Tema: 8 Direccionamiento IP.

1. Elementos de la comunicación.

Llamamos **comunicación** al proceso por el cual se transmite una información entre un emisor y un receptor.

Los elementos que intervienen en el proceso de comunicación son los siguientes:

- **Emisor**: Aquél que transmite la información (un individuo, un grupo o una máquina).
- **Receptor**: Aquél, individual o colectivamente, que recibe la información. Puede ser una máquina.

- **Código**: Conjunto o sistema de signos que el emisor utiliza para codificar el mensaje.

- **Canal**: Elemento físico por donde el emisor transmite la información y que el receptor capta por los sentidos corporales. Se denomina canal tanto al medio natural (aire, luz) como al medio técnico empleado (imprenta, telegrafía, radio, teléfono, televisión, ordenador, etc.) y se perciben a través de los sentidos del receptor (oído, vista, tacto, olfato y gusto).

- **Mensaje**: La propia información que el emisor transmite.

- **Contexto**: Circunstancias temporales, espaciales y socioculturales que rodean el hecho o acto comunicativo y que permiten comprender el mensaje en su justa medida.

Así, un **emisor** envía un mensaje a un **receptor**, a través de un **canal** y de los signos de un **código**, y de acuerdo al **contexto** en que se sitúa ese acto de comunicación.

En el proceso de comunicación, además de estos elementos, también interviene el ruido. El término ruido aplicado a la comunicación no se refiere solo a una molestia sonora, sino a cualquier interferencia en este proceso; también se conoce como perturbación de la información. El ruido puede presentarse en el canal o medio de comunicación, en el código (lenguaje u otro) y en la forma.

El ruido es cualquier interferencia que se produzca en la comunicación que impida que esta se logre. Consiste en toda perturbación en el proceso comunicativo, distorsionando u ocultando el mensaje.

El ruido será aceptable hasta un umbral, superado ese umbral el proceso de comunicación peligra, y la información no llegue al receptor.

Todo proceso de comunicación, será necesario establecer unas normas. Los protocolos de comunicación dictaminan:

- Cómo se debe iniciar y finalizar la comunicación.
- Qué código se va a utilizar y cómo.
- La tolerancia al ruido y a los fallos en la comunicación.
- Cómo actuar si la comunicación se interrumpe o no se lleva a cabo adecuadamente.

No todas las comunicaciones pueden ser correctas, porque los sistemas de comunicación deberá detectarlos, para posteriormente si fuera posible solucionarlo. Esta es la parte del control de errores, en la que se emplea redundancia.

Dependiendo del sentido y la simultaneidad de la dirección del mensaje, existe la siguiente clasificación:

- Simplex: Sólo permiten la transmisión en un sentido. El receptor no se puede comunicar con el emisor.
- Half duplex: Permite la transmisión en los dos sentidos, pero no de forma simultánea.
- Full duplex: permite el envío y recepción simultáneos. Podemos conseguir esa simultaneidad de varias formas:
  - Empleo de frecuencias separadas (multiplexación en frecuencia).
  - Cables separados.

En redes la velocidad de conexión se mide en bps, y en múltiplos. En ocasiones los proveedores de Internet (ISP) intentan confundir y dan la velocidad en bits, cuando se debería dar en bytes.

Para diferenciar estas dos medidas, se utiliza la B mayúscula para indicar bytes y la b minúscula para indicar bits, por lo que no es lo mismo 6 MBps que 6 Mbps.

2. Redes de comunicaciones.

Las redes o infraestructuras de (tele)comunicaciones proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o una comunicación, ya sea ésta en forma de voz, datos, vídeo o una mezcla de los anteriores.

Se entiende por **red de telecomunicación** al conjunto de medios (transmisión y conmutación), tecnologías (procesado, multiplexación, modulaciones), protocolos y facilidades en general, necesarios para el intercambio de información entre los usuarios de la red. La red es una estructura compleja.

El objetivo de una red de comunicaciones es el intercambio de información, pero el sistema completo es muy complicado. Para ello aparecen los protocolos de comunicaciones.

En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de

errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

Los sistemas de comunicación utilizan formatos bien definidos (protocolo) para intercambiar mensajes. Cada mensaje tiene un significado exacto destinado a obtener una respuesta de un rango de posibles respuestas predeterminadas para esa situación en particular. Normalmente, el comportamiento especificado es independiente de cómo se va a implementar. Los protocolos de comunicación tienen que estar acordados por las partes involucradas. Para llegar a dicho acuerdo, un protocolo puede ser desarrollado dentro de estándar técnico. Un protocolo de comunicación, también llamado en este caso protocolo de red, define la forma en la que los distintos mensajes o tramas de bit circulan en una red de computadoras.

Por ejemplo, el protocolo sobre palomas mensajeras permite definir la forma en la que una paloma mensajera transmite información de una ubicación a otra, definiendo todos los aspectos que intervienen en la comunicación: tipo de paloma, cifrado del mensaje, tiempo de espera antes de dar a la paloma por 'perdida'... y cualquier regla que ordene y mejore la comunicación.

2.1. Modelo OSI.

El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como “modelo OSI”, (en inglés, Open System Interconnection) es un modelo de referencia para los protocolos de red la arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization). Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT) y, desde 1984, la Organización Internacional de Normalización (ISO) también lo publicó con estándar. Su desarrollo comenzó en 1977.

Este modelo está dividido en siete capas o niveles:

2.1.1.Nivel físico

Es la primera capa del Modelo OSI. Es la que se encarga de la topología de red y de las conexiones globales de la computadora hacia la red, se refiere tanto al medio físico como a la forma en la que se transmite la información.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), cable coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.

- Manejar las señales eléctricas del medio de transmisión, polos en un enchufe, etc.

- Garantizar la conexión (aunque no la fiabilidad de dicha conexión).

2.1.2.Nivel de enlace de datos

Esta capa se ocupa:

- Direccionamiento físico. Se asigna una dirección física a cada interfaz de red en el momento de su fabricación. Esta dirección se conoce como dirección de Control de Acceso al Medio (MAC). La dirección MAC identifica cada host de origen y de destino de la red. Si al llegar un paquete a esta interfaz la dirección MAC de destino no coincide con la propia del dispositivo, la trama de descarta. Las aplicaciones de sniffer, para capturar el tráfico de red, se configuran en modo promiscuo, para captar todo el tráfico.
- Acceso al medio. Es el conjunto de mecanismos y protocolos de comunicaciones a través de los cuales varios "interlocutores" (dispositivos en una red, como computadoras, teléfonos móviles, etcétera) se ponen de acuerdo para compartir un medio de transmisión común (por lo general, un cable eléctrico o fibra óptica, o en comunicaciones inalámbricas el rango de frecuencias asignado a su sistema).
- Detección y corrección de errores. La detección y corrección de errores es una importante práctica para el mantenimiento e integridad de los datos. Generalmente los canales introducen un ruido externo que produce errores en la transmisión. Los códigos de detección y corrección de errores incluyen suficiente información redundante en cada bloque de datos. Las técnicas para detectar y corregir son,
    - Paridad simple (paridad horizontal).
    - Paridad de bloque (paridad horizontal y vertical).
    - Código Hamming.
    - Verificación de redundancia cíclica CRC.
- Distribución ordenada de tramas. Las tramas pueden llegar desordenadas, y necesitan un método para su correcta ordenación.
- Control del flujo. En transmisiones half dúplex, es necesario llevar un control entre emisor y receptor.

Es uno de los aspectos más importantes que revisar en el momento de conectar dos ordenadores, ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos (MAC, IP), para regular la forma de la conexión entre computadoras así determinando el paso de tramas (trama = unidad de medida de la información en esta capa, que no es más que la segmentación de los datos trasladándolos por medio de paquetes), verificando su integridad, y corrigiendo errores, por lo cual es importante mantener una excelente adecuación al medio físico (los más usados son el cable UTP, par trenzado o de 8 hilos), con el medio de red que redirecciona las conexiones mediante un router.

Dadas estas situaciones cabe recalcar que el dispositivo que usa la capa de enlace es el Switch que se encarga de recibir los datos del router y enviar cada uno de estos a sus respectivos destinatarios (servidor -> computador cliente), dada esta situación se determina como el medio que se encarga de la corrección de errores, manejo de tramas, protocolización de datos (se llaman protocolos a las reglas que debe seguir cualquier capa del modelo OSI).

2.1.3.Nivel de red.

Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de información se denominan paquetes, y se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.

- Enrutables: viajan con los paquetes (IP, IPX, APPLETALK)
- Enrutamiento: permiten seleccionar las rutas (RIP, IGRP, EIGRP, OSPF, BGP)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan encaminadores o enrutadores, aunque es más frecuente encontrarlo con el nombre en inglés routers. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

2.1.4.Nivel de transporte.

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que esté utilizando.

La PDU (unidad de datos) de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP. Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión.

Trabajan, por lo tanto, con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP:Puerto (191.16.200.54:80).

Los puertos lógicos están asignados dependiendo del tipo de tráfico. Los primeros 1023 son estándar y tienen funciones asignadas.

2.1.5.Nivel de sesión.

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

2.1.6.Nivel de presentación

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. Por lo tanto, podría decirse que esta capa actúa como un traductor.

2.1.7.Nivel de aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo

electrónico (Post Office Protocol y SMTP), gestores de bases de datos y servidor de ficheros (FTP), por UDP pueden viajar (DNS y Routing Information Protocol). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

2.2. Modelo TCP/IP.

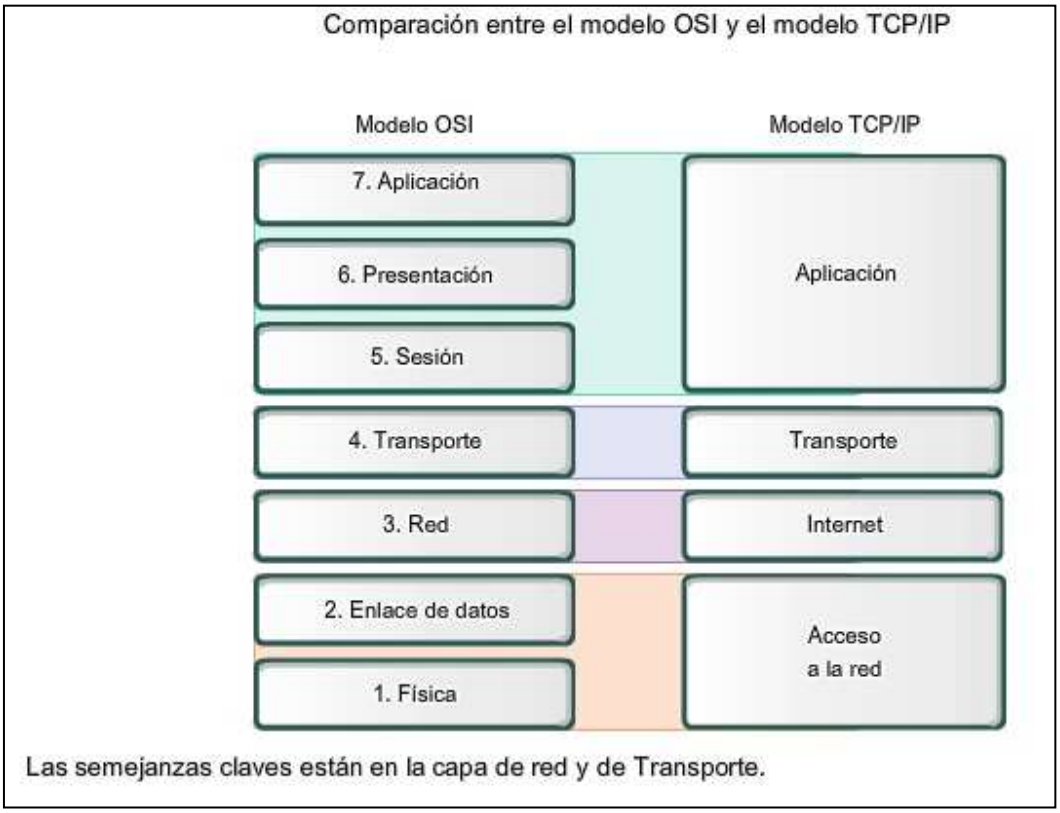
El modelo TCP/IP es una descripción de protocolos de red desarrollado en la década de 1970.

El modelo TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando como los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

Para conseguir un intercambio fiable de datos entre dos equipos, se deben llevar a cabo muchos procedimientos separados. El resultado es que el software de comunicaciones es complejo. Con un modelo en capas o niveles resulta más sencillo agrupar funciones relacionadas e implementar el software modular de comunicaciones.

Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

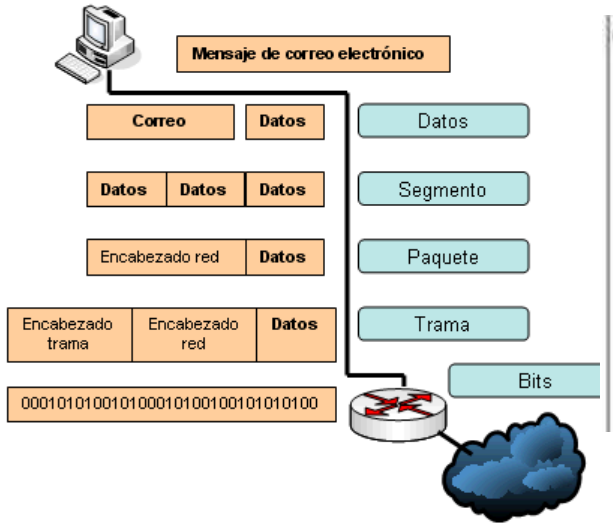
- Capa 4 o capa de aplicación: aplicación, asimilable a las capas: 5 (sesión), 6 (presentación) y 7 (aplicación), del modelo OSI. La capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo.
- Capa 3 o capa de transporte: transporte, asimilable a la capa 4 (transporte) del modelo OSI.
- Capa 2 o capa de internet: Internet, asimilable a la capa 3 (red) del modelo OSI.
- Capa 1 o capa de acceso al medio: acceso al medio, asimilable a la capa 2 (enlace de datos) y a la capa 1 (física) del modelo OSI.



Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación, pero ocultando la complejidad subyacente.

Al enviar la información a través de la red, es necesario que atraviese los diferentes niveles OSI o TCP/IP.

Los datos son particionados recibiendo un nombre en concreto en función de la capa donde están. Esto se denomina encapsulamiento de datos.

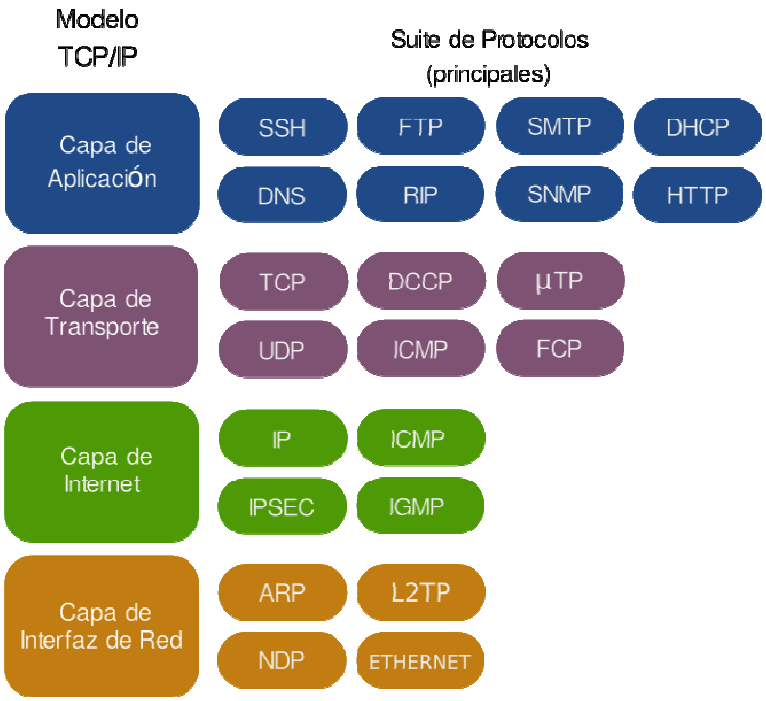


3. Protocolos de comunicación.

El proceso de comunicación es un proceso complicado, donde intervienen multitud de protocolos.

Ejemplos de protocolos de red

- **Capa 1: Nivel físico:** Cable coaxial, UTP (categoría 5, categoría 5e, categoría 6, categoría 6a), cable de fibra óptica, cable de par trenzado, ondas de microondas, ondas de radio, RS-232.
- **Capa 2: Nivel de enlace de datos:** ARP, RARP, Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC.
- **Capa 3: Nivel de red:** IP (IPv4, IPv6), X.25, ICMP, IGMP, NetBEUI, IPX, Appletalk.
- **Capa 4: Nivel de transporte:** TCP, UDP, SPX.
- **Capa 5: Nivel de sesión:** NetBIOS, RPC, SSL.
- **Capa 6: Nivel de presentación:** ASN.1. (prácticamente no se utilizan protocolos en esta capa)
- **Capa 7: Nivel de aplicación:** DHCP, DNS, SNMP, SMTP, NNTP, FTP, SSH, HTTP, CIFS (también llamado SMB), NFS, Telnet, IRC, POP3, IMAP, LDAP, Internet Mail 2000, etc.



4. Dirección IP.

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde

al nivel de red del modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina también dirección IP dinámica (normalmente abreviado como IP dinámica).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Las computadoras se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán, ya que seguirán accediendo por el nombre de dominio.

4.1. Direcciones IPv4.

Las direcciones IPv4 se expresan por un número binario de 32 bits, permitiendo un espacio de direcciones de hasta 4.294.967.296 (2^{32}) direcciones posibles. Las direcciones IP se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el intervalo de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255.

Ejemplo de representación de dirección IPv4: 10.128.1.253
Las direcciones IP tienen una estructura jerárquica. Una parte de la dirección corresponde a la red (netid), y la otra al host dentro de la red (hostid). Cuando un router recibe un datagrama (mensaje) por una de sus interfaces compara la parte de red de la dirección con las entradas contenidas en sus tablas (que normalmente sólo contienen direcciones de red, no de host) y envía el datagrama por la interfaz correspondiente.

Partes de una dirección IP

En esta arquitectura hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{24} - 2 (se excluyen la dirección reservada para broadcast (últimos octetos en 255) y de red (últimos octetos en 0)), es decir, 16.777.214 hosts.
- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts por cada red es 2^{16} - 2, o 65.534 hosts.

- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts por cada red es 2^8 - 2, o 254 hosts.

Clase	Bits iniciales	Intervalo	N.º de redes	N.º de equipos por red	Máscara de red	Id. broadcast
A	0	0.0.0.0 - 127.255.255.255	126	16.777.214	255.0.0.0	x.255.255.255
B	10	128.0.0.0 - 191.255.255.255	16.384	65.534	255.255.0.0	x.x.255.255
C	110	192.0.0.0 - 223.255.255.255	2.097.152	254	255.255.255.0	x.x.x.255
D (Multicast)	1110	224.0.0.0 - 239.255.255.255				
E (experimental)	1111	240.0.0.0 - 255.255.255.255				

Las redes de clase A, 0.X.X.X y 127.X.X.X, están reservadas y no se pueden utilizar.

4.1.1. Direcciones privadas

Existen ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).
- Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
- Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C continuas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

	Rango		Uso
Clase A	0.0.0.0	0.0.0.255	Reservado
	1.0.0.0	9.255.255.255	Público
	10.0.0.0	10.255.255.255	Privado
	11.0.0.0	126.255.255.255	Privado
	127.0.0.0	127.255.255.255	Reservado
Clase B	128.0.0.0	172.15.255.255	Público
	172.16.0.0	172.31.255.255	Privado
	172.32.0.0	191.255.255.255	Público
Clase C	192.0.0.0	192.167.255.255	Público
	192.168.0.0	192.168.255.255	Privado
	192.169.0.0	223.255.255.255	Público
Clase D	224.0.0.0	239.255.255.255	Reservado
Clase E	240.0.0.0	255.255.255.255	Reservado

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño a menudo se usa TCP/IP. Por ejemplo, los bancos pueden utilizar TCP/IP para conectar los cajeros automáticos que no se conectan a la red pública, de manera que las direcciones privadas son ideales para estas circunstancias. Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles.

Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas no se enrutará a través de Internet.

4.1.2. Máscara de subred

La máscara de subred permite distinguir dentro de la dirección IP, los bits que identifican a la red y los bits que identifican al host. En una dirección IP versión 4, de los 32 bits que se tienen en total, se definen por defecto para una dirección clase A, que los primeros ocho (8) bits son para la red y los restantes 24 para host, en una dirección de clase B, los primeros 16 bits son la parte de red y la de host son los siguientes 16, y para una dirección de clase C, los primeros 24 bits son la parte de red y los ocho (8) restantes son la parte de host. Por ejemplo, de la dirección de clase A 10.2.1.2 sabemos que pertenece a la red 10.0.0.0 y el host al que se refiere es el 2.1.2 dentro de la misma.

La máscara se forma poniendo en 1 los bits que identifican la red y en 0 los bits que identifican al host. De esta forma una dirección de clase A tendrá una máscara por defecto de 255.0.0.0, una de clase B 255.255.0.0 y una de clase C 255.255.255.0. Los dispositivos de red realizan un AND entre la dirección IP y la máscara de red para obtener la dirección de red a la que pertenece el host identificado por la dirección IP dada. Por ejemplo:

Dirección IP: 196.5.4.44

Máscara de subred (por defecto): 255.255.255.0

AND (en binario):

11000100.00000101.00000100.00101100 (196.5.4.44) Dirección IP

11111111.11111111.11111111.00000000 (255.255.255.0) Máscara de subred

11000100.00000101.00000100.00000000 (196.5.4.0) Resultado del AND

Esta información la requiere conocer un router necesita saber cuál es la red a la que pertenece la dirección IP del datagrama destino para poder consultar la tabla de encaminamiento y poder enviar el datagrama por la interfaz de salida. La máscara también puede ser representada de la siguiente forma 10.2.1.2/8 donde el /8 indica que los 8 bits más significativos de máscara que están destinados a redes o número de bits en 1, es decir /8 = 255.0.0.0. Análogamente (/16 = 255.255.0.0) y (/24 = 255.255.255.0).

Las máscaras de red por defecto se refieren a las que no contienen subredes, pero cuando éstas se crean, las máscaras por defecto cambian, dependiendo de cuántos bits se tomen para crear las subredes.

4.1.3. Creación de subredes

El espacio de direcciones de una red puede ser subdividido a su vez creando subredes autónomas separadas. Un ejemplo de uso es cuando necesitamos agrupar todos los empleados pertenecientes a un departamento de una empresa. En este caso crearíamos una subred que englobara las direcciones IP de estos. Para conseguirlo hay que reservar bits del campo host para identificar la subred estableciendo a uno los bits de red-subred en la máscara. Por ejemplo, la dirección 172.16.1.1 con máscara 255.255.255.0 nos indica que los dos primeros octetos identifican la red (por ser una dirección de clase B), el tercer octeto identifica la subred (a 1 los bits en la máscara) y el cuarto identifica el host (a 0 los bits correspondientes dentro de la máscara). Hay dos direcciones de cada subred que quedan reservadas: aquella que identifica la subred (campo host a 0) y la dirección para realizar broadcast en la subred (todos los bits del campo host en 1).

Las redes se pueden dividir en redes más pequeñas para un mejor aprovechamiento de las direcciones IP que se tienen disponibles para los hosts, ya que éstas a veces se desperdician cuando se crean subredes con una sola máscara de subred.

La división en subredes le permite al administrador de red contener los broadcast que se generan dentro de una LAN, lo que redunda en un mejor desempeño del ancho de banda.

Para comenzar la creación de subredes, se comienza pidiendo “prestados” bits a la parte de host de una dirección dada, dependiendo de la cantidad de subredes que se deseen crear, así como del número de hosts necesarios en cada subred.

4.2. IP dinámica

Una dirección IP dinámica es una IP asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

DHCP apareció como protocolo estándar en octubre de 1993. El estándar RFC 2131 especifica la última definición de DHCP (marzo de 1997). DHCP sustituye al protocolo BOOTP, que es más antiguo. Debido a la compatibilidad retroactiva de DHCP, muy pocas redes continúan usando BOOTP puro.

Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. El servidor del servicio DHCP puede ser configurado para que renueve las direcciones asignadas cada tiempo determinado.
Ventajas

- Reduce los costos de operación a los proveedores de servicios de Internet (ISP).
- Reduce la cantidad de IP asignadas (de forma fija) inactivas.
- El usuario puede reiniciar el router para que le sea asignada otra IP y así evitar las restricciones que muchas webs ponen a sus servicios gratuitos de descarga o visionado multimedia online.

Desventajas

Obliga a depender de servicios que redirigen un host a una IP.

Asignación de direcciones IP

Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

- manualmente, cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creada manualmente por el administrador de la red. Solo clientes con una dirección MAC válida recibirán una dirección IP del servidor.
- automáticamente, donde el servidor DHCP asigna por un tiempo preestablecido ya por el administrador una dirección IP libre, tomada de un intervalo prefijado también por el administrador, a cualquier cliente que solicite una.
- dinámicamente, el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un intervalo de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

4.3. IP fija

Una dirección IP fija es una dirección IP asignada por el usuario de manera manual (en algunos casos el ISP o servidor de la red no lo permite), o por el servidor de la red (ISP en el caso de internet, router o switch en caso de LAN) con base en la Dirección MAC del cliente. Muchas personas confunden IP fija con IP pública e IP dinámica con IP privada.

Una IP puede ser privada ya sea dinámica o fija como puede ser IP pública dinámica o fija.

Una IP pública se utiliza generalmente para montar servidores en internet y necesariamente se desea que la IP no cambie. Por eso la IP pública se la configura, habitualmente, de manera fija y no dinámica.

En el caso de la IP privada es, generalmente, dinámica y está asignada por un servidor DHCP, pero en algunos casos se configura IP privada fija para poder controlar el acceso a internet o a la red local, otorgando ciertos privilegios dependiendo del número de IP que tenemos. Si esta cambiara (si se asignase de manera fuera dinámica) sería más complicado controlar estos privilegios (pero no imposible).

4.4. Direcciones IPv6

La función de la dirección IPv6 es exactamente la misma que la de su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona en la Tierra tenga asignados varios millones de IPs, ya que puede implementarse con 2^{128} (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 de notación acerca de la representación de direcciones IPv6 son:

Los ceros iniciales 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 solo se puede hacer una vez.

Ejemplo: 2001:0:0:0:0:0:0:4 -> 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)

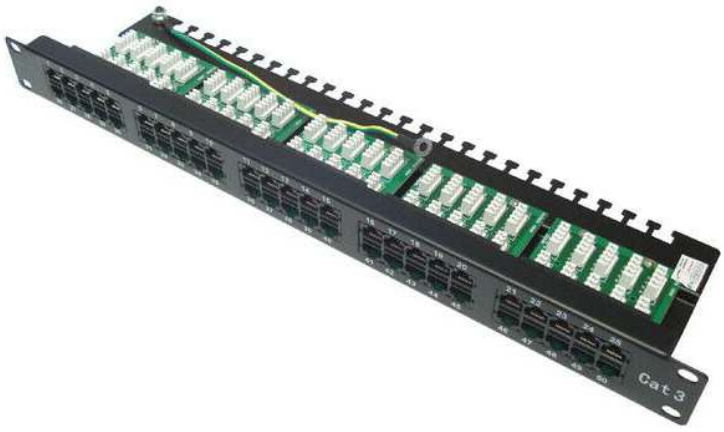
5. Dispositivos de interconexión.

Cuando hablamos de elementos de interconexión nos referimos a todos los elementos que permiten conectar equipos en red. Normalmente nos referiremos a los elementos de interconexión de una red de área local, aunque los elementos de interconexión pueden pertenecer a cualquier tipo de red.

Una forma de clasificar a los equipos de interconexión es teniendo en cuenta el nivel en el que trabajan tomando como referencia el modelo OSI. Por tanto, vamos a hacer una clasificación tomando este modelo como referencia.

5.1. Dispositivos de capa 1.

En el nivel físico tenemos:



5.1.1. Patch panel.

Un panel de conexiones (patch panel), también denominado bahía de rutas, es el elemento encargado de recibir todos los cables del cableado estructurado.

También se puede definir como paneles donde se ubican los puertos de una red o extremos (analógicos o digitales) de una red, normalmente localizados en un bastidor o rack de telecomunicaciones. Todas las líneas de entrada y salida de los equipos (computadoras, servidores, impresoras, entre otros) tendrán su conexión a uno de estos paneles.

5.1.2. Repetidor.

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

Características:

- Reciben el paquete, rectifican la señal (reconstruir los bits en tiempo y en amplitud) y lo pasan al otro segmento.

- Chequean o interpretan la información.
- Todos los segmentos interconectados por repetidores se comportan como un solo segmento lógico.

En telecomunicación es, el término repetidor tiene los siguientes significados normalizados:

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

En el caso de señales digitales el repetidor se suele denominar regenerador porque, de hecho, la señal de salida es una "señal regenerada" a partir de la de entrada. En el modelo de referencia OSI, el repetidor opera en el nivel físico. Los repetidores se utilizan a menudo en los cables transcontinentales y transoceánicos porque la atenuación (pérdida de señal) en tales distancias sería completamente inaceptable sin ellos. Los repetidores se utilizan tanto en cables de cobre portadores de señales eléctricas como en cables de fibra óptica portadores de luz. Los repetidores se utilizan también en los servicios de radiocomunicación. Un subgrupo de estos son los repetidores usados por los radioaficionados. Asimismo, se utilizan repetidores en los enlaces de telecomunicación punto a punto mediante radioenlaces que funcionan en el rango de las microondas, como los utilizados para distribuir las señales de televisión entre los centros de producción y los distintos emisores o los utilizados en redes de telecomunicación para la transmisión de telefonía.

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

5.1.3.Hub (concentrador).

Como su nombre indica, es un concentrador multipuerto al que puedes conectar diferentes dispositivos. Suele utilizarse en redes locales domésticas para conectar distintos dispositivos en una red informática. Verás que hay unos cuantos puertos para conectar dispositivos en red. Cuando lo haces, la señal que el hub recibe a través de la estación (un ordenador) podrá llegar también a los demás dispositivos conectados.

Por ejemplo, con la señal del cable de Internet. El problema es que la señal se transmite a través de todos los puertos. Si un hub pongamos que tiene 7 puertos, se está transmitiendo a todos a la vez, estén o no encendidos los dispositivos. Esto es algo que tiene sus desventajas, ya que puede generar colisiones si hay más de un equipo encendido.

Además, si conectan dispositivos que van más o menos rápido (por ejemplo, un ordenador y una impresora), el hub se adapta al que tiene menor velocidad de la red. Por eso el hub o "concentrador" está en desuso, aunque todavía se utiliza en redes domésticas. Actualmente verás que se hacen muchos hubs de 3 o 4 puertos USB, muy sencillos y baratos.

5.1.4.Punto de acceso.

Un punto de acceso inalámbrico (en inglés: Wireless Access Point, conocido por las siglas WAP o AP), en una red de computadoras, es un dispositivo de red que interconecta

equipos de comunicación alámbrica para formar una red inalámbrica que interconecta dispositivos móviles o con tarjetas de red inalámbricas.

Los WAP son dispositivos que permiten la conexión inalámbrica de un dispositivo móvil de cómputo (computadora, tableta, smartphone) con una red. Normalmente, un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos.

Los WAP tienen asignadas direcciones IP, para poder ser configurados.

Muchos WAP pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar roaming.

5.1.5.PLC

Power Line Communications, también conocido por sus siglas PLC, es un término inglés que puede traducirse por comunicaciones mediante línea de potencia y que se refiere a diferentes tecnologías que utilizan las líneas de transmisión de energía eléctrica convencionales para transmitir señales con propósitos de comunicación. La tecnología PLC aprovecha la red eléctrica para convertirla en una línea digital de alta velocidad de transmisión de datos, permitiendo, entre otras cosas, el acceso a Internet mediante banda ancha.

5.2. Dispositivos de capa 2.

En el **nivel de enlace de datos** tenemos:

5.2.1.Bridge.

Un Puente de red (en inglés: bridge) es el dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Interconecta segmentos de red (o divide una red en segmentos) haciendo la transferencia de datos de una red hacia otra con base en la dirección física de destino de cada paquete. A nivel de enlace el Bridge comprueba la dirección de destino y hace copia hacia el otro segmento si allí se encuentra la estación de destino. La principal diferencia de un receptor y hub es que éstos hacen pasar todas las tramas que llegan al segmento, independientemente de que se encuentre o no allí el dispositivo de destino.

El término bridge, formalmente, responde a un dispositivo que se comporta de acuerdo al estándar IEEE 802.1D. En definitiva, un bridge conecta segmentos de red formando una sola subred (permite conexión entre equipos sin necesidad de routers). Funciona a través de una tabla de direcciones MAC detectadas en cada segmento al que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred, teniendo la capacidad de desechar la trama (filtrado) en caso de no tener dicha subred como destino. Para conocer por dónde enviar cada trama que le llega (encaminamiento) incluye un mecanismo de aprendizaje automático (auto aprendizaje) por lo que no necesitan configuración manual.

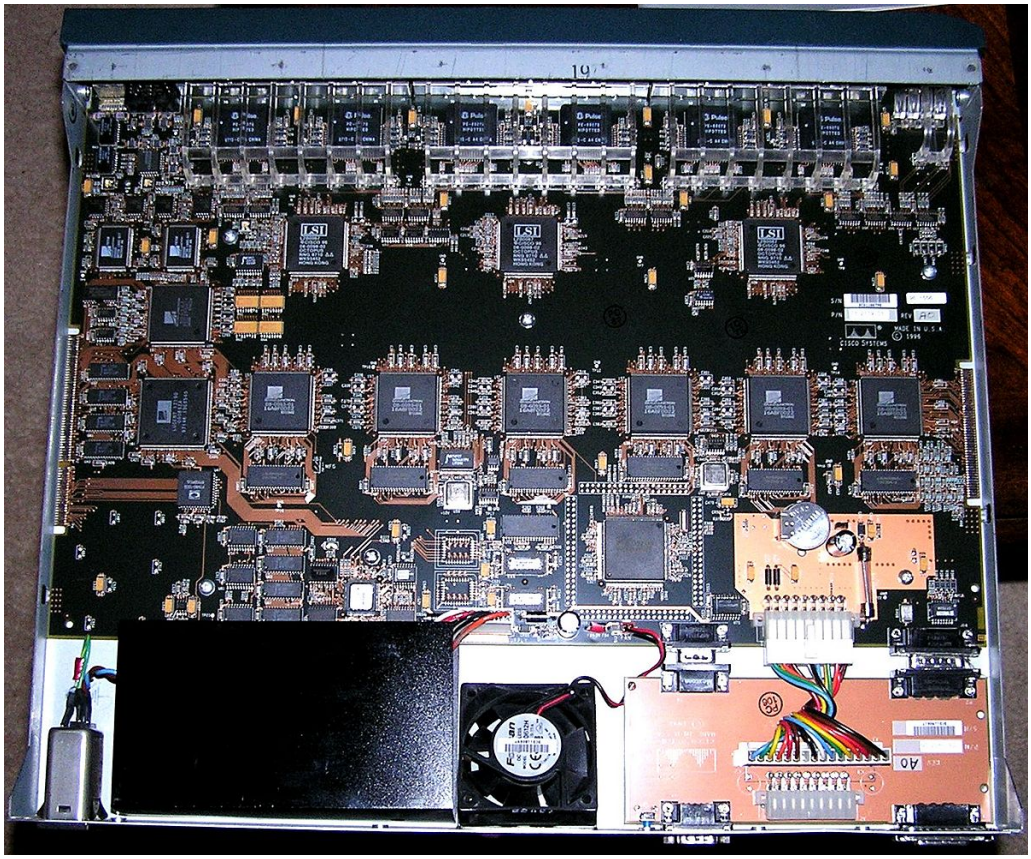
5.2.2.Switch.

Los switches o conmutador, son los encargados de la interconexión de equipos dentro de una misma red, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN, cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

En las primeras versiones de Ethernet, la topología en estrella se implementaba con otro dispositivo conocido como hub. En la actualidad, los hubs se pueden considerar

obsoletos. Y es importante tener en cuenta que, aunque externamente son muy parecidos, los switches tienen prestaciones muy superiores a los hubs por lo que si aún encontramos alguna red que utilice un hub es muy recomendable sustituirlo por un switch.

La función básica de un switch es la de unir o conectar dispositivos en red. Es importante tener claro que un switch NO proporciona por si solo conectividad con otras redes, y obviamente, TAMPOCO proporciona conectividad con Internet. Para ello es necesario un router.



La función básica que realiza un switch se conoce como conmutación y consiste en trasferir datos entre los diferentes dispositivos de la red. Para ello, los switches procesan la información contenida en las cabeceras de la trama Ethernet.

Existen dos técnicas para llevar a cabo la transferencia de los datos entre puertos de un switch:

- Reenvío directo (cut-through). En esta técnica, cuando un switch comienza a recibir datos por un puerto, no espera a leer la trama completa para reenviarla al puerto destino. En cuanto lee la dirección de destino de la trama MAC, comienza a transferir los datos al puerto destino.
  Esta técnica proporciona unos tiempos de retardo bastante bajos, sin embargo, tiene como inconveniente que sólo puede usarse cuando las velocidades de todos los puertos son iguales.
  Otro problema que plantea la técnica cut-through, debido a su forma de funcionamiento, es que los switches propagan tramas erróneas o tramas afectadas por colisiones. Una posible mejora para evitar la propagación de tramas con colisiones es retrasar el reenvío hasta que se lean los primeros 64 bytes de trama, ya que las colisiones sólo se pueden producir en los primeros 64 bytes de la trama. Esta mejora sin embargo aumenta el tiempo de retardo.
- Almacenamiento y reenvío (Store and Forward). En este caso, cuando un switch recibe datos por un puerto, almacena la trama completa en el buffer para luego reenviarla al puerto destino. La utilización de esta técnica permite realizar algunas comprobaciones de error antes de ser enviada al puerto de destino. El tiempo de retardo introducido es variable ya que depende del tamaño de la trama, aunque

suele ser superior al proporcionado por la técnica cut-through, sin embargo, es imprescindible utilizar esta técnica cuando existen puertos funcionando a diferentes velocidades.

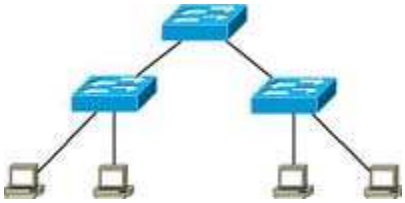
Sin entrar mucho en detalle en el funcionamiento de Ethernet podemos decir que Ethernet es una tecnología de transmisión de datos para redes locales cableadas que divide los datos que se tiene que transmitir en tramas y a cada trama se le añade una determinada información de control llamada cabecera. Dicha cabecera contiene la dirección MAC tanto del emisor como del receptor.

Los switches guardan en una tabla las direcciones MAC de todos los dispositivos conectados junto con el puerto en el que están conectados, de forma que cuando llega una trama al switch, dicha trama se envía al puerto correspondiente.

Características básicas de los switches.

- Puertos: son los elementos del switch que permiten la conexión de otros dispositivos al mismo.
- Cableado: el estándar Ethernet admite básicamente dos tipos de medios de transmisión cableados: el cable de par trenzado y el cable de fibra óptica. El conector utilizado para cada tipo lógicamente es diferente así que otro dato a tener en cuenta es de qué tipo son los puertos. Normalmente los switches básicos sólo disponen de puertos de cable de par trenzado (cuyo conector se conoce como RJ-45) y los más avanzados incluyen puertos de fibra óptica (el conector más frecuente, aunque no el único es el de tipo SC).
- Velocidad: podemos encontrar puertos definidos como 10/100, es decir, que pueden funcionar bajo los estándares 10BASE-T (con una velocidad de 10 Mbps) y 100BASE-TX (velocidad: 100 Mbps). Otra posibilidad es encontrar puertos 10/100/1000, es decir, añaden el estándar 1000BASE-T (velocidad 1000 Mbps). También se pueden encontrar puertos que utilicen fibra óptica utilizando conectores hembra de algún formato para fibra óptica. Existen puertos 100BASE- FX y 1000BASE-X. Por último, los switches de altas prestaciones pueden ofrecer puertos que cumplan con el estándar 10GbE, tanto en fibra como en cable UTP.
- Puertos modulares: GBIC y SFP: no tienen ningún conector específico si no que a ellos se conecta un módulo que contiene el puerto. De esta forma podemos adaptar el puerto al tipo de medio y velocidad que necesitemos.
- Power Over Ethernet: (Alimentación eléctrica por Ethernet), también conocido como POE, es una tecnología que permite el envío de alimentación eléctrica junto con los datos en el cableado de una red Ethernet. Un dispositivo que soporte PoE obtendrá tanto los datos como la alimentación por el cable de red Ethernet: puntos de acceso inalámbricos Wi-Fi, cámaras de video IP, teléfonos de VoIP, etc.

Tipos de switches.



Por increíble que pueda parecer no existe un consenso en el mundo de las redes para establecer una clasificación clara de uno de los dispositivos de red más importantes que existen. La clasificación final aquí propuesta parte de dos parejas de términos que se expondrán a continuación:

- Switch troncal / switch perimetral: El término switch troncal se refiere a los que se utilizan en el núcleo central (core) de las grandes redes. Es decir, a estos switches están conectados otros de jerarquía inferior, además de servidores, routers WAN, etc. Por otro lado, el término switch perimetral se refiere a los utilizados en el nivel jerárquico inferior en una red local y a los que están conectados los equipos de los usuarios finales.
- Switch gestionable (managed) / switch no gestionable (unmanaged): El término gestionable (managed) se refiere a los switches que ofrecen una serie de características adicionales que requieren de configuración y gestión. Por el contrario, los switches no gestionables (unmanaged) suelen ser los que ofrecen funcionalidades básicas que no requieren procedimiento de configuración o gestión.

5.3. Dispositivos de capa 3

En el nivel de red el elemento principal es el router, pero cada equipo final (host o servidor) debe tener una tarjeta de red.

5.3.1. Tarjetas de red.

La tarjeta de red, también conocida como placa de red o adaptador de red, es el periférico que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos (discos duros, impresoras, etcétera) entre dos o más computadoras, es decir, en una red de computadoras. En inglés, se denomina Network Interface Card (NIC), cuya traducción literal es «tarjeta de interfaz de red» (TIR). Cada tarjeta de red tiene un número de identificación único, de 48 bits en hexadecimal, llamado dirección MAC (Media Access Control; control de acceso al medio). Estas direcciones únicas de hardware son administradas por el IEEE. Los tres primeros octetos (24 bits) del número MAC, identifican al proveedor específico y es conocido como número OUI (Organizationally unique identifier, identificador único de organización), designado por IEEE, que combinado con otro número de 24 bits forman la dirección MAC completa.

5.3.2. Router.

El término router se podría traducir como enrutador o encaminador. Desde el punto de vista de la telemática, un router es un dispositivo de red utilizado para unir redes y encaminar datos entre ellas.

Unir redes es la función básica asociada a un router. Sin embargo, la evolución de las redes y de Internet ha hecho evolucionar también a los routers añadiendo cada vez más funcionalidades a los mismos. En la actualidad podemos clasificar los routers en dos grandes grupos:

- Routers de acceso. Son routers utilizados para unir dos redes, normalmente la red de un operador de telecomunicaciones con la red de su cliente, ya sea residencial o corporativo, y ya sea para proporcionar acceso a Internet o proporcionar acceso a otras redes de datos. En este tipo de routers la función de “enrutamiento” es más o menos simple porque solo tienen que intercambiar datos entre dos redes. Por el contrario, suelen incorporar otras funciones adicionales como cortafuegos, NAT, proxy, balanceo de carga, Wi-Fi ...
- Routers de distribución. Son routers que, a diferencia de los anteriores, están conectados a más de dos redes. Este tipo de routers sí mantiene como principal función la de “enrutar” datos entre las diferentes redes a las que están conectados y deben estar preparados para procesar una gran cantidad de información. Utilizan algoritmos de enrutamiento para optimizar la búsqueda de las rutas más óptimas para los datos que manejan.

Para entender la función de “unir redes” de los routers es conveniente tener claro qué es una red desde el punto de vista del enrutamiento. Generalmente el término red se aplica a una agrupación de dispositivos interconectados entre sí. Sin embargo, para un router, una red es una agrupación de dispositivos conectados entre sí... pero que utilizan el mismo rango de direccionamiento. Es decir, los routers se fijan en las direcciones IP de los dispositivos para determinar si pertenecen o no a la misma red.

Una creencia muy extendida es que los routers sólo se usan para conectar redes separadas físicamente, en edificios, ciudades o incluso países diferentes, sin embargo, esto no siempre es así. Dentro de la red de una misma empresa se pueden tener diferentes redes lógicas por cuestiones organizativas, de seguridad o de gestión del propio tráfico de red, de forma que dos equipos conectados a la misma red física pueden pertenecer a redes lógicas diferentes.

5.3.3. Router vs. Switch.

Los dos dispositivos de interconexión por excelencia son los routers y los switches. Es importante diferenciar claramente la función de interconexión en cada uno de ellos.

- Los switches trasfieren datos entre dispositivos ubicados dentro de la misma red.
- Los routers transfieren datos entre dispositivos que se encuentran ubicados en redes diferentes, es decir, transfieren datos entre redes lógicas diferentes.

Desde un punto de vista teórico, estas funciones no son intercambiables, es decir, un switch nunca podrá comunicar equipos ubicados en redes diferentes y un router nunca podrá comunicar equipos dentro de la misma red. Sin embargo, en la práctica hay excepciones...

Los dispositivos “híbridos”.

Efectivamente, la anterior afirmación es cierta sólo en la teoría de redes, ya que en la práctica existen switches con funciones de encaminamiento, llamados switches de nivel 3, y existen routers que incluyen varios puertos Ethernet unidos haciendo las funciones de un switch, por ejemplo, los routers residenciales suelen incluir 4 puertos Ethernet, es decir, un switch de 4 puertos.

Otras funciones de los routers.

Los routers, además de su función como encaminadores del tráfico de red, pueden proporcionar muchas otras funcionalidades. A continuación, describiremos brevemente algunas de ellas:

- Adaptación de los datos entre diferentes tecnologías de transmisión. El caso más típico son los routers residenciales que unen las redes residenciales con las redes de los operadores de telecomunicaciones para proporcionar servicios de conexión a Internet.
- Proporcionar los parámetros de configuración de red. Esta función se lleva a cabo mediante un servicio llamado DHCP y que simplifica mucho la conexión de un dispositivo a la red ya que todos los parámetros de red se configuran de forma automática. Esta función ha cobrado especial importancia en las redes residenciales sobre todo con la tendencia a utilizar dispositivos inalámbricos.
- Filtrado de datos. El filtrado de datos se lleva a cabo principalmente por cuestiones de seguridad. A grandes rasgos, este proceso consiste en establecer unos criterios bajo los cuales los datos pueden pasar o no de una red a otra. Esta función de filtrado se lleva a cabo mediante un elemento conocido como cortafuegos.
- Traducción de direcciones de red. En la actualidad y debido a la escasez de direcciones IP prácticamente todas las redes utilizan un mecanismo de traducción de direcciones de red conocido como NAT que permite el uso de direcciones privadas en redes conectadas a Internet. Esta función es implementada en muchos casos por routers, especialmente en los routers residenciales.
- Otras características que pueden implementarse en los router actualmente:
  - Punto de acceso inalámbrico (Wi-Fi).
  - Redirección de puertos.
  - Servidor proxy.
  - Balanceo de carga/tráfico.
  - Gestión de conexiones VPN.

5.4. Dispositivos de capa 4.

En los **niveles superiores**:

5.4.1. Gateway (o puerta de enlace)

Es el dispositivo que permite interconectar redes de computadoras con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la

información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino. La puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red (Network Address Translation, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada enmascaramiento de IP (IP Masquerading), usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y, por tanto, una única dirección IP externa. La dirección IP de una puerta de enlace a menudo se parece a 192.168.1.1 o 192.168.0.1 y utiliza algunos rangos predefinidos, 127.X.X.X, 10.X.X.X, 172.X.X.X, 192.X.X.x, que engloban o se reservan a las redes locales. Un equipo que haga de puerta de enlace en una red debe tener necesariamente dos tarjetas de red (Network Interface Card, NIC). La puerta de enlace predeterminada (default gateway) es la ruta por defecto que se le asigna a un equipo y tiene como función enviar cualquier paquete del que no conozca por cuál interfaz enviarlo y no esté definido en las rutas del equipo, enviando el paquete por la ruta predeterminada.

En entornos domésticos, se usan los routers ADSL como puertas de enlace para conectar la red local doméstica con Internet; aunque esta puerta de enlace no conecta dos redes con protocolos diferentes, sí que hace posible conectar dos redes independientes haciendo uso de NAT.

5.4.2.Firewall

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

Un firewall puede ser hardware, software o ambos.

Tipos de firewall.

Firewall proxy.

Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como gateway de una red a otra para una aplicación específica. Los servidores proxy pueden brindar funcionalidad adicional, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red. Sin embargo, esto también puede tener un impacto en la capacidad de procesamiento y las aplicaciones que pueden admitir.

Firewall de inspección activa

Un firewall de inspección activa, ahora considerado un firewall “tradicional”, permite o bloquea el tráfico en función del estado, el puerto y el protocolo. Este firewall monitorea toda la actividad, desde la apertura de una conexión hasta su cierre. Las decisiones de filtrado se toman de acuerdo con las reglas definidas por el administrador y con el contexto, lo que refiere a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión.

Firewall de administración unificada de amenazas (UTM)

Un dispositivo UTM suele combinar en forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus. Además, puede incluir servicios adicionales y, a menudo, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso.

Firewall de próxima generación (NGFW)

Los firewalls han evolucionado más allá de la inspección activa y el filtrado simple de paquetes. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado. Un firewall de próxima generación debe incluir lo siguiente:

- Funcionalidades de firewall estándares, como la inspección con estado.
- Prevención integrada de intrusiones.
- Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas.
- Rutas de actualización para incluir fuentes de información futuras

- Técnicas para abordar las amenazas de seguridad en evolución.

Si bien estas funcionalidades se están convirtiendo cada vez más en el estándar para la mayoría de las empresas, los NGFW pueden hacer más.

NGFW centrado en amenazas

Estos firewalls incluyen todas las funcionalidades de un NGFW tradicional y también brindan funciones de detección y corrección de amenazas avanzadas. Con un NGFW centrado en amenazas, puede hacer lo siguiente:

- Estar al tanto de cuáles son los activos que corren mayor riesgo con reconocimiento del contexto completo.
- Reaccionar rápidamente ante los ataques con automatización de seguridad inteligente que establece políticas y fortalece las defensas en forma dinámica.
- Detectar mejor la actividad sospechosa o evasiva con correlación de eventos de terminales y la red.
- Reducir significativamente el tiempo necesario desde la detección hasta la eliminación de la amenaza con seguridad retrospectiva que monitorea continuamente la presencia de actividad y comportamiento sospechosos, incluso después de la inspección inicial.
- Facilitar la administración y reducir la complejidad con políticas unificadas que brindan protección en toda la secuencia del ataque.

5.4.3.Servidor proxy.

Un servidor proxy (cuya traducción literal es “representante”) es una interfaz de comunicación en una red que actúa como mediadora entre dos sistemas informáticos. La tarea básica de un servidor proxy es hacerse cargo, como delegado, de las peticiones de los clientes en un servidor y de transmitirlas con la dirección IP adecuada al ordenador de destino. En este tipo de comunicación no existe una conexión directa entre el remitente y el destinatario. En ocasiones, ni el sistema al que se le hacen las peticiones ni el ordenador de destino saben que hay un proxy de por medio. Los servidores proxy pueden funcionar en dos sentidos. Por un lado, un proxy de reenvío (forward proxy) sirve para proteger a una red cliente frente a influencias de Internet. Si el sistema de destino, por ejemplo, un servidor web, está protegido por medio de un servidor proxy intercalado, se puede hablar en este caso de un proxy inverso (reverse proxy).

- Proxy de reenvío (protección del cliente): si se instala un servidor proxy como interfaz entre una red privada (LAN) e Internet, los terminales locales pueden protegerse de forma efectiva de las influencias de la red pública. El proxy se hará cargo de las peticiones provenientes de la red LAN y las transmitirá con su dirección IP en calidad de remitente al ordenador de destino. Los paquetes de respuesta de la red no se dirigirán al cliente en la red LAN, sino que pasan por el servidor proxy antes de llegar al destino final. En general, el proxy actúa como autoridad de control. Los correspondientes sistemas de seguridad no tienen que instalarse en cada cliente de la red, sino que hay un número considerable de ellos que se ejecutan en servidores proxy.
- Proxy inverso (protección del servidor): los servidores web también pueden protegerse, para lo que se intercalará un servidor proxy al acceder desde la red pública. Los clientes de Internet no pueden acceder de manera directa al ordenador de destino, sino que en su lugar el proxy será el que reciba las peticiones, compruebe su configuración de seguridad y las transmita al servidor de forma segura.

Ámbito de aplicación de un servidor proxy

La implementación de los servidores proxy está ligada a varios factores. En su rol de nexo de unión entre los dos participantes de la comunicación, este componente de red hace posible el intercambio de datos entre dos sistemas en aquellas situaciones en las que no se pueda establecer una conexión directa debido a la presencia de direcciones IP incompatibles, por ejemplo, porque un componente utiliza el protocolo IPv4 y el otro la versión IPv6. Los datos que no adoptan la vía directa, sino que se desvían hacia el proxy, pueden filtrarse, almacenarse de forma intermedia y distribuirse por diversos sistemas de destino mediante el

balanceo de carga. Además, un proxy es un componente fundamental del Firewall que protege a los sistemas informáticos de ataques procedentes de la red pública.

- Caché: esta es otra de las funciones básicas del proxy. Para poder responder con celeridad a las continuas peticiones de una red local, un proxy adecuadamente configurado guarda de manera temporal una copia de los datos obtenidos por parte del servidor desde Internet en el caché. Los contenidos web más solicitados no tienen que cargarse de nuevo cada vez que se quiera acceder a ellos, sino que estos se entregan directamente, lo que ahorra tiempo y ancho de banda.
- Filtrado: cuando se instala un proxy en calidad de interfaz entre dos sistemas informáticos puede usarse como filtro para la transmisión de datos con el objetivo de bloquear determinados contenidos web para los clientes o para rechazar automáticamente peticiones anómalas.
- Control del ancho de banda y distribución de cargas: si se utiliza un proxy para controlar el ancho de banda, este distribuirá los recursos definidos para los clientes de una red en función de la capacidad de carga. Así se puede tener la seguridad de que las aplicaciones no bloquearán el ancho de banda por completo. Debido a su papel de interfaz central, el servidor proxy permite depositar en diferentes sistemas las peticiones de clientes que requieren muchos recursos o las respuestas del servidor, de forma que la carga se pueda distribuir de manera uniforme dentro de una misma red informática.

Ya que el servidor proxy impide la conexión directa entre remitente y destinatario, puede que la dirección IP de un cliente se oculte tras la interfaz de comunicación. Esto permite cierto anonimato, ya que el usuario puede operar de manera externa con la dirección IP y la ubicación del proxy. Aquellos países que tienen una estricta censura en lo referente al uso de Internet o que tienen un acceso restringido a contenidos protegidos por derechos de autor recurren en ocasiones a un servidor proxy en el extranjero para evitar el geoblocking.

Tipos de servidores proxy

Junto a la definición de proxy más general, se dan diversas denominaciones para diferentes tipos de servidores proxy, referentes tanto a la realización técnica de los componentes de red como a las diferencias en cuanto a su aplicación. Lo más habitual es establecer una división entre servidores proxy de aplicación y de circuito y servidores dedicados y genéricos.

6. Tecnologías de redes.

6.1. NAT

La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

6.2. VLAN

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único switch físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local.

Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo switch, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (Local).

La norma que implementa el estándar es la IEEE 802.1q.

Para comunicar los diferentes segmentos se emplean los puertos troncales o puertos trunk.

6.3. VPN

Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

Usa el protocolo IPSec.

VPN de acceso remoto.

Es quizás el modelo más usado actualmente, y consiste en usuarios que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Para conectarse a la red es necesario el software específico llamado Home Agent.

VPN se sitio a sitio.

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.