UT 1: INTRODUCCIÓN A LOS SERVICIOS EN RED

1. Introducción

Las redes informáticas son un conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras. Estas redes permiten la conexión para enviar, compartir y distribuir información y recursos (como programas, impresoras, archivos de bases de datos, ...)

En este módulo nos vamos a centrar en los programas informáticos necesarios para que la red, cómo conjunto de dispositivos físicos, tenga un sentido de ser. La red tiene que ofrecer las suficientes herramientas cómo para que desde los equipos conectados a ella se pueda realizar la labor por la que ha sido implementada.

2. La arquitectura TCP/IP, el modelo Cliente/servidor y los servicios de red.

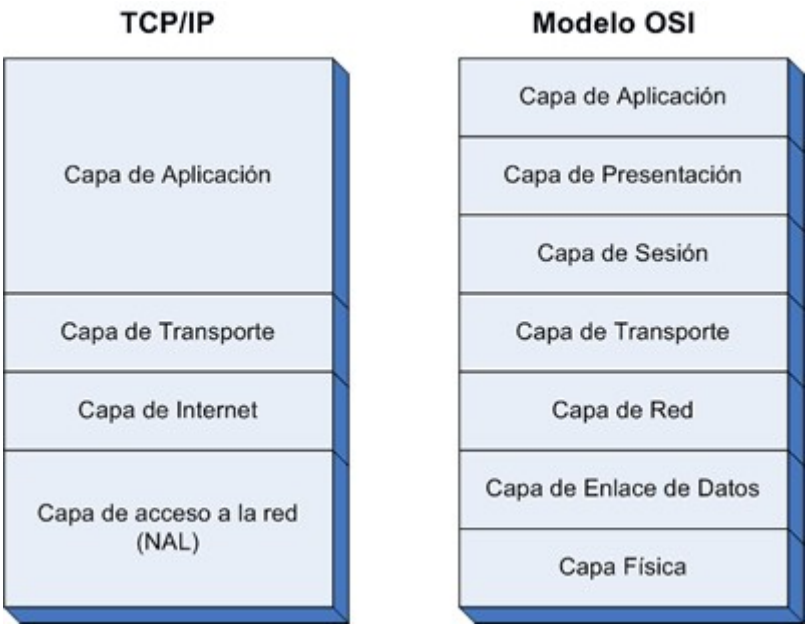
La arquitectura TCP/IP está orientada a funcionar en un entorno cliente/servidor, por lo que facilita la tarea de la implantación de servicios en la red, ya que los que vamos a ver a lo largo del curso están integrados en ella.

2.1.La arquitectura TCP/IP y el modelo OSI

El modelo OSI es simplemente un modelo de referencia que ha pasado a ser un referente para establecer lo que serían después las familias de protocolos, nunca se llegó a implementar ni a imponerse cómo estándar. Sin embargo TCP/IP, aún siendo una arquitectura anterior a OSI, nos proporciona una estructura y una serie de normas de funcionamiento para poder interconectar sistemas.

Cabe recordar que toda arquitectura está establecida mediante un conjunto de capas que definirán el orden jerárquico de las operaciones, además de englobarlas en un conjunto de protocolos orientados a realizar trabajos para una misma función de la acción de la comunicación entre dispositivos.

Para ver más claro de lo que hablamos hay que tener en cuenta que la arquitectura TCP/IP está estructurada en 4 capas o niveles relativamente bien definidos.



1 Arquitectura TCP/IP y modelo de referencia OSI

Las funciones de las diferentes capas en TCP/IP son las siguientes:

- **capa de acceso a la red**: especifica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado;
- **capa de Internet**: es responsable de proporcionar el paquete de datos (datagrama);
- **capa de transporte**: brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión;
- **capa de aplicación**: incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.).

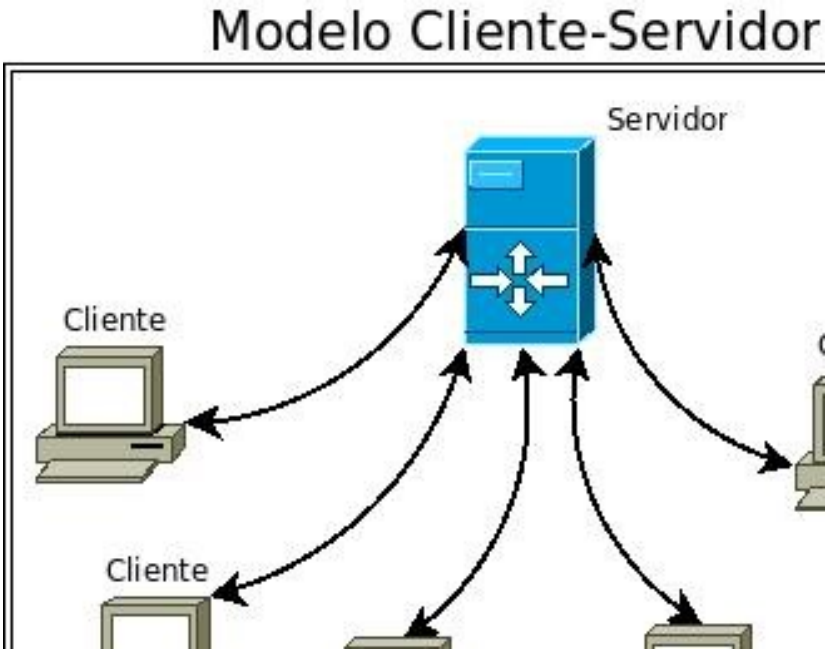
2.2.El modelo Cliente/Servidor

Para la comunicación de aplicaciones a través de una red se emplean tres modelos:

- **El modelo cliente/servidor:** En este modelo se distingue entre un proceso cliente (que generalmente solicita servicios) y un proceso servidor (que presta el servicio al cliente).
- **El modelo entre iguales o P2P**. En este modelo todos los nodos de la red son responsables por igual en la comunicación de las aplicaciones y no existe un elemento que centralice la comunicación.
- **El modelo híbrido**. Es una combinación de los dos anteriores, el servidor no presta servicios sino que es un mero intermediario entre los clientes que son los que en realidad ofrecen sus prestaciones.

El modelo **cliente/servidor** es el más extendido y el que se aplica en la mayoría de los diferentes servicios, por lo tanto será en el que nos vamos a centrar en este curso.

La separación entre **cliente** y **servidor** es una separación de tipo lógico, donde el servidor no se ejecuta necesariamente sobre una sola máquina ni es necesariamente un sólo programa.



Este modelo está formado básicamente por dos procesos que van a interactuar entre sí, el proceso **cliente** y el proceso **servidor.**

- El cliente es el proceso que habitualmente inicia la comunicación a través de peticiones al servidor, quedando a la espera de respuesta.
- El servidor es el proceso que inicialmente está a la espera de posibles peticiones de los clientes.

A. Ventajas de la arquitectura cliente/servidor

El modelo cliente/servidor se recomienda, en particular, para redes que requieran un alto grado de fiabilidad. Las principales ventajas son:

- **recursos centralizados**: debido a que el servidor es el centro de la red, puede administrar los recursos que son comunes a todos los usuarios, por ejemplo: una base de datos centralizada se utilizaría para evitar problemas provocados por datos contradictorios y redundantes.
- **seguridad mejorada**: ya que la cantidad de puntos de entrada que permite el acceso a los datos no es importante.
- **administración al nivel del servidor**: ya que los clientes no juegan un papel importante en este modelo, requieren menos administración.
- **red escalable**: gracias a esta arquitectura, es posible quitar o agregar clientes sin afectar el funcionamiento de la red y sin la necesidad de realizar mayores modificaciones.

B. Desventajas del modelo cliente/servidor

La arquitectura cliente/servidor también tiene las siguientes desventajas:

- **costo elevado**: debido a la complejidad técnica del servidor.
- **un eslabón débil**: el servidor es el único eslabón débil en la red de cliente/servidor, debido a que toda la red está construida en torno a él. Afortunadamente, el servidor es altamente tolerante a los fallos (principalmente gracias al sistema RAID).

2.3. Los servicios de red

Un servicio de red es una función o prestación que ofrecen las aplicaciones y protocolos a los usuarios o a otras aplicaciones, las cuales se comunican e intercambian información con otras aplicaciones, con la ayuda de los protocolos de la arquitectura TCP/IP, tanto a nivel de aplicación como de niveles inferiores.

Aunque muchas veces vamos a hablar de protocolos y aplicaciones que se llaman igual, no hay que confundirlos.

- Los **protocolos** son normas concretas, descritas formalmente, que detallan cómo se produce la comunicación entre sistemas para ofrecer los servicios de red.
- Las **aplicaciones** son los diferentes programas que se sirven de los protocolos para comunicarse.

Ejemplo de esto son:

- Servicio web:
  - -Aplicaciones: Apache, Google Chrome.
  - -Protocolos: HTTP, HTTPS,..
- Servicio de correo electrónico:
  - -Aplicaciones: Postfix, Exchange, Thunderbird, Outlook,..
  - -Protocolos: POP, SMTP, IMAP.

Para entender claramente el funcionamiento de un servicio de red es importante conocer los niveles de red y transporte de la arquitectura TCP/IP.

3. Líneas conmutadas y dedicadas

A la hora de tratar los sistemas de telecomunicaciones tenemos que tratar las diferentes formas en las que podemos conectar nuestra red a la red pública.

A. **Líneas de acceso conmutado (LAC).** Necesitan establecer una llamada entre ambos extremos para realizar la comunicación. Las tecnologías que funcionan como LAC son las siguientes:
   - Red telefónica conmutada o red telefónica básica (RTC/RTB).

- Red Digital de Servicios Integrados (RDSI).
- Sistemas de telefonía móvil analógicos (NMT/AMPS/TACS).
- Sistema Global de Comunicaciones Móviles (GSM).
- Servicio General de Paquetes de Radio Mejorado (EGPRS/EDGE).

B. **Líneas de acceso dedicado (LAD):** Son exclusivas de los clientes que las han contratado, las utilizan a tiempo completo. En todo momento se mantienen activas y se dispone de la capacidad de transmisión de forma permanente sin que sea preciso establecer una llamada previa. Poseen un ancho de banda mucho mayor y en consecuencia son más caras. Podemos encontrarnos las siguientes tecnologías:
   - La familia XDSL, líneas de abonado digital.
   - Redes mixtas de TV e Internet por cable (CATV).
   - Conexión por cable eléctrico (PLC/BPL).
   - Redes de fibra hasta el hogar (FTTx).
   - Vía satélite (VSAT).
   - Servicio de distribución multipunto (LMDS/MMDS).
   - Redes metropolitanas inalámbricas (WiMaX).
   - Sistema de telefonía móvil universal (UMTS/WCDMA).
   - Sistema de telefonía móvil universal avanzado (HSDPA/HSUPA).
   - Sistema de telefonía móvil sobre IP (LTE/SAE).

3.1. Red de telefonía conmutada (RTC/RTB).

Es la primera tecnología que surgió, se trata de una red de banda estrecha que funciona de manera analógica sobre un par trenzado de cobre, del cual solo utiliza dos hilos, uno para transmisión y otro para recepción. Usa señales analógicas, por lo tanto las señales digitales de los ordenadores hay que convertirlas previamente en analógicas para poder viajar por este medio.

3.2. Red digital de servicios integrados (RDSI).

Funciona sobre par trenzado de cobre también, aunque de manera digital. Normaliza e integra los servicios disponibles hasta su aparición, con señales digitales entre emisor y receptor.

Existen dos tipos de RDSI:

- De banda ancha, pudiéndose utilizar con velocidades superiores a 2Mbps para dar servicios de TV y videoconferencia.
- De banda estrecha, empleado en conexiones conmutadas de 64Kbps hasta los 2 Mbps. Este caso tiene 2 interfaces de abonado:
  - Acceso básico (BRI). Dos canales B para datos a 64kbps, que se pueden agrupar en más canales y conseguir una mayor velocidad de transferencia, y un canal de control D a 16kbps.
  - Acceso primario (PRI). 30 canales B para datos a 64kbps y un canal de control D a 6 kbps.

3.3. Familia de tecnologías de línea de abonado digital (xDSL).

Utilizan el bucle actual de abonado de cable de par trenzado de cobre, sobre los que trabajan para convertirlo en una línea digital de alta velocidad de banda ancha, aprovechando la parte que no utilizan debido a que el canal de voz solo usa una ínfima parte del mismo.

Podemos encontrarnos dos tipos básicos de DSL.

- DSL simétricos: Tienen la misma velocidad de subida que de bajada.
- DSL asimétricos: La velocidad de bajada es inferior a la de subida.

ADSL ha sido la tecnología predominante en nuestro país hasta hace poco tiempo, consiguiendo cómo máximas velocidades 24/1,2Mbps. La tecnología **VDSL** implantada como sustituto a ADSL por algunas compañías consigue aumentar el bitrate hasta los 50/20 Mbps.

3.4. Conexión por cable eléctrico (PLC/BPL).

La tecnología de conexión por cable eléctrico aprovecha las redes de cables eléctricos de baja tensión para convertirlos en una línea digital de alta velocidad.

No se ha implantado ya que supone un alto coste para las compañías, por lo tanto su uso se ha restringido al ámbito local/domestico.

3.5.Redes de fibra hasta el hogar (FTTx).

Redes que están teniendo un gran auge en los últimos tiempos, la implantación de esta red hasta el hogar requiere de una gran inversión por lo que se van implantando poco a poco.

A modo de resumen podemos encontrarnos con las siguientes clasificaciones de fibra óptica.

- FTTN (Fibra hasta el nodo). La fibra llega hasta el nodo o punto de terminación de red óptica (ONU, Optical Network Unit), compartido por varios usuarios que acceden a través del par trenzado.
- FTTC(Fibra hasta la acera). La fibra llega hasta un punto ONU situado en la esquina de la manzana del abonado y al que se accede a través de la red de cobre.
- FTTB (Fibra hasta el edificio). La fibra llega hasta el edificio donde hay un punto que suministra el servicio.
- FTTH (Fibra hasta el hogar). La fibra llega desde el nodo de servicio de la central hasta el nodo terminal del abonado que se encuentra en la casa del cliente.

3.6. Redes mixtas de TV e Internet por cable (CATV).

Las redes de TV por cable constituyen otra tecnología digital utilizada en la actualidad como banda ancha para el acceso a Internet, tradicionalmente usan cómo medio de transmisión cable coaxial, aunque actualmente se tratan de redes mixtas de fibra óptica y cable coaxial.

El cable módem o router se conecta a la toma coaxial que el operador haya instalado, esta tecnología permite velocidades de superiores a los 100Mbps de descarga.

3.7.Vía satélite (VSAT).

Los satélites usados para transmitir información pueden clasificarse en dos grupos:

- **Satélites banda-C:** más antiguos, frecuencias de 3,7 a 6,4 GHz y requieren antenas parabólicas grandes.
- **Satélites banda-Ku:** más modernos, frecuencias de 11 a 12 GHz y requieren de antenas parabólicas pequeñas (uso domestico).

4. Nivel de red en TCP/IP – El protocolo IP.

En este nivel se realiza el direccionamiento de los dispositivos y el encaminamiento de la información a través de la red. Todo ello se lleva a cabo con el protocolo IP, el principal protocolo de este nivel en la arquitectura TCP/IP. La comunicación a nivel IP se hace mediante unidades de datos denominadas **datagramas** que siguen el formato especificado en el propio protocolo IP.

Actualmente se sigue empleando de forma mayoritaria (y más si hablamos de redes privadas) la versión 4 del protocolo IP (**IPv4),** aunque la versión **IPv6** se sigue implantando de forma paulatina. Nosotros nos enfocaremos en la versión 4 de IP.

4.1.Direccionamiento IP

El protocolo IP proporciona conectividad extremo a extremo en la comunicación. Esto supone que debe ser capaz de direccionar de forma única todos los dispositivos que tengamos conectados en nuestra red y en todo Internet. Este direccionamiento es lógico, de forma que es independiente del dispositivo físico al que es asignado y puede ser modificado.

Hay que tener en cuenta que una dirección IP se asigna a una interfaz de red, por lo que un equipo con más de una interfaz de red puede estar conectado a diferentes segmentos de la red o diferentes redes, mediante una asignación de IP diferente a cada interfaz que tenga.

4.1.1. Formato de direcciones IP

Una dirección IP es un número binario de 32 bits. Esto permite un espacio de direcciones de 2^{32} direcciones diferentes posibles. Habitualmente, la notación empleada para facilitar la legibilidad de las direcciones IP es la notación decimal con

puntos. Así, se dividen los 32 bits en 4 grupos de 8 bits, escribiendo cada uno de ellos en base decimal, separando por puntos los cuatro números resultantes.

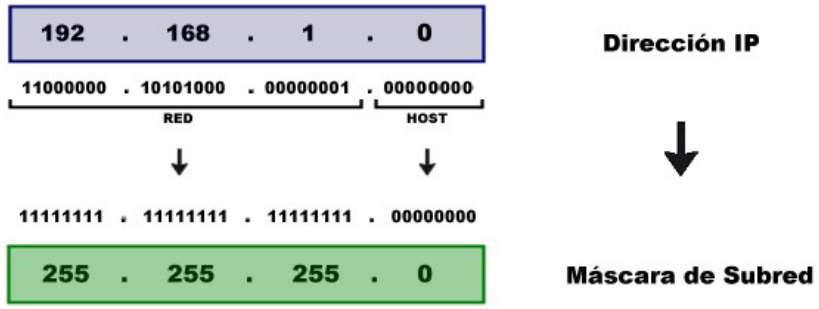
A efectos de direccionamiento y de encaminamiento, las direcciones IP constan de dos partes:

- **Identificador de red**, que determina en la red que se encuentra el dispositivo.
- **Identificador del host** dentro de la red.

De esta forma todos los hosts de una misma red comparten el identificador de la red. Para poder establecer estas partes de dirección IP, necesitamos la **máscara de red.**

4.1.2. Máscara de red

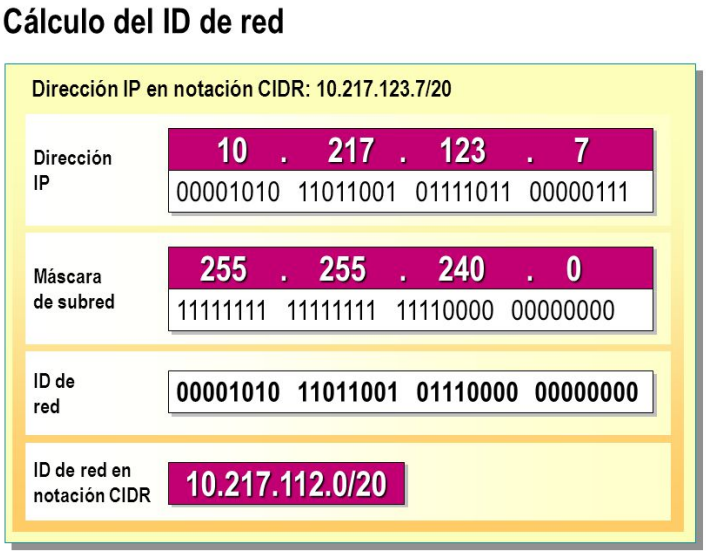
La **máscara de red** se emplea para diferenciar el prefijo de la dirección IP correspondiente al **identificador de red**, de la parte correspondiente al identificador del host. La máscara de red es un número de 32 bits que define en las posiciones a "1" el prefijo o **identificador** de red, y en las posiciones a "0" el sufijo o **identificador del host**.



Si tenemos la máscara de red y una dirección IP cualquiera, **podemos conocer a que segmento de la red (dirección de red)** pertenece con una simple operación en binario. Consiste en hacer un **Y lógico** entre la dirección **IP** y la **máscara de red** en binario. El resultado de la operación será la dirección de red.

```
10101100.00010001.00010111.00000100  = 172.17.23.4
                  AND
11111111.11111111.00000000.00000000  = 255.255.0.0
-------------------------------------
10101100.00010001.00000000.00000000  = 172.17.0.0
```

La máscara de red también puede expresarse mediante la notación CIDR (Classless Inter-Domain Routing) consistente en situar un sufijo a continuación de la dirección IP que indica cuántos bits de la máscara de red están a 1.



4.1.3. Clases de direcciones IP.

En un principio se predeterminaron una serie de máscaras de red concretas para facilitar el proceso de encaminamiento que dieron como resultado 5 clases de direcciones:

- Clase A: Empiezan por 0 en binario, el primer byte identifica la red y el resto al hots. Esta clase es para las redes muy grandes, tales como las de una gran compañía internacional. Del IP con un primer octeto a partir de 0 al 127 son parte de esta clase. Los otros tres octetos son usados para identificar cada anfitrión. Esto significa que hay 126 redes de la clase A con 16,777,214 (2^24 -2) posibles anfitriones para un total de 2,147,483,648 (2^31) direcciones únicas del IP. Las redes de la clase A totalizan la mitad de las direcciones disponibles totales del IP.

- Clase B: Empiezan por 10 en binario, los dos primeros bytes identifican la red y el resto al host. La clase B se utiliza para las redes de tamaño mediano. Un buen ejemplo es un campus grande de la universidad. Las direcciones del IP con un primer octeto a partir del 128 al 191 son parte de esta clase. Las direcciones de la clase B también incluyen el segundo octeto como parte del identificador neto. Utilizan a los otros dos octetos para identificar cada anfitrión (host). Esto significa que hay 16,384 (2^14) redes de la clase B con 65,534 (2^16 -2) anfitriones posibles cada uno para un total de 1,073,741,824 (2^30) direcciones únicas del IP.

- Clase C: Empiezan por 110 en binario, los tres primeros bytes identifican la red y el resto al host. Las direcciones de la clase C se utilizan comúnmente para los negocios pequeños a medianos de tamaño. Las direcciones del IP con un primer octeto a partir del 192 al 223 son parte de esta clase. Las direcciones de la clase C también incluyen a segundos y terceros octetos como parte del identificador neto. Utilizan al último octeto para identificar cada anfitrión. Esto significa que hay 2,097,152 (2^21) redes de la clase C con 254 (2^8 -2) anfitriones posibles cada uno para un total de 536,870,912 (2^29) direcciones únicas del IP.
- Clase D: Utilizado para los **multicast**, la clase D es levemente diferente de las primeras tres clases. Empezando por 1110 en binario, los otros 28 bits se utilizan para identificar el grupo de computadoras al que el mensaje del multicast está dirigido. La clase D totaliza 1/16ava (268,435,456 o 2^28) de las direcciones disponibles del IP.
- Clase E: La clase E se utiliza para propósitos experimentales solamente. Como la clase D, es diferente de las primeras tres clases. Empiezan por 1111 en binario.

4.1.4. Direcciones IP especiales.

Dentro del conjunto de direcciones IP hay algunas particularmente importantes que merecen una explicación aparte:

- **Dirección de red:** identifica al conjunto de la red. En ella la parte correspondiente al identificador del dispositivo tiene todos sus bits a 0. Así, la dirección IP 204.51.170.5/24 tiene la dirección de red 204.51.170.0/24.
- **Dirección de difusión limitada:** se emplea para mandar un mensaje de difusión o broadcast al conjunto de dispositivos de la propia red. Es la misma para todas las redes (255.255.255.255).
- **Dirección de difusión dirigida:** se emplea para mandar un mensaje de difusión obradcast al conjunto de dispositivos de una red. Por tanto, no puede asignarse a una interfaz de red en concreto. Viene dado por el identificador de la red en la que queramos hacer la difusión a la izquierda y los bits correspondientes a la dirección del dispositivo van todos a 1 a la derecha. Por ejemplo, la dirección IP 204.41.170.255/24 hace difusión dirigida en la red 204.51.170.0/24.
- **Dirección de bucle local (loopback):** El rango de la dirección IP 127.0.0.0 - 127.255.255.255 es reservado para bucle, es decir, un Host de la dirección, también conocido como dirección localhost. Esta dirección IP de bucle es totalmente administrado por y dentro del sistema operativo. Las direcciones de loopback, permiten que el servidor y el cliente los procesos en un único sistema para comunicarse con los demás. Cuando un proceso crea un paquete con dirección de destino como dirección de bucle, el sistema operativo los bucles a si mismo sin tener ninguna interferencia de NIC.

4.1.5. Direcciones públicas y privadas.

Hay que diferenciar entre las direcciones públicas de las privadas.

- **Direcciones públicas:** Identifican un dispositivo conectado a Internet. Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet. Algunos ejemplos son: los servidores que alojan sitios web como

Google, los ***router o modems*** que dan a acceso a Internet, otros elementos de hardware que forman parte de su infraestructura, etc.
Las IP públicas son siempre únicas. No se pueden repetir. Dos equipos con IP de ese tipo pueden conectarse directamente entre sí. Por ejemplo, tu router con un servidor web. O dos servidores web entre sí.

- **Direcciones privadas**: Rangos de direcciones empleados en redes privadas o intranet. Hay unos rangos de direcciones que se reservan para redes privadas y por tanto los routers conectados a redes públicas descartan el tráfico dirigido a estas direcciones privadas. *Para IPv4*

  De 10.0.0.0 a 10.255.255.255

  172.16.0.0 a 172.31.255.255

  192.168.0.0 a 192.168.255.255

  Estas IP deben ser únicas dentro de una misma red. Cada equipo o dispositivo ha de tener la suya, distinta de la de los demás. De lo contrario habría problemas. Sería como si dos vecinos tuvieran el mismo nombre y la misma dirección física. El cartero nunca sabría a quién corresponde la carta que les envíen.

4.1.6. Direcciones de enlace local.

En el caso de que un host no es capaz de obtener una dirección IP del servidor de DHCP y que no se ha asignado ninguna dirección IP de forma manual, el host puede asignarse a sí mismo una dirección IP de un rango de direcciones de enlace local. Dirección de vínculo local oscila entre 169.254.0.0 - 169.254.255.255.

Supongamos que un segmento de la red en caso de que todos los sistemas están configurados para obtener las direcciones IP de un servidor DHCP conectados al mismo segmento de red. Si el servidor DHCP no está disponible, no en el segmento será capaz de comunicarse con cualquier otro. Windows (98 o superior), y Mac OS (8.0 o posterior) admite esta funcionalidad de auto-configuración de dirección IP local de enlace. En ausencia de servidor DHCP, cada máquina host elige al azar una dirección IP de la mencionada y, a continuación, comprueba para determinar por medio de la ARP, si algún otro host no ha configurado a sí mismo con la misma dirección IP. Una vez todos los hosts están utilizando las direcciones locales de enlace de la misma gama, se pueden comunicar con los demás.

4.2.Encaminamiento IP.

El encaminamiento es el proceso de llevar un datagrama desde la máquina origen a la máquina destino, independientemente de si ambas máquinas están o no en la misma red. Por tanto esta función proporciona los mecanismos necesarios para interconectar distintas redes físicas. La formación de la red virtual que conecta múltiples redes se consigue por medio de unos *hosts* especiales denominados **encaminadores o routers.**

4.2.1. Encaminadores.

Los encaminadores son dispositivos que enlazan diferentes redes y realiza el encaminamiento de todo el tráfico de datagramas que pase por él, para ello tiene las llamadas tablas de encaminamiento con la información necesaria de las redes que interconectan.

Los propios equipos también realizan una función de enrutamiento, aunque solo encaminan el tráfico saliente. Los routers encaminan todo el tráfico que pasa por ellos, pudiendo darse dos situaciones:

- El datagrama que recibe va dirigido a una red que conecta directamente y la entrega es directa. La entrega directa es la transmisión de un datagrama desde el *host* origen hasta el *host* destino a través de una sola red física, dicho de otra forma, dos *hosts* sólo pueden comunicarse mediante entrega directa si ambos están conectados directamente a la misma red física (por ejemplo, una sola red Ethernet). Básicamente en la entrega directa el emisor encapsula el datagrama dentro de una trama física, transforma la dirección IP destino en una dirección física y envía la trama resultante al destino a través del *driver* del dispositivo *hardware* correspondiente.
- El datagrama que recibe va dirigido a una red que no conecta directamente, entonces el datagrama lo envía a otro encaminador (entrega indirecta). La entrega indirecta es más compleja ya que el *host* origen ha de identificar al *router* al que debe entregar el datagrama, el primer *router* debe identificar cuál será el siguiente *router* al que debe enviar el datagrama, esto también se denomina identificar el "siguiente salto".

4.2.2. Tablas de encaminamiento.

Almacenan la información necesaria para realizar el encaminamiento de los datagramas, siendo los campos más importantes:

- **Destino (D):** Dirección IP del destino.
- **Máscara de red (MR):** Asociada al destino.
- **Interfaz:** dirección IP del propio encaminador por la que se envía el datagrama.

Se distinguen tres tipos de destinos:

- **Ruta de red:** La entrada se refiere a toda una red (dirección de red).
- **Ruta de host:** La entrada se refiere a un host.
- **Ruta por defecto:** Si el destino no está en ninguna de las entradas anteriores (no es conocido) se envía a esta ruta.

4.2.3. Protocolos de encaminamiento.

Los routers calculan el mejor camino para enviar un paquete a destino mediante los protocolos de encaminamiento. Los protocolos de encaminamiento no son los protocolos enrutables (aquellos de nivel de red).

Hay dos conceptos que utilizan los protocolos de enrutamiento:

- **El mejor camino** es la ruta mas eficiente para llegar a destino. El mejor camino dependerá de la actividad de la red, de los enlaces fuera de servicio o saturados, velocidad de transmisión de los enlaces, etc.
- **El coste de una ruta** es un valor numérico que indica lo bueno que es una ruta.
- **El tiempo de convergencia** es el tiempo que tarda un router en encontrar la mejor ruta cuando se produce una alteración topológica en la red que exige que se recalculen las rutas.

Al arrancar los equipos las tablas de encaminamiento se inicializan con las redes adyacentes, a partir de aquí se pueden configurar las tablas de dos formas:

a) **Encaminamiento estático:** La configuración de las tablas se hace de forma manual, es una técnica no adaptativa, cualquier cambio en la red debe ser supervisado por el administrador para evitar rutas imposibles o bucles. Es muy sensible a fallos y solo recomendable en redes pequeñas con topología fija.

b) **Encaminamiento dinámico:** El propio encaminador actualiza sus tablas gracias a protocolos específicos cómo **RIP, OSPF** y **BGP.** los encaminadores mantienen sus propias tablas actualizadas intercambiando información unos con otros. Los encaminadores pueden descubrir dinámicamente:
   - Si se ha añadido una nueva red a la Internet.
   - Que el camino a un destino ha fallado y que ya no se puede alcanzar dicho destino.
   - Se ha añadido un nuevo encaminador a la Internet. Este encaminador proporciona un camino más corto a ciertos lugares.

5. Nivel de transporte en TCP/IP – Protocolos TCP y UDP

Este nivel nos provee de elementos para diferenciar y gestionar, de forma simultánea, múltiples orígenes y destinos en una comunicación y múltiples comunicaciones en cada equipo, además de permitirnos realizar comunicaciones con servicios orientados a conexión.

5.1.Puertos de comunicaciones.

Un puerto de comunicaciones nos permite identificar los procesos del nivel de aplicación entre los que se establece la comunicación, cada proceso del nivel de aplicación tiene asignado uno o varios puertos. Un puerto se identifica con un número binario de 16 bits. (0 a 65535)

Existen varias clases de puertos:

- **Puertos conocidos (0 – 1023):** conocidos como **well known ports,** están reservados para aplicaciones y servicios estándar.
- **Puertos registrados (1024 – 49151):** para aplicaciones no estándar instaladas por el usuario. Se asignan dinámicamente si ningún servicio hace uso de ellos.
- **Puertos dinámicos (49152 – 65535):** habitualmente se emplean para iniciar conexiones desde el cliente.

La correspondencia entre procesos y puertos se hace de dos formas:

- **Asignación estática:** asignados previamente (los puertos conocidos).
- **Asignación dinámica:** cuando un proceso necesita un puerto y no lo tiene asignado, se le asigna uno disponible.

En nivel de transporte disponemos de dos protocolos, ambos manejan puertos, pero son independientes. Son el **TCP** y el **UDP.**

5.2. Protocolo UDP.

Al igual que IP este protocolo proporciona un servicio no orientado a conexión, suele emplearse en casos en los que prevalece la velocidad o en aplicaciones con requerimientos sencillos. (DHCP, DNS, streaming, VoIP).

5.3. Protocolo TCP.

El protocolo TCP proporciona un servicio orientado a conexión con lo que existen diferencias respecto a UDP. TCP obliga al establecimiento de una conexión, ofrece control de flujo y de errores con o que garantiza un servicio fiable.

5.3.1. Conexiones TCP.

La conexión TCP se hace antes de iniciar una comunicación, una vez establecida se puede empezar a transmitir. Cada conexión TCP se identifica por estos cuatro elementos. (IP origen, puerto TCP origen) → (IP destino, puerto TCP destino). No puede haber dos conexiones TCP que tengan en común estos 4 elementos.

6. Elementos de interconexión de redes

El objetivo de la Interconexión de Redes (internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.

- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

Tipos de Interconexión de redes.

Se pueden distinguir dos tipos de interconexión de redes, dependiendo del ámbito de aplicación:

- Interconexión de Área Local (RAL con RAL)

Una interconexión de Área Local conecta redes que están geográficamente cerca, como puede ser la interconexión de redes de un mismo edificio o entre edificios, creando una Red de Área Metropolitana (MAN)

- Interconexión de Área Extensa (RAL con MAN y RAL con WAN)

La interconexión de Área Extensa conecta redes geográficamente dispersas, por ejemplo, redes situadas en diferentes ciudades o países creando una Red de Área Extensa (WAN)

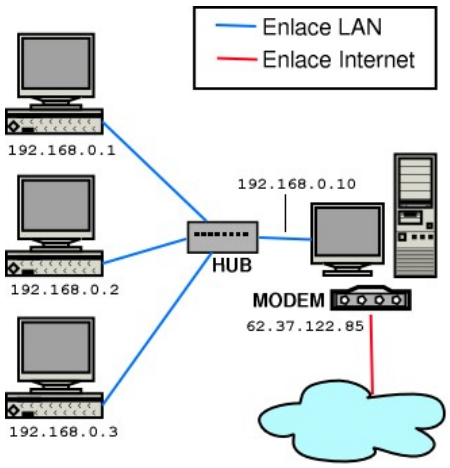
Nos podemos encontrar una gran variedad de dispositivos de interconexión.

Concentrador o hub: Son equipos que permiten compartir el uso de una línea entre varios ordenadores. Todo los ordenadores conectados a los concentradores pueden usar la línea aunque no de forma simultánea, ni utilizando distintos protocolos, ni distintas velocidades de transmisión.

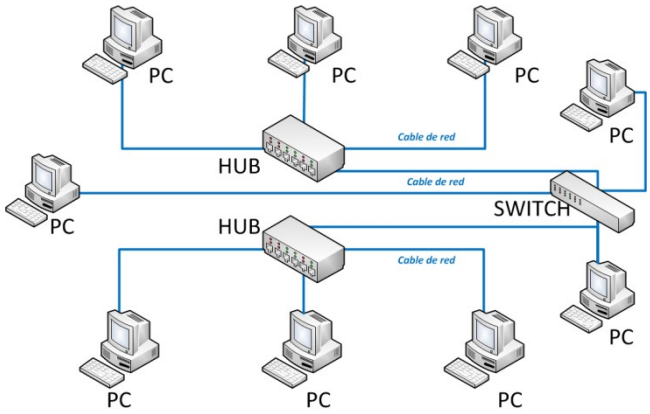
Repetidores: Es un dispositivo encargado de regenerar la señal en un segmento de una red homogénea ampliando su cobertura.

Su forma de actuar es la siguiente: Recoge la señal que circula por la red y la reenvía sin efectuar ningún tipo de interpretación.

Gatewey (pasarela): Es un sistema formado por hw y sw que permite la comunicación entre una red local y un gran ordenador, se suelen colocar en el servidor de comunicaciones



Switch (conmutador): Se caracterizan por no enviar los paquetes a todos los puertos sino únicamente al puerto correspondiente al destinatario. La diferencia entre switch y un puente (bridge), es que el puente debe recibir todo el paquete antes de dirigirlo al puerto correspondiente y un conmutador dirige el paquete a su destino una vez recibido el encabezado del paquete, en ella encuentra la IP del destinatario.



Utilizando un conmutador se puede dividir una red en segmentos a los que pertenece el paquete con menos colisiones y mejor tiempo de respuesta.

Router (encaminador): Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Puede ser un dispositivo, sw, hw o una combinación de ambos.

A parte de los diferentes dispositivos de interconexión que nos podemos encontrar, también cabe puntualizar los diferentes medios de transmisión.

7. VPN, VLAN

7.1.VPN

Las VPN (Redes Privadas Virtuales) constituyen la tecnología más utilizada por las empresas para crear redes que aprovechan estructuras o redes públicas (en muchos casos, la propia red de Internet) para el envío de datos privados. Es decir, forman una red virtual con segmentos físicos de red local propia, separados en la distancia pero que aprovechan infraestructuras públicas de tipo WAN.

Conviene resaltar que la característica de este tipo de redes no reside en la parte intermedia (la red WAN), sino en la capacidad de interconexión de las redes de área local, tanto cableada como inalámbrica, además de su conformación como una sola red privada virtual.

Las VPN utilizan protocolos de autenticación y tunelización, así como de encriptación y compresión de datos, para que la red lógica virtual resultante sea lo más segura, fiable y óptima posible.

Protocolos	Siglas	Capa TCP/IP	Descripción
Point-to-Point Protocol	PPP	2 de nivel de enlace	Protocolo asociado a la pila TCP/IP que perite conectar de forma segura a un cliente con su ISP. En un principio se utilizaba con RTC/RDSI
Point-to-Point Protocol over ATM	PPPoA	2 de nivel de enlace	Variante del PPP que utiliza la tecnología ATM con xDSL/FTTx/CATV.
Point-to-Point Protocol over Ethernet	PPPoE	2 de nivel de enlace	Similar a PPPoA, pero utiliza la tecnología Ethernet en vez de ATM.
Internet Protocol Security	IPSec	3 de red	Conjunto de protocolos que aseguran las comunicaciones. Se utiliza conjuntamente con IP. Aunque con la versión 4 su uso es opcional, con la 6 es obligatorio.
Secure Sockets Layer	SSL	4 de transporte	Protocolo criptográfico, encargado de asegurar las comunicaciones desde el nivel de transporte hasta el de aplicación. Se utiliza para asegurar protocolos que surgieron sin seguridad como HTTP, SMTP, etcétera.
Transport Layer Security	TLS	4 de transporte	Sucesor de SSL, al que actualiza y mejora en algunos aspectos del cifrado. Existe una versión libre denominada GnuTLS.
Secure Shell	SSH	4 capa de transporte	Protocolo, así como el programa que lo implementa. Sirve para establecer comunicaciones seguras entre máquinas remotas y puede ser utilizado como túnel para el tráfico de otras aplicaciones.

Tabla: Relación de protocolos que se utilizan para crear VPN.

Desde el punto de vista de la interconexión, pueden distinguirse tres tipos de redes privadas virtuales:

- **De acceso remoto:** el usuario se conecta a la red de área local corporativa y conforma la VPN con el resto de nodos conectados de la misma forma.
- **Intranet:** la conexión une segmentos de redes de área local de la misma organización mediante una WAN corporativa (no pública).
- **Extranet:** se permite el acceso restringido a los recursos mediante una WAN pública.

Algunos productos con estas tecnologías VPN propietarias –como el VPN de Cisco u otros fabricantes- o de fuentes abiertas o libres, como la implementación del paquete openVPN.

7.2. VLAN

Una **VLAN** (*Red de área local virtual* o *LAN virtual*) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).

7.2.1. Tipos de VLAN.

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

VLAN de nivel 1 (también denominada *VLAN basada en puerto*) define una red virtual según los puertos de conexión del conmutador;

VLAN de nivel 2 (también denominada *VLAN basada en la dirección MAC*) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación;

VLAN de nivel 3: existen diferentes tipos de VLAN de nivel 3:

- la **VLAN basada en la dirección de red** conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.
- la **VLAN basada en protocolo** permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

8. Proxy, Cortafuegos

8.1. El Proxy.

Un **proxy**, o **servidor proxy**, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina ***A*** solicita un recurso a ***C***, lo hará mediante una petición a ***B***, que a su vez trasladará la petición a ***C***; de esta forma ***C*** no sabrá que la petición procedió originalmente de ***A***. Esta situación

estratégica de punto intermedio le permite ofrecer diversas funcionalidades: control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, caché web, etc. Dependiendo del contexto, la intermediación que realiza el proxy puede ser considerada por los usuarios, administradores o proveedores como legítima o delictiva y su uso es frecuentemente discutido.

Hay dos tipos de proxys atendiendo a quién es el que quiere implementar la política del proxy:

- **proxy local**: En este caso el que quiere implementar la política es el mismo que hace la petición. Por eso se le llama local. Suelen estar en la misma máquina que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y pueda establecer reglas de filtrado que por ejemplo pueden asegurar que no se revela información privada (Proxys de filtrado para mejora de la privacidad).
- **proxy de red** o **proxy externo**: El que quiere implementar la política del proxy es una entidad externa. Por eso se le llama externo. Se suelen usar para implementar cacheos, bloquear contenidos, control del tráfico, compartir IP, etc.

Hay tanto tipo de Proxys, atendiendo a su función, como de servicios que puede ofrecernos la red.

Atendiendo a su configuración nos encontramos dos tipos:

- Proxy transparente: Un **proxy transparente** combina un servidor proxy con un cortafuegos de manera que las conexiones son interceptadas y desviadas hacia el proxy sin necesidad de configuración en el cliente, y habitualmente sin que el propio usuario conozca de su existencia. Este tipo de proxy es habitualmente utilizado por las empresas proveedoras de acceso de Internet.
- Proxy no transparente: Son proxys que requieren de su configuración en la maquina cliente. Estos proxys son fácilmente evadibles cambiando la configuración.

8.2. Cortafuegos.

Un **cortafuegos** (***firewall***) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente

conectar el cortafuegos a una tercera red, llamada *zona desmilitarizada o* DMZ*,* en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

8.2.1. Tipos de cortafuegos

A. Nivel de aplicación de pasarela

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

B. Circuito a nivel de pasarela

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

C. Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

D. Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder, e incluso puede aplicar reglas en función de los propios valores de los parámetros que aparezcan en un formulario web.

Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los ordenadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

E. Cortafuegos personal

Es un caso particular de cortafuegos que se instala como software en un ordenador, filtrando las comunicaciones entre dicho ordenador y el resto de la red. Se usa por tanto, a nivel personal.