Arquitectura web

Concepto de web y su evolución

Una aplicación web es una aplicación a la que se accede vía web por una red, ya sea una intranet o internet. Las aplicaciones web necesitan un navegador para ser ejecutadas. Algunos ejemplos de aplicaciones web son blogs, wikis, redes sociales, escritorios virtuales,...

La web ha evolucionado mucho a lo largo de los años, no pareciendose mucho la web actual a la sus años iniciales. Podemos hablar de:

- **Web 1.0**. Durante los años 90 había pocos generadores de contenido y muchos consumidores. Las páginas web eran estáticas y muy poco atractivas visualmente. Su principal finalidad era divulgativa.
- **Web 2.0** o **Web Social**. Aproximadamente por 2004. Los usuarios empiezan a hacer más cosas e interactúan más entre ellos. Aparecen redes sociales, blogs, wikis,… El contenido empieza a dinámico e interactivo. Las características de las páginas web 2.0 son:
  - ✗ **Apliaciones Ricas en Internet** (**RIA**, Rich Internet Application). Aplicaciones con prestaciones muy similares a las de escritorio como puedan ser Office o documentos de Google.
  - ✗ **Arquitectura Orientada a Servicio** (**SOA**, Service Oriented Architecture). Los elementos del software son diseñados para usarse como un servicio en la red.
  - ✗ **Web social**. El usuario es el centro de las aplicaciones.
- **Web 3.0** o **Web Semántica**. Se intenta acercar al usuario lo más posible al lenguaje natural y adaptar la navegación a las preferencias de este. Surgen nuevas formas de búsqueda y almacenamiento. La experiencia de navegación es más personalizada, especialmente por el uso de cookies para que la publicidad sea más personal.
- **Web 4.0**. Se pretende dar soluciones completas a las necesidades del usuario que automatice todo sin la intervención de éste como, por ejemplo, que la nevera hace la compra. Hay quien piensa que las aplicaciones invaden la privacidad del usuario.

Elementos de la arquitectura Cliente–Servidor

La arquitectura cliente–servidor es un modelo de aplicación distribuida en dos componentes principales, el cliente, equipo que necesita un recurso que es proporcionado por un servidor y crea peticiones para solventar dicha necesidad, y servidor, que proporciona respuestas a las peticiones de los clientes.

Las ventajas de la arquitectura cliente–servidor son:

- **Escalabilidad**. Es fácil aumentar las capacidades tanto de los clientes como de los servidores.

- **Disponibilidad**. Al estar distribuidas las funciones y las responsabilidades entre varios ordenadores independientes, es posible reparar, actualizar, reemplazar o trasladar un servidor sin que los clientes se vean afectados.
- **Control centralizado**. Se centraliza el control en el servidor.

Las desventajas de la arquitectura cliente–servidor son:

- **Congestión del tráfico en la red**. Si hay muchas peticiones al servidor puede que se congestiones y tarde más en responder o, incluso, deje de responder.
- Los recursos de hardware del servidor deben ser adecuados y normalmente es más caro que un cliente medio.
- El mantenimiento del servidor es complejo que el del cliente y hay que invertir más en seguridad.

Arquitectura en dos o tres niveles

Cuando hablamos de cliente-servidor en dos niveles nos referimos a que tenemos cliente y los resuelve todo un único servidor o conjunto de servidores que funcionan como si fuesen uno solo.

El proceso que se sigue cuando hay dos niveles es:

1. El servidor espera a que le llegue alguna solicitud.
2. El cliente genera una solicitud y la manda al servidor.
3. El servidor responde al cliente. Si puede responder adecuadamente lo que pide el cliente, hace lo que le solicita y manda la respuesta. Si no puede satisfacer la solicitud envía un mensaje de error.
4. El servidor queda a la espera de otra petición.

Este modelo no es eficiente si hay muchas solicitudes, éstas tardan mucho en ser resueltas o se mandan como respuesta muchos datos al cliente, el llamado cliente pesado, que congestiona la red.

La arquitectura en tres niveles es más flexible, escalable y segura. Las tres capas de la arquitectura en tres niveles son:

- **Cliente**. Equipo que hace la petición de recursos al servidor.
- **Servidor de aplicaciones**. Servidor que hace uso de otro servidor para resolver las peticiones de recursos de los clientes.
- **Servidor de datos**. Proporciona datos al servidor de aplicaciones..

Aplicaciones web y aplicaciones de escritorio

Las aplicaciones de escritorio son las aplicaciones que se desarrollan en un sistema operativo específico para ser utilizadas en él. Son muy utilizadas por la gran cantidad de prestaciones y su bajo tiempo de respuesta ya que todo se desarrolla en local y el hardware se razonablemente potente.

Algunos problemas que generan las aplicaciones de escritorio son:

- Incompatibilidad entre versiones.
- Puede ser difícil la instalación o las actualizaciones.
- Posible coste elevado del equipo.

- Podemos tener varios equipos con distintas versiones del programa y se generen problemas de consistencia o pérdidas de funcionalidades.
- Puede no haber portabilidad entre los distintos sistemas operativos.

Las aplicaciones web son aplicaciones que están disponibles a través de un navegador, programa que permite visualizar páginas web.
Las ventajas del software en web son:

- **Movilidad**. Se puede acceder desde casi cualquier sitio simplemente con una conexión a Internet.
- **Ausencia de instalación**. Solo hace falta un navegador en el equipo.
- **Ausencia de costes de actualización**. Las actualizaciones se hacen en el servidor y el cliente disfruta siempre de la última versión.
- **Actualización constante**. Siempre se accede a la última versión.
- **Datos centralizados**. Es en el servidor donde están las páginas web, la aplicación, y los datos.

Las desventajas del software en web son:

- **Menor potencia**. Las aplicaciones web suelen tener menores prestaciones y ser menos potentes ya que la parte principal se realiza en el servidor.
- **Infrautilización del hardware**. Solo se usa el navegador del equipo.
- **Conectividad rápida y constante**. Para ser eficientes, las aplicaciones web requieren una conexión rápida, fiable y constante a Internet.

Escalabilidad

La **escalabilidad** es la capacidad de adaptación y respuesta de un sistema a medida que aumentan de forma significativa el número de usuarios del mismo.
Para mejorar el rendimiento tenemos varias opciones de escalado:

- **Escalabilidad vertical**. Se migra hacia un hardware más potente que el actual, con lo que aumenta las prestaciones y el coste. En un futuro se puede tener el mismo problema y tener que volver a actualizar. En algún momento puede ser inviable aumentar el hardware.
- **Escalabilidad horizontal**. Se añaden más equipos similares al actual y, cuando llegan las peticiones de los clientes, se dividen entre los distintos equipos, para no sobrecargar ningún equipo, mediante el balanceo de carga. El balanceo puede ser por software, más lento pero más barato, o por hardware, más rápido pero más complicado de configurar.
- **Cluster**. Son varios equipos, no necesariamente iguales, unidos en red que vistos desde fuera parecen un único equipo.

Introducción a redes

Un equipo u ordenador no tiene capacidad para hacer todo por sí mismo. Es mucho más fácil, cómodo y práctico si hay ciertos equipos que se encargan de realizar tareas especializadas (impresión, bases de datos, guardar archivos, temas de seguridad (certificados)) para que los equipos "normales" hagan su trabajo sin necesidad de muchos recursos. Los sistemas informáticos (ordenadores, consola) pueden ser de tres tipos (pueden conectarse entre sí):

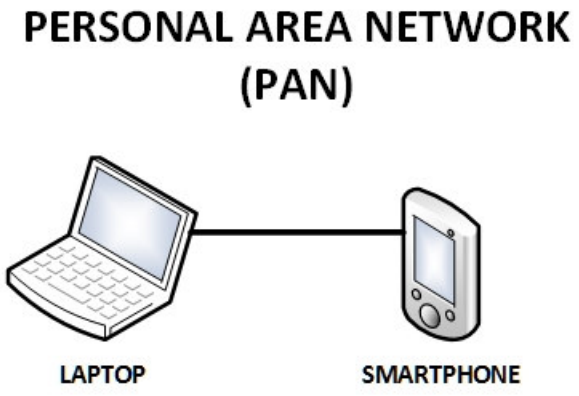
- **Aislados**. El ordenador no está conectado a una red y no comparte ninguna información con otro ordenador. Se considera que un ordenador que se conecta a una red muy de vez en cuando entra en esta categoría.
- **Sistema de red**. Son varios equipos conectados entre sí mediante una forma de conexión concreta. Es lo más usual.
- **Sistema distribuido**. Similar al anterior pero los datos del ordenador al que se conecta son transparentes ya que no se conocen, o no importan, los datos del ordenador al que se conecta. Es lo más normal en internet donde importa recibir un servidcio y no quién lo hace.

El objetivo de las redes es compartir información. Según como lo hagan se puede dividir en:

- **Redes cliente-servidor**. Los ordenadores se dividen entre los que demandan una información o un servicio, los clientes, y los que la ofrecen, servidores. Normalmente los servidores son equipos con mejores prestaciones. Un equipo concreto puede ser tanto cliente como servidor puesto que compartir una carpeta hace que un equipo se considere un servidor.
- **Redes entre iguales (peer-to-peer)**. Todos los ordenadores pueden ofrecer y demandar servicios de los demás ordenadores. Se usa en torrent, voz sobre ip o en monedas digitales.

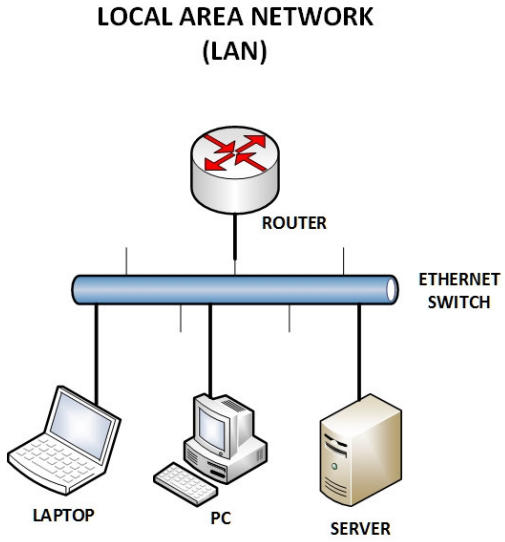
Según el área que ocupan las redes pueden ser:

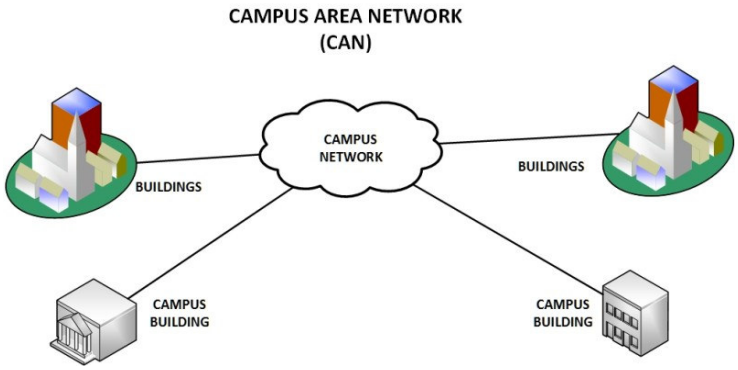
- **PAN** (personal area network). Red formada por elementos que no pueden situarse unos muy lejos de los demás.
- **LAN** (local area network). Es una red que ocupa una sala, una planta o un edificio entero.
- **CAN** (campus area network). Los equipos están distribuidos por un campus universitario. El área que ocupa suele ser mayor que una lan.

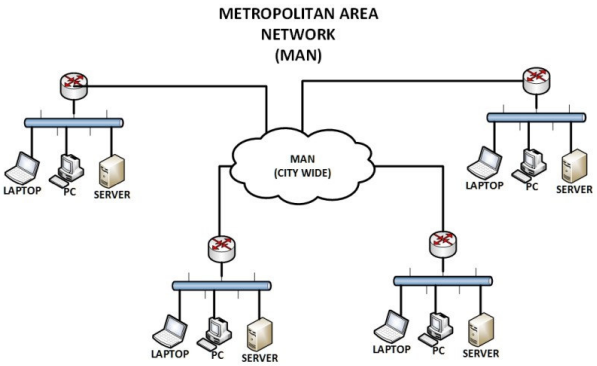


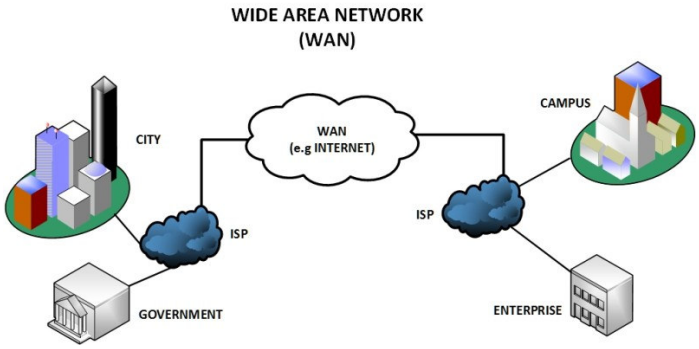
- **MAN** (metropolitan area network). Red que ocupa un municipio o ciudad y está compuesta por varias lan.

- **WAN** (wide area network). Red de área extensa. Ocupa varios países y continentes.



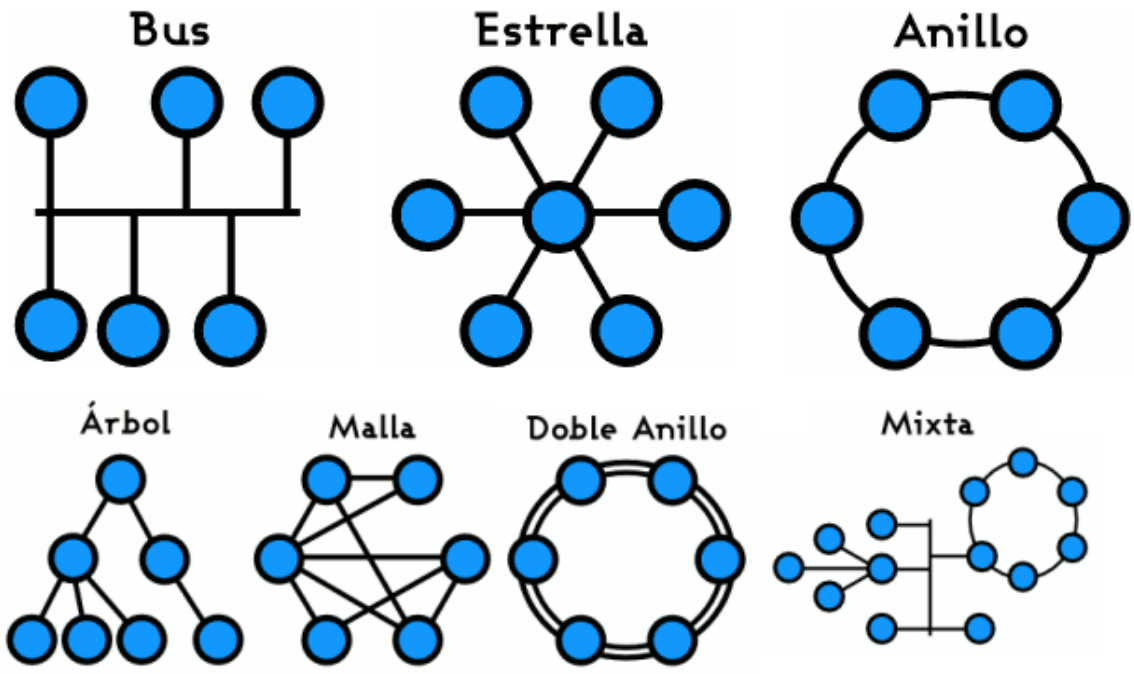






La topología de una red hace referencia a la forma física de la misma (forma en la que están conectados los ordenadores). Puede ser:

- **Bus**. Todos los ordenadores están conectados a un mismo medio físico, normalmente un cable coaxial. La señal, mediante un token o indicador, va de un extremo a otro y rebota en los extremos. Si falla un equipo, la conexión se mantiene para el resto. No si lo que falla es el cable.
- **Estrella**. Se caracteriza por un nodo o equipo central por el que pasa toda la información. Solo deja de funcionar si se estropea el elemento central. Pueden crearse cuellos de botella ya que toda la información pasa por el nodo central.
- **Anillo**. Cada equipo está conectado con otros dos, mediante conectores de entrada y salida, de manera que el último se conecta con el primero y forman un círculo. Se usa un indicador o token, el token ring, similar al token de la topología en bus. Puede usarse un doble círculo redundante para mayor seguridad. Si falla un equipo, toda la red se va abajo.



- **Malla**. Cada nodo de la red está conectado con uno o más nodos. Cada equipo debe tener varias interfaces de red. Si falla un equipo, la conexión se mantiene para el resto de los equipos.
- **Árbol** o **jerárquica**. Varias redes estrella ordenadas en una jerarquía. Los nodos centrales, switches, pueden conocer la red para enviar más eficientemente los paquetes.
- **Mixta** o **híbrida**. Compuestas por, al menos, dos topologías distintas.

Puede darse el caso de que la topología física sea distinta a la topología lógica. Por ejemplo, la lógica puede ser de anillo pero los puestos están situados en varias filas una detrás de otra.

Protocolos

Un protocolo es, según la rae (punto 5 inform), conjunto de reglas que se establecen en el proceso de comunicación entre dos sistemas. En el caso de la conexión en red, se entiende que un protocolo es un conjunto de normas que permite la comunicación entre ordenadores, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos y la forma en que la información debe procesarse.

Hay muchos protocolos de red y algunos constan de varios protocolos. Algunos protocolos importantes son:

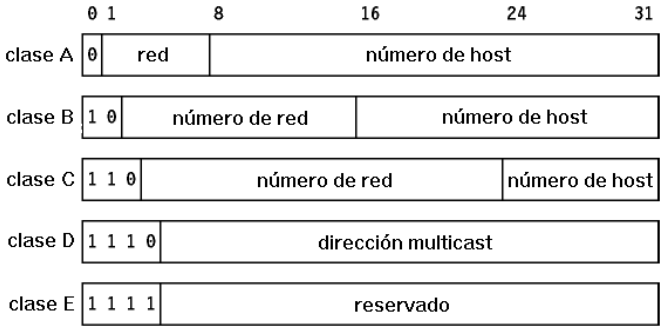
1. **TCP**. Protocolo de Control de Transmisión. Permite establecer una conexión y el intercambio de datos entre dos anfitriones. Comprueba que los paquetes no tengan errores y, llegado el caso, solicitan el reenvío del paquete erróneo. Da soporte a otros protocolos (HTTP, POP3, FTP,

SSH,...).

2. **UDP**. Protocolo de Datagramas de Usuario. Similar a TCP, se utiliza para transmitir datagramas de forma rápida en redes IP. No comprueba que lleguen todos los paquetes. Su uso principal es consultar DNS, conexiones VPN, streaming de audio y vídeo, juegos en línea y llamadas de voz sobre ip. Da soporte a otros protocolos (DNS, DHCP, RIP,...).
3. **IP**. Protocolo de Internet. Pone una dirección, ip, y encamina o enruta los datos (paquetes o datagramas) hacia su destino. Es un protocolo no orientado a conexión.
4. **NAT**. Traducción de Direcciones de Red. Se encarga de transformar las ip públicas en ip privadas. Proporciona seguridad ya que las máquinas de la red local no son visibles desde fuera. Permite ahorrar muchas direcciones ipv4. El equipo que hace la transformación requiere más potencia de computación ya que modifica los paquetes y hay que recalcular las comprobaciones o checksums.
5. **HTTP**. Hypertext Transfer Protocol o Protocolo de transferencia de hipertexto. Permite realizar peticiones de datos y recursos desde un cliente a un servidor web. Es un protocolo sin estado ya que no se recuerdan las peticiones o conexiones anteriores. Si hace falta se pueden usar cookies para crear una sesión y relacionar en el servidor una serie de peticiones para un mismo cliente. El puerto por defecto es el 80.
6. **HTTPS**. Hypertext Transfer Protocol o Protocolo seguro de transferencia de hipertexto. Similar a html pero usa un protocolo de seguridad, TLS), para cifrar el contenido que se envía al servidor. Es más adecuado que http cuando se quiere mandar información confidencial. El puerto por defecto es el 443.
7. **TLS**. Transport Layer Security o Seguridad de la Capa de Transporte. Protocolo que permite cifrar el contenido que se comparte en una red. Es la base de otros protocolos seguros como https o ftps. Se basa en certificados de criptografía asimétrica. Las versiones anteriores del certificado son SSL (Secure Socket Layer o Capa de Puerto Seguros).
8. **SSH**. Secure SHell. Es un protocolo y programa que permite acceder de manera segura a un servidor remoto. Hay una versión libre del protocolo, OpenSSH. Entre otras funciones permite transferir archivos o cambiar la configuración remotamente. El puerto por defecto es el 22.
9. **FTP**. File Transfer Protocol o Protocolo de Transferencia de Archivos. Permite el intercambio archivos entre dos equipos, cliente y servidor. Los datos que se envían no se cifran. Se puede añadir un cifrado usando el protocolo TLS, en este caso pasa a ser FTPS. Los puertos por defecto son el 20 para los datos y el 21 para la gestión de la conexión.
10. **DNS** (Domain Name System o Sistema de Nombres de Dominio). Transforma las direcciones en forma de nombres de dominio a direcciones ip.

IPv4

Cada nodo de la red posee una única dirección ip, una dirección por interfaz, tarjeta de red, que posea. Una dirección ipv4 está formada por 32 bits (número binario 0 ó 1) divididos en 4 octetos. Cada octeto es un número decimal entre 0 y 255. La dirección puede dividirse en dos partes, la dirección de red (identificar la red) y la dirección de host (identifica el equipo).
El número de direcciones máximo es 2^32, 4.294,967.296
Las direcciones se pueden conseguir a través de un ISP, Internet Service Provider, o la IANA, Internet Asigned Numbers Authority.
Las direcciones ip se organizan en clases. Estas clases determinan el tipo y el tamaño de la red en la que están las direcciones ip. Las clases definen qué bits se utilizan para identificar la red y el equipo, el número posible de redes y el número de equipos por red.
Los tipos de clase son:



- **Clase A**. Son redes con un gran número de equipos, hosts. El primer octeto determina la red y el primer bit es un 0. Hay 126 redes útiles, 128 (2^7) reales, cada una con 2^24 equipos, 16,777.216. El valor de red entre 1 y 127.
- **Clase B**. Son redes de tamaño medio a grande. Los dos primeros octetos determinan la red, primeros bits son 10. Hay 16384, 2^14, redes y 65536, 2^16, equipos por red. El valor de red está entre 128 y 191.
- **Clase C**. Se usan en redes de área local pequeñas. Los tres primeros octetos determinan la red, primeros bits son 110. Hay 2,097.152, 2^21, redes y 256, 2^8, hosts red, 254 reales. El valor de red está entre 192 y 223.
- **Clase D**. Se usa para multidifusión. Los 4 primeros bits son 1110 y determinan la red. Hay 2^28 equipos, 268,435.456. El valor de red está entre 224 y 239.
- **Clase E**. No se usan ya que se guardan para uso futuro. Los 4 primeros bits, 1111, determinan la red. El valor de red está entre 240 y 255.

Hay algunas redes y direcciones que son especiales y tienen un uso especial. Las más destacadas son:

- **0.0.0.0**. Indica que no ay una dirección asignada.
- **10.0.0.0 – 10.255.255.255**. Red privada de tipo A.
- **127.0.0.0**. Dirección de loopback, la propia interfaz del host.
- **169.254.0.0 – 169.254.255.255**. Dirección autoasignada cuando no funciona correctamente, o no se encuentra, el servidor dhcp.
- **172.16.0.0 – 172.32.255.255**. Red privada de tipo B.

- **192.168.0.0 – 192.168.255.255**. Red privada de tipo C.
- **255.255.255.255**. Difusión o broadcast, se envía la información a todas las interfaces en la red.

Para configurar una ip en un dispositivo hay que establecer los siguientes parámetros:

- **Dirección ip**. IP que defina la dirección de red del equipo en la red.
- **Máscara de red**. Número de bits que delimitan la dirección de red. Para clase A se usaría 255.0.0.0 ó /8.
- **Puerta de enlace predeterminada**. Equipo que conecta dos redes y por el que pasa el tráfico de datos de una red propia al exterior.
- **DNS**. Dirección de un servidor de nombres que transforma el nombre de un sitio en una ip.

Para no poner una a una todas las configuraciones de red en todos los equipos podemos usar el servicio de un servidor dhcp para que asigne dinámicamente las direcciones de red y no haya problemas de colisión.
A través del subneting podemos modificar el tamaño de las redes para adecuarlas a nuestras necesidades, por ejemplo tener más redes con menos equipos. Consiste en calcular el número de bits necesarios para obtener las redes o host necesarios, modificando el número de bits de la máscara de red.

Un puerto lógico es una zona de la memoria de un ordenador que asocia un puerto físico o con un canal de comunicación. Proporciona un espacio para el almacenamiento temporal de la información que se va a transferir entre la localización de memoria y el canal de comunicación.
Los puertos tienen 16 bits, luego hay 2^16, 65536, puertos. Pueden ser:

- Bien conocidos. Menores de 1024. Son usados por servicios que usa el sistema operativo.
- Registrados. De 1024 a 49151. Pueden ser usados por cualquier aplicación. Son gestionados por la IANA.
- Dinámicos. De 49152 a 65535. Se asignan de forma dinámica a los clientes. Se usan en conexiones P2P.

Algunos puertos conocidos son:

  - 20. FTP.
  - 22. SSH.
  - 80. HTTP.
  - 443. HTTPS.

IPv6

Una dirección ipv6 está formada por 128 bits divididos en 8 campos de 16 bits cada uno y separados por :. Cada campo se representa mediante un número hexadecimal (0-9 y a-f).
La dirección puede dividirse en tres partes:

- **Prefijo**. Son los tres primeros campos. Describen la topología pública que el ISP asigna al sitio de manera similar al código postal.
- **Subred**. Lo forma un campo, el cuarto. Describe la topología privada. En cada red hay 2^16, 65536, posibles subredes.
- **Interfaz**. Los cuatro últimos campos. Cada dirección está relacionada con la MAC de la tarjeta de red, los tres últimos campos.

Si hay un campo con todo 0, se puede sustituir por ::. Solo se puede hacer una vez puesto que si hay más no se sabría cuantos campos son 0 a cada lado. En vez de poner 0000, se puede poner 0, en particular si en el otro lado se ha puesto ::. Por ejemplo son equivalentes:

- fe80:0000:0000:0000:9e2e:a1ff:fe3c:295s
- fe80::9e2e:a1ff:fe3c:295s
- fe80:0:0:0:9e2e:a1ff:fe3c:295s

El número de direcciones máximo es 2^128, 3,40282*10^38. Si la superficie terrestre 510,072.000 km², tenemos 2^128/sup terrestre = 667,126*10^24 direcciones por km² = 667,126*10^18 direcciones por m².

Cifrado

La criptografía es, según la RAE, el arte de escribir con clave secreta o de un modo enigmático. En informática consiste en hacer ilegible un documento de manera que solo pueda entenderlo el destinatario del mensaje.

Terminología

- **Criptografía**. Arte de escribir con clave secreta o de un modo enigmático.
- **Criptología**. Estudio de los sistemas, claves y lenguajes ocultos o secretos.
- **Cifrado**. Escrito en cifra.
- **Cifra**. Escritura en que se usan signos, guarismos o letras convencionales, y que solo puede comprenderse conociendo la clave.
- **Cifrar** o **Encriptar**. Transcribir con una clave.
- **Clave**. Conjunto de caracteres usado para cifrar el texto claro.
- **Algoritmo de cifrado**. Técnica matemática que usa una o más claves para transformar un texto claro en cifrado o viceversa.
- **Texto plano o claro**. Información antes de ser cifrada.
- **Texto cifrado**. Texto al que se le ha aplicado un proceso de cifrado.
- **Esteganografía**. Estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros, de modo que pase inadvertido a observadores casuales que no sean el destinatario real.

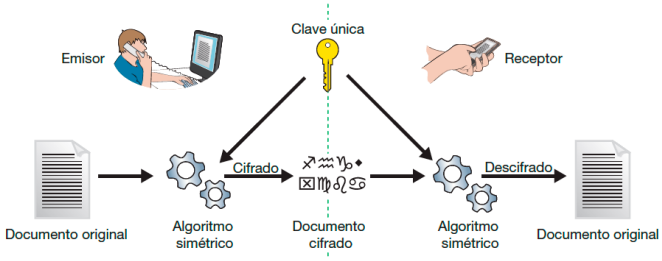
Objetivo

El objetivo de la criptografía es dar solución a los siguientes procesos:

- **Privacidad**. La información solo puede ser leída o interpretada por el destinatario autorizado.
- **Integridad**. La información no puede ser modificada en la transmisión sin que el destinatario lo advierta.
- **Autenticidad**. Se garantiza que el mensaje procede de quien se afirma que procede.
- **No repudio**. El emisor no puede negar la autoría del mensaje.

Cifrado simétrico

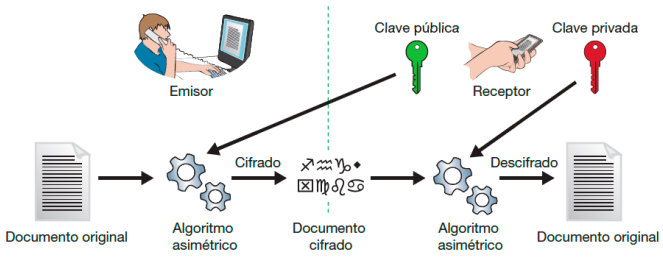
El cifrado simétrico es aquel en el que se usa la misma clave tanto para cifrar y como para descifrar. Hasta los años 70 del siglo 20 todos los algoritmos de cifrado eran simétricos.



En caso del cifrado simétrico la seguridad del mensaje depende de la fortaleza de la clave. El intercambio de claves es un problema ya que si interfieres la clave, puedes leer el mensaje. Si hay muchos usuarios es engorroso porque hacen falta muchas claves. Si

tenemos n individuos hacen falta n(n-1)/2 claves para que no se repitan.

Cifrado asimétrico



El cifrado asimétrico se basa en dos claves distintas, la clave privada, que no se debe divulgar, y la clave pública, que se puede entregar a todo el mundo. Ambas claves están relacionadas matemáticamente de manera que, lo que cifra una de ellas, lo puede descifrar la otra y es imposible conocer la clave privada a partir de la clave pública.
Para usar la clave privada en otra máquina aparte de la que se crea, hay que transportarla, con lo que puede haber un fallo de seguridad. Las claves privadas de una organización suelen estar protegidas todas juntas en un archivo cifrado, keyring o llavero. Es importante hacer una copia de seguridad de este archivo frecuentemente.

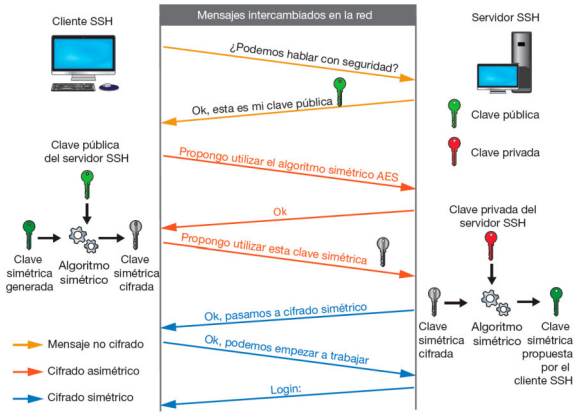
Las ventajas del cifrado asimétrico son:

- La clave pública no hay que protegerla.
- Un par de claves es suficiente para cada persona.

Las desventajas del cifrado asimétrico son:

- Es poco eficiente ya que se tarda mucho en cifrar y descifrar.
- Usar mucho la clave privada es arriesgado ya que se puede un análisis de los paquetes cifrados.
- Hay que tener mucho cuidado con la clave privada. Si se pierde u olvida la clave privada hay que revocar las claves.
- Las claves deben ser de gran tamaño, con un mínimo recomendado de 1024 bits.
- El mensaje cifrado ocupa más espacio que el original.

Cifrado híbrido



Es una combinación de cifrado simétrico y asimétrico. Se usa para proporcionar más seguridad, con el cifrado asimétrico, en la autenticación o paso de claves y más eficiencia, usando el cifrado simétrico, en el trabajo normal.

Aplicaciones

Cifrar o descifrar

Para cifrar un archivo que quiera que solo lo lea un destinatario único hay que cifrar el mensaje con la clave pública del

receptor de manera que solo puede ser descifrado por la clave privada del mismo.

Función resumen o hash
Sirve para verificar que los datos transmitidos son correctos. Se aplica al archivo una serie de operaciones y, como resultado, obtenemos un único resultado de números y letras, normalmente muy largo.
El receptor del mensaje realiza la misma operación y, si coinciden ambos resultados, el mensaje se ha transmitido correctamente. Si cambia algo, por mínimo que sea, el resultado es distinto.
Hay varios algoritmos de resumen, SAH, MD5,…

Firma
Se usa la firma para demostrar que quien ha enviado el archivo es quien dice ser y que el archivo no ha sido modificado por el camino. Con la firma se consigue autenticación o que el emisor es quien dice ser, integridad ya que demuestra que el mensaje no ha sido modificado y no repudio en origen pues el emisor no puede negar haber enviado el mensaje.
El procedimiento para firmar un archivo es:

1. Se hace un resumen del archivo o documento.
2. Se firma el resumen con la clave privada.
3. Se envía el archivo y el resumen al destinatario.
4. El destinatario descifra el resumen con la clave pública del emisor.
5. Hace un resumen del archivo con el mismo algoritmo.
6. Comprueba si ambos resúmenes coinciden.

PKI, Public Key Infraestructure

Hay entidades que son reconocidas por todo el mundo y expiden certificados que contienen las claves privadas y públicas.
Los actores que intervienen en el PKI son:

- **Autoridad de Certificación, CA**. Emiten los certificados. FNMT.
- **Autoridad de Validación, VA**. Comprueba la validez de los certificados emitidos. Suelen coincidir con la CA.
- **Autoridad de Registro, RA**. Comprueba que el solicitante es quien dice ser. Policia, TGSS.
- **Repositorios**. Almacenes de certificados; contienen los certificados activos y las revocaciones que aún no han caducado.

Un certificado digital es un archivo que emite la CA que recoge información de un usuario, una empresa,… Contiene muchos datos entre los que se incluye:

- Clave pública del que será el propietario del certificado.
- Identidad del propietario. Nombre, DNI, correo electrónico,…
- Firma digital de una tercera entidad, la CA, que tanto el emisor como el receptor conocen y confían en ella.

Normalmente la CA crea el certificado, se visita una vez la RA para que te de el

certificado una vez que demuestres quién eres y la VA comprueba el certificado cada vez que se usa.

DNIe

El DNIe es una tarjeta con un chip que contiene los datos de un ciudadano español y un par de claves asimétricas, pública y privada. Se adquiere en la Policía al crear o renovar el DNI o el NIE. Se pueden usar en sitios que lo admitan como bancos o administraciones públicas, aunque para usarlo hace falta un lector de tarjetas.