

MODULO 4:

“Redes Informáticas”

Objetivos Específicos:

- Analizar los tipos de redes informáticas y su rol en la comunicación actual
- Reconocer las distintas topologías y las ventajas de la utilización de una red
- Comprender los beneficios de utilizar una red informática en la comunicación telefónica de la empresa

Contenidos Específicos:

Introducción a las Redes Informáticas ¿Qué es una Red Informática?

Servicios de una Red

Modelos OSI-TCP

Tipos de Redes:

Según su extensión

Según su nivel de acceso

Redes a nivel lógico

Topologías

Tipo Bus

Tipo Anillo

Tipo Estrella

Componentes de conexión

Medios de transmisión

Direccionamiento

IPV4-IPV6

Tecnologías de red

VPN

Protocolos de red

→ como DENWA IP-PBX utiliza esta tecnología



4.1 INTRODUCCION A LAS REDES INFORMATICAS

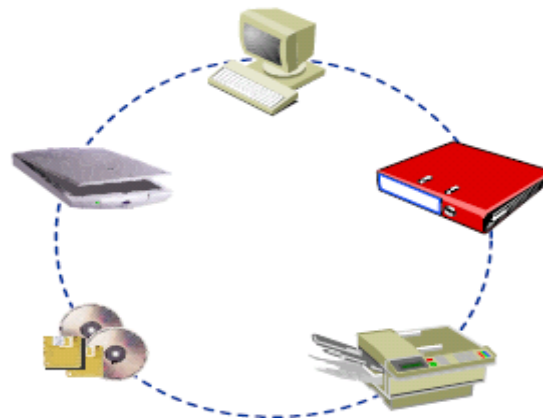
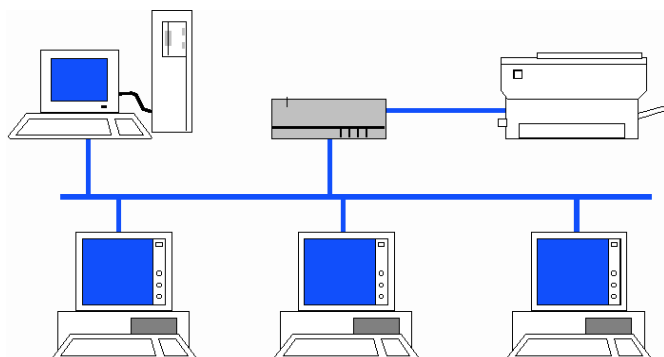
¿QUÉ ES UNA RED INFORMÁTICA?

Las redes informáticas surgieron como una necesidad de interconectar diferentes computadoras de una empresa o institución para poder así compartir recursos y equipos específicos. Como tal, debemos pensar en un soporte físico que abarque el cableado, las placas necesarias para las computadoras, y un conjunto de programas que formen el Sistema Operativo de la Red.

Se puede definir una red informática como un sistema de comunicación que conecta computadoras y otros equipos informáticos o dispositivos entre sí, con la finalidad de compartir información, recursos y por sobre todas las cosas, economiza el presupuesto de hardware y software.

Compartir recursos implica que se necesita menos Hardware a la hora de contar con los recursos necesarios. Recursos tales como:

- Dispositivos (Impresoras, almacenamientos, modems, ...)
- Transferencia de archivos entre sistemas
- Aplicaciones y Servicios
- Internet, etc.



Este concepto facilita en gran medida el trabajo en grupo y no solamente se puede conectar computadoras en un mismo entorno físico sino también permite conectar equipos separados por distancias geográficas extensas, como por ejemplo: una PC en Argentina puede conectarse sin inconvenientes con una PC en cualquier parte del mundo.

Con el beneficio de compartir información y recursos en una red, los usuarios de los sistemas informáticos de una organización podrán hacer un mejor uso de los mismos, mejorando de este modo el rendimiento global de la organización. Entre las ventajas que supone tener instalada una red, podemos citar las siguientes:

- Mayor facilidad en la comunicación entre equipos
- Reducción en el presupuesto para software
- Reducción en el presupuesto para hardware
- Posibilidad de organizar grupos de trabajo
- Mejoras en la administración de los equipos y programas
- Mejoras en la integridad de los datos
- Mayor seguridad para acceder a la información

4.2 Servicios de una Red

Podemos determinar los siguientes servicios.

a. Acceso a la red

Los servicios de acceso se encargan tanto de verificar la identidad del usuario, (para asegurar que sólo pueda acceder a los recursos para los que tiene permiso), como de permitir la conexión de usuarios a la red desde **lugares**

remotos .

b. Compartir Archivos

La posibilidad de compartir archivos es la prestación principal de las redes locales. La aplicación básica consiste en utilizar archivos de otros usuarios, sin necesidad de utilizar un pendrive, CD u otro medio de transporte de información.

La ventaja fundamental es la de disponer de carpetas en la red a los cuales un grupo de usuarios tenga acceso.



c. Impresión

Permite compartir impresoras entre varias computadoras de la red, lo cual evitará la necesidad de tener una impresora para cada equipo, con la consiguiente reducción en los costos. Las impresoras de red pueden ser conectadas a un servidor de impresión, que se encargará de gestionar la impresión de trabajos para los usuarios de la red, almacenando trabajos en espera (cola de impresión), asignando prioridades a los mismos, etc.



d. Información

Los servidores de información pueden almacenar bases de datos para su consulta por los usuarios de la red u otro tipo de información.



e. Acceso a Internet

Una de las prestaciones de Red que con el tiempo ha aumentado considerablemente su uso, es Internet.



Portapapeles

Lugares remotos:

Generalmente, el enlace entre lugares remotos se realiza a través de la red pública de teléfono, pero una organización podría crear sus propios enlaces WAN mediante satélites, microondas u otras tecnologías de comunicación.

Internet a grandes rasgos permite la posibilidad de configurar una PC con una conexión permanente a servicios en línea externos, de forma tal que los usuarios de la

Intranet no necesitan utilizar un modem personal para acceder a ellos.

Mediante un servidor de comunicaciones se puede mantener una línea permanente a alta velocidad que enlace la red local, Intranet, con Internet

El servidor puede estar equipado con una **NIC**, que activa la conexión cuando algún usuario de la red lo necesita. Cuando la conexión está activa, cualquier otro usuario puede compartirla, aunque en este caso las prestaciones de cada usuario serán menores que si tuvieran una conexión individual.

4.3 Modelos OSI-TCP

Existen diversos protocolos, estándares y modelos que determinan el funcionamiento general de las redes. Destacan el modelo **OSI** y el **TCP/IP**

. Cada modelo estructura el funcionamiento de una red de manera distinta: El modelo OSI cuenta con 7 capas muy definidas y con funciones diferenciadas y el TCP/IP con 4 capas diferenciadas pero que combinan las funciones existentes en las 7 capas del modelo OSI. Los protocolos están repartidos por las diferentes capas pero no están definidos como parte del modelo en sí, sino como entidades diferentes de normativas internacionales, de modo que el modelo OSI no puede ser considerado una arquitectura de red.

El modelo de Referencia OSI es una herramienta conceptual que se encarga de la conexión entre sistemas abiertos, esto es, sistemas abiertos a la comunicación con otros sistemas. Los principios en los que basó su creación son, una mayor definición de las funciones de cada capa, evitar agrupar funciones diferentes en la misma capa y una mayor simplificación en el funcionamiento del modelo en general.



Portapapeles

INTRANET: una intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.

NIC: Network Interface Card, es Un controlador de interfaz de red es un hardware componente que conecta un ordenador a una red informática. El controlador también puede ser denominado como un adaptador de red, o un adaptador de LAN

OSI: Open Systems Interconnection fue creado por la ISO. (International Organization for Standardization)


TCP/IP: La familia de protocolos de Internet es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.

APLICACIÓN	Transferencia de Archivos, intercambio de Mensajes
PRESENTACION	Representación y Formateo de los datos
SESION	Organización y Sincronización del Intercambio de Datos
TRANSPORTE	Canal de transferencia de mensajes de una aplicación a otra
RED	Direcciones y mejor ruta
ENLACE	Acceso al medio. Detección de errores. Retransmisión
FÍSICA	Transmisión binaria. Definiciones eléctricas y mecánicas del sistema físico



Portapapeles

ARPANET: La red de computadoras Advanced Research Projects Agency Network (ARPANET) fue creada por encargo del Departamento de Defensa de los Estados Unidos ("DoD" por sus siglas en inglés) como medio de comunicación para los diferentes organismos del país. El primer nodo se creó en la Universidad de California, Los Ángeles y fue la espina dorsal de Internet hasta 1990, tras finalizar la transición al protocolo TCP/IP iniciada en 1983.

El modelo TCP/IP fue desarrollado antes que OSI. Es más simple y está formado por menos capas. Este modelo es el implantado actualmente a nivel mundial: Fue utilizado en **ARPANET**  y es utilizado actualmente a nivel global en Internet y redes locales. Su nombre deriva de los dos principales protocolos que lo conforman: TCP en la Capa de transporte e IP en la Capa de red. Se compone de 4 capas.

MODELO OSI

APLICACIÓN		
PRESENTACIÓN		
SESIÓN		
TRANSPORTE		
RED		
ENLACE		
FÍSICA		

MODELO TCP/IP

HTTP – SMTP – FTP – TELNET
– MODBUS – DHCP – SNMP

UDP – TCP

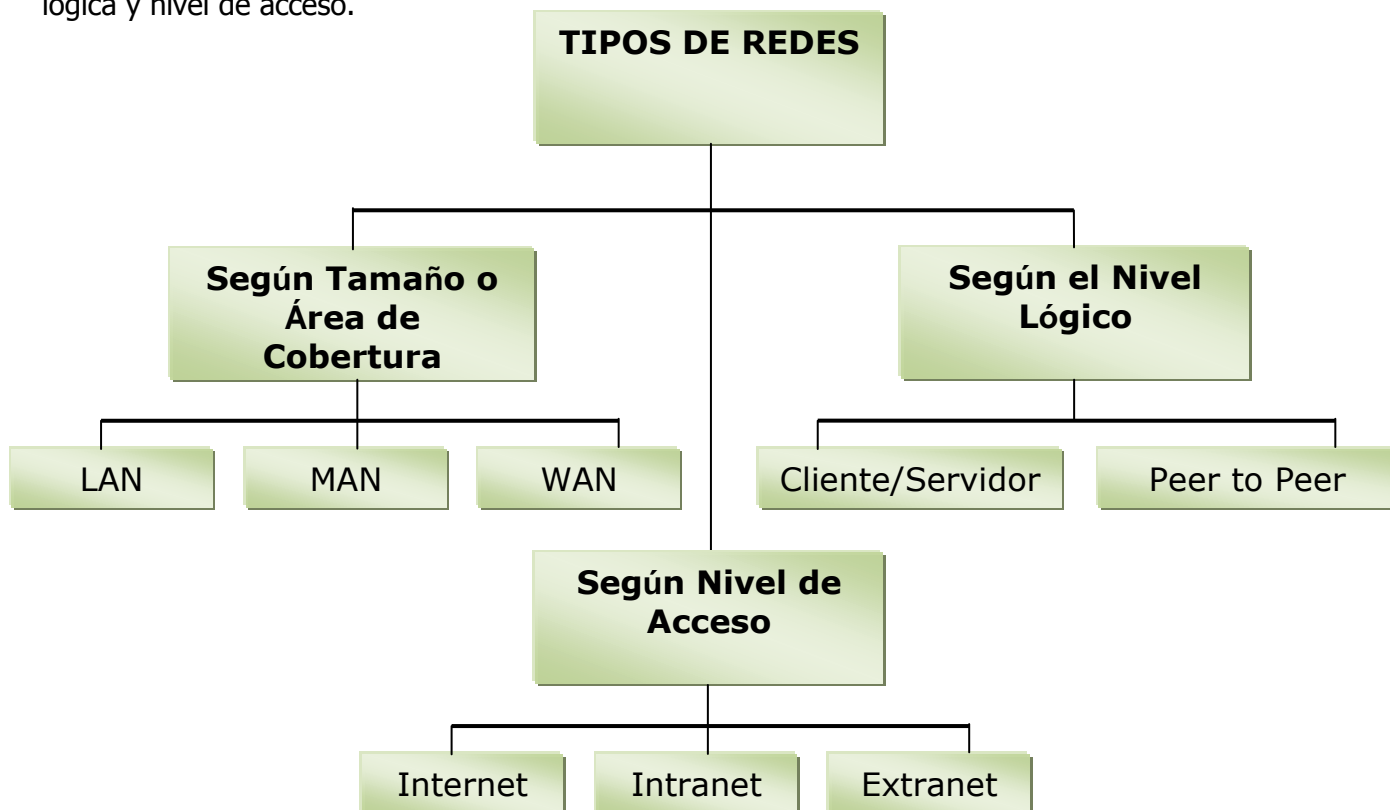
IP

CSMA/ CD

ETHERNET II ó IEEE 802.3

4.4 Niveles - TIPOS DE REDES

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



TIPOS DE REDES SEGÚN SU EXTENSIÓN

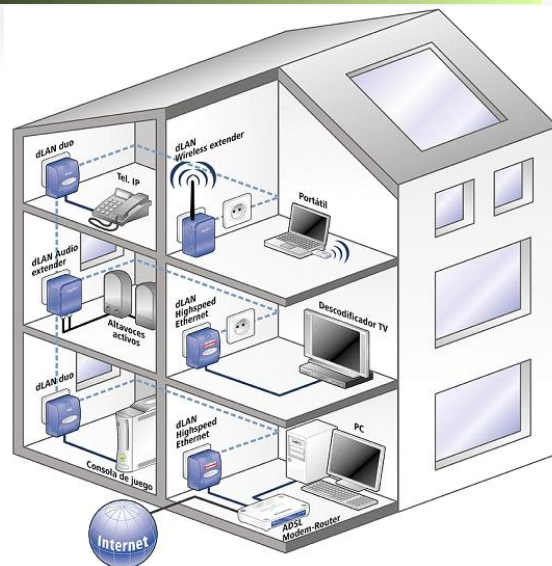
Al definir las redes conectadas por medio de una placa específica, se las puede catalogar con respecto a su área de cobertura en tres tipos:

- LAN (Local Área Network/Redes de Área Local)
- MAN (Metropolitan Área Network/Redes de Área Metropolitana)
- WAN (Wide Area Network/Redes de Área Extensa)

a. LAN

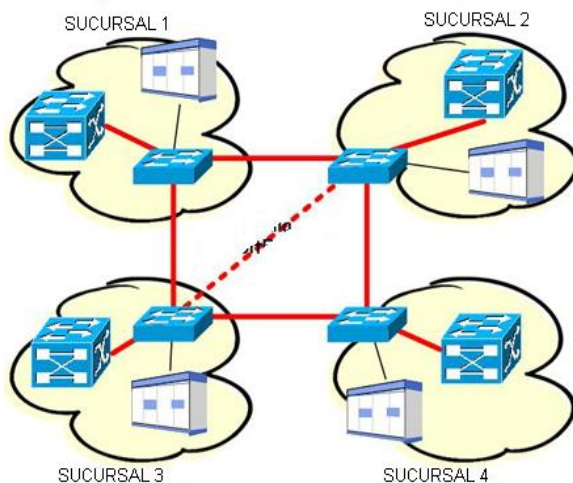
Una LAN es un sistema de interconexión de equipos informáticos basado en líneas de alta velocidad y que suele abarcar, como mucho, un edificio.

Un caso típico de LAN es cuando 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. Se pueden compartir archivos con otros usuarios. Los accesos a estos archivos están controlados por un administrador de la LAN. Además, permite compartir el acceso a Internet de una computadora (Servidor) a las que están conectadas a ella.



b. MAN

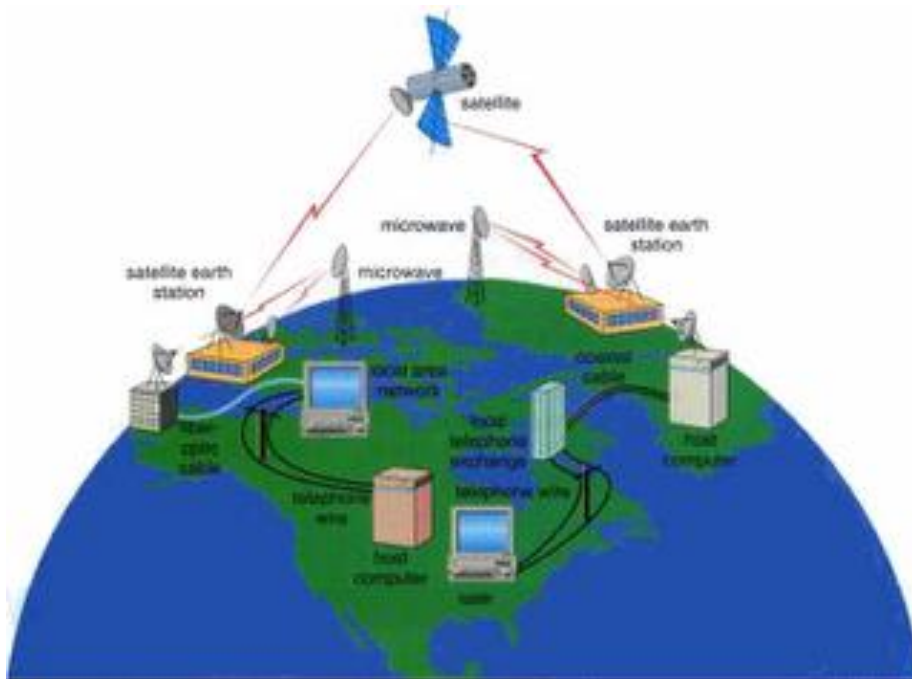
Una MAN es un sistema de interconexión de equipos informáticos distribuidos en una zona que abarque diversos edificios, o pueden conectarse equipos dentro de ciudades vecinas. Por ejemplo, podría utilizarse para la conexión de equipos por medio de la línea telefónica de dos sucursales de una empresa para compartir datos. Este tipo de redes se utiliza normalmente para interconectar redes de área local.



c. WAN

Una WAN es un sistema de interconexión de equipos informáticos geográficamente dispersos, que pueden estar incluso en continentes distintos. El sistema de conexión para estas redes normalmente involucra a redes públicas de transmisión de datos.

Esta red une equipos y/o redes a nivel mundial. Una de las redes WAN más conocidas es INTERNET la cual permite conectar computadoras entre sí a través del mundo entero.



TIPOS DE REDES A NIVEL LÓGICO

Podemos definir dos categorías de redes que son aplicables a nivel lógico (nivel Software), estas son las redes:

- Cliente - Servidor
- Peer to Peer (Igual a igual)

a. Cliente - Cliente

Este tipo de red cuenta con una computadora principal a la que denominamos. SERVIDOR especialmente configurado para centralizar datos, brindar seguridad y ofrecer servicios a los CLIENTES (usuarios).





Portapapeles

RAM: La memoria de acceso aleatorio (en inglés: random-access memory), memoria desde donde el procesador recibe las instrucciones y guarda los resultados.

WINDOWS NT: (New Technology) familia de sistemas operativos producidos por Microsoft, de la cual la primera versión fue publicada en julio de 1993. Microsoft concibió una nueva línea de sistemas operativos orientados a estaciones de trabajo y servidores de red. Un sistema operativo con interfaz gráfica propia, estable y con características similares a los sistemas de red UNIX.

LINUX: Sistema operativo gratuito, o de bajo coste en caso de ser una distribución, basado en Unix. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU).

Servidores:

Un servidor es una computadora que ejecuta un sistema operativo de red y ofrece servicios de red a las estaciones de trabajo. El servidor debe ser un sistema fiable con un procesador potente, con discos de alta capacidad y con gran cantidad de memoria **RAM** y un sistema operativo de red como **Windows NT** o **Linux**.

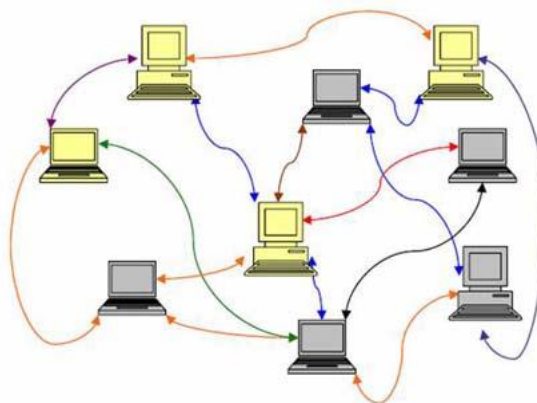


Cliente:

Los equipos que se conectan a los servidores son llamados Clientes o equipos concurrentes, los cuales dependen de este servidor central para efectuar su conexión a la red, llegando en algunos casos hasta depender de la carga del sistema operativo ya que en este caso el equipo cliente no cuenta con unidades de disco debiendo trabajar en memoria principal y descargar todos los datos en el disco del servidor.

b. Peer to Peer

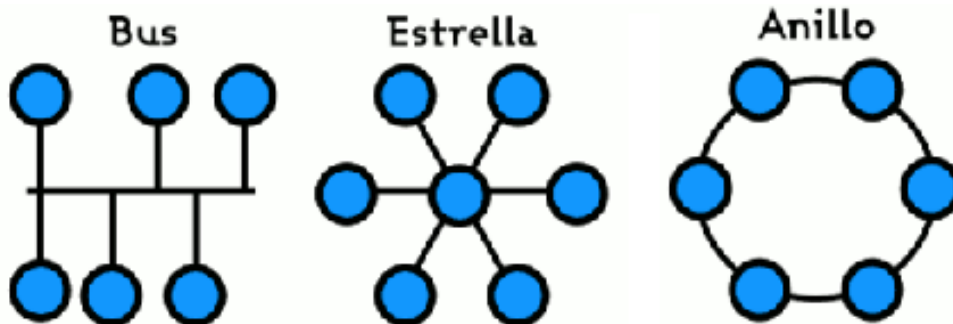
Este tipo de red se caracteriza porque los equipos conectados a la red cuentan con la misma jerarquía, también comparten datos y periféricos al igual que la Servidor-Cliente, pero sin un equipo central que controle el acceso a estos recursos.



4.5 TOPOLOGÍAS DE RED

La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse. La arquitectura o topología de red es la disposición física en la que se conectan los nodos, es decir, la conjunción del método de cableado y la metodología de conexión, hay varios tipos de topologías encontrándose entre las más frecuentes y accesibles:

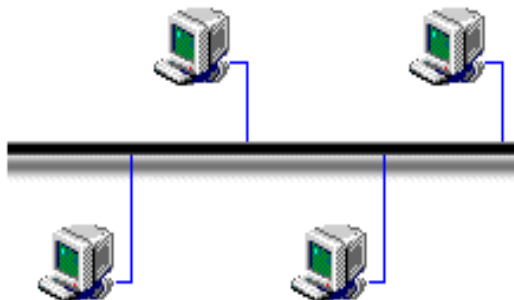
- Tipo Bus
- Tipo Anillo
- Tipo Estrella



La selección de alguna de estas topologías para la creación de una red informática, va a depender de las variables disponibles, como economía, velocidad necesaria, espacio disponible, etc.

TIPO BUS

En este tipo de topología todos los equipos se conectan sobre un mismo tramo de cable. 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.



Portapapeles

HUB: Concentrador. Dispositivo capaz de enlazar físicamente varios ordenadores de forma pasiva, enviando los datos para todos los ordenadores que estén conectados, siendo éstos los encargados de discriminar la información.

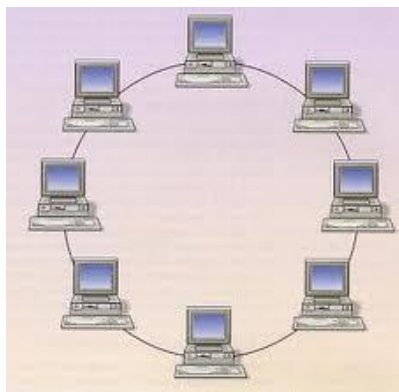


SWITCH: Un conmutador o switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

También representa una desventaja ya que si el cable se rompe, ninguno de los servidores siguientes tendrá acceso a la red.

TIPO ANILLO

En esta topología la señal viaja codificada, pero a diferencia de la topología tipo bus, esta es activa lo cual significa que cada equipo que participa a la red absorbe la señal, la reconstruye y la retransmite lo cual desencadena en una desventaja, en el caso de falla de algún integrante de la red esta falla, ocasionando que se caiga el sistema. Además, tiene un sistema de transmisión llamado paso de testigo, de esta forma el equipo que transmite bloquea el equipo vecino logrando de esta forma que la línea esté libre, ya que en este tipo de red la transmisión

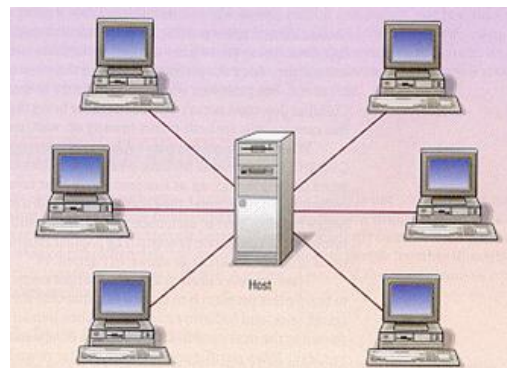


de datos también es **half-duplex**, y de esta forma llega hasta el equipo que contiene el mismo código y este la absorbe. Otro detalle que puede agregarse es que los datos viajan en un solo sentido y se asume que es horario.

TIPO ESTRELLA

Esta topología es una de las más utilizadas hoy en día. En esta red todos los equipos van a estar conectados entre sí, no directamente, sino por medio de un HUB o concentrador el cual cumple la función de una especie de central telefónica, interconectando todas las máquinas. En este caso como mayormente se utiliza cable de par trenzado el sistema

de datos es **full-duplex**, logrando de esta forma mayor velocidad de transmisión y recepción de datos. El sistema de transmisión es codificando la señal inicial, la cual al ser escuchada por el equipo con el mismo código es decodificado.



Portapapeles

HALF DUPLEX:

semidúplex, significa que el método o protocolo de envío de información es bidireccional pero no simultáneo. Es utilizado en las telecomunicaciones para definir a un sistema que es capaz de mantener una comunicación bidireccional, enviando y recibiendo mensajes.

FULL DUPLEX:

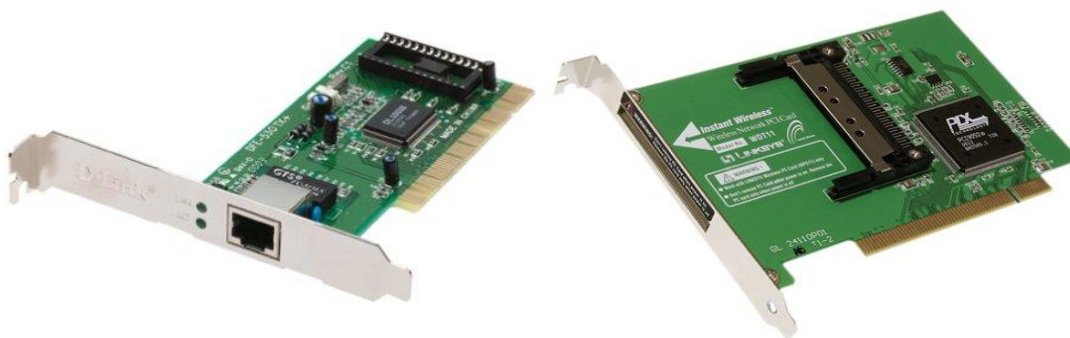
Característica de las redes de comunicación que permite la entrada y salida (envío y recepción) de datos simultáneamente. Todas las tarjetas de red existentes disponen de Full Duplex.

4.6 Componentes de una Conexión de Red

Los dispositivos de conexión de redes son aquellos que hacen posible conectar computadoras entre sí o redes entre sí.

Al hablar de una red es indispensable mencionar una placa de red o Nic. La NIC puede ser definida como la Placa de Red propiamente dicha, la cual conecta computadoras entre sí por medio de un cable u ondas celulares.

Aquí un ejemplo de las diferentes NIC Comunes (**PCI**) Para conexión con medios físicos (cables) e inalámbricas.



Placas para puerto **PMCIA** (Para computadoras portátiles), para medios físicos e inalámbricos



Modem:

Un módem es un dispositivo que sirve para enviar una señal llamada moduladora mediante otra señal llamada portadora. Permite conectar la PC a la línea telefónica y por ende a otras computadoras o la placa CABLE-MODEM que permite conectar la PC a Internet por medio de cable de la televisión.

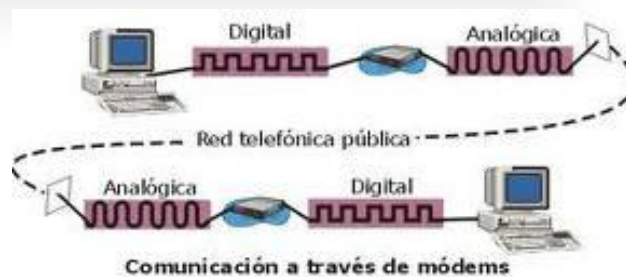


Portapapeles

PCI: Un Peripheral Component Interconnect (PCI, "Interconexión de Componentes Periféricos") consiste en un bus de ordenador estándar para conectar dispositivos periféricos directamente a su placa base.

PMCIA: es el acrónimo de Personal Computer Memory Card International Association, una asociación Internacional centrada en el desarrollo de tarjetas de memoria para ordenadores personales que permiten añadir al ordenador nuevas funciones. Existen muchos tipos de dispositivos disponibles en formato de tarjeta PCMCIA: módems, tarjeta de sonido, tarjeta de red.

El modulador emite una señal denominada portadora. Generalmente, se trata de una simple señal eléctrica sinusoidal de mucha mayor frecuencia que la señal moduladora. La señal moduladora constituye la información que se prepara para una transmisión (un módem prepara la información para ser transmitida, pero no realiza la transmisión). La moduladora modifica alguna característica de la portadora (que es la acción de modular), de manera que se obtiene una señal, que incluye la información de la moduladora. Así el demodulador puede recuperar la señal moduladora original, quitando la portadora.



Tipos de módems:

Existen tres tipos diferentes de módems, puesto que los distintos entornos de comunicación requieren diferentes métodos de envío de datos. Estos entornos se pueden dividir en dos áreas relacionadas con el ritmo de las comunicaciones:

- Asíncrona.
- Síncrona.

El tipo de módem que utiliza una red depende de si el entorno es asíncrono o síncrono.

a. Comunicación asíncrona (Async)

La comunicación asíncrona, conocida como «async», es probablemente la forma de conexión más extendida. Esto es debido a que async se desarrolló para utilizar las líneas telefónicas.



Portapapeles


V.32: Protocolo estándar para módems full-duplex para el envío y recepción de datos a través de líneas telefónicas a 4.800 o 9.600 bps. Los módems V.32 automáticamente ajustan sus velocidades de transmisión basados en la calidad de las líneas.

Cada carácter (letra, número o símbolo) se introduce en una cadena de bits. Cada una de estas cadenas se separa del resto mediante un bit de inicio de carácter y un bit de final de carácter. Los dispositivos emisor y receptor deben estar de acuerdo en la secuencia de bit inicial y final. El equipo destino utiliza los marcadores de bit inicial y final para planificar sus funciones relativas al ritmo de recepción, de forma que esté preparado para recibir el siguiente byte de datos.

La comunicación no está sincronizada. No existe un dispositivo reloj o método que permita coordinar la transmisión entre el emisor y el receptor. El equipo emisor sólo envía datos y el equipo receptor simplemente los recibe. A continuación, el equipo receptor los comprueba para asegurarse de que los datos recibidos coinciden con los enviados. Entre el 20 y el 27 por 100 del tráfico de datos en una comunicación asíncrona se debe al control y coordinación del tráfico de datos. La cantidad real depende del tipo de transmisión, por ejemplo, si se está utilizando la paridad (una forma de comprobación de errores).

Las transmisiones asíncronas en líneas telefónicas pueden alcanzar hasta 28.800 bps. No obstante, los métodos de compresión de datos más recientes permiten pasar de 28.800 bps a 115.200 bps en sistemas conectados directamente.

Control de errores. Debido al potencial de errores que puede presentar, async puede incluir un bit especial, denominado bit de paridad, que se utiliza en un esquema de corrección y comprobación de errores, denominado comprobación de paridad. En la comprobación de paridad, el número de bits enviados debe coincidir exactamente con el número de bits recibidos.

El estándar de módem original **V.32**  no proporcionaba control de errores.

Coordinación de los estándares. Los módems asíncronos, o serie, son más baratos que los módems síncronos, puesto que los asíncronos no necesitan la circuitería y los componentes necesarios para controlar el ritmo que de las transmisiones síncronas requieren los módems síncronos.

b. Comunicación síncrona

La comunicación síncrona confía en un esquema temporal coordinado entre dos dispositivos para separar los grupos de bits y transmitirlos en bloques conocidos como «tramas». Se utilizan caracteres especiales para comenzar la sincronización y comprobar periódicamente su precisión.



Portapapeles

SDLC: Synchronous Data Link Control, controlador de enlace de datos síncrono) se utiliza para nombrar el protocolo diseñado por IBM para enlaces síncronos a través de una línea para la capa 2 del modelo OSI de comunicaciones. Como su nombre implica, es un protocolo síncrono, lo que supone la transmisión de la señal de reloj con los datos.




HDLC (control de enlace síncrono de datos) es un protocolo de comunicaciones de propósito general punto a punto y multipunto, que opera a nivel de enlace de datos. Se basa en ISO 3309 e ISO 4335. Surge como una evolución del anterior SDLC. Proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros, por lo que ofrece una comunicación confiable entre el transmisor y el receptor.

Dado que los bits se envían y se reciben en un proceso controlado (sincronizado) y cronometrado, no se requieren los bits de inicio y final. Las transmisiones se detienen cuando se alcanza el final de una trama y comienzan, de nuevo, con una nueva. Este enfoque de inicio y final es mucho más eficiente que la transmisión asíncrona, especialmente cuando se están transfiriendo grandes paquetes de datos.

Los protocolos síncronos realizan un número de tareas que no realizan los protocolos asíncronos. Principalmente son:

- Formatear los datos en bloques.
- Agregar información de control.
- Comprobar la información para proporcionar el control de errores.

Los principales protocolos de comunicaciones síncronas son:

- Control síncrono de enlace de datos (SDLC , Synchronous Data Link Control).
- Control de enlace de datos de alto nivel (HDLC , High-level Data Link Control).
- Protocolo de comunicaciones síncronas binarias (bysnc ).

La comunicación síncrona se utiliza en la mayoría de todas las comunicaciones de red y digitales. Por ejemplo, si está utilizando líneas digitales para conectar equipos remotos, debería utilizar módems síncronos, en lugar de asíncronos, para conectar el equipo a la línea digital. Normalmente, su alto precio y complejidad ha mantenido a los módems síncronos fuera del mercado de los equipos personales.

Línea digital abonada asimétrica (ADSL, Asymetric Digital Subscriber Line)

La última tecnología de módem disponible es una línea digital abonada asimétrica (ADSL).

Esta tecnología convierte las líneas telefónicas actuales de par trenzado en vías de acceso para las comunicaciones de datos de alta velocidad y multimedia. Estas nuevas conexiones pueden transmitir por encima de los 8 Mbps para el abonado y de hasta 1Mbps desde el propio abonado.



Portapapeles

BYSNC: Binario síncrono Comunicación (BSC o Bisync) es un IBM protocolo de enlace, anunció en 1967 después de la introducción del System/360. Se sustituye el síncrono de transmisión-recepción (STR), protocolo que se utiliza con las computadoras de segunda generación. La intención era que las normas comunes de gestión de enlace podría ser utilizado con tres alfabetos diferentes para codificar mensajes

La tecnología requiere un hardware especial, incluyendo un módem ADSL en cada extremo de la conexión. Además, necesita un cableado de banda amplia, que está disponible actualmente en muy pocas localizaciones y existe un límite en la longitud de conexión.

Hub:

El Hub o concentrador es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Los hubs han dejado de ser utilizados, debido al gran nivel de colisiones y tráfico de red que propician.



Switch:

Un switch (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de ordenadores similar al Hub, pero que tiene la capacidad de poder "conocer" las computadoras que tiene conectadas en sus puertos y poder administrar el ancho de banda en el tráfico de información de una red, repartiéndola de manera pareja según se vaya necesitando de manera eficiente.



Router:

Son dispositivos electrónicos de interconexión que mantienen el tráfico fluyendo eficientemente sobre caminos predefinidos en una interconexión de redes complejas, ofreciendo un encaminamiento "inteligente" hacia el destino de la información.



4.7 Medios de transmisión

Cables

El cable utilizado para formar una red corresponde a medio de transmisión. Los tres factores que se deben tener en cuenta a la hora de elegir el cable que será el medio de transmisión para una red son:

- Velocidad de transmisión que se quiere conseguir.
- Distancia máxima entre ordenadores que se van a conectar.
- Nivel de ruido e interferencias habituales en la zona que se va a instalar la red.

Los cables más utilizados son el par trenzado, el cable coaxial y la fibra óptica.

a. Par trenzado

Es uno de los más antiguos en el mercado y en algunos tipos de aplicaciones es el más común. Consiste en dos alambres de cobre o a veces de aluminio aislados con una cobertura plástica, con un grosor de 1 mm aproximadamente. Los pares trenzados se agrupan bajo una cubierta que actúa de malla protectora en cables multipares de pares trenzados (de 2, 4, 8, hasta 300 pares).



Un ejemplo de par trenzado es el sistema de telefonía, ya que la mayoría de aparatos se conectan a la central telefónica por medio de un par trenzado.

Actualmente, se han convertido en un estándar en el ámbito de las redes LAN (Local Area Network) como medio de transmisión en las redes de acceso a usuarios (típicamente cables de 4 pares trenzados). A pesar que las propiedades de transmisión de cables de par trenzado son inferiores (sobre todo ante perturbaciones extremas), su gran adopción se debe al costo, flexibilidad y facilidad de instalación, así como las mejoras tecnológicas constantes introducidas en enlaces de mayor velocidad, longitud, etc.

Debajo de la aislación coloreada existe otra capa de aislación también de polietileno, que contiene en su composición una sustancia antioxidante para evitar la corrosión del cable. El conducto sólo tiene un diámetro de aproximadamente medio milímetro, y más la aislación el diámetro puede superar el milímetro.

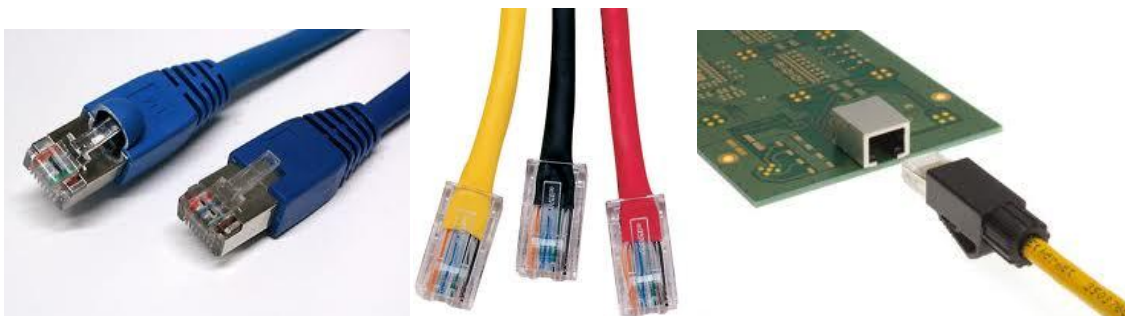
Sin embargo es importante aclarar que habitualmente este tipo de cable no se maneja por unidades, sino por pares y grupos de pares, paquete conocido como cable multipar. Todos los cables del multipar están trenzados entre sí con el objeto de mejorar la resistencia de todo el grupo hacia diferentes tipos de interferencia electromagnética externa. Por esta razón surge la necesidad de poder definir colores para los mismos que permitan al final de cada grupo de cables

conocer qué cable va con cual otro. Los colores del aislante están normalizados a fin de su manipulación por grandes cantidades. Para Redes Locales los colores estandarizados son:

- Naranja/Blanco – Naranja
- Verde/Blanco – Verde
- Blanco/Azul – Azul
- Blanco/Marrón – Marrón

En telefonía, es común encontrar dentro de las conexiones grandes cables telefónicos compuestos por cantidades de pares trenzados, aunque perfectamente identificables unos de otros a partir de la normalización de los mismos. Los cables una vez fabricados unitariamente y aislados, se trenzan de a pares de acuerdo al color de cada uno de ellos; aún así, estos se vuelven a unir a otros formando estructuras mayores: los pares se agrupan en subgrupos, los subgrupos de agrupan en grupos, los grupos se agrupan en superunidades, y las superunidades se agrupan en el denominado cable.

De esta forma se van uniendo los cables hasta llegar a capacidades de 2200 pares; un cable normalmente está compuesto por 22 superunidades; cada subunidad está compuesta por 12 pares aproximadamente; esta valor es el mismo para las unidades menores. Los cables telefónicos pueden ser armados de 6, 10, 18, 20, 30, 50, 80, 100, 150, 200, 300, 400, 600, 900, 1200, 1500, 1800 ó 2200 pares.



Categorías de cable de par trenzado

Cada categoría especifica características eléctricas para el cable: atenuación, capacidad de la línea e impedancia.

Existen actualmente 8 categorías dentro del cable UTP:

Categoría 1: Este tipo de cable esta especialmente diseñado para redes telefónicas, es el típico cable empleado para teléfonos por las compañías telefónicas. Alcanzan como máximo velocidades de hasta 1 Mbps.



Categoría 2: De características idénticas al cable de categoría 1, pero alcanzan como máximo velocidades de hasta 4 Mbps.

Categoría 3: Es utilizado en redes de ordenadores de hasta 16 Mbps. de velocidad.

Categoría 4: Esta definido para redes de ordenadores tipo anillo como Token Ring con un ancho de banda de hasta 20 Mhz y con una velocidad de 20 Mbps.

Categoría 5: Es un estándar dentro de las comunicaciones en redes LAN. Es capaz de soportar comunicaciones de hasta 100 Mbps. con un ancho de banda de hasta 100 Mhz. Este tipo de cable es de 8 hilos, es decir cuatro pares trenzados.

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



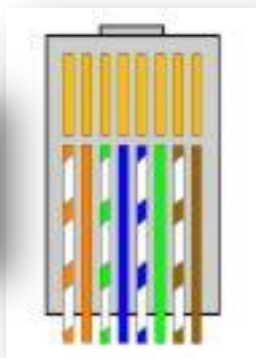
Categoría 5e: Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque si esta diferenciada por los diferentes organismos.

Categoría 6: No está estandarizada aunque ya esta utilizándose. Se definirán sus características para un ancho de banda de 250 Mhz.

Categoría 7: No está definida y mucho menos estandarizada. Se definirá para un ancho de banda de 600 Mhz. El gran inconveniente de esta categoría es el tipo de conector seleccionado que es un RJ-45 de 1 pines.

En esta tabla podemos ver para las diferentes categorías, teniendo en cuenta su ancho de banda, cual sería las distancia máxima recomendada sin sufrir atenuaciones que hagan variar la señal:

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



Cable de par trenzado con conector RJ45 en su extremo.

b. Cable Coaxial

Se usa normalmente en la conexión de redes con topología de Bus. La velocidad de transmisión que podemos alcanzar con el cable coaxial llega solo hasta 10Mbps, en cambio con el par trenzado se consiguen 100Mbps.

Este cable está estructurado por los siguientes componentes de adentro hacia fuera:

- Un núcleo de cobre sólido, o de acero con capa de cobre.
- Una capa de aislante que recubre el núcleo o conductor,



este aislante tiene la función de guardar una distancia uniforme del conductor con el exterior.

- Una capa de blindaje metálico, generalmente cobre o aleación de aluminio entretejido (a veces solo consta de un papel metálico) cuya función es la de mantenerse lo más apretado posible para eliminar las interferencias, además de que evita de que el eje común se rompa o se tuerza demasiado, ya que si el eje común no se mantiene en buenas condiciones, trae como consecuencia que la señal se vaya perdiendo, y esto afectaría la calidad de la señal.
- Por último, tiene una capa final de recubrimiento, de color negro en el caso del cable coaxial delgado o amarillo en el caso del cable coaxial grueso, este recubrimiento normalmente suele ser de vinilo ó polietileno uniforme para mantener la calidad de las señales.

c. Fibra Óptica

A partir de 1970, surgen los cables que transportan luz en lugar de una corriente eléctrica. Estos cables son mucho más ligeros, de menor diámetro y repetidores que los tradicionales cables metálicos. Además, la densidad de información que son capaces de transmitir, es también mucho mayor. En un cableado de fibra óptica, el emisor está formado por un láser que emite un potente rayo de luz, que varía en función de la señal eléctrica que le llega. El receptor está constituido por un fotodiodo, que transforma la luz incidente de nuevo en señales eléctricas.



Es como un cable (tan parecido que al verlo exteriormente no se nota la diferencia), que en lugar de conducir corriente eléctrica, transmite luz.

Esa luz es modulada de forma similar a las ondas de radio, y puede por lo tanto transportar información de cualquier tipo de un extremo al otro.

Como la frecuencia de la luz "portadora" es muchísimo más alta que la de las ondas de radio, es capaz de transportar mayor cantidad de información.

La fibra óptica está compuesta por filamentos de vidrio de alta pureza muy compactos. El grosor de una fibra es como la de un cabello humano aproximadamente. Fabricadas a alta temperatura con base en silicio, su proceso de elaboración es controlado por medio de computadoras, para permitir que el índice de refracción de su núcleo, que es la guía de la onda luminosa, sea uniforme y evite las desviaciones.

La velocidad de transmisión de es muy alta, desde 10 Mb/seg. y llegando hasta 1 Gb/seg. en algunas instalaciones especiales.

Como características de la fibra podemos destacar que son compactas, ligeras, con bajas pérdidas de señal, amplia capacidad de transmisión y un alto grado de confiabilidad ya que son inmunes a las interferencias electromagnéticas de radio-frecuencia. Las fibras ópticas no conducen señales eléctricas, conducen rayos luminosos, por lo tanto son ideales para incorporarse en cables sin ningún componente conductivo y pueden usarse en condiciones peligrosas de alta tensión.



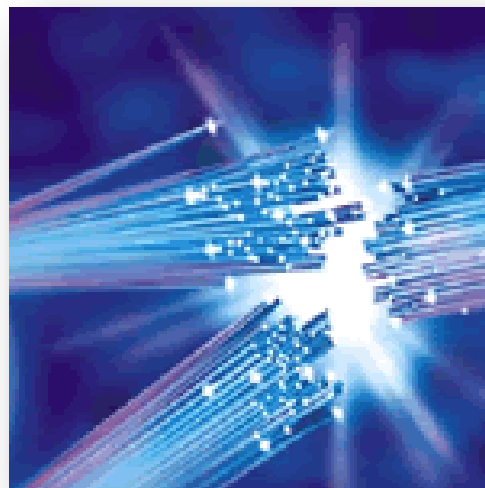
En la última década la fibra óptica ha pasado a ser una de las tecnologías más avanzadas que se utilizan como medio de transmisión. Los logros con este material fueron más que satisfactorios, desde lograr una mayor velocidad y disminuir casi en su totalidad ruidos e interferencias, hasta multiplicar las formas de envío en comunicaciones y recepción por vía telefónica.

La fibra óptica está compuesta por filamentos de vidrio de alta pureza muy compactos. El grosor de una fibra es como la de un cabello humano aproximadamente. Fabricadas a alta temperatura con base en silicio, su proceso de elaboración es controlado por medio de computadoras, para permitir que el índice de refracción de su núcleo, que es la guía de la onda luminosa, sea uniforme y evite las desviaciones.

Como características de la fibra podemos destacar que son compactas, ligeras, con bajas pérdidas de señal, amplia capacidad de transmisión y un alto grado de confiabilidad ya que son inmunes a las interferencias electromagnéticas de radio-frecuencia. Las fibras ópticas no conducen señales eléctricas, conducen rayos luminosos, por lo tanto son ideales para incorporarse en cables sin ningún componente conductivo y pueden usarse en condiciones peligrosas de alta tensión

Las fibras ópticas se caracterizan por pérdidas de transmisión realmente bajas, una capacidad extremadamente elevada de transporte de señales, dimensiones mucho menores que los sistemas convencionales, instalación de repetidores a lo largo de las líneas (gracias a la disminución de las pérdidas debidas a la transmisión), una mayor resistencia frente a las interferencias, etc.

La transmisión de las señales a lo largo de los conductores de fibra óptica se verifica gracias a la



reflexión total de la luz en el interior de los conductores ópticos. Dichos conductores están constituidos por fibras delgadas, hechas de vidrios ópticos altamente transparentes con un índice de reflexión adecuado, rodeada por un manto de varias milésimas de espesor, compuesto por otro vidrio con índice de reflexión inferior al del que forma el ánima. La señal que entra por un extremo de dicho conductor se refleja en las paredes interiores hasta llegar al extremo de salida, siguiendo su camino independientemente del hecho de que la fibra esté o no curvada.

Estos cables son la base de las modernas autopistas de la información, que hacen técnicamente posible una interconectividad a escala planetaria.

Los tipos de fibra óptica son:

a) Fibra multimodal

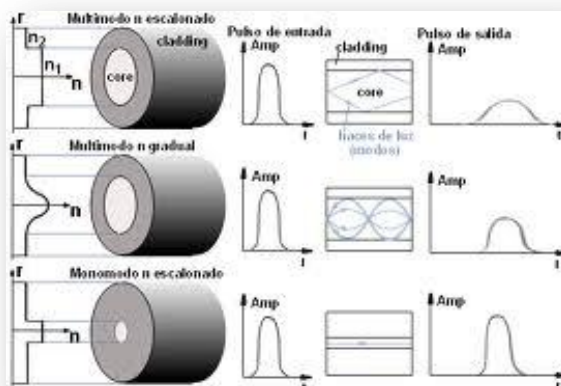
En este tipo de fibra viajan varios rayos ópticos reflejándose a diferentes ángulos, los diferentes rayos ópticos recorren diferentes distancias y se desfasan al viajar dentro de la fibra. Por esta razón, la distancia a la que se puede transmitir está limitada.

b) Fibra multimodal con índice graduado

En este tipo de fibra óptica el núcleo está hecho de varias capas concéntricas de material óptico con diferentes índices de refracción. En estas fibras el número de rayos ópticos diferentes que viajan es menor y, por lo tanto, sufren menos el severo problema de las multimodales.

c) Fibra monomodal:

Esta fibra óptica es la de menor diámetro y solamente permite viajar al rayo óptico central. No sufre del efecto de las otras dos pero es más difícil de construir y manipular. Es también más costosa pero permite distancias de transmisión mayores.



En comparación con el sistema convencional de cables de cobre, donde la atenuación de sus señales es de tal magnitud que requieren de repetidores cada dos kilómetros para regenerar la transmisión, en el sistema de fibra óptica se pueden instalar tramos de hasta 70 Km. sin que haya necesidad de recurrir a repetidores, lo que también hace más económico y de fácil mantenimiento este material.

Con un cable de seis fibras se puede transportar la señal de más de cinco mil canales o líneas principales, mientras que se requiere de 10,000 pares de cable de cobre convencional para brindar servicio a ese mismo número de usuarios, con la desventaja que este último medio ocupa un gran espacio en los canales y requiere de grandes volúmenes de material, lo que también eleva los costes.

Originalmente, la fibra óptica fue propuesta como medio de transmisión debido a su enorme ancho de banda; sin embargo, con el tiempo se ha introducido en un amplio rango de aplicaciones además de la telefonía, automatización industrial, computación, sistemas de televisión por cable y transmisión de información de imágenes astronómicas de alta resolución entre otros.

En un sistema de transmisión por fibra óptica existe un transmisor que se encarga de transformar las ondas electromagnéticas en energía óptica o en luminosa. Por ello, se le considera el componente activo de este proceso. Cuando la señal luminosa es transmitida por las pequeñas fibras, en otro extremo del circuito se encuentra un tercer componente al que se le denomina detector óptico o receptor, cuya misión consiste en transformar la señal luminosa en energía electromagnética, similar a la señal original. El sistema básico de transmisión se compone en este orden, de señal de entrada, amplificador, fuente de luz, corrector óptico, línea de fibra óptica (primer tramo), empalme, línea de fibra óptica (segundo tramo), corrector óptico, receptor, amplificador y señal de salida.



Se puede decir que en este proceso de comunicación, la fibra óptica funciona como medio de transporte de la señal luminosa, generado por el transmisor de LED's (diodos emisores de luz) y lasers. Los diodos emisores de luz y los diodos lasers son fuentes adecuadas para la transmisión mediante fibra óptica, debido a que su salida se puede controlar rápidamente por medio de una

corriente de polarización. Además su pequeño tamaño, su luminosidad, longitud de onda y el bajo voltaje necesario para manejarlos son características atractivas.

WIRELESS (WLAN)

Una WLAN es un sistema de comunicaciones de datos que transmite y recibe datos utilizando ondas electromagnéticas, en lugar del par trenzado, coaxial o fibra óptica utilizado en las LAN convencionales, y que proporciona conectividad inalámbrica de igual a igual (peer to peer).

Las WLAN se encuadran dentro de los estándares desarrollados por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) para redes locales inalámbricas.

El estándar 802.11b es un estándar de redes WLAN que opera en la frecuencia de los 2.4Ghz (banda no licenciada de Radio Frecuencia). La transmisión de datos es hasta de 11 Mbps.

La principal ventaja de este tipo de redes (WLAN), que no necesitan licencia para su instalación, es la libertad de movimientos que permite a sus usuarios, ya que la posibilidad de conexión sin hilos entre diferentes dispositivos elimina la necesidad de compartir un espacio físico común y soluciona las necesidades de los usuarios que requieren tener disponible la información en todos los lugares por donde puedan estar trabajando. Además, a esto se añade la ventaja de que son mucho más sencillas de instalar que las redes de cable y permiten la fácil reubicación de los terminales en caso necesario.



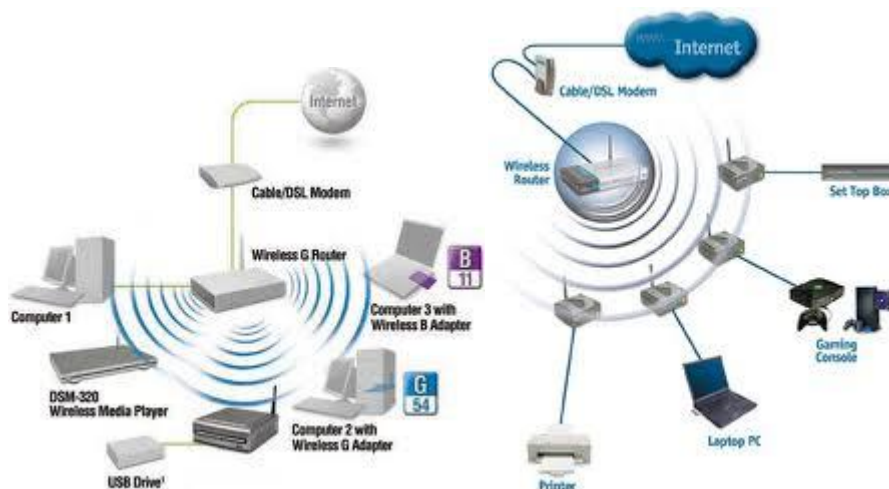
ENLACES INALAMBRICOS

El principio de funcionamiento de un enlace óptico al aire libre, es similar al de un enlace de fibra óptica, sin embargo el medio de transmisión no es una fibra de vidrio sino el aire.

Las comunicaciones ópticas al aire libre son una alternativa de gran ancho de banda a los enlaces de fibra óptica o a los cables eléctricos. Las prestaciones de este



tipo de enlace pueden verse empobrecidas por la lluvia fuerte o niebla intensa, pero son inmunes a las interferencias eléctricas y no necesitan permiso de las autoridades responsables de las telecomunicaciones.

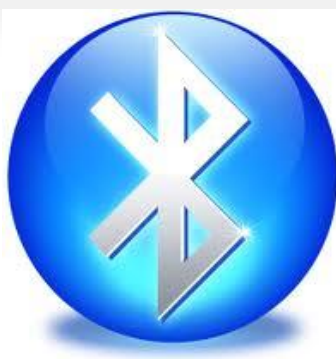


Las mejoras en los emisores y detectores ópticos han incrementado el rango y el ancho de banda de los enlaces ópticos al aire libre, al tiempo que reducen los costos. Se puede transmitir voz o datos sobre estos enlaces a velocidades de hasta 45 Mbits/s. El límite para comunicaciones fiables se encuentra sobre los dos kilómetros.

Bluetooth

Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz. Los principales objetivos que se pretenden conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

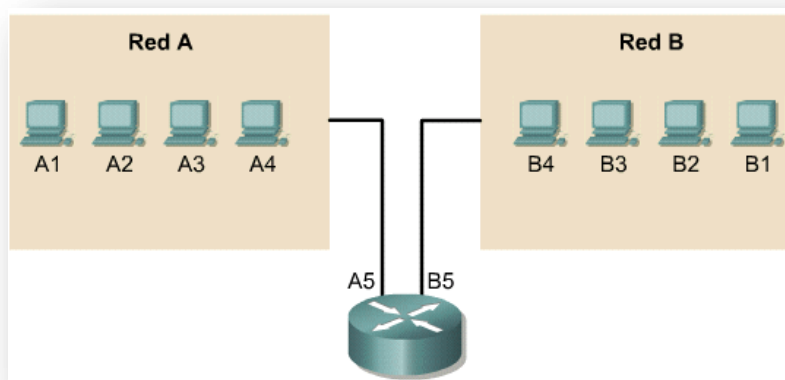


Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a sectores de las telecomunicaciones y la informática personal, como PDA, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras o cámaras digitales.

4.6 DIRECCINAMIENTO IP

Para que dos sistemas se comuniquen, se deben poder identificar y localizar entre sí. Aunque las direcciones de la Figura no son direcciones de red reales, representan el concepto de agrupamiento de las direcciones.

Este utiliza A o B para identificar la red y la secuencia de números para identificar el host individual.

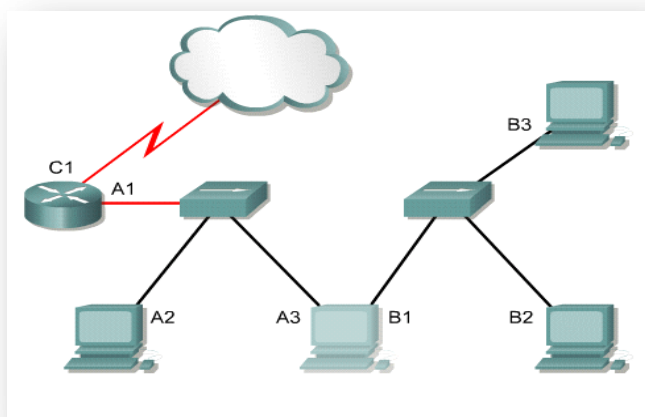


Aunque estas direcciones no son direcciones de red reales, representan y muestran el concepto de agrupación de direcciones. Se utiliza la letra A o B para identificar la secuencia de redes y de números para identificar al host individual. La combinación de letra (dirección de red) y el número (dirección de host) crea una dirección única para cada dispositivo de la red.

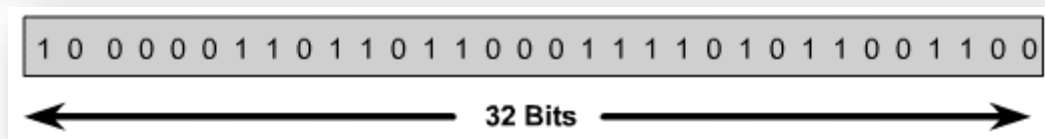
Un computador puede estar conectado a más de una red. En este caso, se le debe asignar al sistema más de una dirección. Cada dirección identificará la conexión del computador a una red diferente. No se suele decir que un dispositivo tiene una dirección sino que cada uno de los puntos de conexión (o interfaces) de dicho dispositivo tiene una dirección en una red. Esto permite que otros computadores localicen el dispositivo en una determinada red.

La combinación de letras (dirección de red) y el número (dirección del host) crean una dirección única para cada dispositivo conectado a la red. Cada computador conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP. Esta dirección, que opera en la Capa 3, permite que un computador localice otro computador en la red.

Todos los computadores también cuentan con una dirección física exclusiva, conocida como dirección MAC. Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.



Una dirección IP es una secuencia de unos y ceros de 32 bits. La Figura muestra un número de 32 bits de muestra.



Para que el uso de la dirección IP sea más sencillo, en general, la dirección aparece escrita en forma de cuatro números decimales separados por puntos. Por ejemplo, la dirección IP de un computador es 192.168.1.2. Otro computador podría tener la dirección 128.10.2.1. Esta forma de escribir una dirección se conoce como formato decimal punteado.

En esta notación, cada dirección IP se escribe en cuatro partes separadas por puntos. Cada parte de la dirección se conoce como octeto porque se compone de ocho dígitos binarios.

Por ejemplo, la dirección IP 192.168.1.8 sería 11000000.10101000.00000001.00001000 en una notación binaria. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros.

Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si sólo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos.

Tanto los números binarios como los decimales de la Figura representan a los mismos valores, pero resulta más sencillo apreciar la notación decimal punteada.

Binario: 11000000.10101000.00000001.00001000 y 11000000.10101000.00000001.00001001
Decimal: 192.168.1.8 y 192.168.1.9

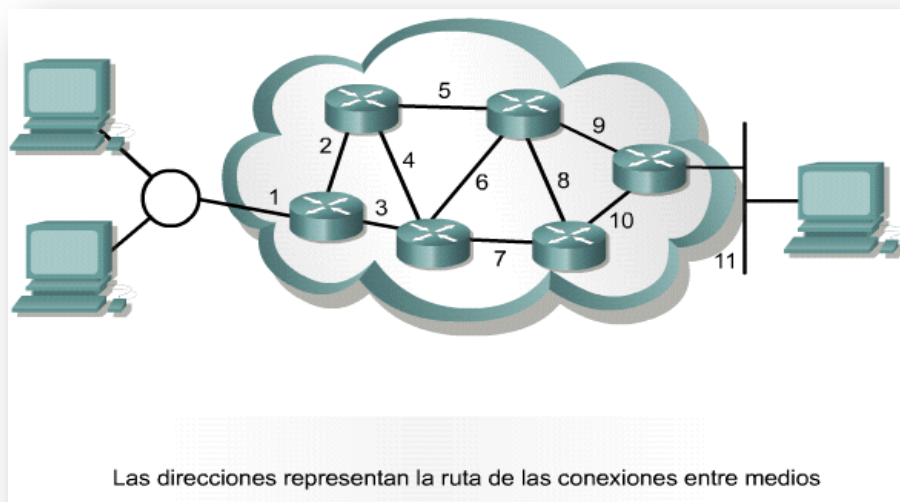
Los números binarios y decimales representan los mismos valores pero es mucho más fácil ver con los valores decimales punteados. Este es uno de los problemas más comunes que se encuentran al trabajar directamente con los números binarios. Las largas cadenas de unos y ceros repetidos aumentan la probabilidad de errores de transposición y omisión.

Este es uno de los problemas frecuentes que se encuentran al trabajar directamente con números binarios. Las largas cadenas de unos y ceros que se repiten hacen que sea más probable que se produzcan errores de transposición y omisión.

Resulta más sencillo observar la relación entre los números 192.168.1.8 y 192.168.1.9, mientras que 11000000.10101000.00000001.00001000 y 11000000.10101000.00000001.00001001 no son fáciles de reconocer. Al observar los binarios, resulta casi imposible apreciar que son números consecutivos.

IPV4 - DIRECCIONAMIENTO

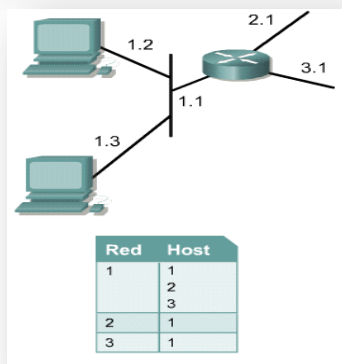
Un Router envía los paquetes desde la red origen a la red destino utilizando el protocolo IP. Los paquetes deben incluir un identificador tanto para la red origen como para la red destino.



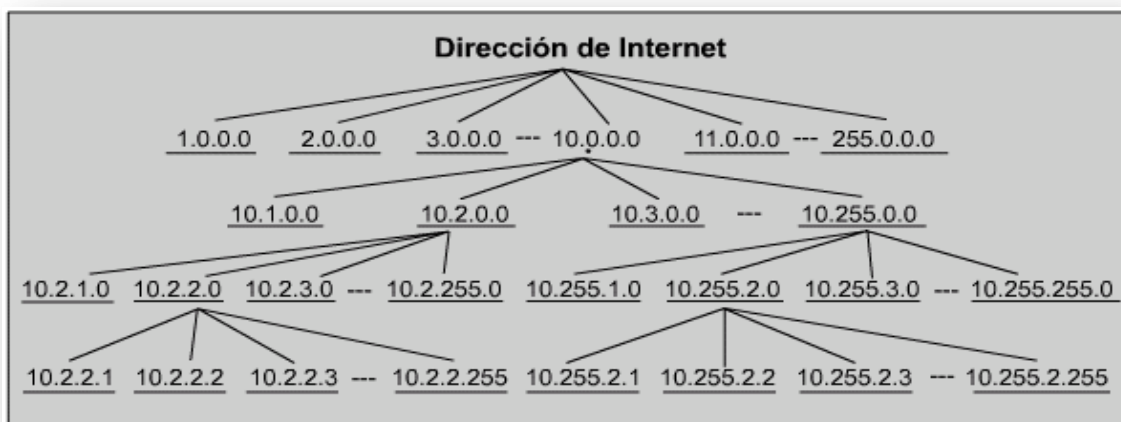
Utilizando la dirección IP de una red destino, un Router puede enviar un paquete a la red correcta. Cuando un paquete llega a un Router conectado a la red destino, este utiliza la dirección IP para localizar el computador en particular conectado a la red.

Este sistema funciona de la misma forma que un sistema nacional de correo. Cuando se envía una carta, primero debe enviarse a la oficina de correos de la ciudad destino, utilizando el código postal. Dicha oficina debe entonces localizar el destino final en la misma ciudad utilizando el domicilio. Es un proceso de dos pasos.

De igual manera, cada dirección IP consta de dos partes. Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red.



Como muestra la Figura, cada octeto varía de 0 a 255. Cada uno de los octetos se divide en 256 subgrupos y éstos, a su vez, se dividen en otros 256 subgrupos con 256 direcciones cada uno. Al referirse a una dirección de grupo inmediatamente arriba de un grupo en la jerarquía, se puede hacer referencia a todos los grupos que se ramifican a partir de dicha dirección como si fueran una sola unidad.



Este tipo de dirección recibe el nombre de dirección jerárquica porque contiene diferentes niveles. Una dirección IP combina estos dos identificadores en un solo número. Este número debe ser un número exclusivo, porque las direcciones repetidas harían imposible el enrutamiento.

La primera parte identifica la dirección de la red del sistema. La segunda parte, la parte del host, identifica qué máquina en particular de la red.

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas.

Clase de dirección	Cantidad de redes	Cantidad de hosts por red
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (Multicast)	No es aplicable	No es aplicable

* El intervalo de direcciones 127.x.x.x está reservado como dirección de loopback, con propósitos de prueba y diagnóstico

Clase de dirección IP:	Bits de mayor peso	Primer intervalo de dirección de octeto	Número de bits en la dirección de red
Clase A	0	0 - 127 *	8
Clase B	10	128 - 191	16
Clase C	110	192 - 223	24
Clase D	1110	224 - 239	28

El primer paso para determinar qué parte de la dirección identifica la red y qué parte identifica el host es identificar la clase de dirección IP.

Clase de dirección	Bits de mayor peso	Intervalo de dirección del primer octeto	Número de bits en la dirección de red	Número de redes	Número de hosts por red
Clase A	0	0-127	8	126	16,777,216
Clase B	10	128-191	16	16,384	65,536
Clase C	110	192-223	24	2,097,152	254
Clase D	1110	224-239	28	No es aplicable	No es aplicable

DIRECCIONES IP CLASE A, B, C, D, Y E

Para adaptarse a redes de distintos tamaños y para ayudar a clasificarlas, las direcciones IP se dividen en grupos llamados clases.

Clase A	Red	Host		
Octet	1	2	3	4

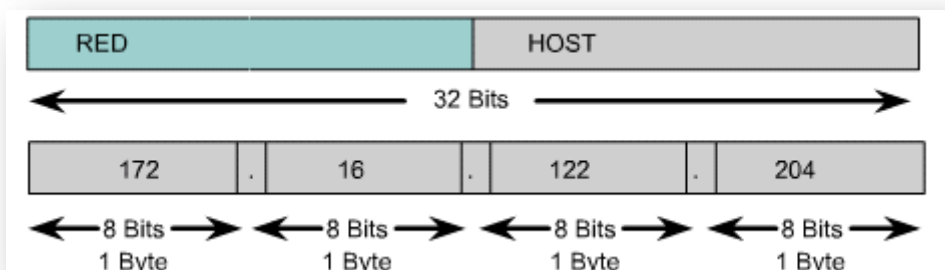
Clase B	Red		Host	
Octet	1	2	3	4

Clase C	Red			Host
Octet	1	2	3	4

Clase D	Host			
Octet	1	2	3	4

Las direcciones Clase D se utilizan para grupos de multicast. No hay necesidad de asignar octetos o bits a las distintas direcciones de red o de host. Las direcciones Clase E se reservan para fines de investigación solamente.

Esto se conoce como direccionamiento classful. Cada dirección IP completa de 32 bits se divide en la parte de la red y parte del host.



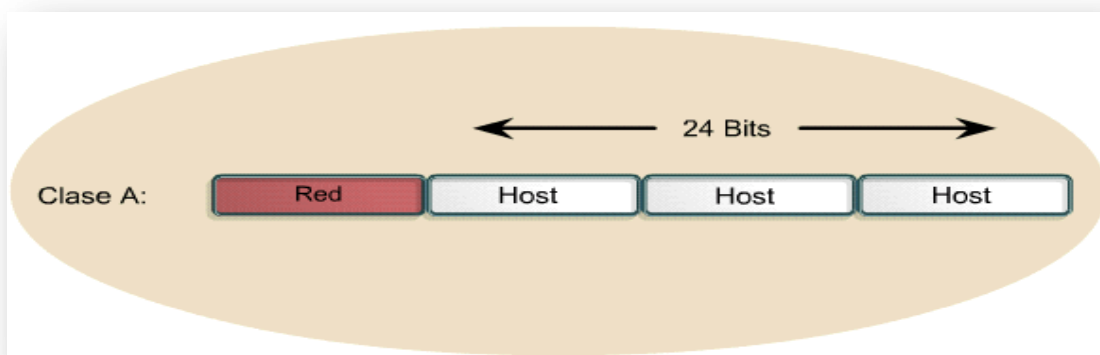
Una dirección IP siempre se divide en una parte de red y una parte de host. En un esquema de direccionamiento con clases, estas divisiones tienen lugar en los límites de los octetos.

Un bit o una secuencia de bits al inicio de cada dirección determinan su clase. Son cinco las clases de direcciones IP como muestra la Figura

Clase de dirección IP	Intervalo de dirección IP (Valor decimal d)
Clase A	1-126 (00000001-01111110) *
Clase B	128-191 (10000000-10111111)
Clase C	192-223 (11000000-11011111)
Clase D	224-239 (11100000-11101111)
Clase E	240-255 (11110000-11111111)

Determine la clase basándose en el valor decimal del primer octeto *127 (01111111), es una dirección clase A reservada para pruebas loopback y no puede ser asignada a una red.

La dirección Clase A se diseñó para admitir redes de tamaño extremadamente grande, de más de 16 millones de direcciones de host disponibles.



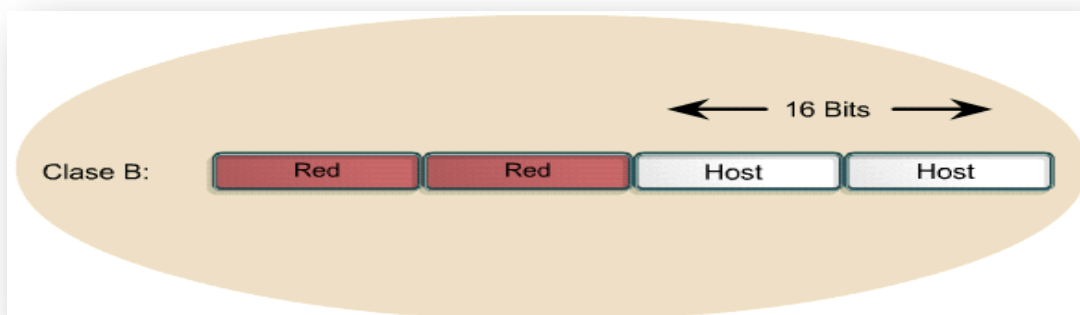
Las direcciones IP Clase A utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones host.

El primer bit de la dirección Clase A siempre es 0. Con dicho primer bit, que es un 0, el menor número que se puede representar es 00000000, 0 decimal.

El valor más alto que se puede representar es 01111111, 127 decimal. Estos números 0 y 127 quedan reservados y no se pueden utilizar como direcciones de red. Cualquier dirección que comience con un valor entre 1 y 126 en el primer octeto es una dirección Clase A.

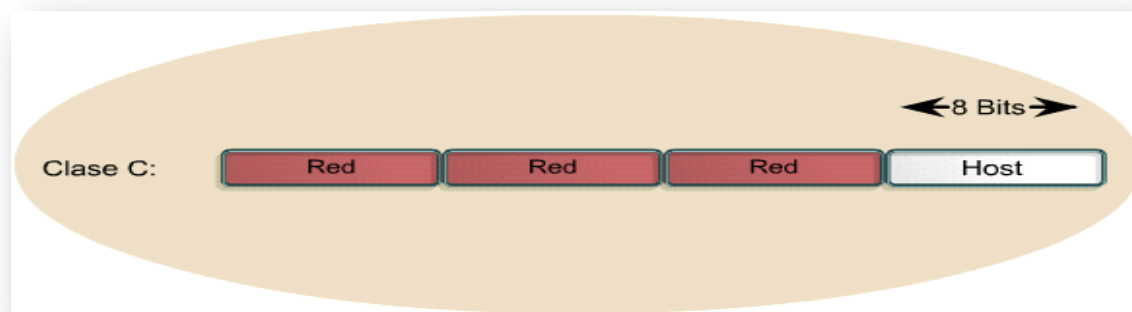
La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.

La dirección Clase B se diseñó para cumplir las necesidades de redes de tamaño moderado a grande. Una dirección IP Clase B utiliza los primeros dos de los cuatro octetos para indicar la dirección de la red. Los dos octetos restantes especifican las direcciones del host.



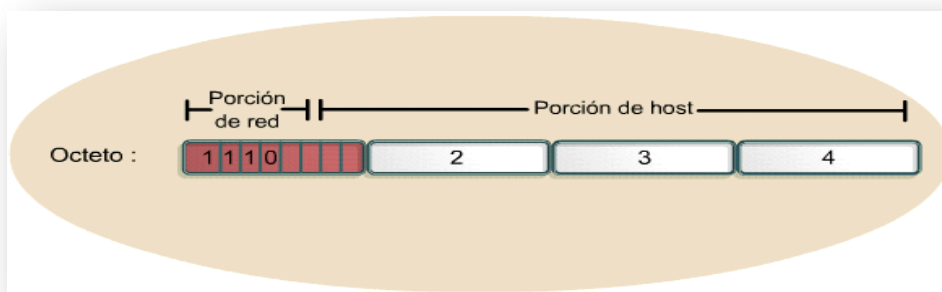
Los primeros dos bits del primer octeto de la dirección Clase B siempre son 10. Los seis bits restantes pueden poblarse con unos o ceros. Por lo tanto, el menor número que puede representarse en una dirección Clase B es 10000000, 128 decimal. El número más alto que puede representarse es 10111111, 191 decimal. Cualquier dirección que comience con un valor entre 128 y 191 en el primer octeto es una dirección Clase B.

El espacio de direccionamiento Clase C es el que se utiliza más frecuentemente en las clases de direcciones originales. Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts.



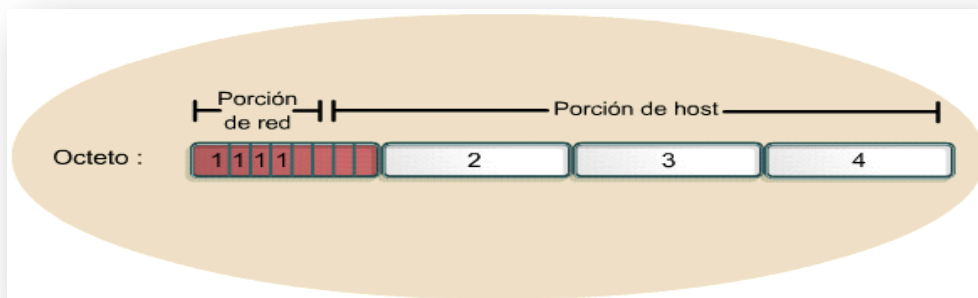
Una dirección Clase C comienza con el binario 110. Por lo tanto, el menor número que puede representarse es 11000000, 192 decimal. El número más alto que puede representarse es 11011111, 223 decimal. Si una dirección contiene un número entre 192 y 223 en el primer octeto, es una dirección de Clase C.

La dirección Clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.



El espacio de direccionamiento Clase D, en forma similar a otros espacios de direccionamiento, se encuentra limitado matemáticamente. Los primeros cuatro bits de una dirección Clase D deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 11100000 a 11101111, o 224 a 239. Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D.

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.



IPv6 - DIRECCIONAMIENTO

IPv6 es la versión 6 del Protocolo de Internet (IP por sus siglas en inglés, Internet Protocol), es el encargado de dirigir y encaminar los paquetes en la red, fue diseñado en los años 70 con el objetivo de interconectar redes.

Esta nueva versión del Protocolo de Internet está destinada para sustituir al estándar IPv4, la misma cuenta con un límite de direcciones de red, lo cual impide el crecimiento de la red.

IPv4 posibilita 4.294.967.296 (232) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etcétera. En cambio, IPv6 admite

340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 o 340 sextillones de direcciones) — cerca de 3.4×10^{20} (340 trillones de direcciones) por cada pulgada cuadrada (6.7×10^{17} o 670 mil billones de direcciones/mm²) de la superficie de La Tierra.

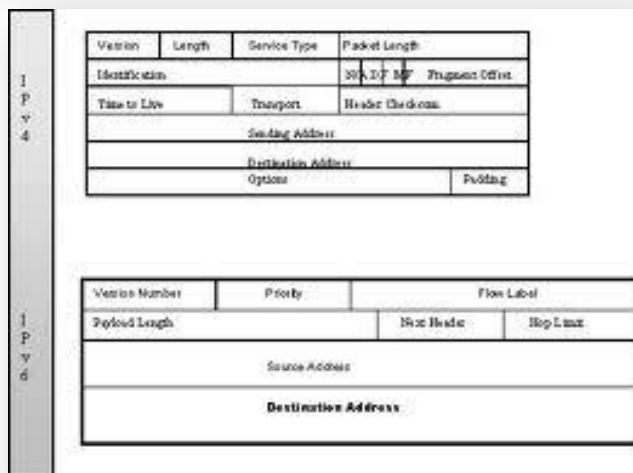
El IPv6 fue diseñado por Steve Deering y Craig Mudge, adoptado por Internet Engineering Task Force (IETF) en 1994. IPv6 también se conoce por "IP Next Generation" o "IPng".

IPv6 empieza a ganar terreno en el mercado del gobierno federal de los E.E.U.U. y los portadores asiáticos de comunicaciones. A pesar de que IPv6 fue diseñado para ofrecer una seguridad mejor que Ipv4, la seguridad sigue siendo una edición en nuevas instalaciones debido a la escasez de las herramientas de seguridad para estos protocolos. Para ello podemos hacer uso de los cortafuegos (firewall) actuales.

IPv4 vs IPv6

Actualmente se utiliza con más frecuencia la versión 4 del Protocolo de Internet, el aumento de usuarios, aplicaciones, servicios y dispositivos está provocando la migración a una nueva versión.





IPv4 soporta 4.294.967.296 (232) direcciones de red, este es un número pequeño cuando se necesita otorgar a cada computadora, teléfonos, PDA, autos, etc. IPv6 soporta 340.282.366.920.938.463.374.607.431.768.211.456 (2128 ó 340 sextillones) direcciones de red.

Por lo general las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC (Media Access Control address) de la interfaz a la que está asignada la dirección.

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

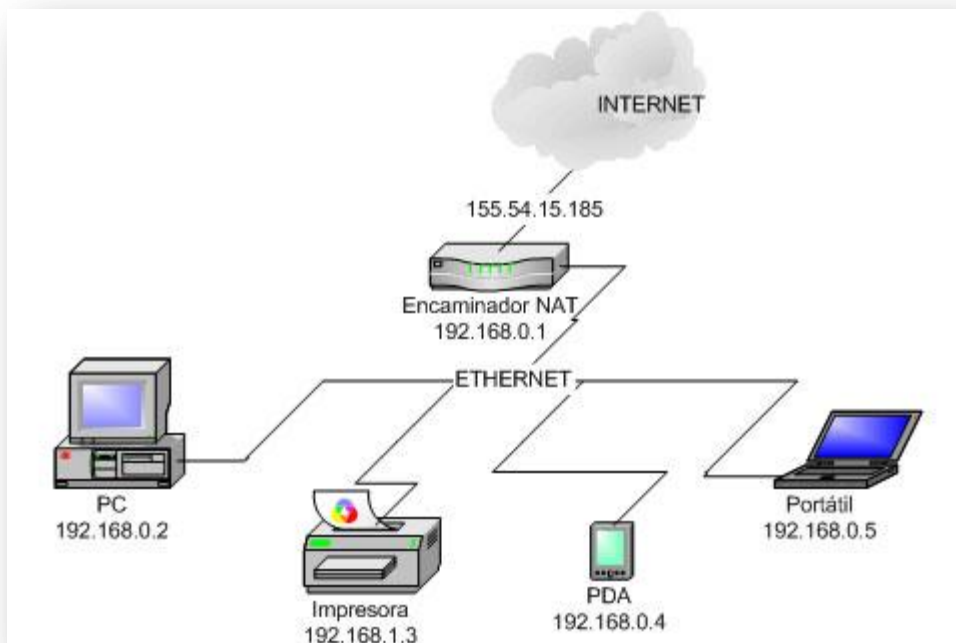
No debemos confundir la dirección MAC que es un número hexadecimal fijo asignado a la tarjeta o dispositivo de red por el fabricante por la dirección IP, mientras que la dirección IP se puede cambiar.

Solución actual

La utilización de IPv6 se ha frenado por la Traducción de Direcciones de Red (NAT, Network Address Translation), temporalmente alivia la falta de estas direcciones de red.

Este mecanismo consiste en usar una dirección IPv4 para que una red completa pueda acceder a internet. Pero esta solución nos impide la utilización de varias aplicaciones, ya que sus

protocolos no son capaces de atravesar los dispositivos NAT, por ejemplo P2P, voz sobre IP (VoIP), juegos multiusuarios, entre otros.



Características de la IPv6

Quizás las principales características de la IPv6 se sintetizan en el mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad. Pero también hay otras que son importantes mencionar:

- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.

- Seguridad Integrada (IPsec): IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.
- Capacidad de ampliación.
- Calidad del servicio.
- Velocidad.

Tipos de direcciones IP

- a) Unicast: Este tipo de direcciones son bastante conocidas. Un paquete que se envía a una dirección unicast debería llegar a la interfaz identificada por dicha dirección.
- b) Multicast: Las direcciones multicast identifican un grupo de interfaces. Un paquete destinado a una dirección multicast llega a todos los interfaces que se encuentran agrupados bajo dicha dirección.
- c) Anycast: Las direcciones anycast son sintácticamente indistinguibles de las direcciones unicast pero sirven para identificar a un conjunto de interfaces. Un paquete destinado a una dirección anycast llega a la interfaz "más cercana" (en términos de métrica de "routers"). Las direcciones anycast sólo se pueden utilizar en "routers".

Direcciones IPv6

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6.

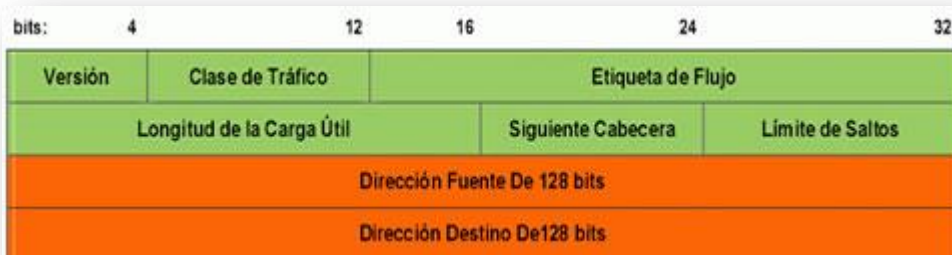
Está compuesta por 8 segmentos de 2 bytes cada uno, que suman un total de 128 bits, el equivalente a unos 3.4×10^{38} hosts direccionables. La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas acerca de la representación de direcciones IPv6 son:

- Los ceros iniciales, como en IPv4, se pueden obviar.
Ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 -> 2001:123:4:ab:cde:3403:1:63.
- Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación sólo se puede hacer una vez.
- Ejemplo: 2001:0:0:0:0:0:4 -> 2001::4.

- Ejemplo no válido: 2001:0:0:0:2:0:0:1 -> 2001::2::1 (debería ser 2001::2:0:0:1 ó 2001:0:0:0:2::1).

Paquetes IPv6

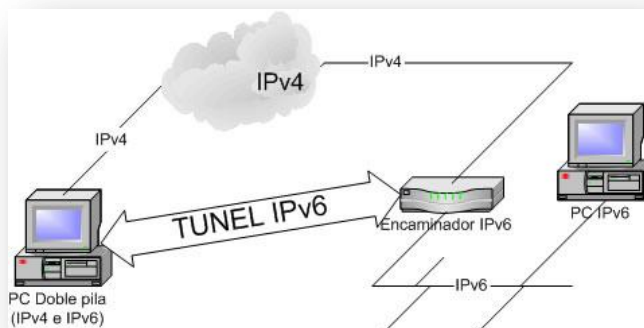


La cabecera se encuentra en los primeros 40 bytes del paquete, contiene las direcciones de origen y destino con 128 bits cada una, la versión 4 bits, la clase de tráfico 8 bits, etiqueta de flujo 20 bits, longitud del campo de datos 16 bits, cabecera siguiente 8 bits, y límite de saltos 8 bits.

¿Qué es un túnel IPv6 en IPv4?

Es un mecanismo de transición que permite a máquinas con IPv6 instalado comunicarse entre sí a través de una red IPv4.

El mecanismo consiste en crear los paquetes IPv6 de forma normal e introducirlos en un paquete IPv4. El proceso inverso se realiza en la máquina destino, que recibe un paquete IPv6.



DNS en IPv6

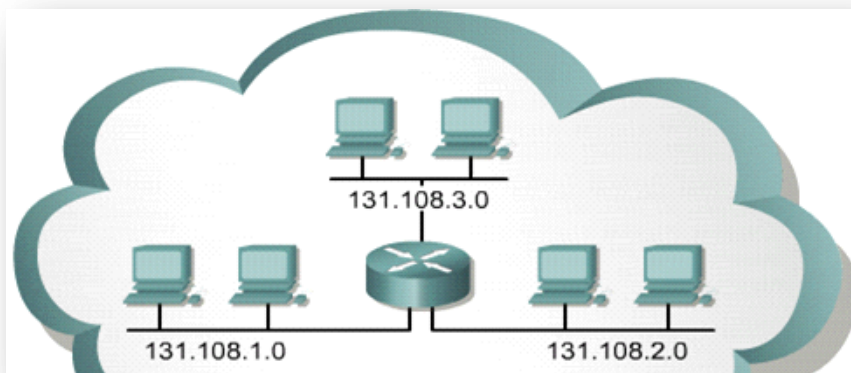
Existen dos tipos de registros de DNS para IPv6. El IETF ha declarado los registros A6 y CNAME como registros para uso experimental. Los registros de tipo AAAA son hasta ahora los únicos estándares.

La utilización de registros de tipo AAAA es muy sencilla. Se asocia el nombre de la máquina con la dirección IPv6 de la siguiente forma: NOMBRE_DE_LA_MÁQUINA AAAA MIDIRECCION_IPv6

De igual forma que en IPv4 se utilizan los registros de tipo A. En caso de no poder administrar su propia zona de DNS se puede pedir esta configuración a su proveedor de servicios. Las versiones actuales de bind (versiones 8.3 y 9) y el "port" dns/djbdns (con el parche de IPv6 correspondiente) soportan los registros de tipo AAAA.

El tema de IPv6 no es nada nuevo, hace varios años se viene hablando de esta evolución, pero el proceso es algo que vale la pena discutir, enriquecer con noticias, comentarios sobre el mismo y conocer la perspectiva de los usuarios con respecto a la evolución hacia el IPv6.

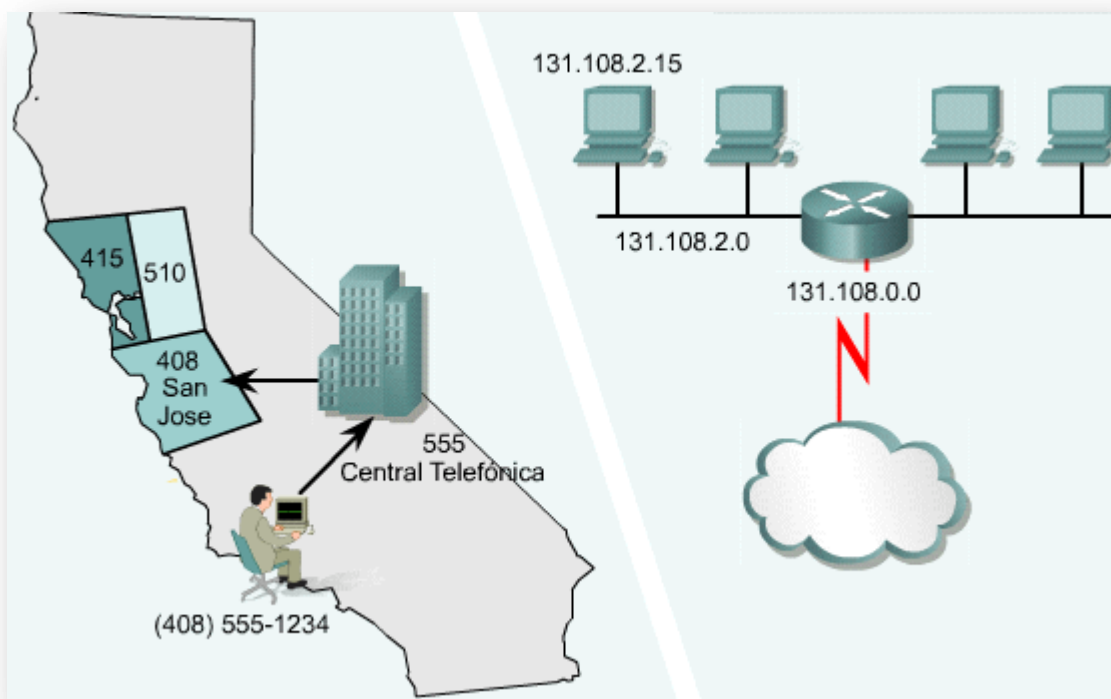
LA DIVISIÓN EN SUBREDES



Internamente, las redes se dividen en redes más pequeñas llamadas subredes. Al proporcionar un tercer nivel de direccionamiento, las subredes aportan flexibilidad adicional al administrador de red. Por ejemplo, una dirección de red clase B proporcionada por el Registro Americano de Números de Internet (American Registry for Internet Numbers - ARIN), se puede dividir en varias subredes. En este ejemplo, 131.108.1.0, 131.108.2.0 y 131.108.3.0 son subredes dentro de la red 131.108.0.0

La división en subredes es otro método para administrar las direcciones IP. Este método, que consiste en dividir las clases de direcciones de red completas en partes de menor tamaño, ha evitado el completo agotamiento de las direcciones IP.

Resulta imposible hablar sobre el TCP/IP sin mencionar la división en subredes. Como administrador de sistemas, es importante comprender que la división en subredes constituye un medio para dividir e identificar las redes individuales en toda la LAN. No siempre es necesario subdividir una red pequeña. Sin embargo, en el caso de redes grandes a muy grandes, la división en subredes es necesaria.



Las subredes son similares al sistema de numeración telefónica de Estados Unidos. Este sistema de numeración se divide en códigos de área, que a su vez se dividen en intercambios, que

a su vez se dividen en conexiones individuales. Las direcciones de subred incluyen un número de red, un número de subred dentro de la red y un número de host dentro de la subred.

Dividir una red en subredes significa utilizar una máscara de subred para dividir la red y convertir una gran red en segmentos más pequeños, más eficientes y administrables o subredes. Un ejemplo sería el sistema telefónico de los EE.UU. que se divide en códigos de área, códigos de intercambio y números locales.

El administrador del sistema debe resolver estos problemas al agregar y expandir la red. Es importante saber cuántas subredes o redes son necesarias y cuántos hosts se requerirán en cada red. Con la división en subredes, la red no está limitada a las máscaras de red por defecto Clase A, B o C y se da una mayor flexibilidad en el diseño de la red.

Las direcciones de subredes incluyen la porción de red más el campo de subred y el campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original de la red entera. La capacidad para decidir cómo se divide la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad en el direccionamiento al administrador de red.

Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred.

Notación decimal para el primer octeto de host	Número de subredes	Número de Hosts de clase A por subred	Número de Hosts de clase B por subred	Número de Hosts de clase C por subred
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

El número mínimo de bits que se puede pedir es dos. Al crear una subred, donde se solicita un sólo bit, el número de la red suele ser red .0. El número de broadcast entonces sería la red .255. El número máximo de bits que se puede pedir prestado puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host.

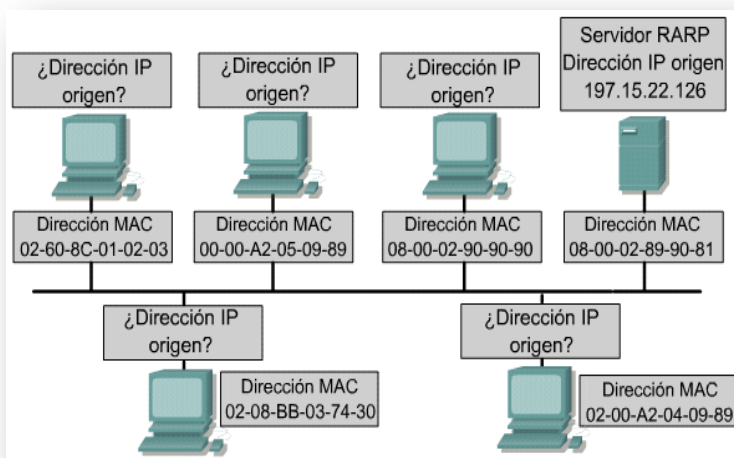
CÓMO OBTENER UNA DIRECCIÓN IP?

Un host de red necesita obtener una dirección exclusiva a nivel global para poder funcionar en Internet. La dirección MAC o física que posee el host sólo tiene alcance local, para identificar el host dentro de la red del área local. Como es una dirección de Capa 2, el Router no la utiliza para realizar transmisiones fuera de la LAN.

Las direcciones IP son las direcciones que más frecuentemente se utilizan en las comunicaciones en la Internet. Este protocolo es un esquema de direccionamiento jerárquico que permite que las direcciones individuales se asocien en forma conjunta y sean tratadas como grupos. Estos grupos de direcciones posibilitan una eficiente transferencia de datos a través de la Internet.

Los administradores de redes utilizan dos métodos para asignar las direcciones IP. Estos métodos son el estático y el dinámico.

Más adelante, en esta lección, se tratará el direccionamiento estático y las tres variantes del direccionamiento dinámico. Independientemente del esquema de direccionamiento elegido, no es posible tener dos interfaces con la misma dirección IP. Dos hosts con la misma dirección IP pueden generar conflictos que hacen que ambos no puedan operar correctamente. Como muestra la Figura, los hosts tienen una dirección física ya que cuentan con una tarjeta de interfaz de red que les permite conectarse al medio físico.



Los hosts poseen una dirección física debido a una tarjeta de interfaz de red que permite la conexión al medio físico. Las direcciones IP deben asignarse al host de alguna forma. Los dos métodos de asignación de dirección IP son: estático o dinámico.




Portapapeles

VPN: Una red privada virtual (virtual private network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.


4.7 TECNOLOGIAS DE RED

VPN:

Afortunadamente con la aparición de Internet, las empresas, centros de formación, organizaciones de todo tipo e incluso usuarios particulares, tienen la posibilidad de crear una **VPN** , que permita mediante una moderada inversión económica y utilizando Internet, la conexión entre diferentes ubicaciones salvando la distancia entre ellas.

Las redes virtuales privadas utilizan protocolos especiales de seguridad que permiten obtener acceso a servicios de carácter privado, únicamente a personal autorizado, de una empresa, centros de formación, organizaciones, etc.; cuando un usuario se conecta vía Internet, la configuración de la red privada virtual le permite conectarse a la red privada del organismo con el que colabora y acceder a los recursos disponibles de la misma como si estuviera tranquilamente sentado en su oficina.

Una VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, al fin y al cabo no es más que la creación en una red pública de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local.

En la mayoría de los casos la red pública es Internet, pero también puede ser una red **ATM**  o Frame Relay

El funcionamiento de una VPN es similar al de cualquier red normal, aunque realmente para que el comportamiento se perciba como el mismo hay un gran número de elementos y factores que hacen esto posible.

La comunicación entre los dos extremos de la red privada a través de la red pública se hace estableciendo túneles virtuales entre esos dos puntos y usando sistemas de encriptación y autenticación que aseguren la confidencialidad e integridad de los datos transmitidos a través de esa red pública. Debido al uso de estas redes públicas, generalmente Internet, es necesario prestar especial atención a las cuestiones de seguridad para evitar accesos no deseados.

La tecnología de túneles (**Tunneling** ) es un modo de envío de datos en el que se encapsula un tipo de paquetes de datos dentro del paquete de datos



Portapapeles

ATM: Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

TUNNELING: La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras.

propio de algún protocolo de comunicaciones, y al llegar a su destino, el paquete original es desempaquetado volviendo así a su estado original.

En el traslado a través de Internet, los paquetes viajan encriptados, por este motivo, las técnicas de autenticación son esenciales para el correcto funcionamiento de las VPNs, ya que se aseguran a emisor y receptor para el intercambio de información con el usuario o dispositivo correcto.

La autenticación en redes virtuales es similar al sistema de inicio de sesión a través de usuario y contraseña, pero tienes unas necesidades mayores de aseguramiento de validación de identidades.

La mayoría de los sistemas de autenticación usados en VPN están basados en sistema de claves compartidas.

La autenticación se realiza normalmente al inicio de una sesión, y luego, aleatoriamente, durante el transcurso de la sesión, para asegurar que no haya algún tercer participante que se haya podido entrometer en la conversación.

Todas las VPNs usan algún tipo de tecnología de encriptación, que empaqueta los datos en un paquete seguro para su envío por la red pública.

La encriptación hay que considerarla tan esencial como la autenticación, ya que permite proteger los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión.

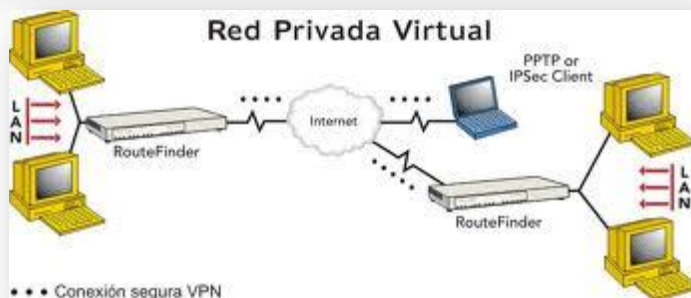
Existen dos tipos de técnicas de encriptación que se usan en las VPN: Encriptación de clave secreta, o privada, y Encriptación de clave pública.

En la encriptación con clave secreta se utiliza una contraseña secreta conocida por todos los participantes que van a hacer uso de la información encriptada. La contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de sistema tiene el problema que, al ser compartida por todos los participantes y debe mantenerse secreta, al ser revelada, tiene que ser cambiada y distribuida a los participantes, lo que puede crear problemas de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).



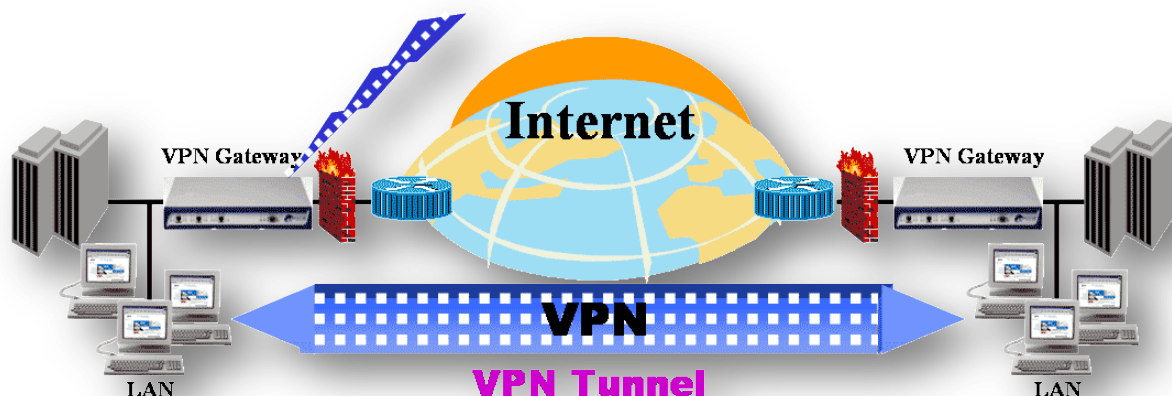
VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.



Tunneling

Como mencionamos anteriormente, la técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.



El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil. (conceptos por el autor- Fernando Martin Rivas Fuentes Rivera)

VPN over LAN

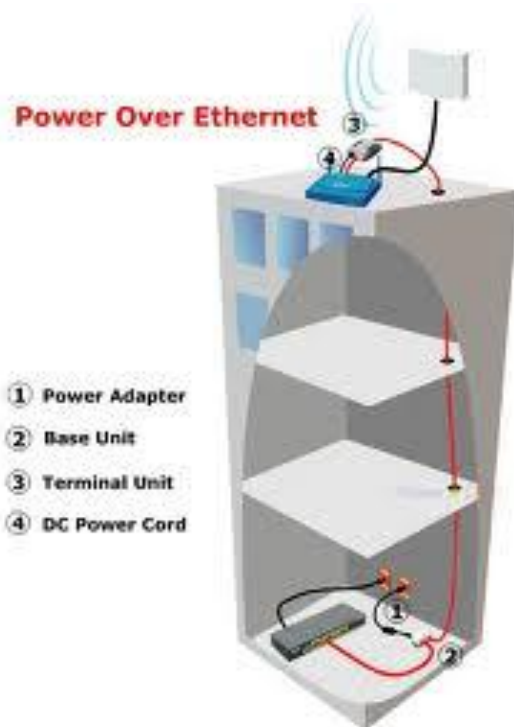
Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.



Otro ejemplo es la conexión a redes WIFI haciendo uso de túneles cifrados IPSEC o SSL que además de pasar por los métodos de autenticación tradicionales (WAP, WEP, MACaddress, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN internas o externas.

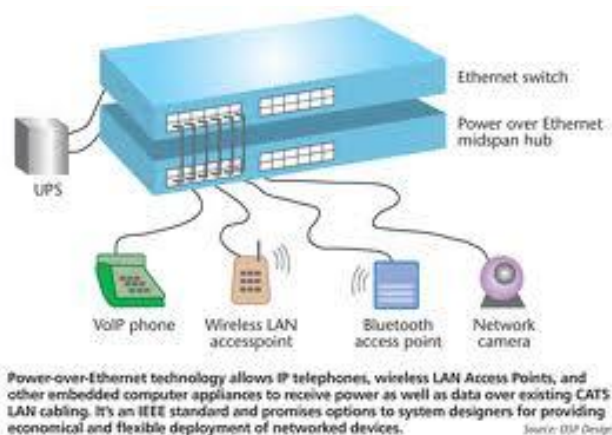
En las redes virtuales, la encriptación debe ser realizada en tiempo real, de esta manera, los flujos de información encriptada a través de una red lo son utilizando encriptación de clave secreta con claves que son válidas únicamente para la sesión usada en ese momento.



POWER OVER ETHERNET:

La alimentación a través de Ethernet (PoE) es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como, por ejemplo, un teléfono IP o una cámara de red, usando el mismo cable que se utiliza para una conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones de la cámara y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

Power over Ethernet se regula en una norma denominada IEEE 802.3af, y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos preexistentes que no sean compatibles. Esta característica permite a los usuarios mezclar en la red con total libertad y seguridad dispositivos preexistentes con dispositivos compatibles con PoE.



Actualmente existen en el mercado varios dispositivos de red como switches o hubs que soportan esta tecnología. Para implementar PoE en una red que no se dispone de dispositivos que la soporten directamente se usa una unidad base (con conectores RJ45 de entrada y de salida) con un adaptador de alimentación para recoger la electricidad y una unidad terminal (también con conectores RJ45) con un cable de alimentación para que el dispositivo final obtenga la energía necesaria para su funcionamiento.

Podemos mencionar algunas ventajas de esta reciente tecnología.

- a. PoE es una fuente de alimentación inteligente: Los dispositivos se pueden apagar o reiniciar desde un lugar remoto usando los protocolos existentes, como el Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol).
- b. PoE simplifica y abarata la creación de un suministro eléctrico altamente robusto para los sistemas: La centralización de la alimentación a través de concentradores (hubs) PoE significa que los sistemas basados en PoE se pueden enchufar al Sistema de alimentación ininterrumpida (SAI) central, que ya se emplea en la mayor parte de las redes informáticas formadas por más de uno o dos PC, y en caso de corte de electricidad, podrá seguir funcionando sin problemas.
- c. Los dispositivos se instalan fácilmente allí donde pueda colocarse un cable LAN, y no existen las limitaciones debidas a la proximidad de una base de alimentación (dependiendo la longitud del cable se deberá utilizar una fuente de alimentación de mayor voltaje debido a la caída del mismo, a mayor longitud mayor pérdida de voltaje, superando los 25 metros de cableado aproximadamente).
- d. Un único juego de cables para conectar el dispositivo Ethernet y suministrarle alimentación, lo que simplifica la instalación y ahorra espacio.
- e. La instalación no supone gasto de tiempo ni de dinero ya que no es necesario realizar un nuevo cableado.
- f. PoE dificulta enormemente cortar o destrozar el cableado: Generalmente el cableado se encuentra unido a bandejas en los huecos del techo o detrás de conductos de plástico de muy difícil acceso. Cualquier corte de estos cables resultará obvio al momento para quien pase por el lugar y, por supuesto, para los usuarios de los ordenadores que serán incapaces de proseguir con su trabajo.



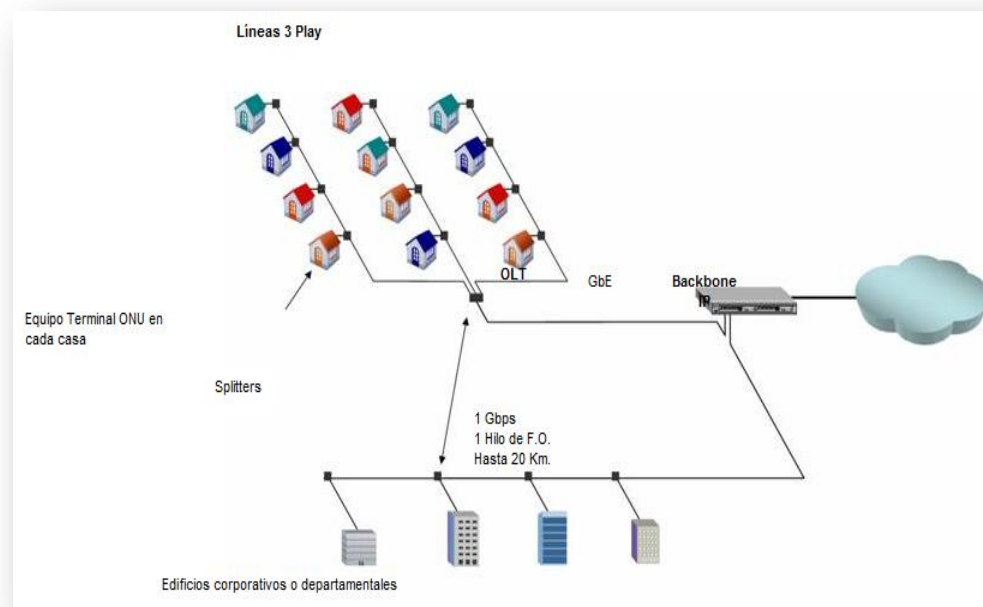
GEPON:

La tecnología Gigabit Ethernet – PON, es la evolución de la tecnología PON (por sus siglas en inglés: Passive Optical Network) con la integración de la tecnología Ethernet a velocidades de 1 Gbps, utilizando Fibra Optica, de ahí su nombre: Gigabit Ethernet Passive Optical Network.

Algunas de las ventajas más importantes al usar GEPON son las siguientes:

- a) Ancho de banda seguro para diferentes servicios al ser el número de abonados por trayectoria de fibra de un máximo de 32.
- b) Gran alcance entre los equipos distribuidores y los suscriptores (20 Km).
- c) Soporte para datos, voz y video.
- d) Varios usuarios pueden usar una sola fibra ahorrando costos.
- e) Bajas tasas de administración y mantenimiento en la red al usarse equipos de fibra pasivos y no activos.

La principal ventaja de esta solución es que finalmente permite hacer llegar directamente fibra óptica a cada uno de los subscriptores del servicio de banda ancha (o a nodos de la red en el caso de un campus o una MAN), por supuesto a un costo que hace factible su implementación y comercialización. Esto es posible gracias a los precios accesibles del equipo electrónico, al hecho de que se maneja directamente la tecnología Ethernet como medio de comunicación, así como a la gran optimización que se logra en la utilización de la fibra óptica.



Como se aprecia en la figura anterior, existe un equipo distribuidor (OLT) el cual se conecta a la red principal; de éste equipo salen múltiples trayectorias, cada una de solamente 1 hilo de fibra óptica con capacidad de transportar 1 Gbps de información. Este ancho de banda se reparte entre las conexiones terminales

de la trayectoria, que son rematadas en un equipo **CPE** (ONU), el cual se ubica en la instalación del subscriptor o nodo de red. Existen varios modelos de ONU, para proporcionar desde un puerto de Ethernet para la conexión del subscriptor, hasta 24 puertos de Ethernet en el caso de un edificio de departamentos; también existen modelos para instalarse en intemperie, así como





Portapapeles

CPE: Equipo Local del Cliente) es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación. El equipo puede proveer una combinación de servicios incluyendo datos, voz, video y un host de aplicaciones multimedia interactivos.

ONU: optic network unit- unidad de red óptica - nodo de acceso que convierte las señales ópticas a base de fibra óptica en señales eléctricas que pueden transmitirse a través del cable coaxial o de cobre de par trenzado

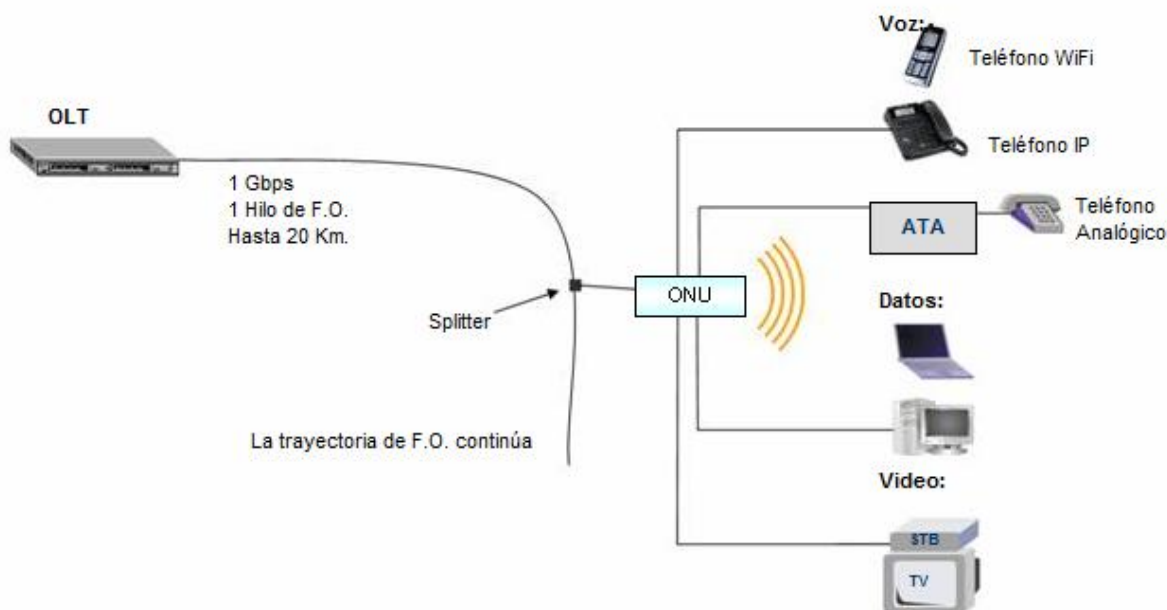
Splitters : Los splitters o cajas separadoras son unidades especiales de interconexion empleadas en tomas de sonido.

ONUs  que incluyen puertos para conectar directamente una TV en el caso de aplicaciones triple play (voz, dato y video).

La forma de repartir el ancho de banda entre los subscriptores que comparten una misma trayectoria es completamente determinista y ajustable. Los equipos mediante los cuales se comparte la fibra son llamados **Splitters**  y son totalmente pasivos, es decir, no requieren ningún tipo de energía. La forma de derivar la fibra puede ser en bus, estrella, o una combinación de ambas (que es el caso representado en la figura).

Esta solución tiene la facilidad de manejar el tráfico a nivel capa 2 o capa 3, y se pueden configurar VLANs para mantener el tráfico totalmente aislado entre subscriptores distintos, mientras que subscriptores que requieran tener comunicación directa (como puede ser el caso de varias oficinas de una misma empresa) pueden agruparse dentro de una misma VLAN.

Las posibilidades de conexión en el punto terminal de servicio (vivienda, habitación, oficina, etc).



Las redes GE-PON están distribuidas de la siguiente manera: OLT (Línea Terminal Óptica) los cuales están conectados a las redes IP u otras por un extremo, luego están las ODN (Redes de Distribución Óptica) de la cual se desprenden los POS (Splitter Óptico Pasivo), y

estos le dan acceso a los ONU (Unidad de Red Óptica), los cuales brindan el servicio a cada abonado.

Las características más relevantes que podemos observar son las siguientes:

Cada trayectoria de fibra óptica puede soportar hasta 32 subscriptores, con lo cual se tiene el ancho de banda garantizado necesario para soportar aplicaciones "Triple Play" (Voz, Datos y Video), además de estar preparado para implementar cualquier servicio futuro.

Se logra un alcance de hasta 20 Km entre el equipo distribuidor y el punto de terminación (subscriber).

La instalación del equipo ONU no requiere ninguna configuración especializada en el domicilio del subscriptor, al conectarse a la red automáticamente se integra a ésta y, desde una interfaz gráfica de administración centralizada se le asignan los atributos necesarios de forma muy rápida.

Permite la combinación con otras tecnologías de backbone y acceso de forma simple (Ethernet, xDSL, WiFi, WiMax).

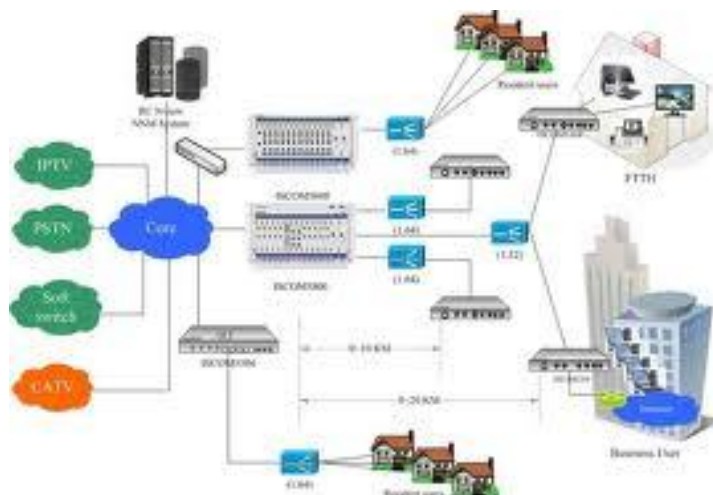
Los principales sectores de aplicación de esta tecnología son:

OPERADORES DE TELECOMUNICACIONES

Los proveedores de servicios de telecomunicaciones, ahora tiene una forma económica y eficiente de entregar fibra óptica a sus subscriptores, inclusive residenciales, lo que les permite ofrecer planes mucho más agresivos, introducir nuevos servicios y realizar alianzas con otros proveedores, además de garantizar que la implementación permanecerá rentable por un plazo sumamente largo.

SECTOR DE SERVICIOS TURÍSTICOS (HOTELES)

GEPON representa una excelente opción para entregar servicios de Voz, Datos y Video por una infraestructura unificada. Por ejemplo es posible tender un solo hilo de Fibra Óptica para la entrega de los 3 servicios a múltiples habitaciones. El hotel ahora puede ofrecer además de banda ancha, las ventajas que se describen en los servicios de IPTV y VoIP.






Portapapeles

BACKBONE: principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante mangueras de fibra óptica.

AMBIENTES TIPO CAMPUS

En estos ambientes (universidades, parques industriales, etc) siempre es deseable contar con el máximo ancho de banda disponible para llevar a cabo sus operaciones de forma rápida y eficiente. Es común ver la implementación de fibra

óptica, sin embargo esto se realiza solamente en el **backbone**  y requiere de equipos activos para redistribuir la señal. La tecnología GEPON les brinda la oportunidad de llevar la fibra óptica más allá del backbone, selectivamente a aquellos nodos que requieren un mayor ancho de banda, o que por la distancia a la que se encuentran, la única opción para interconectarlos es la fibra óptica. Por supuesto que esto se logra de manera eficiente y con costos bajos





Portapapeles

DHCP: siglas de Dynamic Host Configuration Protocol y significa, Protocolo de configuración dinámica de host.

BOOTP: Es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente. Normalmente se realiza en el proceso de arranque de los ordenadores o del sistema operativo.


DNS: Domain Name System (sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

Puerta de enlace (Gateway) permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Traduce la información del protocolo utilizado en una red al protocolo usado en la red destino.


4.8 PROTOCOLOS

Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. En su forma más simple, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos. A su más bajo nivel, un protocolo define el comportamiento de una conexión de hardware. Los protocolos son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás.

a. DHCP:

DHCP , es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red, pero desde sus inicios se diseñó como un complemento del protocolo

BOOTP  (Protocolo Bootstrap), que se utiliza, por ejemplo, cuando se instala un equipo a través de una red (BOOTP se usa junto con un servidor TFTP donde el cliente encontrará los archivos que se cargarán y copiarán en el disco duro). Un servidor DHCP puede devolver parámetros BOOTP o la configuración específica a un determinado host.

Funcionamiento del protocolo DHCP

Primero, se necesita un servidor DHCP que distribuya las direcciones IP. Este equipo será la base para todas las solicitudes DHCP por lo cual debe tener una dirección IP fija. Por lo tanto, en una red puede tener sólo un equipo con una dirección IP fija: el servidor DHCP.

Existe la posibilidad de utilizar los parámetros configurables del DHCP. Un servidor DHCP puede proveer de una configuración opcional a la computadora cliente. Dichas opciones están definidas en RFC 2132. Lista de opciones configurables:

- Dirección del servidor **DNS**
- Nombre DNS
- **Puerta de enlace** de la dirección IP
- Dirección de Publicación Masiva (**broadcast address**)
- **Máscara de subred**
- Tiempo máximo de espera del ARP (Protocolo de Resolución de Direcciones)
- **MTU** (Unidad de Transferencia Máxima) para la interfaz
- Servidores **NIS** (Servicio de Información de Red)
- Dominios NIS
- Servidores **NTP** (Protocolo de Tiempo de Red)
- Servidor **SMTP**
- Servidor **TFTP**
- Nombre del servidor WINS (Windows Internet Naming Service (WINS) es un servidor de nombres de Microsoft para NetBIOS, que mantiene una tabla con la correspondencia entre direcciones IP y nombres NetBIOS de ordenadores. Esta lista permite localizar rápidamente a otro ordenador de la red).

El sistema básico de comunicación es BOOTP (con la trama UDP). Cuando un equipo se inicia no tiene información sobre su configuración de red y no hay nada especial que el usuario deba hacer para obtener una dirección IP. Para esto, la técnica que se usa es la transmisión: para encontrar y comunicarse con un servidor DHCP, el equipo simplemente enviará un paquete especial de transmisión (transmisión en 255.255.255.255 con información adicional como el tipo de solicitud, los puertos de conexión, etc.) a través de la red local. Cuando el DHCP recibe el paquete de transmisión, contestará con otro paquete de transmisión (no olvide que el cliente no tiene una dirección IP y, por lo tanto, no es posible conectar directamente con él) que contiene toda la información solicitada por el cliente.

Se podría suponer que un único paquete es suficiente para que el protocolo funcione. En realidad, hay varios tipos de paquetes DHCP que pueden emitirse tanto desde el cliente hacia el servidor o servidores, como desde los



Portapapeles

Broadcast: es una dirección lógica en la que todos los dispositivos conectados a una red de acceso múltiple de comunicaciones están habilitadas para recibir los datagramas.

Máscara de subred: es una combinación de bits que sirve para delimitar el ámbito de una red. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

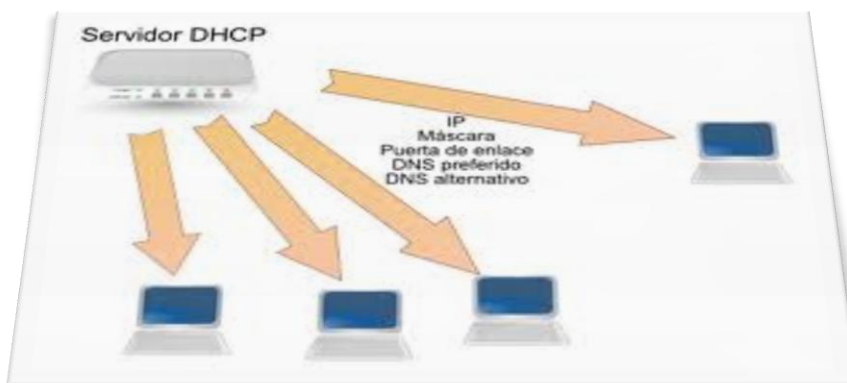
MTU: Maximum Transfer Unit. Expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un Protocolo de Internet - IP.

NIS: Network Information Service. Protocolo de servicios de directorios cliente-servidor desarrollado por Sun Microsystems.

servidores hacia un cliente:

- DHCPDISCOVER (para ubicar servidores DHCP disponibles)
- DHCPOFFER (respuesta del servidor a un paquete DHCPDISCOVER, que contiene los parámetros iniciales)
- DHCPREQUEST (solicitudes varias del cliente, por ejemplo, para extender su concesión)
- DHCPACK (respuesta del servidor que contiene los parámetros y la dirección IP del cliente)
- DHCPNAK (respuesta del servidor para indicarle al cliente que su concesión ha vencido o si el cliente anuncia una configuración de red errónea)
- DHCPDECLINE (el cliente le anuncia al servidor que la dirección ya está en uso)
- DHCPRELEASE (el cliente libera su dirección IP)
- DHCPINFORM (el cliente solicita parámetros locales, ya tiene su dirección IP)

El primer paquete emitido por el cliente es un paquete del tipo DHCPDISCOVER. El servidor responde con un paquete DHCPOFFER, fundamentalmente para enviarle una dirección IP al cliente. El cliente establece su configuración y luego realiza un DHCPREQUEST para validar su dirección IP (una solicitud de transmisión ya que DHCPOFFER no contiene la dirección IP) El servidor simplemente responde con un DHCPACK con la dirección IP para confirmar la asignación. Normalmente, esto es suficiente para que el cliente obtenga una configuración de red efectiva, pero puede tardar más o menos en función de que el cliente acepte o no la dirección IP...



Portapapeles

NTP: Network Time Protocol. Es un protocolo para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123.

SMTP: Simple Mail Transfer Protocol. Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.)

TFTP: Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial). Es un protocolo de transferencia muy simple semejante a una versión básica de FTP.

Concesiones:

Para optimizar los recursos de red, las direcciones IP se asignan con una fecha de inicio y de vencimiento para su validez. Esto es lo que se conoce como "concesión". Un cliente que detecta que su concesión está a punto de vencer, puede solicitarle al servidor una extensión de la misma por medio de un DHCPREQUEST. Del mismo modo, cuando el servidor detecta que una concesión va a vencer, enviará un DHCPNAK para consultarle al cliente si desea extenderla. Si el servidor no recibe una respuesta válida, convertirá la dirección IP en una dirección disponible.

Esta es la efectividad de DHCP: se puede optimizar la asignación de direcciones IP planificando la duración de las concesiones. El problema es que si no se liberan direcciones, en un momento determinado no se podrá cumplir con nuevas solicitudes DHCP debido a que faltarán direcciones que puedan distribuirse.

En una red en la cual muchos equipos se conectan y desconectan permanentemente (redes de escuelas o de oficinas de ventas, por ejemplo), es aconsejable ofrecer concesiones por períodos cortos. En cambio, para una red compuesta principalmente por equipos fijos que se reinician rara vez, las concesiones por períodos largos son más que suficientes. No se olvide que DHCP trabaja principalmente por transmisión y que puede ocupar ancho de banda en redes pequeñas con alta demanda.

Obtención de un servidor DHCP

Internet Software Consortium desarrolla servidores DHCP en el mundo del software libre. Este es el servidor DHCP más usado y uno de los que mejor "cumple" las RFC. ¡ATENCIÓN! No es sencillo desarrollar un servidor DHCP y distribuyen parches y mejoras continuas para los servidores que ofrecen.




b. SNMP:


Sigla en inglés de "Simple Network Management Protocol". El Protocolo Simple de Administración de Red, es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados;
- Agentes;
- Sistemas administradores de red (**NMS's** ).

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, **bridges** , hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

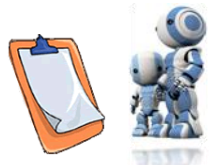
Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.



Portapapeles

NMS's: Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP.

BRIDGES: 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 hacia otra, con base en la dirección física de destino de cada paquete.



Portapapeles

MIB: (Management Information Base) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones. Es parte de la gestión de red definida en el modelo OSI.

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: lectura, escritura, notificación y operaciones transversales.

El comando de lectura es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

El comando de escritura es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

El comando de notificación es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.

Las operaciones transversales son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como por ejemplo, una tabla de rutas.

Base de información de administración SNMP (**MIB** ):

Una Base de Información de Administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB's son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

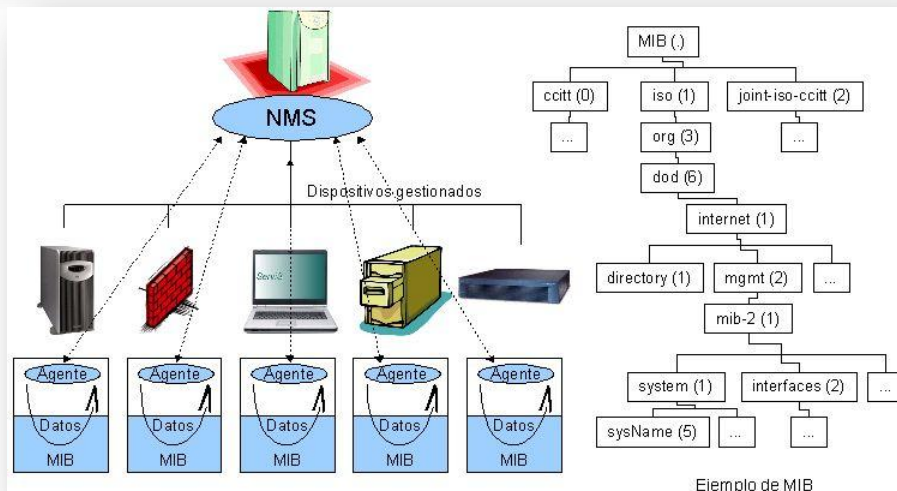
La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones.




Portapapeles

PDA's: personal digital assistant (asistente digital personal), también denominado ordenador de bolsillo, es una computadora de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

CRLF: se refiere a la combinación de dos códigos de control: CR (retorno de carro) y LF (salto de línea), uno detrás del otro; normalmente con el objetivo de crear una nueva línea.




c. SMTP: Simple Mail Transfer Protocol

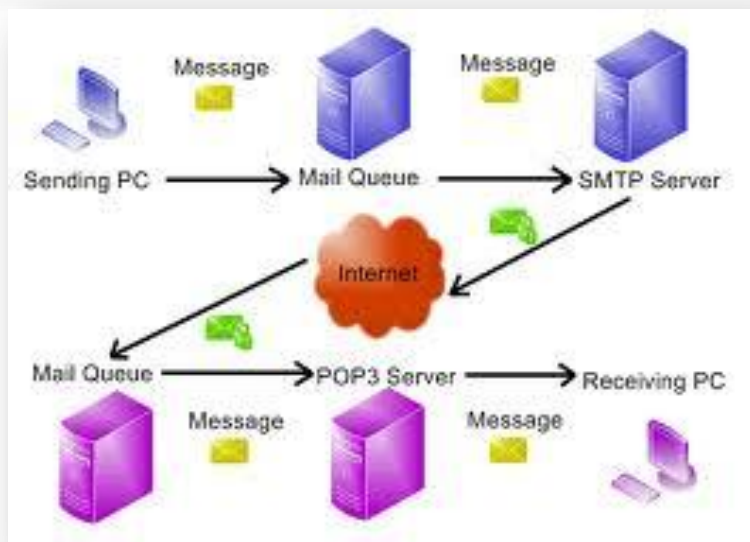
Es un Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (**PDA's** , teléfonos móviles, etc.). Protocolo Simple de Transferencia de Correo que se encuentra en la capa de aplicación.

Se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo. El número va dirigido a un procesamiento automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En el protocolo SMTP todas las órdenes, réplicas o datos

son líneas de texto, delimitadas por el carácter **<CRLF>** . Todas las réplicas tienen un código numérico al comienzo de la línea.

En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión.



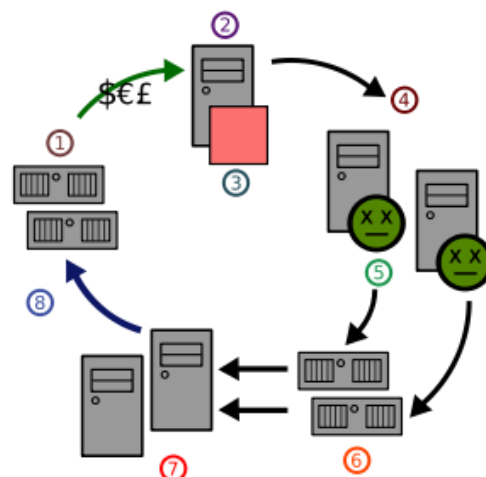
Una de las limitaciones del SMTP original, es que no facilita métodos de autenticación a los emisores, así que se definió la extensión SMTP-AUTH.

A pesar de esto, el spam es aún el mayor problema. No se cree que las extensiones sean una forma práctica para prevenirlo. Se define SPAM a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico pero puede presentarse por programas de mensajería instantánea o por teléfono celular.



Ciclo del SPAM

- (1): Sitio web de Spammers
- (2): Spammer
- (3): Spamware
- (4): ordenadores infectados
- (5): Virus o troyanos
- (6): Servidores de correo
- (7): Usuarios
- (8): Tráfico Web.



d. XMPP:

Es el Protocolo extensible de mensajería y comunicación de presencia, Extensible Messaging and Presence Protocol, más conocido como XMPP (anteriormente llamado Jabber1), es un protocolo abierto y extensible basado en XML, originalmente ideado para mensajería instantánea.

Con el protocolo XMPP queda establecida una plataforma para el intercambio de datos XML que puede ser usada en aplicaciones de mensajería instantánea. Las características en cuanto a adaptabilidad y sencillez del XML son heredadas de este modo por el protocolo XMPP.

A diferencia de los protocolos propietarios de intercambio de mensajes como ICQ, Y! y Windows Live Messenger, se encuentra documentado y se insta a utilizarlo en cualquier proyecto. Existen servidores y clientes libres que pueden ser usados sin coste alguno.

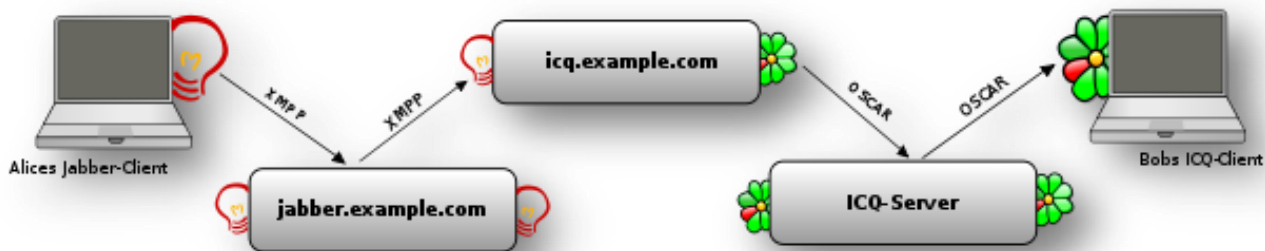


Este es el protocolo que seleccionó Google para su servicio de mensajería Google Talk.



La red XMPP está basada en servidores, pero descentralizada; por diseño, no hay ningún servidor central, como sucede con servicios como AOL Instant Messenger o MSN Messenger. Sobre este punto, surge cierta confusión, puesto que existe un servidor XMPP público en "Jabber.org", al que están suscritos un gran número de usuarios, pero no hay que olvidar que cualquiera puede poner en marcha su propio servidor. El puerto estandar utilizado para XMPP es el 5222.

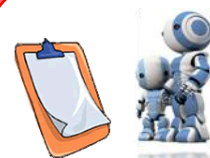
Otra característica muy útil del protocolo XMPP son las pasarelas, que permiten a los usuarios el acceso a redes con otros protocolos de mensajería instantánea como MSN Messenger, ICQ u otros tipos de mensajería como SMS o E-mail. Este servicio no es proporcionado desde el cliente, sino desde el servidor mediante servicios de pasarela que proporcionan conectividad con alguna otra red. Cualquier usuario se puede registrar con alguna de estas pasarelas proporcionando sus datos de acceso a la nueva red como nombre de usuario y contraseña, y comunicarse con los usuarios de la nueva red. Esto significa que cualquier cliente XMPP puede ser usado para acceder cualquier red para la que haya una pasarela, sin necesidad de adaptar el cliente o de que tenga acceso directo a Internet.



Como puede observar en la figura, Alice envía un mensaje a través de la red XMPP a la pasarela de ICQ, posteriormente, el mensaje es dirigido a Bob mediante la red ICQ.

PPPOE:


(Point-to-Point Protocol over Ethernet o Protocolo Punto a Punto sobre Ethernet) es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayoritariamente para proveer conexión de banda ancha mediante servicios de cabledem y xDSL. Este ofrece las ventajas del protocolo PPP como son la autenticación, cifrado, mantención y compresión.



Portapapeles

PPP: Point-to-point Protocol, es decir, Protocolo punto a punto. El protocolo PPP permite establecer una comunicación a nivel de enlace entre dos computadoras.

IETF: (Internet Engineering Task Force - Grupo Especial sobre Ingeniería de Internet1), es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

En esencia, es un protocolo túnel, que permite implementar una capa IP sobre una conexión entre dos puertos Ethernet, pero con las características de software del protocolo PPP, por lo que es utilizado para virtualmente "marcar" a otra máquina dentro de la red Ethernet, logrando una conexión "serial" con ella, con la que se pueden transferir paquetes de datos IP, basado en las características del protocolo **PPP** .


Esto permite utilizar software tradicional basado en PPP para manejar una conexión que no puede usarse en líneas seriales pero con paquetes orientados a redes locales como Ethernet para proveer una conexión clásica con autenticación para cuentas de acceso a Internet. Además, las direcciones IP en el otro lado de la conexión sólo se asignan cuando la conexión PPPoE es abierta, por lo que admite la reutilización de direcciones IP (direccionamiento dinámico).

PPPoE fue desarrollado por UUNET, Redback y RouterWare. El protocolo está publicado en la RFC 2516.



RTP:

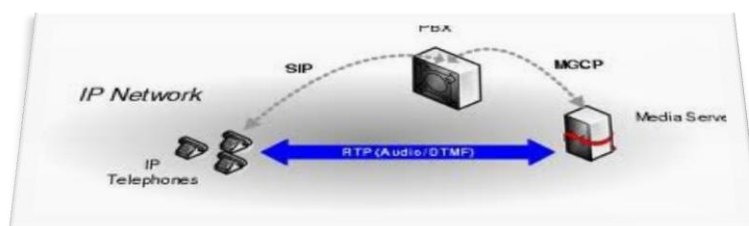
RTP son las siglas de Real-time Transport Protocol (Protocolo de Transporte de Tiempo real). Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia.

Está desarrollado por el grupo de trabajo de transporte de Audio y Video del **IETF** , publicado por primera vez como estándar en 1996 como la RFC

1889, y actualizado posteriormente en 2003 en la RFC 3550, que constituye el estándar de Internet STD 64.

Inicialmente se publicó como protocolo multicast, aunque se ha usado en varias aplicaciones unicast. Se usa frecuentemente en sistemas de streaming, junto a RTSP, videoconferencia y sistemas push to talk (en conjunción con H.323 o SIP). Representa también la base de la industria de VoIP.

La RFC 1890, obsoleta por la RFC 3551 (STD 65), define un perfil para conferencias de audio y vídeo con control mínimo. La RFC 3711, por otro lado, define SRTP (Secure Real-time Transport Protocol), una extensión del perfil de RTP para conferencias de audio y vídeo que puede usarse opcionalmente para proporcionar confidencialidad, autenticación de mensajes y protección de reenvío para flujos de audio y vídeo.



Va de la mano de RTCP (RTP Control Protocol) y se sitúa sobre UDP en el modelo OSI.

Estructura del encabezado del RTP:

Byte 0		Byte 1		Byte 2		Byte 3	
V	P	X	CC	M	PT	Sequence Number	
Time Stamp							
Synchronization Source (SSRC)							
Content Source (CSRC)							
Extension header (EH - opcional)							
Datos							

- Número de versión de RTP (V - versión number): 2 bits. La versión definida por la especificación actual es 2.
- Relleno (P - Padding): 1 bit. Si el bit del relleno está colocado, hay uno o más bytes al final del paquete que no es parte de la carga útil. El último byte del paquete indica el número de bytes de relleno. El relleno es usado por algunos algoritmos de cifrado.
- La extensión (X - Extensión): 1 bit. Si el bit de extensión está colocado, entonces el encabezado fijo es seguido por una extensión del encabezado. Este mecanismo de la extensión posibilita implementaciones para añadir información al encabezado RTP.
- Conteo CSRC (CC): 4 bits. El número de identificadores CSRC que sigue el encabezado fijo. Si la cuenta CSRC es cero, entonces la fuente de sincronización es la fuente de la carga útil.
- El marcador (M - Marker): 1 bit. Un bit de marcador definido por el perfil particular de media.
- Tipo de Carga útil (PT - Payload Type): 7 bits. Un índice en una tabla del perfil de media que describe el formato de carga útil. Los mapeos de carga útil para audio y vídeo están especificados en el RFC 1890.
- El número de Secuencia: 16 bits. Un único número de paquete que identifica la posición de este en la secuencia de paquetes. El número del paquete es incrementado en uno para cada paquete enviado.
- Sellado de tiempo: 32 bits. Refleja el instante de muestreo del primer byte en la carga útil. Varios paquetes consecutivos pueden tener el mismo sellado si son lógicamente generados en el mismo tiempo - por ejemplo, si son todo parte del mismo frame de vídeo.
- SSRC: 32 bits. Identifica la fuente de sincronización. Si la cuenta CSRC es cero, entonces la fuente de carga útil es la fuente de sincronización. Si la cuenta CSRC es distinta a cero, entonces el SSRC identifica el mixer(mezclador).
- CSRC: 32 bits cada uno. Identifica las fuentes contribuyentes para la carga útil. El número de fuentes contribuyentes está indicado por el campo de la cuenta CSRC; Allí puede haber más de 16 fuentes contribuyentes. Si hay fuentes contribuyentes múltiples, entonces la carga útil son los datos mezclados de esas fuentes.
- EH: El tamaño de este dato debe ser $CC \times 32$ en bits
- Datos: El tamaño de los datos debe ser de $X \times ((EHL + 1) \times 32)$ donde EHL es la longitud de la extensión del la cabecera en unidades de 32 bits.

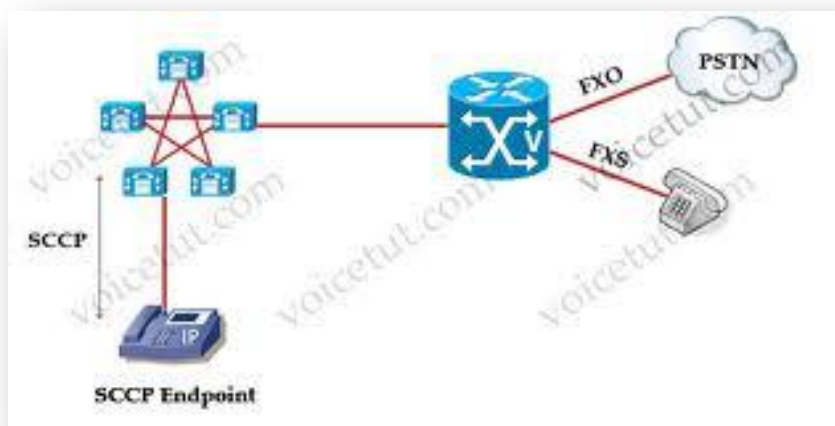
SCCP:

Skinny Client Control Protocol o protocolo de control del cliente, es un protocolo propietario de control de terminal desarrollado originariamente Selsius Corporation. Actualmente es propiedad de Cisco Systems y se define como un

conjunto de mensajes entre un cliente ligero y el **CallManager**. Ejemplos conocidos de clientes ligeros son los de la serie Cisco 7900 de teléfonos IP como. Skinny es un protocolo ligero que permite una comunicación eficiente con un sistema Cisco Call Manager. El Call Manager actúa como un proxy de señalización para llamadas iniciadas a través de otros protocolos como H.323, SIP, RDSI o MGCP.

Un cliente skinny utiliza TCP/IP para conectarse a los Call Managers en un **cluster**. Para el tráfico de datos (flujo de datos de audio en tiempo real) se utiliza RTP/UDP/IP]. SCCP es un protocolo basado en estímulos y diseñado como un protocolo de comunicación para puntos finales hardware y otros sistemas embebidos, con restricciones de procesamiento y memoria significativas.

Cisco adquirió la tecnología SCCP cuando compró la empresa Selsius a finales de los años 1990. Como una reminiscencia del origen de los actuales teléfonos IP Cisco, el nombre por defecto de los teléfonos Cisco registrados en un CallManager es SEP (Selsius Ethernet Phone) seguido de su **MAC address**.



Portapapeles

CallManager: es un software basado en un sistema de tratamiento de llamadas y telefonía sobre IP, desarrollado por Cisco Systems.

cluster : Simplemente, un cluster es un grupo de múltiples ordenadores unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador, más potente que los comunes de escritorio.

MAC address: (Media Access Control o control de acceso al medio) es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una ethernet de red. Se conoce también como la dirección física en cuanto a identificar dispositivos de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada.

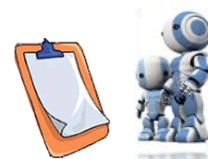
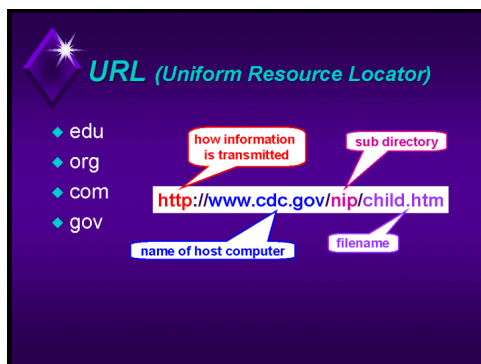
HTTP:

Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web y es el fundamento de la comunicación de datos para la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la IETF - Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616.

Desde 1990, el protocolo HTTP es el protocolo más utilizado en Internet. El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML). Entre un navegador (el cliente) y un servidor web (denominado, entre otros, **httpd** en equipos UNIX) localizado mediante una cadena de caracteres denominada dirección URL.

HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, **proxies**) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (**URL**). Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.



Portapapeles

Httpd: Programa que corre de fondo en un servidor web y espera peticiones de entrada para responderles.

Proxy: es un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

URL: *uniform resource locator*, es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para su localización o identificación, como por ejemplo documentos textuales, imágenes, videos, presentaciones digitales, etc.



Portapapeles

Cookies: es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su **navegador**, a petición del servidor de la página.

TCP: Protocolo de Control de Transmisión) o TCP, es uno de los protocolos fundamentales en Internet.

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las **cookies**, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

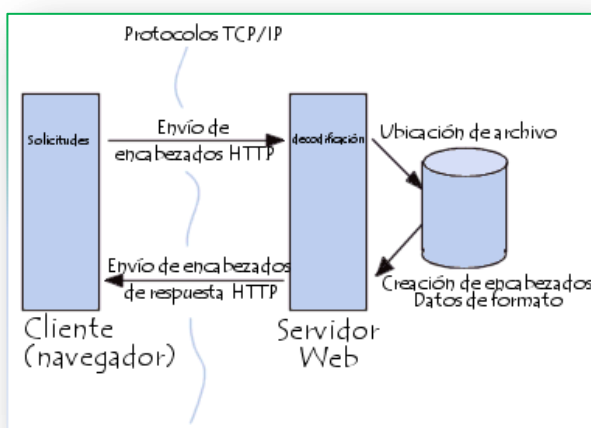
Ello sucede cuando la transacción de los mismos ha terminado, cosa que da lugar a las cookies (galletitas), archivos livianos que se guardan en determinado sitio del disco duro con el objetivo de almacenar información del usuario. De tal forma, el sitio Web sabrá de quién se trata al volver a acceder al mismo, mostrando por ejemplo su nombre y o permitiendo su acceso sin necesidad de ingresar contraseña, etc.

Las cookies también son utilizadas por ciertos sitios Web para llevar una estadística de sus visitantes.

Es útil saber que los sitios Web cuya dirección de Internet comienza con HTTPS serán seguros; por lo general los navegadores Web informan de esto mostrando un fondo amarillo detrás del texto de la URL, y algún candado.

Comunicación entre el navegador y el servidor

La comunicación entre el navegador y el servidor se lleva a cabo en dos etapas:







- El navegador realiza una solicitud HTTP
- El servidor procesa la solicitud y después envía una respuesta HTTP

Cada transacción de información realizada en la Web es realizada utilizando el protocolo HTTP, Protocolo de Transferencia de HyperTexto.

De este modo, las peticiones de acceso a una página y la respuesta brindada por la misma en forma de contenido de hipertexto utilizan este sistema de comunicación, el cual permanece un tanto "oculto" al usuario final. El protocolo HTTP es utilizado también para enviar formularios con campos de texto, u otro tipo de información en ambos sentidos.

HTTP es una capa de aplicación del protocolo diseñado en el marco del conjunto de protocolos de Internet. Las definiciones de protocolo suponen una fiable del nivel de transporte de protocolo para el host de transferencia de

datos. El Transmission Control Protocol (**TCP** ) es el protocolo dominante en uso para este propósito. En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad. Sin embargo, HTTP ha encontrado una aplicación, incluso con protocolos fiables, como el Protocolo de datagramas de usuario (**UDP** ) , en los métodos como el Simple Service Discovery Protocol (**SSDP** )).

HTTP recursos son identificados y localizados en la red mediante identificadores uniformes de recursos (**URI**), más específicamente, localizadores de recurso uniforme (URL), con el http o https esquemas de URI. URI y el Lenguaje de marcado de hipertexto (HTML), forman un sistema de alternancia entre los recursos, llamado hipertexto documentos, en la Internet, que condujo a la creación de la World Wide Web en 1990 por el Inglés el físico **Tim Berners-Lee** .

En HTTP, un navegador web, por ejemplo, actúa como un cliente, mientras que una aplicación que se ejecuta en un equipo de alojamiento un sitio web funciona como un servidor. El cliente envía un mensaje



Portapapeles

TCP: Protocolo de Control de Transmisión o TCP, es uno de los protocolos fundamentales en Internet.

UDP: protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

SSDP: El Protocolo Simple de Descubrimiento de Servicios (Simple Service Discovery Protocol) es un protocolo que sirve para la búsqueda de dispositivos UPnP en una red.

Tim Berners-Lee: se licenció en Ingeniería Física en 1976 en el Queen's College de la Universidad de Oxford. Es considerado como el padre de la web.

de solicitud HTTP al servidor. El servidor, que almacena contenido, o proporciona los recursos, tales como HTML archivos o realiza otras funciones en nombre del cliente, devuelve un mensaje de respuesta al cliente. Una respuesta contiene información de estado sobre la finalización de la solicitud y pueden contener cualquier contenido solicitado por el cliente en su cuerpo del mensaje.

Sesión HTTP

Una sesión HTTP es una secuencia de operaciones de red de petición-respuesta. Un cliente HTTP inicia una solicitud. Se establece un Transmission Control Protocol (TCP) con un determinado puerto en un host (normalmente el puerto 80). Un servidor HTTP escuchando en ese puerto espera mensaje de solicitud de un cliente. Al recibir la solicitud, el servidor devuelve una línea de estado, tales como "HTTP/1.1 200 OK", y un mensaje propio, el cuerpo de la que es quizás el recurso solicitado, un mensaje de error, o alguna otra información.

