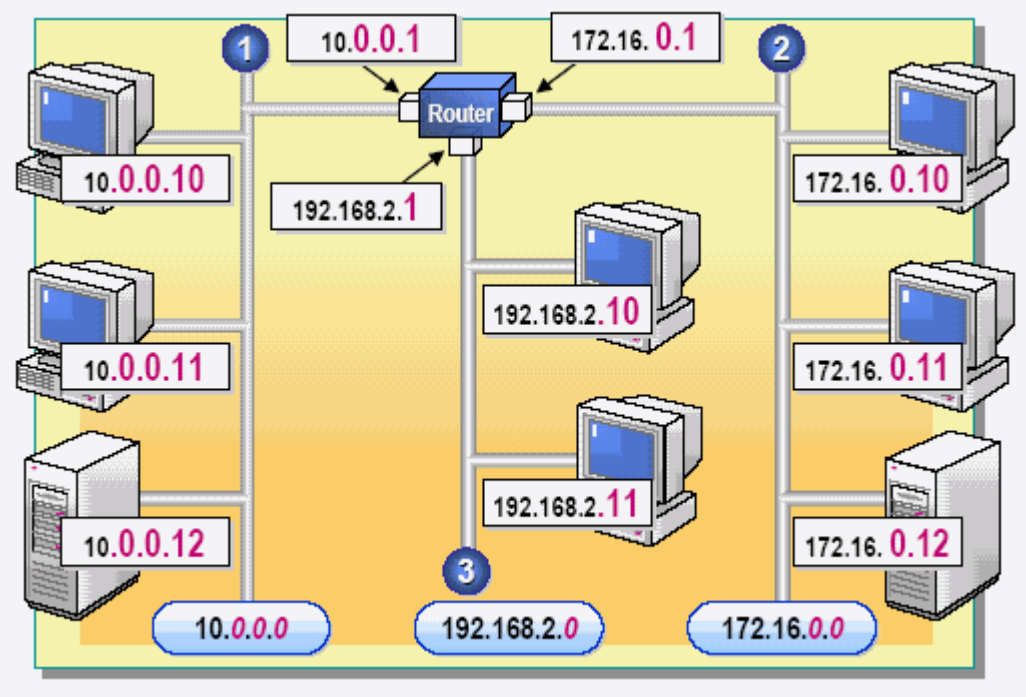
Todas las subredes deben tener un ID de red exclusivo. Por ejemplo, la subred A podría tener el ID de red 10.0.0.0, la subred B podría tener el ID de red

192.168.2.0, y la subred C podría tener el ID de red 172.16.0.0. La siguiente tabla muestra una lista de intervalos válidos de IDs de red para una red.

Clase de dirección	Inicio del intervalo	Fin del intervalo
Clase A	1.0.0.0	126.0.0.0
Clase B	128.0.0.0	191.255.0.0
Clase C	192.0.0.0	223.255.255.0

Nota: Si tiene previsto conectar su red a Internet, debe asegurarse de que la parte de ID de red de la dirección IP es exclusiva respecto al resto de redes en Internet. Para obtener una asignación de un número válido de red IP, puede contactar con su proveedor de servicios de Internet. Puede dividir en subredes su red utilizando máscaras de subred.

ASIGNACIÓN DE IDs DE HOST



El ID de host identifica a un host TCP/IP de una red y debe ser exclusivo para un ID de red determinado. Todos los hosts TCP/IP, incluyendo los routers, requieren IDs de host exclusivos. No existen normas para la asignación de IDs de host en una subred. Por ejemplo, podemos numerar todos los hosts TCP/IP consecutivamente, o podemos numerarlos para que puedan ser identificados fácilmente, por ejemplo asignando al router de cada subred el número 1 para el último número del ID de host.

IDs de host válidos La siguiente tabla muestra una lista de intervalos válidos de IDs de host para cada clase de red.

Clase de dirección	Inicio del intervalo	Fin del intervalo
Clase A	*w*.0.0.1	*w*.255.255.254
Clase B	*w.x*.0.1	*w.x*.255.254
Clase C	*w.x.y*.1	*w.x.y*.254

Puerta de enlace predeterminada

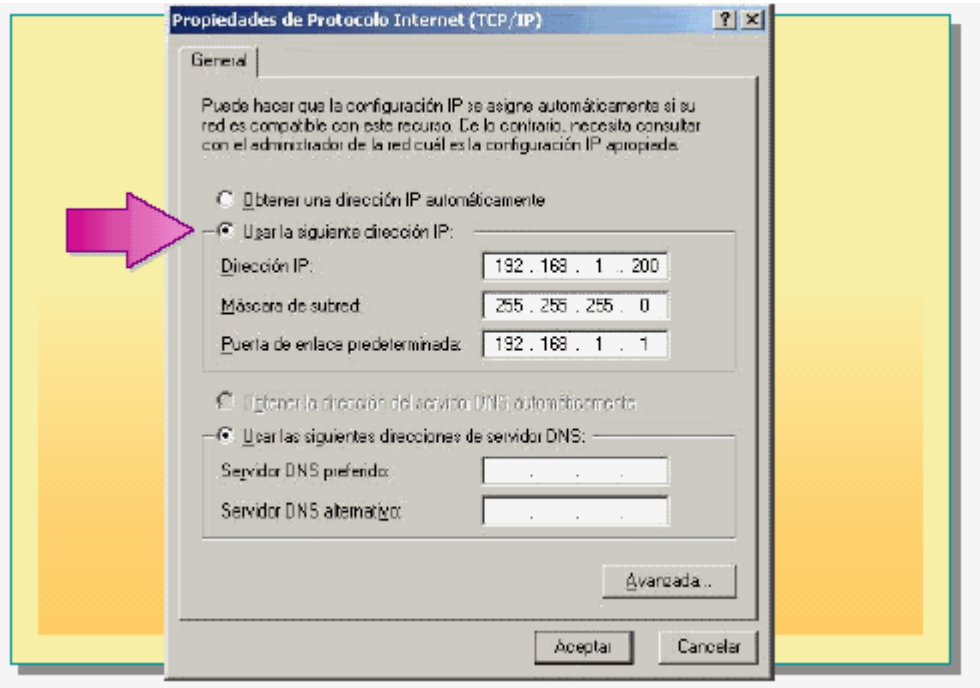
Para un host específico, la dirección IP del router que se encuentra en el mismo segmento que el host recibe el nombre de la puerta de enlace predeterminada del host. Toda la información que el host necesite enviar a segmentos distintos de los suyos, es enrutada a través de la puerta de enlace predeterminada. Como un host y su puerta de enlace predeterminada se encuentran en el mismo segmento, tienen el mismo ID de red pero diferentes IDs de host. Por ejemplo, para el host con la dirección IP 192.168.2.11, la dirección IP de la puerta de enlace predeterminada es 192.168.2.1.

ASIGNACIÓN DE DIRECCIONES TCP/IP

Podemos establecer direcciones IP utilizando el método estático o el método automático. Si decidimos establecer la dirección IP de forma estática, deberemos configurar manualmente la dirección de cada equipo de la red. Si decidimos establecer la dirección IP automáticamente, podremos configurar las direcciones IP para toda una red desde una sola ubicación y asignarlas dinámicamente a cada equipo.

Una vez hemos establecido la dirección IP, podemos ver su configuración TCP/IP utilizando el cuadro de diálogo **Propiedades del protocolo de Internet (TCP/IP)** o la utilidad *Ipconfig*.

DIRECCIONAMIENTO IP ESTÁTICO



El direccionamiento IP estático hace referencia a configurar direcciones IP manualmente. En este método, utilizamos una utilidad proporcionada por Windows 2000 para asignar una dirección IP. Windows 2000 proporciona el cuadro de diálogo **Propiedades del protocolo de Internet (TCP/IP)** para asignar manualmente una dirección IP a un host o dispositivo TCP/IP.

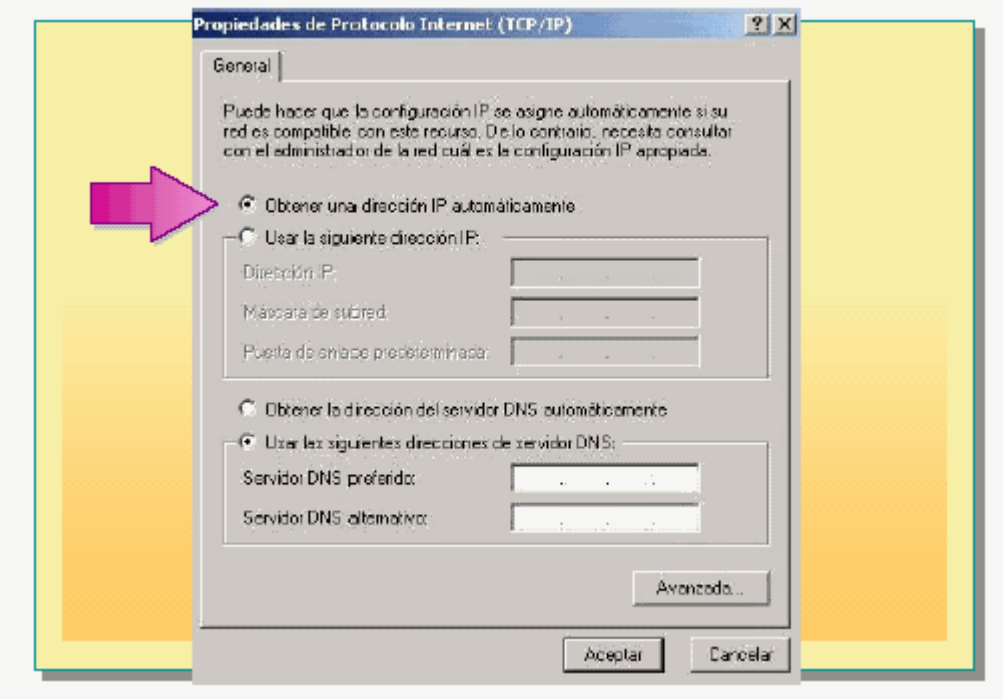
Abrir el cuadro de diálogo Propiedades de TCP/IP

1. 1. En el menú Inicio, seleccione Configuración y haga clic en Conexiones de red y de acceso telefónico.
2. 2. En la ventana **Conexiones de red y de acceso telefónico**, haga clic con el botón derecho en el icono **Conexión de área local**, y clic en **Propiedades**.
3. 3. En el cuadro de diálogo **Propiedades de la conexión de área local**, haga clic en **Protocolo de Internet (TCP/IP)**, y clic en **Propiedades** para mostrar el cuadro de diálogo **Propiedades del protocolo de Internet (TCP/IP)**.

En este cuadro de diálogo, haga clic en **Utilice la siguiente dirección IP** para introducir los valores de la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

En general, la mayoría de equipos sólo tiene un adaptador de red instalado y por ello únicamente requieren una sola dirección IP. Si un dispositivo, como un router, tiene instalados múltiples adaptadores de red, cada adaptador necesita su propia dirección IP.

DIRECCIONAMIENTO IP AUTOMÁTICO



De forma predeterminada, Windows 2000 está configurado para obtener una dirección IP automáticamente utilizando el protocolo de configuración de host dinámica (*Dynamic Host Configuration Protocol*, DHCP).

DHCP

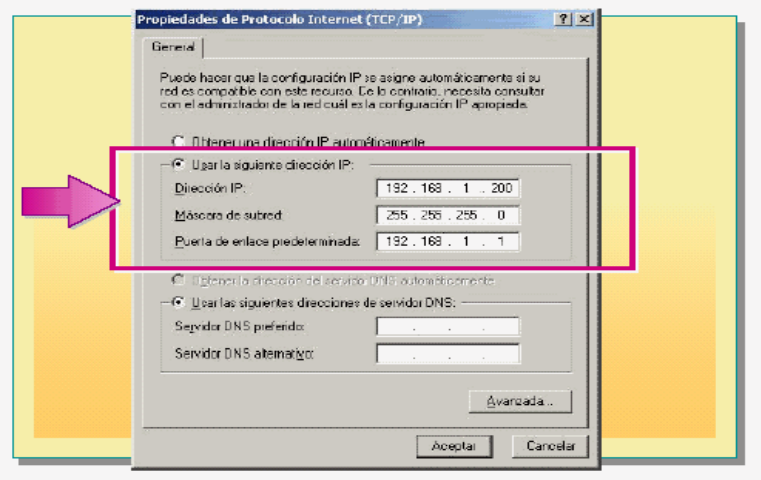
DHCP es un estándar de TCP/IP para simplificar la administración de la configuración y asignación de direcciones IP en una red interconectada. DHCP utiliza un servidor DHCP para gestionar la asignación dinámica de direcciones IP. Los servidores DHCP contienen una base de datos de direcciones IP que pueden asignarse a hosts de la red. Par utilizar DHCP en una red, los hosts deben estar habilitados para usar DHCP. Para habilitar DHCP, debemos hacer clic en **Obtener una dirección IP automáticamente**, que está seleccionado de forma predeterminada en Windows 2000.

DHCP reduce la complejidad y el trabajo de administración relacionado con la reconfiguración de equipos en redes basadas en TCP/IP. Cuando movemos un equipo de una subred a otra, debemos cambiar su dirección IP para reflejar el nuevo ID de red. DHCP nos permite asignar automáticamente una dirección IP a un host, denominado también cliente DHCP, desde una base de datos asignada a una subred. Además, cuando un equipo está sin conexión durante un determinado periodo de tiempo, DHCP puede reasignar su dirección IP.

Direcciones IP privadas automáticas (Automatic Private IP Addressing, APIPA)

Si no se puede localizar un servidor DHCP para asignar una dirección IP automáticamente, Windows 2000 determina una dirección en la clase de direccionamiento IP reservada por Microsoft, que va desde 169.254.0.1 hasta 169.254.255.254. Esta dirección sólo se usará hasta que se localice un servidor DHCP. Este método de obtener una dirección IP se denomina direccionamiento IP automático. No se asigna DNS, WINS o una puerta de enlace predeterminada porque el método está diseñado sólo para una red pequeña formada por un solo segmento.

Visualización de la configuración de TCP/IP

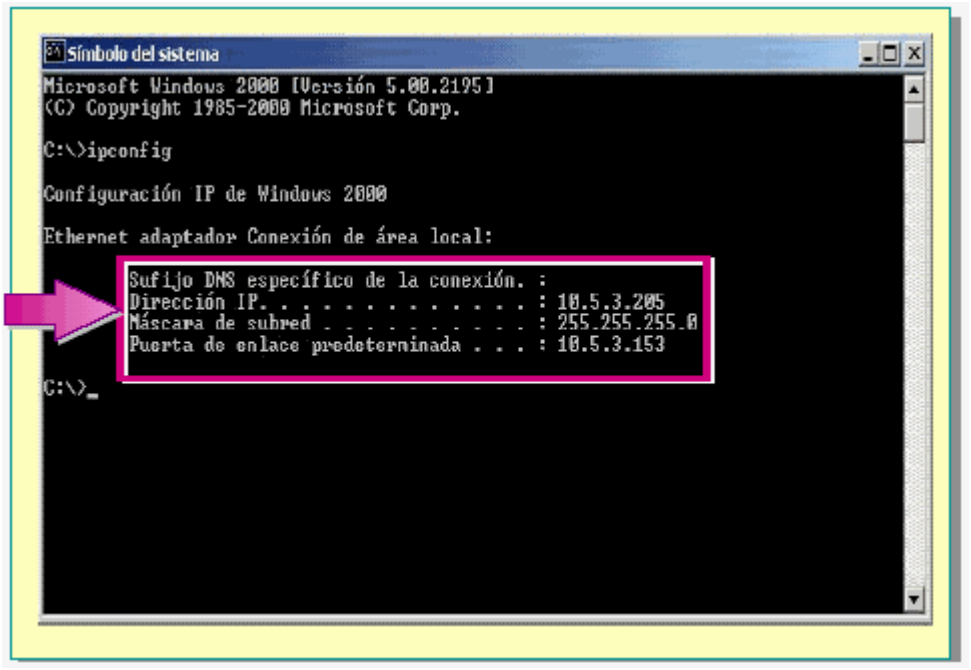


Podemos encontrarnos en situaciones en las que necesitemos ver la información de la dirección IP de un determinado equipo. Por ejemplo, si nuestro equipo no puede comunicarse con otros equipos de la red, u otros equipos no pueden comunicarse con el nuestro. En estas situaciones, necesitamos conocer la dirección IP de los otros equipos para poder resolver el problema.

Podemos utilizar el cuadro de diálogo **Propiedades del protocolo de Internet (TCP/IP)** para ver la información estática de TCP/IP. **Cuadro de diálogo Propiedades del protocolo de Internet (TCP/IP)** Utilizando el cuadro de diálogo **Propiedades del protocolo de Internet (TCP/IP)**, podemos determinar si la configuración de la dirección IP se ha realizado dinámica o estáticamente.

No obstante, si la dirección IP se ha configurado dinámicamente utilizando DHCP o ha sido configurada dinámicamente por Windows 2000, no podremos determinar los valores de las opciones de configuración de TCP/IP. Estas opciones incluyen la dirección IP, la máscara de subred y la puerta de enlace predeterminada. Únicamente podemos determinar estos valores si la configuración se ha realizado estáticamente.

VISUALIZACIÓN DE LA CONFIGURACIÓN DE TCP/IP UTILIZANDO IPCONFIG



Windows 2000 Y XP proporcionan una utilidad en línea de comandos denominada *Ipconfig* para visualizar la información de TCP/IP.

Ipconfig

La utilidad *Ipconfig* se utiliza para verificar, pero no para establecer, las opciones de configuración de TCP/IP en un host, incluyendo la dirección IP, la máscara de subred y la puerta de enlace predeterminada. La sintaxis del comando para esta utilidad es *ipconfig*.

Para iniciar la utilidad *Ipconfig*, escriba **ipconfig** en la línea de comandos. Se mostrarán los valores de los tres principales parámetros de configuración. Sin embargo, si utilizamos esta utilidad, no podremos determinar si se ha utilizado el método estático o el dinámico para asignar la dirección IP.

Ipconfig /all

Podemos obtener información más detallada utilizando la utilidad *Ipconfig* especificando el argumento **all**. Para utilizar la utilidad *Ipconfig* con este argumento, escriba **ipconfig /all** en la línea de comandos.

La pantalla muestra información sobre todas las opciones de configuración de TCP/IP. Podemos determinar si DHCP está habilitado. Si el valor del parámetro DHCP habilitado es Sí y se muestra la dirección IP de un servidor DHCP, significa que la dirección IP se ha obtenido utilizando DHCP.

Un servidor DHCP asigna una dirección IP a un cliente durante un periodo de tiempo determinado. Las etiquetas relacionadas con la obtención y expiración de asignaciones muestran información de cuando se obtuvo la asignación y cuando vence, respectivamente.

Si no había ningún servidor DHCP disponible para asignar una dirección IP y la dirección IP se asignó automáticamente, el término autoconfiguración precederá a la etiqueta de la dirección IP del equipo. La etiqueta Autoconfiguración habilitada sería Sí. Además, no se mostraría la dirección IP del servidor DHCP.

Seguridad en la Red

Hoy en día todos dependemos de la información que radica y generamos en nuestras computadoras; estos objetos ya no se encuentran aislados como en los 80´s y principios de los 90´s; si no por el contrario, hoy dependemos de una conexión física para podernos comunicar, el avance que se ha tenido con las redes nos ha permitido solucionar problemas y hacer provecho de sistemas que nos ayudan a manipulara la información.

Empresas, organizaciones y cualquier persona que utiliza una computadora envía y recibe correos electrónicos, comparte información de manera local o a nivel mundial, realiza transacciones, ofrece servicios y encuentra soluciones a sus requerimientos. Es así que la información se vuelve algo muy preciado tanto para los usuarios como para los Hackers. Es por eso que tenemos que tener una serie de precauciones para evitar que alguien no deseado busque en nuestra información y seamos presa fácil de extorsiones, fraudes y pérdidas irreparables.

Tipos de ataques

Ataques de intromisión: Este tipo de ataque es cuando alguien abre archivos, uno tras otro, en nuestra computadora hasta encontrar algo que le sea de su interés. Puede ser alguien externo o inclusive alguien que convive todos los días con nosotros. Cabe mencionar que muchos de los ataque registrados a nivel mundial, se dan internamente dentro de la organización y/o empresa.

Ataque de espionaje en líneas: Se da cuando alguien escucha la conversación y en la cual, él no es un invitado. Este tipo de ataque, es muy común en las redes inalámbricas y no se requiere, como ya lo sabemos, de un dispositivo físico conectado a algún cable que entre o salga del edificio. Basta con estar en un rango donde la señal de la red inalámbrica llegue, a bordo de un automóvil o en un edificio cercano, para que alguien esté espiando nuestro flujo de información.

Ataque de intercepción: Este tipo de ataque se dedica a desviar la información a otro punto que no sea la del destinatario, y así poder revisar archivos, información y contenidos de cualquier flujo en una red.

Ataque de modificación: Este tipo de ataque se dedica a alterar la información que se encuentra, de alguna forma ya validada, en computadoras y bases de datos. Es muy común este tipo de ataque en bancos y casas de bolsa. Principalmente los intrusos se dedican a cambiar, insertar, o eliminar información y/o archivos,

utilizando la vulnerabilidad del los sistemas operativos y sistemas de seguridad (atributos, claves de accesos, etc.).

Ataque de denegación de servicio: Son ataques que se dedican a negarles el uso de los recursos a los usuarios legítimos del sistema, de la información o inclusive de algunas capacidades del sistema. Cuando se trata de la información, esta, se es escondida, destruida o ilegible. Respecto a las aplicaciones, no se pueden usar los sistemas que llevan el control de la empresa, deteniendo su administración o inclusive su producción, causando demoras y posiblemente pérdidas millonarias. Cuando es a los sistemas, los dos descritos anteriormente son inutilizados. Si hablamos de comunicaciones, se puede inutilizar dispositivos de comunicación (tan sencillo como cortar un simple cable), como saturar e inundar con tráfico excesivo las redes para que estas colisionen.

Ataque de suplantación: Este tipo de ataque se dedica a dar información falsa, a negar una transacción y/o a hacerse pasar por un usuario conocido. Se ha puesto de moda este tipo de ataques; los "nuevos ladrones" ha hecho portales similares a los bancarios, donde las personas han descargado sus datos de tarjetas de crédito sin encontrar respuesta; posteriormente sus tarjetas de crédito son vaciadas.

Es importante mencionar, que así como se llevan estos tipos de ataques en medios electrónicos, muchas veces se llevan a cabo en archivos físicos (expedientes, archiveros con información en papel, y en otro tipo de medios con los que las personas están familiarizadas a trabajar todos los días (como teléfonos convencionales, celulares, cajeros automáticos, etc.); inclusive los ataques a computadoras, muchas veces, comienzan precisamente con información obtenida de una fuente física (papeles, basura, intervención de correo, cartas, estados de cuenta que llegan a los domicilios; o simplemente de alguien que vigila lo que hacemos).

Hago mención de estos últimos puntos, porque muchas veces pensamos que la intrusión, pérdida, alteración, inserción, bloqueo de información en sistemas, bloqueo de sistemas operativos y de dispositivos, suceden por casualidad o simplemente por que existen los Hackers.

Lo que motiva a un pirata informático y/o Hacker a realizar los ataques son: los *retos*, ya que ellos trabajan en generar códigos que pueden burlar la seguridad, infiltrarse en redes y sistemas para extraer o alterar la información sintiéndose así superiores; *codicia*, unos de los motivos más antiguos por lo que las personas delinquen, tratado de hacer "dinero fácil" y un *propósito mal intencionado* o también definido como vandalismo o terrorismo.

Los métodos tradicionales de los Hackers son: buscar comparticiones abiertas, contraseñas deficientes, fallas y vulnerabilidades en programación, desbordamiento de buffer y denegaciones de servicios. Los Métodos más avanzados son: Rastreo de redes conmutadas (transmisión de paquetes entre nodos o redes); métodos de falseamiento y enmascaramientos de IP; códigos malintencionados y virus.

Ingeniería social

Con este tipo de práctica, el intruso puede obtener horarios de trabajo, claves de acceso, nombres de empleados e infiltrarse indirectamente en la organización, empresa y/o inclusive en nuestras casas. Puede obtener información con una simple plática, siendo amigables y mintiendo con alguien que trabaja en la empresa y/o organización. También a través de una llama telefónica haciéndose pasar por un empleado que pide soporte técnico a la empresa que le proporciona dicho servicio, o también haciéndose pasar por algún agente bancario y/o de seguros que trata de vender o prestar su servicio y todo esto hecho vía telefónica. Es también común recibir un correo electrónico informado que se ha ganado un premio y se requieren algunos datos para enviar el supuesto premio a al domicilio.

Mejores prácticas para la seguridad informática

Las prácticas no son otra cosa que una cultura y educación que debemos adquirir para evitar problemas futuros en usos de equipos y sistemas. Hoy en día es tan común que usemos computadoras, cajeros automáticos, tecnologías de comunicaciones, redes e Internet, que no caemos en la cuenta de toda la que la información que manejamos, nuestra propia información, correos electrónicos, información a través de chat, datos bancarios, archivos de interés y todo nuestro trabajo cotidiano se encuentra precisamente manejado por computadoras y equipo que son vulnerables y que en un abrir y cerrar de ojos pueden sufrir de una ataque, alteraciones o descomposturas.

La seguridad en un equipo, nodo o computadora: Uno de los primero puntos a cubrir son las claves de acceso, no se deben usar claves que en su constitución

son muy comunes, como es el caso de las iniciales del nombre propio y la fecha de nacimiento, apodos o sobrenombres que todo mundo conoce, o constituirlas de solo letras o solo números; estos tipos de claves son en las que los intrusos, Hackers y ladrones buscan de primera mano; hay que hacer combinaciones de letras mayúsculas, minúsculas y números alternadamente. No hay que compartir las claves, es común que cuando alguien más necesita usar nuestros equipos, computadoras y sistemas les damos las claves de uso y muchas veces hasta en voz alta, enfrente de muchas personas que no son parte de la empresa las damos a conocer. Hay que cambiar periódicamente las claves de acceso, los equipos o computadoras que se encuentran más expuestos, tienen que tener un cambio más recurrente.

En cada nodo y servidor hay que usar antivirus, actualizarlo o configurarlo para que automáticamente integre las nuevas actualizaciones del propio software y de las definiciones o bases de datos de virus registrados.

Si los equipos, computadoras o servidores tienen niveles de permisos de uso de archivos y de recursos, hay que configurarlos de acuerdo a los requerimientos de la empresa o usuario, y no usar la configuración predeterminada que viene de fábrica, así como nombres y usuarios. Los intrusos, ladrones y Hackers conocen muy bien las configuraciones predeterminadas y son las que usan al momento de realizar un ataque.

En computadoras que utilicen sistemas operativos de Microsoft, hay que realizar actualizaciones periódicamente, ya que constantemente los Hacker y creadores de virus encuentran vulnerabilidades en dichos sistemas operativos. También, hay que utilizar programas que detecten y remuevan "spywares" (programas o aplicaciones que recopilan información sobre una persona u organización sin su conocimiento), existen diferente softwares que realizan esta tarea, algunos son gratuitos y trabajan muy bien; así la recomendación es contar con uno de ellos y realizar un escaneo periódico de el equipo o computadora.

La seguridad administrativa: Esta se basa en políticas y normas que se deben de implantar y seguir. Las políticas proporcionan las reglas que gobiernan el cómo deberían ser configurados los sistemas y cómo deberían actuar los empleados de una organización en circunstancias normales y cómo deberían reaccionar si se presentan circunstancias inusuales. Define lo que debería de ser la seguridad dentro de la organización y pone a todos en la misma situación, de modo que todo el mundo entienda lo que se espera de ellos.

Toda política debe de tener un propósito y procedimiento bien específico que articule claramente por qué fueron creadas tales políticas o procedimientos y qué beneficios se espera la organización derivada de las mismas.

Cada política y procedimiento debe tener una sección que defina su aplicabilidad. Por ejemplo: una política de seguridad debe aplicarse a todos los sistemas de cómputo y redes. Una política de información, puede aplicarse a todos los empleados.

La sección de responsabilidad de una política o procedimiento, define quién se hará responsable por la implementación apropiada del documento. Quienquiera que sea designado como el responsable de aplicar una política o procedimiento de ser capacitado de manera adecuada y estar conciente de los requerimientos del documento.

Las políticas de información definen qué información es confidencial y cual es de dominio público dentro de la organización, y cómo debe estar protegida esta misma. Esta política esta construida para cubrir toda la información de la organización.

Las políticas de seguridad definen los requerimientos técnicos para la seguridad en un sistema de cómputo y de redes. Define la manera en que un administrador de redes o sistema debe de configurar un sistema respecto a la seguridad que requiere la empresa o el momento. Esta configuración también afecta a los usuarios y alguno de los requerimiento establecidos en la política y debe de comunicarse a la comunidad de usuarios en general de una forma pronta, oportuna y explícita.

Las políticas de uso de las computadoras extienden la ley en lo que respecta a quién puede utilizar los sistemas de cómputo y cómo pueden ser utilizados. Gran parte de la información en esta política parece de simple sentido común, pero si las organizaciones no las establecen específicamente, toda la organización queda expuesta a demandas legales por parte de los empleados.

Las políticas de uso de Internet y correo electrónico se incluyen con frecuencia en la política más general del uso de las computadoras. Sin embargo, en ocasiones se plantea en una política aparte, debido a la naturaleza específica del uso de Internet. Las organizaciones conceden conectividad a Internet a sus empleados para que éstos puedan realizar sus labores con mayor eficacia y de este modo beneficia a las organizaciones. Desgraciadamente, Internet proporciona un mecanismo para que los empleados hagan uso de los recursos de cómputo.

Las políticas de respaldo y normalización de actividades después de un desastre tienen que ser muy bien especificadas para que en un lapso muy corto de tiempo, la empresa u organización regrese a sus actividades y las pérdidas económicas sean mínimas o nulas.

La seguridad lógica: Cada empresa debe de desarrollar un procedimiento para identificar la vulnerabilidad en sus sistemas de cómputo; normalmente las exploraciones son realizadas por el departamento de seguridad y los ajustes son realizados por los administradores del sistema canalizándolos a los programadores y/o proveedores del sistema. Existen algunas herramientas para realizar estas pruebas, también se puede recurrir a pruebas de desempeño y análisis de código, pero también se puede recurrir a la experiencia de uso de los usuarios.

Seguridad técnica: Las medidas técnicas de seguridad se ocupan de la implementación de los controles de seguridad sobre los sistemas de cómputo y de

red. Estos controles son manifestaciones de las políticas y los procedimientos de la organización.

En las empresas como en las casas ya se cuenta con conexiones permanentes a las redes o a Internet y estas deben de estar protegidas mediante muros de fuego que actúan de manera que su homónimo arquitectónico entre dos habitaciones de un edificio. Puede ser físico (equipo) ó lógico (software).

Las conexiones de acceso remoto pueden ser intervenidas para obtener acceso no autorizado hacia las organizaciones y, por consiguiente, deben de estar protegidas. Este tipo de conexiones pueden ser por marcación telefónica o atreves de Internet.

Puesto que estas conexiones entran a la red de la empresa o a la computadora tiene que tener un sistema de autentificación como los módems de retroalimentación (que contienen en si mecanismos de autentificación); las contraseñas dinámicas son apropiadas para utilizarse como un mecanismo de autentificación mientras las contraseña dinámica sea combinada con algo conocido por el usuario; también existen programas y dispositivos de encriptación para asegurar que la información no es altera desde su creación hasta su lectura por el receptor.

El monitoreo en redes debe de llevarse a cabo para detectar diversos tipos de actividades inesperadas de virus, códigos maliciosos o uso inapropiado de esta, existen programas como los sniffers para ver el tráfico o todo aquello que pasa por la red, también existen equipos como los IDS´s (Intrusión Detection System) que cuentan con mecanismos para hacer análisis de paquetes y errores en las redes.

La seguridad física: La seguridad física debe ser empleada junto con la seguridad administrativa y técnica para brindar una protección completa. Ninguna cantidad de seguridad técnica puede proteger la información confidencial si no se controla el acceso físico a los servidores, equipos y computadoras. Igualmente, las condiciones climáticas y de suministro de energía pueden afectar la disponibilidad de los sistemas de información.

El acceso físico es importante, todos los equipos delicados deben de estar protegidos del acceso no autorizado; normalmente esto se consigue concentrando los sistemas en un centro de datos. Este centro esta controlado de diferentes maneras, se puede limitar el acceso con dispositivos, o instalar cerraduras de combinación para restringir los accesos a empleados y personas ajenas a las instalaciones.

Los sistemas de cómputo son sensibles a las altas temperaturas. Los equipos de cómputo también generan cantidades significativas de calor. Las unidades de control de clima para los centros de cómputo o de datos deben de ser capaces de mantener una temperatura y humedad constante.

Los sistemas de extinción de incendios para los equipos deben ser los apropiados, estos no tienen que tener base de agua para que no dañen los equipos.

Para evitar pérdidas y daños físicos a equipos y computadoras hay que contar con una instalación eléctrica adecuada, no hay que saturar las tomas de corriente (que es muy común), se recomienda utilizar fuentes reguladas como no-breaks y reguladores para la protección de equipos. Si existen instalaciones específicas para los equipos y computadoras se recomienda utilizar fuentes redundantes y una planta de energía auxiliar.