IES N1 Gijón

Principado de Asturias
Consejería de Educación

UNIDAD DE TRABAJO 0

Repaso de Conceptos básicos de TCP/IP

Celia C. Pellico Llera

Cofinanciado por la Unión Europea

Contenidos

1. Introducción
2. Estructura de las redes de comunicaciones
3. Servicios de red
4. Protocolos en redes de comunicaciones
5. El sistema operativo como gestor de servicios
6. TCP/IP
7. Configuración de TCP/IP
8. El protocolo IP
9. Traducción de direcciones de red. NAT y PAT

1. Introducción

Los orígenes de internet se remontan a **1969**, cuando se estableció la primera red de computadores. Esta red de computadores arcaica fue conocida como **ARPANET**, (Advanced Research Projects Agency Network). Fue el resultado de un encargo del Ministerio de Defensa de los EEUU, para comunicar los diferentes organismos del país.

Posteriormente pasó a ser de uso privado entre organismos públicos y universidades, para, finalmente, expandirse de forma revolucionaria hasta llegar a la superred que es hoy día **Internet**.
La red ya funcionaba, se había expandido, y mediante ella las personas se intercambiaban archivos principalmente. Pero aún faltaba algo: la **World Wide Web**.



Por **www** entendemos aquel sistema de distribución de la información basado en **hipertexto** que permitía al usuario hacer clic y acceder a contenidos relacionados con la página que estaba visitando.

La World Wide Web fue creada por **Tim Berners Lee** con la ayuda de **Robert Cailliau** y se publicó en **1992**.



Historia de Internet

Internet engloba a las tecnologías que hacen posible que los ordenadores ubicados en diferentes lugares del mundo se conecten entre sí y puedan compartir información. La web es solo uno de los servicios que proporciona Internet.

Se puede definir web como el conjunto de documentos que se conectan entre ellos a través de enlaces o links.

El **protocolo de comunicaciones** que se utiliza en la web es el **HTTP** (HyperText Transfer Protocol - Protocolo de Transferencia de Hipertexto), que permite solicitar documentos que contengan hipertexto. **Hipertexto** es el nombre que recibe el texto que en la pantalla de un dispositivo electrónico conduce a otro texto relacionado.

Un **navegador** web (browser) es un programa que permite visualizar la información que contiene una página web, pues interpreta el código de la página y lo visualiza en pantalla.

Un **servidor web** es un programa diseñado para aceptar peticiones HTTP del navegador y servir las páginas web que tiene alojadas. Para navegar a un sitio web se necesita saber la dirección web exacta del sitio. Cada sitio web tiene una dirección única conocida como **URL** (Uniform Resource Locator - Localizador Uniforme de Recursos), formada por varias partes: el **protocolo**, el **nombre de dominio** del ordenador servidor y la **ruta en el servidor**. Por ejemplo:



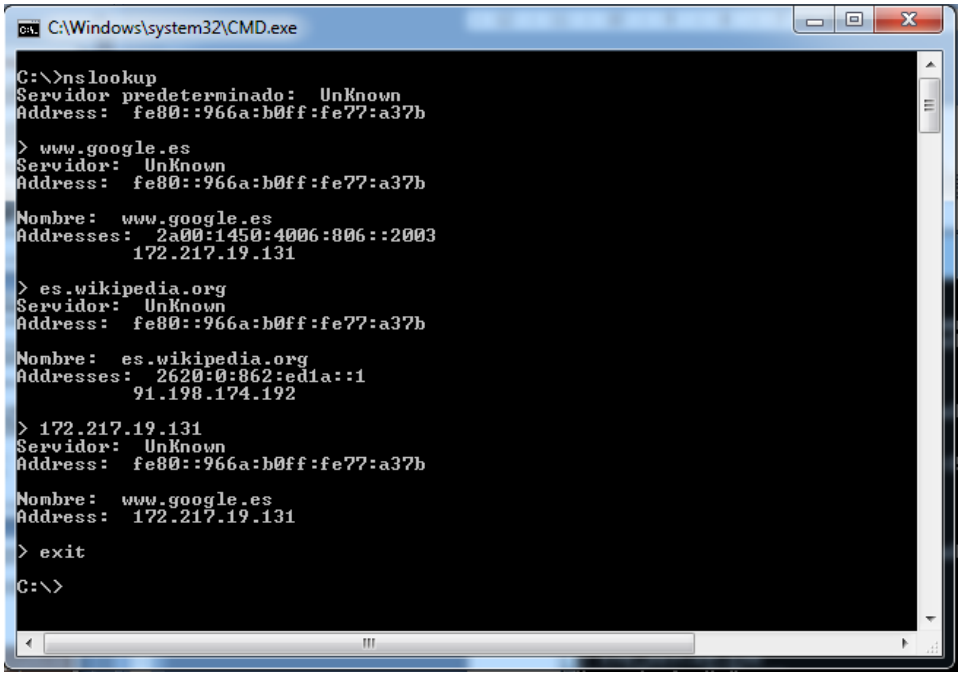
El propósito principal de los **nombres de dominio en Internet** y del sistema de nombres de dominio **DNS** (Domain Name System), es traducir las direcciones **IP** (Internet Protocol) de cada nodo activo en la red, a términos memorizables y fáciles de encontrar.

Esta abstracción hace posible que cualquier servicio (de red) pueda moverse de un lugar geográfico a otro en la red Internet, aún cuando el cambio implique que tendrá una dirección IP diferente.

www.google.es --> 74.125.196.105

Como saber la IP de una pagina web: comando *nslookup*

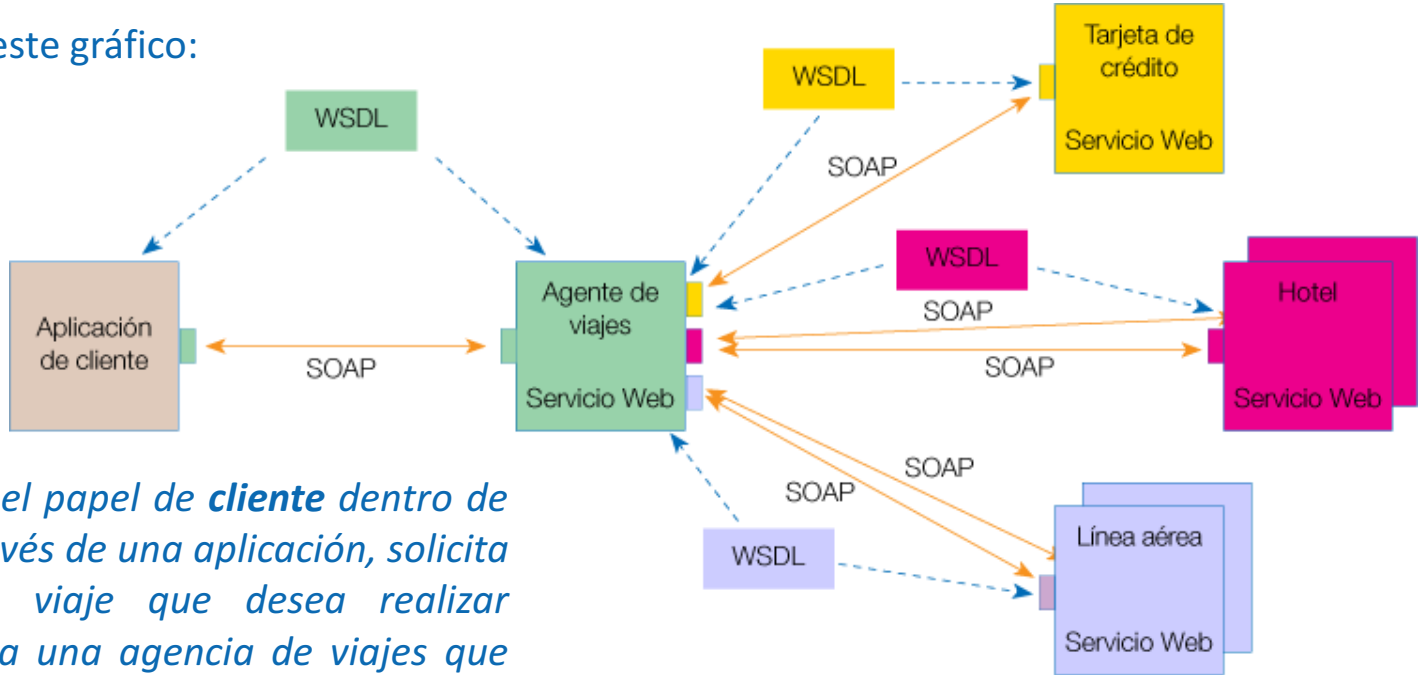
nslookup es una herramienta de línea de comandos muy práctica y fácil de usar, cuya función básica es encontrar la dirección IP de un equipo determinado o realizar una búsqueda DNS inversa, es decir, encontrar el nombre de dominio de una determinada dirección IP). Se ejecuta en la interfaz de líneas de comando del sistema operativo correspondiente. En la actualidad existen varios servicios web que permiten usar nslookup también online.



Los servicios web

Un **servicio web** representa un recurso de información al que puede acceder otra aplicación a través de la web y con el cual se puede comunicar a través de protocolos estándares de Internet. Están diseñados para permitir la comunicación de una aplicación con otra sin intervención humana.

Veamos el ***ejemplo*** de este gráfico:



*Un usuario (que juega el papel de **cliente** dentro de los Servicios Web), a través de una aplicación, solicita información sobre un viaje que desea realizar haciendo una petición a una agencia de viajes que ofrece sus servicios a través de Internet.*

**SOAP y WSDL son protocolos de comunicación*

La agencia de viajes ofrecerá a su cliente (usuario) la información requerida.

Para ello, la agencia de viajes solicita a su vez información a otros recursos (otros Servicios Web) en relación con el hotel y la compañía aérea.

La agencia de viajes obtendrá información de estos recursos, lo que la convierte a su vez en cliente de esos otros Servicios Web.

Por último, el usuario realizará el pago del viaje a través de la agencia de viajes que servirá de intermediario entre el usuario y el servicio Web que gestionará el pago

2. Estructura de las redes de comunicaciones

Las **redes de ordenadores** se han convertido en un elemento imprescindible en nuestra vida y podemos darles diversos usos:

- práctico: acceder al banco, realizar compras
- laboral: acceder a la oficina
- educativo: universidad a distancia, cursos online
- lúdico: jugar en red, compartir videos, fotografías, etc., con personas de cualquier lugar del mundo

....las posibilidades son prácticamente ilimitadas.



jsinformatica.es

Resumiendo: las redes proporcionan servicios muy variados: acceso a internet, intercambio de datos entre empresas, comercio electrónico, conexión de varios equipos, trabajo colaborativo, control de un edificio o casa domótica, etc.



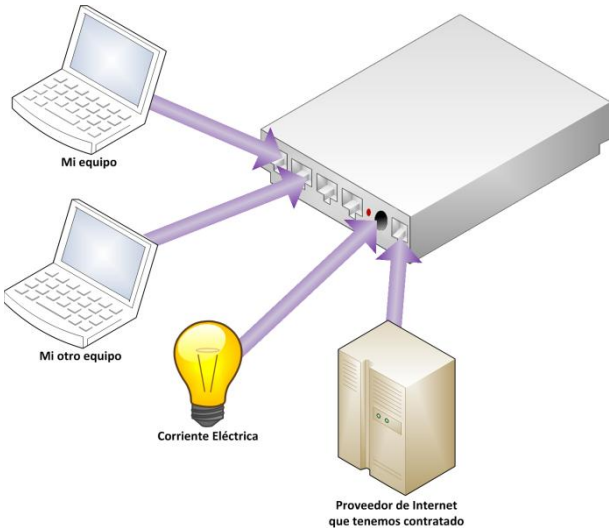
Redes informáticas

¿Qué es una red?

Una **red de área local** es un conjunto de ordenadores y dispositivos de hardware unidos entre sí, con el fin de compartir datos (imágenes, documentos, etc.) y recursos (impresoras, escáner, discos duros, etc..) en una zona geográfica limitada.



arc-tec-science.blogspot.com

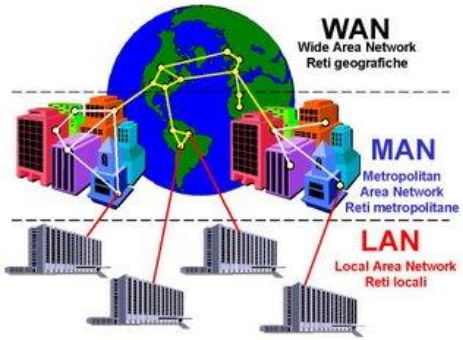


La red más simple consta de dos ordenadores y su complejidad puede aumentar hasta conectar miles de ordenadores en todo el mundo, tal y como sucede con la red Internet (**INTER**connected **NET**works - redes interconectadas).

Si tenemos un ***router*** para conectarnos a Internet ya disponemos de una red local.

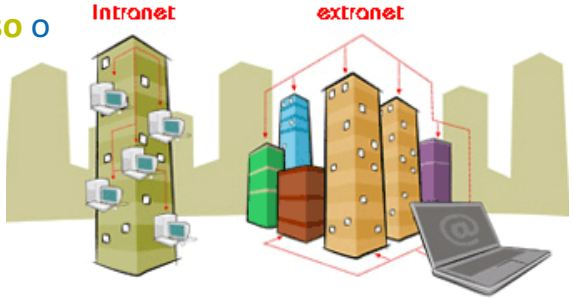
Tipos de redes informáticas

Según su **tamaño** o área de cobertura



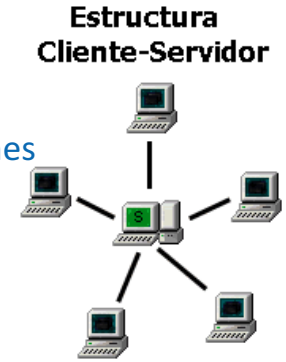
freepressreleasesubmit.com

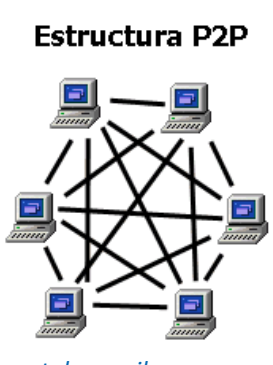
Según su **nivel de acceso** o privacidad



ondemand.es

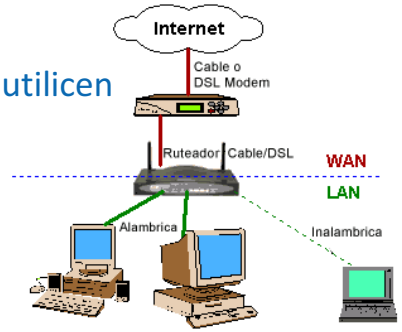
Según la **comunicación** entre aplicaciones





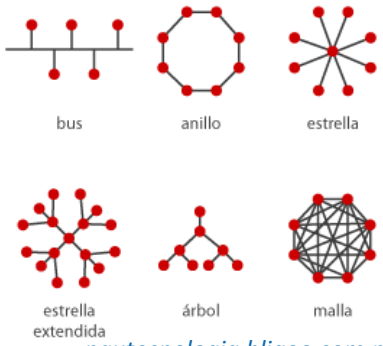
www.xatakamovil.com

Según el medio que utilicen para su **conexión**



652584934.blogspot.com.es

Según la **topología** o la arquitectura de la red



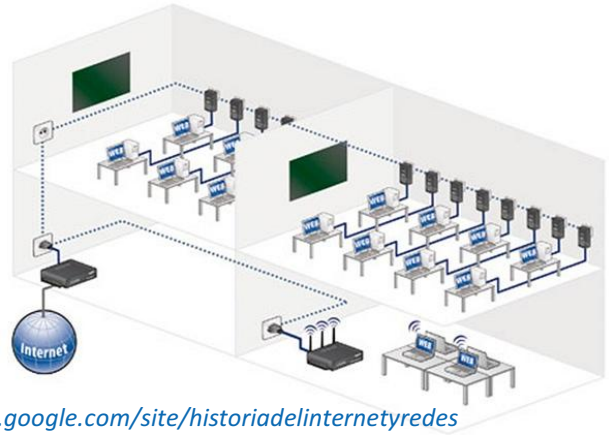
pautecnologia.bligoo.com.mx

Según su tamaño



conceptdraw.com

Red de área personal (**PAN**, Personal Area Network). Está formada por la interconexión de dispositivos con un alcance de escasos metros. Por ejemplo el manos libres de un teléfono móvil, conexiones entre móvil vía bluetooth o infrarrojos



sites.google.com/site/historiadelinternetyredes

Red de área local (**LAN**, Local Area Network). Son redes de pequeña extensión (red de una universidad, un edificio, un instituto, una casa, etc.)



tipos-de-redes-segun-cobertura.weebly.com

Red de área metropolitana (**MAN**, Metropolitan Area Network). Es una red formada por un conjunto de redes LAN en las que se conectan equipos. Por ejemplo la red de empresas de un polígono industrial, un campus universitario o la red de servicios municipales.



tecno4b.wikispaces.com

Red de área extensa (**WAN**, Wide Area Network). Estas redes interconectan equipos geográficamente más dispersos (una ciudad, un país, o incluso distintos continentes)

Según la comunicación entre aplicaciones

Modelo Cliente/Servidor

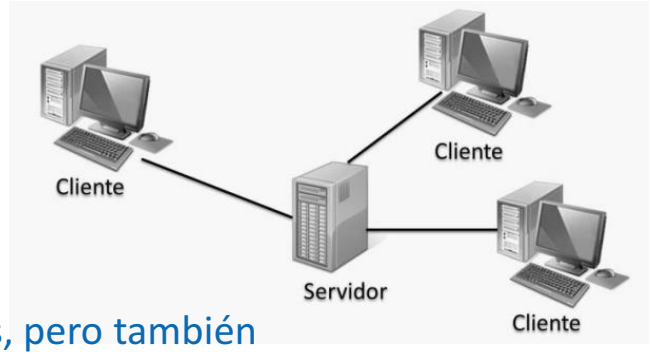
Es el más extendido y utilizado. En él se distingue entre un proceso ***cliente*** (que solicita servicios) y un proceso ***servidor*** (que presta el servicio).

El **cliente** es el que habitualmente inicia la comunicación, por lo que su papel suele ser activo en la misma: envía una petición a un proceso servidor y a continuación queda a la espera de la respuesta.

El **servidor** suele ser un proceso que inicialmente permanece a la espera escuchando las posibles conexiones de los potenciales clientes. Aunque parezca que tiene un papel pasivo en la comunicación, son sistemas complejos, difíciles de diseñar y programar, además de requerir privilegios del sistema. En su diseño deben de tenerse en cuenta cuestiones como autenticación, autorización, seguridad y privacidad de la información.

Es habitual que el proceso servidor pueda gestionar simultáneamente peticiones de varios clientes

Desde el punto de vista funcional, se puede definir el modelo Cliente/Servidor como una **arquitectura distribuida que permite a los usuarios finales obtener acceso a recursos de forma transparente en entornos multiplataforma**.



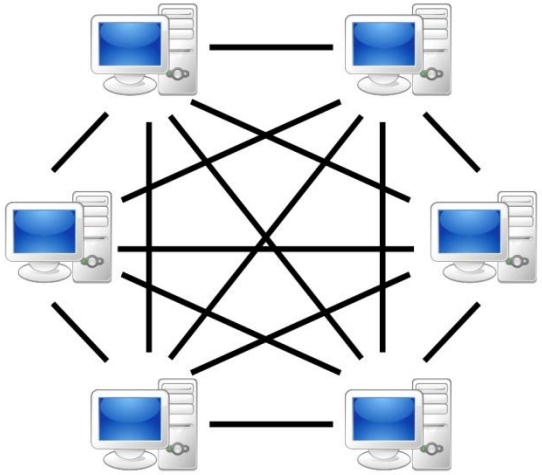
Normalmente, los recursos que suele ofrecer el servidor son datos, pero también puede permitir acceso a dispositivos hardware, tiempo de procesamiento, etc.

El término modelo Cliente/Servidor se acuñó por primera vez en los años 80 para explicar un sencillo paradigma: ***un equipo cliente requiere un servicio de un equipo servidor****.*

Modelo Peer to Peer (P2P)

Las tecnologías 'peer to peer' (P2P, entre pares o entre iguales) hacen referencia a un tipo de arquitectura para la comunicación entre aplicaciones que permite a individuos comunicarse y compartir información con otros individuos sin necesidad de un servidor central que facilite la comunicación.

Se trata de una red de computadores que pueden actuar indistintamente como clientes o servidores respecto a los demás nodos de la red.



proyectoidis.org/p2p/

Es importante destacar que el término "P2P" se refiere a un tipo de arquitectura de aplicaciones y no a la funcionalidad específica de una aplicación final; sin embargo, a menudo se utiliza el término "P2P" como sinónimo de "intercambio de archivos", ya que éste es uno de los usos más populares de dicha tecnología. No obstante, existen muchos otros usos de la tecnología P2P, por ejemplo **Skype** utiliza una arquitectura P2P híbrida para ofrecer servicios VoIP, mientras que **Tor** utiliza una arquitectura P2P para ofrecer una funcionalidad de enrutamiento anónimo.

La ventaja principal de la tecnología P2P es que saca el máximo partido de los recursos (ancho de banda, capacidad de almacenamiento, etc.) de los muchos clientes/peers para ofrecer servicios de aplicación y red, sin tener que confiar en los recursos de uno o más servidores centrales. De este modo se evita que tales servidores se conviertan en un cuello de botella para toda la red. Otra ventaja es que no existe una autoridad central única que se pueda eliminar o bloquear y colapsar toda la red P2P. Esto dota a la red de la capacidad de sobrevivir por sí misma y de una gran robustez.

Modelo Híbrido

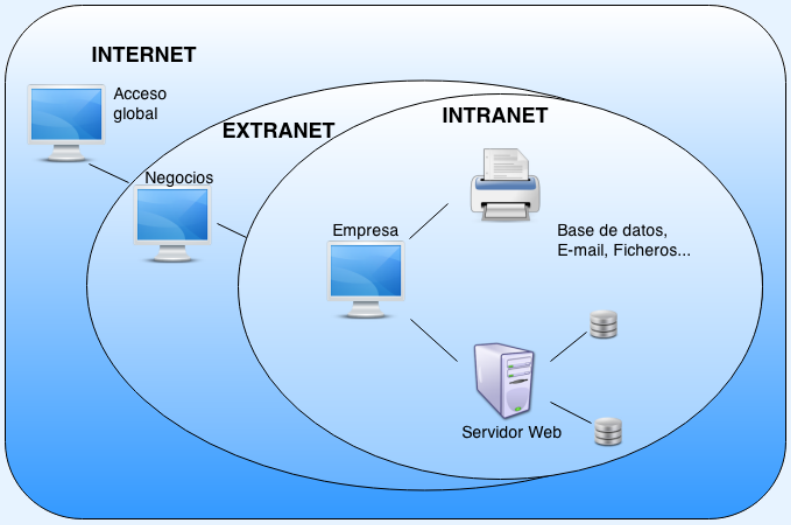
Es una combinación de las dos anteriores, y donde el servidor no presta los servicios como tal, sino que generalmente pone en contacto a los clientes para que éstos se comuniquen entre sí.

Según su nivel de acceso

Internet: red mundial de ordenadores caracterizada por ser de acceso público y permitir a sus usuarios comunicarse y compartir información y servicios en todo el mundo.

Intranet: Es una red local que utiliza herramientas de internet (web, correo, ftp, etc.) Se considera una red privada que funciona dentro de una misma institución, como por ejemplo un universidad, un banco, etc.

Extranet: Es una red privada virtual resultante de la interconexión de dos o más intranet utilizando para ello internet como medio de comunicación.

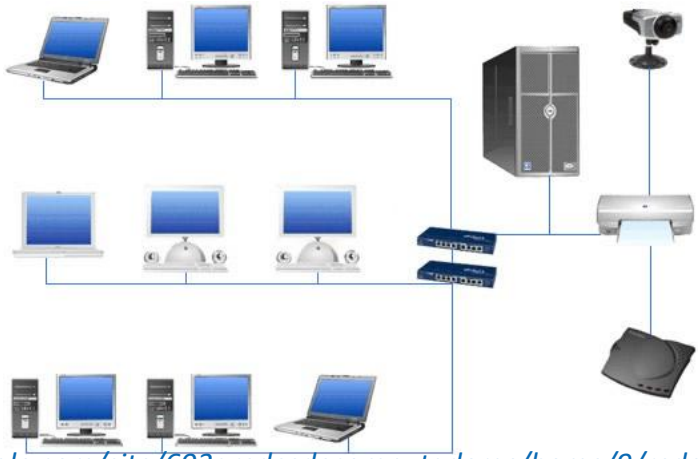


DIFERENCIAS			
	INTERNET	INTRANET	EXTRANET
Acceso	Público	Privado	Semi-público
Usuarios	Cualquiera	Miembros de una organización	Grupo de empresas estrechamente relacionadas
Información	Fragmentada	Propietaria	Compartida dentro de un círculo de empresas.

noeli-rossi.blogspot.com.es

Según el medio de conexión

Redes **alámbricas**: conectan cada una de las tarjetas de red de los ordenadores generalmente a través de un concentrador (***hub*** o ***switch***). Se pueden emplear varios tipos de cable: coaxial, fibra óptica y par trenzado.



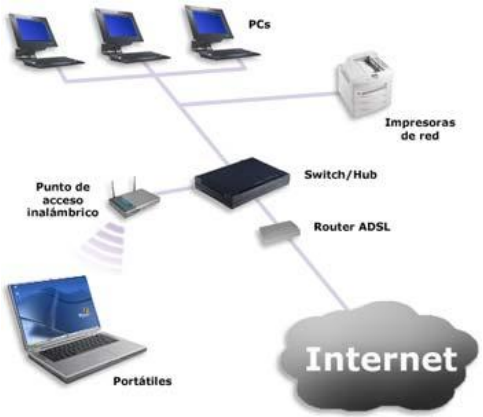
sites.google.com/site/603aredesdecomputadoras/home/9/redes-alambricas



silviscaballero.blogspot.com/p/red-inalambrica.html

Redes **inalámbricas**: La conexión inalámbrica se realiza mediante las ondas electromagnéticas que se propagan entre una antena emisora y una receptora. Para conectar un ordenador a una red wifi es necesario por tanto una antena receptora y el software adecuado.

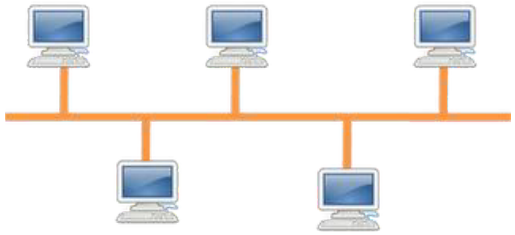
Redes **hibridas** es decir redes LAN que tienen conexión por cable pero en las que alguno de sus nodos es un punto de acceso wireless que permite la conexión inalámbrica de otros dispositivos wifi.



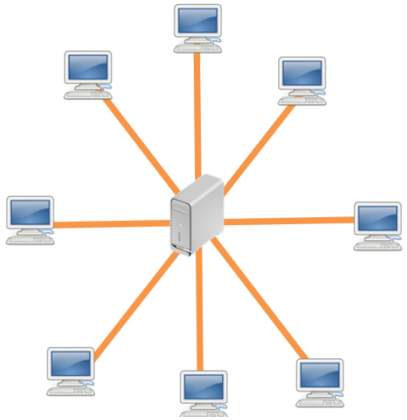
seg-nanogenerador.blogspot.com

Según la topología

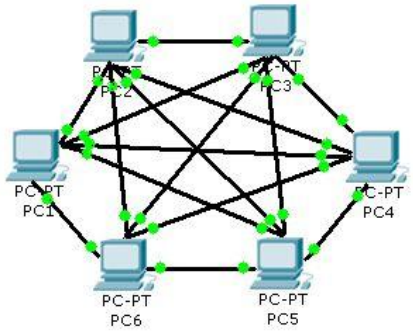
Bus o lineal: tiene un cable central con derivaciones.



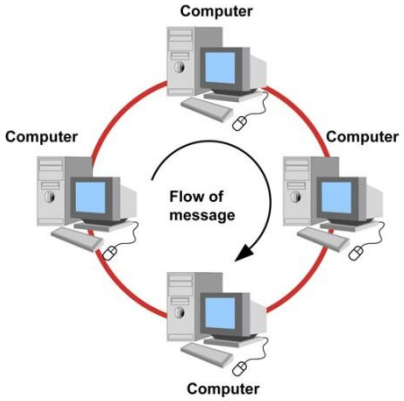
Estrella: todos los ordenadores están conectados a un concentrador o Hub central y no están conectados entre sí.



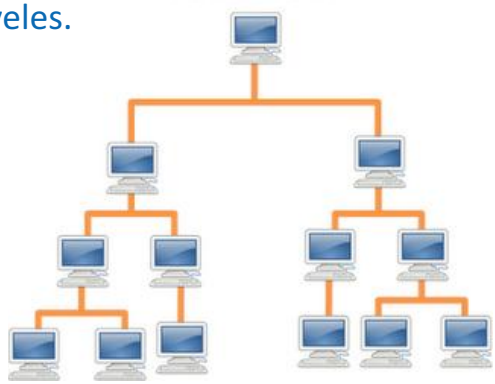
Malla: cada ordenador esta conectado al resto de los equipos con más de un cable. Cada nodo está conectado a todos los nodos.



Anillo: todos se conectan describiendo un anillo, la información llega a un ordenador y si no la necesita la pasa al siguiente.



Jerárquica: los ordenadores se conectan al superior y van descendiendo sucesivamente por niveles.



3. Servicios de red

Un **servicio de red** es una función o prestación que ofrecen las aplicaciones y los protocolos a los usuarios o a otras aplicaciones.

- Las **aplicaciones** son los diferentes programas, instalados por el usuario o que son parte del sistema operativo, que se sirven de los protocolos de la arquitectura TCP/IP para comunicarse.
- Los **protocolos** son normas concretas, descritas formalmente, que detallan como se produce la comunicación entre sistemas para ofrecer servicios en red.

Normalmente se usará una **arquitectura cliente servidor** en la que el servicio lo proporcionará uno o más equipos denominados servidores y será accesible a través de la red por aplicaciones cliente que funcionarán en otros dispositivos.



Un servicio en red **funciona en el nivel de aplicación del modelo OSI**. Puede proporcionar almacenamiento y manipulación de datos, acceso remoto a sistemas, monitorización de equipos o cualquier otra funcionalidad que se nos ocurra siempre siguiendo alguno de los protocolos establecidos.

Los principales servicios que puede ofrecer una red son:

Acceso: Comprende tanto la verificación de la identidad del usuario para determinar cuáles son los recursos de la red que puede utilizar, como permitir la conexión de usuarios de la red desde lugares remotos.

Ficheros: Consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones de trabajo. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.

Impresión: Permite compartir impresoras entre múltiples usuarios, reduciendo así el gasto. En estos casos, existen equipos servidores con capacidad para almacenar los trabajos en espera de impresión. Una variedad de servicio de impresión es la disponibilidad de servidores de fax los cuales convierten la impresora en fax.

Correo/Mensajería: La aplicación de red más utilizada que ha permitido claras mejoras en la comunicación frente a otros sistemas. Este servicio además de la comodidad, ha reducido los costes en la transmisión de información y la rapidez de entrega de la misma, la cual, dependiendo de la velocidad de la red de internet que nos permita nuestro proveedor, nunca tarda más de 1min por lo general después de ser enviado.

Aunque los servicios más conocidos en Internet son el servidor Web y el de correo electrónico, existen otros servicios como:

- **DHCP**. Permite asignar automáticamente la configuración IP de los equipos clientes de la red. Este servicio es muy importante ya que facilita la conexión de los equipos a la red. Por ejemplo, cuando un portátil se conecta a una red obtiene su configuración IP a través de un servidor DHCP.
- **DNS**. Permite mantener una equivalencia entre un nombre y su dirección IP. Por ejemplo, el nombre *www.adminso.es* equivale a 150.214.150.30.
- **FTP**. Protocolo de red para la transferencia de archivos entre sistemas conectados a una red.
- **SSH**. Permite el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

Estos servicios de red se dividen en dos tipos: de alto nivel y de bajo nivel.

Servicios de alto nivel

Solicitados directamente por los usuarios de la red:

- Transferencia de archivos (FTP)
- Correo electrónico (SMTP, POP3, IMAP)
- Mensajería instantánea (IRC, SIP, OSCAR, XMPP)
- Acceso remoto a los equipos (TELNET, RSH, SSH, VNC, RDP)
- Hipertexto (HTTP)

Servicios de bajo nivel

Solicitados por los equipos de la red de comunicación:

- Asignación dinámica de Ips (DCHP)
- Servicio de nombres de dominio (DNS)

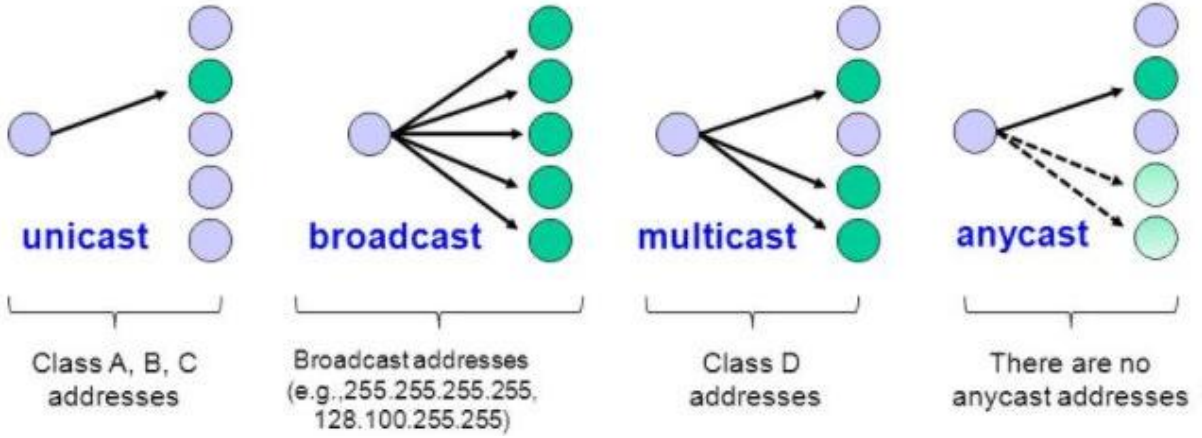
Otras clasificaciones son:

- **Servicios orientados a conexión**.
  - Garantizan que los paquetes lleguen intactos y en orden.
  - Necesitan interacción entre origen y destino.
  - Implican un inicio y cierre de sesión.
- **Servicios no orientados a conexión**.
  - Sin garantía de recibo.
  - No hay un inicio y cierre de sesión, aumentando la eficiencia.

También se debe tener en cuenta los **tipos de envío** de los paquetes en la red.

- **Unicast**: Uno a uno
- **Broadcast**: Uno a todos
- **Multicast**: Uno a varios
- **Anycast**: Uno a alguno

- Supported by IPv4
  - one-to-one (unicast)
  - one-to-all (broadcast)
  - one-to-many (multicast)
- Not supported by IPv4:
  - one-to-any (anycast)



4. Protocolos en redes de comunicaciones

Un **protocolo** es un conjunto de reglas usadas por los ordenadores para comunicarse unos con otros a través de una red. Aunque pueden variar bastante, en su mayoría especificarán las siguientes propiedades:

- Detección de la conexión física sobre la que se realiza la conexión (alámbrica/inalámbrica)
- Pasos necesarios para comenzar a comunicarse (handshaking)
- Negociación de las características de la conexión.
- Cómo se inicia y cómo se termina un mensaje.
- Formato de los mensajes.
- Qué hacer con los mensajes erróneos o corruptos.
- Cómo detectar la pérdida inesperada de la conexión, y qué posteriormente
- Terminación de la sesión y/o conexión.
- Estrategias para asegurar la seguridad (autenticación, cifrado).



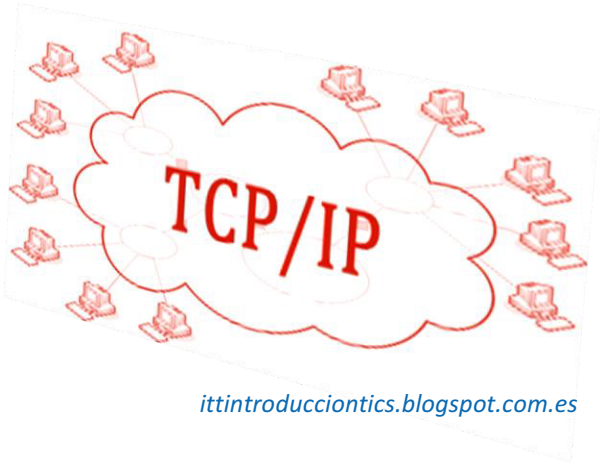
Protocolos básicos de Internet

Telnet (Telecommunication Network)

Es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente.

TCP (**T**ransmision **C**ontrol **P**rotocol)

Es el protocolo encargado del transporte de los datos. Se asegura de que los datos (paquetes) sean entregados, que lo que se recibe es lo que se pretendía enviar y que los paquetes lleguen en el orden correcto en el que fueron enviados.



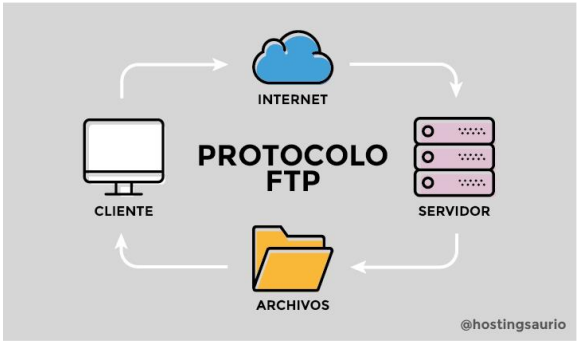
ittintroduccionticts.blogspot.com.es

IP (**I**nternet **P**rotocol)

Es el protocolo de la capa de red. Utiliza direcciones numéricas denominadas ***direcciones IP*** compuestas por 4 números enteros (4 Bytes) entre 0 y 255, y escritos en el formato XXX.XXX.XXX.XXX. Por ejemplo: 192.168.0.1

FTP (File Transfer Protocol)

Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.



HTTP (**H**yper**T**ext **T**ransfer **P**rotocol)
Es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.



tecnoarnel.com.ve

SSL/TLS
Es la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol)
Es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre ordenadores u otros dispositivos.

RPC (**R**emote **P**rocedure **C**all)
Es un programa que utiliza un ordenador para ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambas.

DNS (**D**omain **N**ame **S**ystem)
El uso más común es para asignar el nombre de dominio a una dirección IP.
Es una enorme base de datos que almacena y distribuye la información de todos los nombres de dominio que existen en la red.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol)
Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SSL y TLS

SSL (Secure Socket Layer) y **TLS** (Transport Layer Security) son protocolos que proporcionan comunicación seguras en una red, como Internet. Ambos son protocolos de cifrado para la capa de transporte de internet. Su función es cifrar el **tráfico de datos entre el cliente y el servidor.**



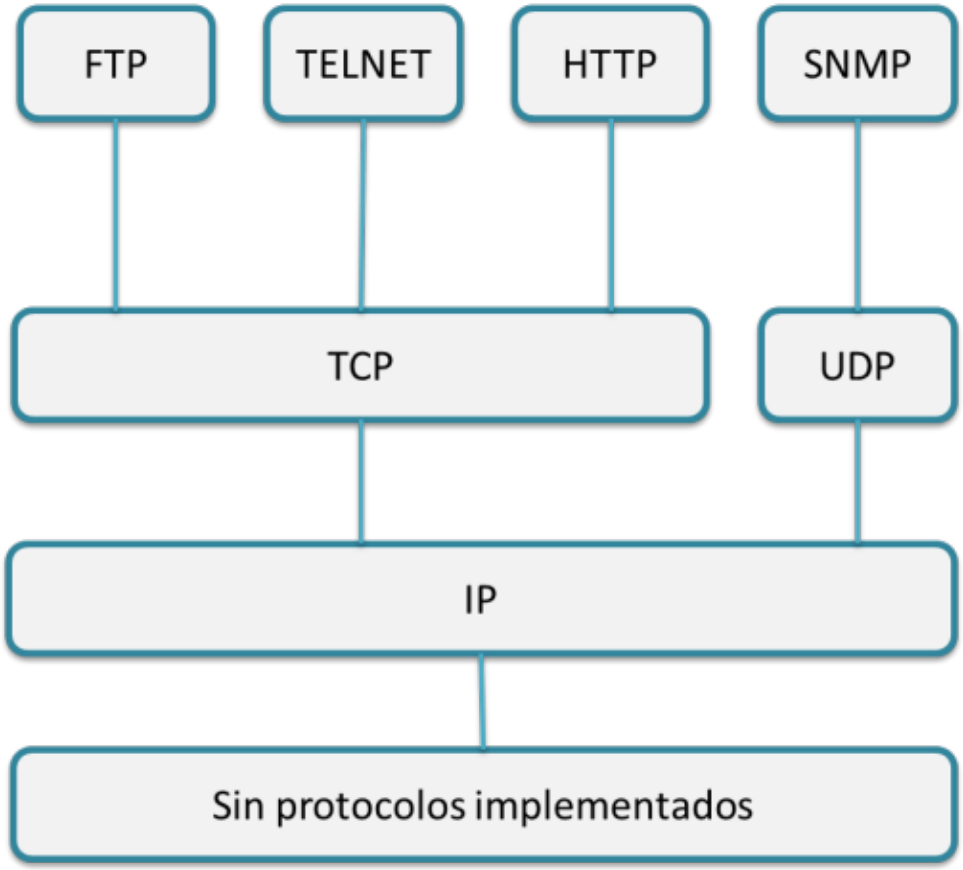
Una de las principales aplicaciones practicas de estos protocolos es formar **https** junto a http garantizando el envío y recepción de información de forma segura en un navegador web.

TLS es el **protocolo sucesor de SSL** (cuyo uso ahora es ilegal). Es **más seguro, flexible y eficiente** que su antecesor. Sin embargo, como las siglas SSL siguen siendo mucho más conocidas que TLS, muchos proveedores de *software* de cliente o enrutadores usan el término SSL o alternativamente el doble término SSL/TLS.



SSL, TLS, HTTPS, HTTP
Explicado fácilmente

Jerarquía de protocolos en TCP/IP



5. El sistema operativo como gestor de servicios

Los sistemas operativos ofrecen un conjunto de funciones necesarias para los programas de las diferentes aplicaciones instaladas en el ordenador, y los vínculos necesarios para controlar y sincronizar el hardware. Este conjunto de servicios incluye, entre otros muchos:

- Ejecución de programas
- Operaciones de E/S
- Manipulación de archivos y directorios
- Comunicación entre procesos
- Comunicación con equipos remotos
- Administración de la protección y seguridad
- Detección de errores
- Asignación de recursos
- Leer el estado del sistema (hora, nº de procesos, etc.)
- …….

6. TCP-IP

TCP/IP es una familia de protocolos desarrollados para permitir la comunicación entre cualquier par de ordenadores de cualquier red o fabricante, respetando los protocolos de cada red individual.

Tiene 4 capas o niveles de abstracción:

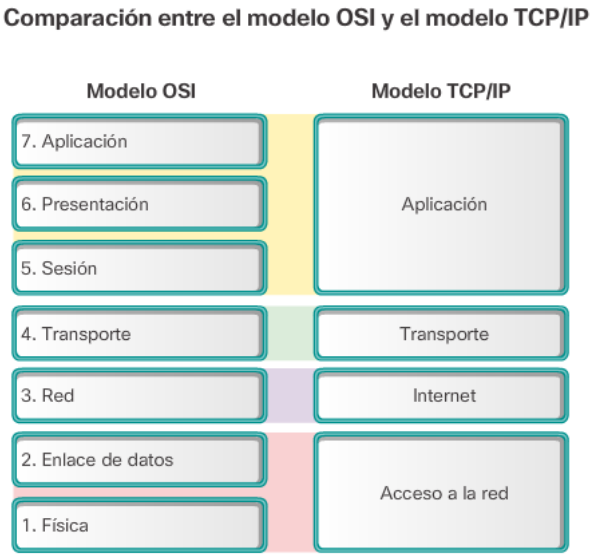
- Aplicación
- Transporte
- Internet (o Red o IP)
- Acceso a la red (o Interfaz de red o Enlace). En esta capa se incluye la parte física.

Este modelo se basa en el de referencia OSI, También conocido como “Modelo de Capas”.

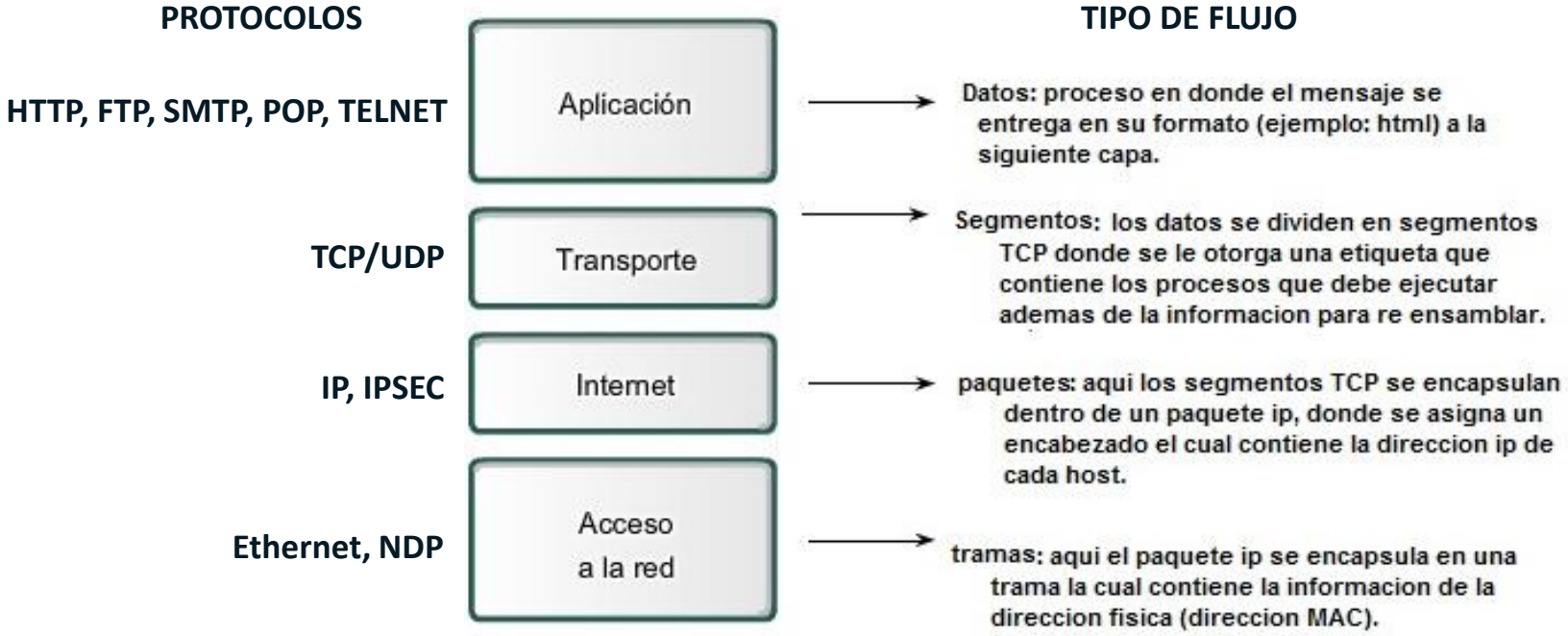
- Cada capa provee servicios a la capa inmediata superior.
- Cada capa es cliente de la capa inmediatamente inferior.
- Conversación horizontal: cada capa dialoga con su homóloga remota.
- Flujo de datos vertical hacia/desde capa física.
- Un protocolo es la implementación de la lógica de una capa.
- Se pueden especificar uno o más protocolos por capa.

El modelo OSI de ISO

El modelo de Interconexión de Sistemas Abiertos (**OSI**, Open System Interconection) lanzado en 1984 fue el modelo de red descriptivo creado por **ISO** (International Organization for Standardization). Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial



Las similitudes se encuentran en la capa de transporte y en la capa de red.



Conexiones TCP/UDP

TCP y UDP son dos protocolos fundamentales para las comunicaciones a través de Internet. Estos dos protocolos se sitúan en la **capa de transporte** del modelo TCP/IP, y es la primera capa donde origen y destino se comunican directamente.

TCP (TRANSMISSION CONTROL PROTOCOL)

Es un protocolo **orientado a la conexión** (para enviar la información se debe establecer una conexión previa entre cliente y servidor) que permite que un flujo de bytes originado en una máquina se entregue sin errores en cualquier máquina destino. Este protocolo fragmenta el flujo entrante de bytes en mensajes y pasa cada uno a la capa de internet (o red). El proceso TCP receptor reensambla los mensajes recibidos para formar el flujo de salida.
TCP también se encarga del control de flujo para asegurar que un emisor rápido no pueda saturar a un receptor lento con más mensajes de los que pueda gestionar.

UDP (USER DATAGRAM PROTOCOL)

Es un protocolo **sin conexión**, es decir, no hay una fase de establecimiento de la conexión como en TCP, directamente se envían los datagramas sin previo aviso. Este protocolo también se utiliza para las consultas de petición y respuesta del tipo cliente-servidor, y en aplicaciones en las que la velocidad es más importante que la entrega precisa, como las transmisiones de voz o de vídeo.
Uno de sus usos es en la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

7. Configuración TCP-IP

El éxito de TCP/IP como protocolo de red de Internet se debe, en gran medida, a su capacidad para conectar redes de tamaño diferente y sistemas de distinto tipo.

Cuando se configura un protocolo TCP/IP en un equipo, las opciones de configuración de dicho protocolo requieren una **dirección IP**, una **máscara de subred** y, normalmente, una **puerta de enlace predeterminada**.

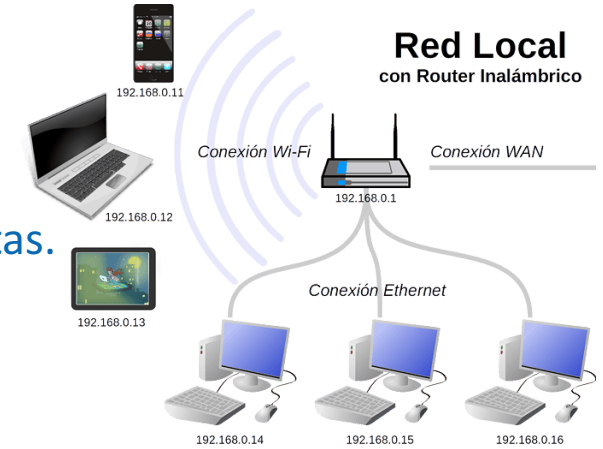
Sus principales funciones son:

- El **enrutamiento** de paquetes de datos.
- **Asignar** direcciones a los paquetes de datos.
- **Identificar** el tipo de contenido y el tipo de servicio.
- **Fragmentar** paquetes demasiado grandes.

El protocolo IP utilizado habitualmente en Internet es su versión 4 (**IPv4**).
Existe una versión más reciente **IPv6**, en la que se utilizan más bits para direccionar y
de esta forma se pueden tener más direcciones IP.

Las direcciones Internet son asignadas por **InterNIC**, organización que administra Internet. El documento Internet RFC 1878 describe las subredes y máscaras de subred válidas que se pueden usar en redes TCP/IP.

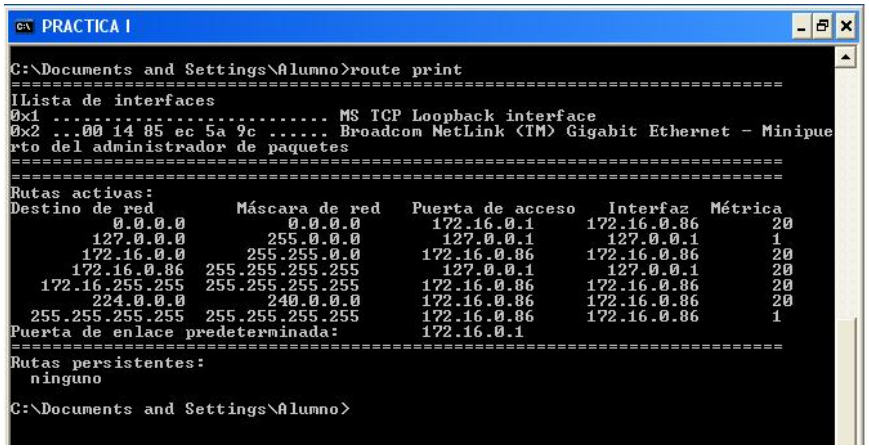
Enrutadores



electricidadyelectronica.com

- Son dispositivos con interfaces en varias redes físicas.
- Tienen una dirección IP (y subred) por cada interfaz.
- Deciden el trayecto de los paquetes basados en tablas de rutas.
- Su flujo de trabajo es:
  - Recibe un paquete en una interfaz.
  - Determina si el paquete está dirigido a él.
  - Decrementa el **TTL**.
  - Compara la dirección destino con la **tabla de enrutamiento**.
  - Envía el paquete al próximo enrutador (o nodo de destino), o declara error.
- Cada decisión es un salto hacia la dirección de destino.
  - El enrutador A puede enviar paquetes a otro enrutador B sólo si ambos tienen al menos una interfaz conectada a la misma subred física.
- Cada enrutador tiene sus propias tablas de rutas que se deben mantener actualizadas.

Una **tabla de enrutamiento** (o de encaminamiento) almacena las rutas o caminos hacia los diferentes nodos en una red informática. Los nodos pueden ser cualquier tipo de dispositivo electrónico conectado a la red. Generalmente se almacena en un router, aunque también está contenida en cualquier host conectado a la red. Cuando los datos deben ser enviados desde un nodo a otro de la red, se hace referencia a la tabla de enrutamiento con el fin de encontrar la mejor ruta para la transferencia de datos.

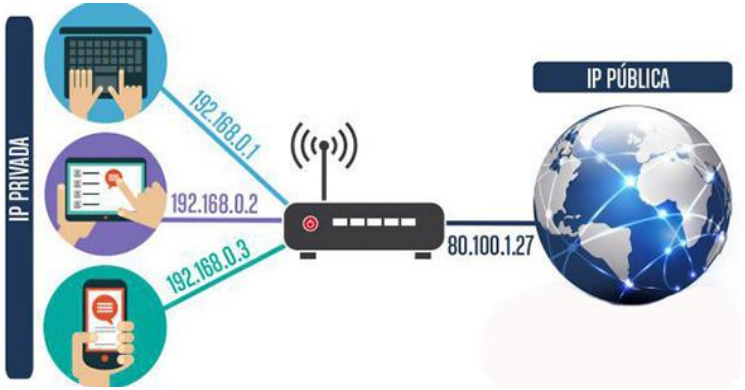


Conexión de equipos

Los servicios web funcionan en red sobre el protocolo TCP/IP. Por tanto, el primer paso para poder usar un servicio es tener acceso desde el cliente al servidor. Para ello, el servidor deberá tener una IP conocida y ser accesible desde el cliente. Deberemos configurar una **IP fija**.

Si estamos en una red de área local, esa IP será una **dirección privada** de alguno de los rangos permitidos y los equipos cliente deberán conectarse a la red local.
Si el servicio va a estar disponible en Internet, tendremos que conseguir una **dirección pública**. Realmente el servidor no tendrá configurada la IP pública. Tendrá una IP privada y será el ***router*** el que se encargue de traducir y reencaminar las peticiones de la dirección pública hacia la IP privada del servidor correspondiente mediante **NAT** (Network Address Translation).

Normalmente cuando contratamos Internet, el router-firewall que instalan dispone de una IP pública para poder navegar por Internet y otra privada para la conexión a nuestra red de área local y a todos los dispositivos que usamos. Además, se encargará de proteger nuestra red de accesos no deseados y de redirigir nuestras consultas hacia Internet.



Sin embargo, la IP pública de la que disponemos es **dinámica** y puede cambiar con el tiempo.

*Una **dirección IP fija o estática** es una dirección cuyo número es siempre el mismo. Las direcciones IP públicas y estáticas son, por ejemplo, las que utilizan los servidores de los proveedores de Internet u otros proveedores de servicios web.*

*Las **direcciones IP dinámica**s son direcciones que utilizan un número distinto cada vez que un dispositivo se conecta a Internet. Habitualmente los proveedores de Internet utilizan direcciones IP dinámicas y públicas para dar acceso a la conexión a sus clientes. Cuando un cliente se conecta a la red de Internet, su proveedor le asigna de manera automática una dirección IP pública dinámica que no esté siendo utilizada en ese momento por otro cliente.*

Los servicios de red necesitan direcciones IP públicas fijas por lo que necesitaremos contratarla con un proveedor de Internet o ubicar nuestro servicio en la nube. En muchos casos, también supondrá contratar el servicio.

Puertos de red

Un **puerto de red** es una interfaz para comunicarse con un programa a través de una red.

Para poder realizar varias intercambios de datos de forma simultánea, existen **65536** puntos de salida y entrada conocidos como puertos y que se identifican de forma numérica.

La definición técnica es: un número de **16 bits**, empleado por un protocolo host a host para identificar a qué protocolo del nivel superior o programa de aplicación se deben entregar los mensajes recibidos.

Aunque muchos de los puertos se asignan de manera arbitraria, ciertos puertos se asignan, por convenio, a ciertas aplicaciones particulares o servicios de carácter universal. De hecho, la **IANA** (**I**nternet **A**ssigned **N**umbers **A**uthority) determina, las asignaciones de todos los puertos.

Existen tres rangos de puertos establecidos:

- Puertos bien conocidos.
- Puertos registrados.
- Puertos dinámicos.



Tipos de puertos: bien conocidos, asignados y efímeros.

Anexo: Números de puertos de red

- **Puertos bien conocidos [0, 1023]**. Los puertos inferiores al 1024 son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos" como por ejemplo HTTP (servidor web), POP3/SMTP (servidor de e-mail) y Telnet. Si queremos usar uno de estos puertos tendremos que arrancar el servicio que los use teniendo permisos de administrador.

  21 – FTP (File Transfer Protocol

  22 – SSH (Secure SHell)

  53 – DNS (Servicio de nombres de dominio)

  80 – HTTP (Hypertext Transfer Protocol)

- **Puertos registrados [1024, 49151]**. Estos puertos son asignados por IANA para un servicio específico o aplicaciones. Estos puertos pueden ser utilizados por los usuarios libremente. Existe una lista pública en la web del IANA donde se puede ver qué protocolo usa cada uno de ellos. Cuando se desarrolla una aplicación que utilice un puerto de comunicación, optaremos por utilizar puertos comprendidos en este rango.
- **Puertos dinámicos [49152, 65535]**. Este rango de puertos no puede ser registrado y su uso se establece para conexiones temporales entre aplicaciones. Normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Se usan en conexiones peer to peer (P2P).

Comunicación entre aplicaciones

Para que dos programas puedan comunicarse entre sí es necesario que se cumpla:

- Que un programa sea capaz de localizar al otro.
- Que ambos programas sean capaces de intercambiarse cualquier secuencia de ***octetos***, es decir, datos.

Para ello son necesarios dos recursos:

- Un **par de direcciones** del protocolo de red (dirección IP, si se utiliza el protocolo TCP/IP), que identifican la computadora de origen y la remota.
- Un **par de números de puerto**, que identifican a un programa dentro de cada computadora.

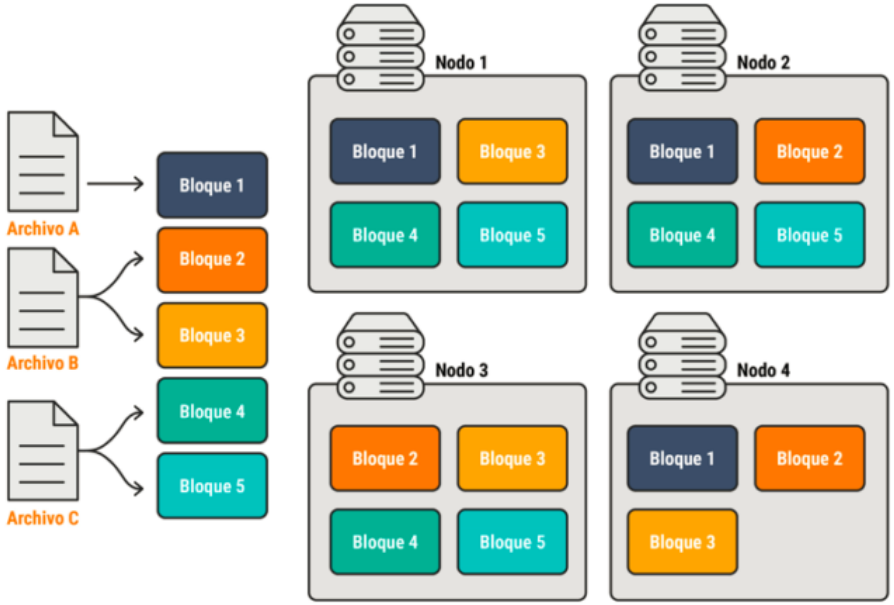
El modelo de comunicación que ha revolucionado los sistemas informáticos es el modelo **cliente/servidor**. Este modelo está compuesto por un servidor que ofrece una serie de servicios y unos clientes que acceden a dichos servicios a través de la red. Por ejemplo, el servicio más importante de Internet, el **www**, utiliza el modelo cliente/servidor. Por un lado tenemos el servidor que aloja las páginas web y por otro lado los clientes que solicitan al servidor una determinada página web.



Otro modelo ampliamente utilizado son los **Sistemas de Información Distribuidos**. Un Sistema de Información Distribuido está compuesto por un conjunto de equipos que interactúan entre sí y pueden trabajar a la vez como cliente y servidor. Desde el punto de vista externo es igual que un sistema cliente/servidor ya que el cliente ve al Sistema de Información Distribuido como una entidad. Internamente, los equipos del Sistema de Información Distribuido interactúan entre sí (actuando como servidores y clientes de forma simultánea) para compartir información, recursos, realizar tareas, etc.

En lugar de tener un solo servidor muy potente, tenemos muchos más pequeños. Si algo llegara a fallar, probablemente no nos enteraríamos ya que la pérdida de capacidad sería marginal. Además, cada uno de ellos tiene un coste mucho menor, pues son equipos más normales lo que hace que no tengamos que invertir grandes sumas en servidores grandes.

Además, son más tolerantes a fallos.



8. El protocolo IP

A nivel de red 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 que es el principal de este nivel en la arquitectura TCP/IP. Las funciones principales de este protocolo son:

- El esquema de direccionamiento utilizado en cada nodo de la red.
- Los procesos de encaminamiento, que se ejecutan en los dispositivos que interconectan las redes.

La comunicación a nivel IP se hace mediante unidades de datos llamadas **datagramas** que siguen el formato especificado en el protocolo IP.

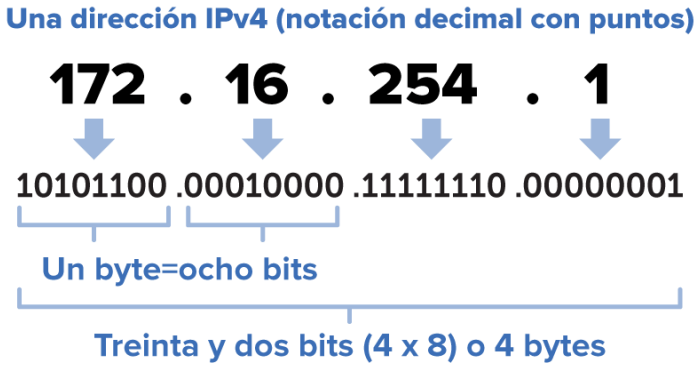
El protocolo IP debe ser capaz de direccionar de forma única todos los dispositivos que tengamos conectados en nuestra red y, por extensión, en todo Internet. Este direccionamiento es abstracto, de forma que es independiente del dispositivo físico al que se asigna y puede ser modificado vía software.

*Una dirección IP no identifica a un ordenador en la red, sino que **identifica a un interfaz de red** de un ordenador en la red. Por eso es posible que un mismo equipo pueda tener varias direcciones IP, una por interfaz, y eso hace posible que pueda estar contacto a redes diferentes de manera simultánea. Incluso es posible que un interfaz pueda tener varias direcciones IP denominándose entonces direccionamiento virtual.*

Formato de direcciones IP

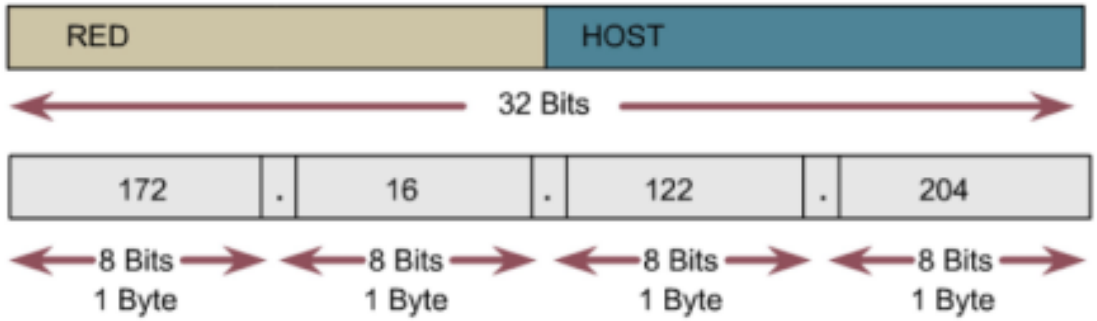
Las direcciones IP que identifican a los dispositivos y estaciones de la red tienen un tamaño fijo de **32 bits** (IPv4).

Estas direcciones se pueden expresar directamente en binario, aunque resulta más cómodo utilizar 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 números resultantes.



Una dirección IP consta de dos partes:

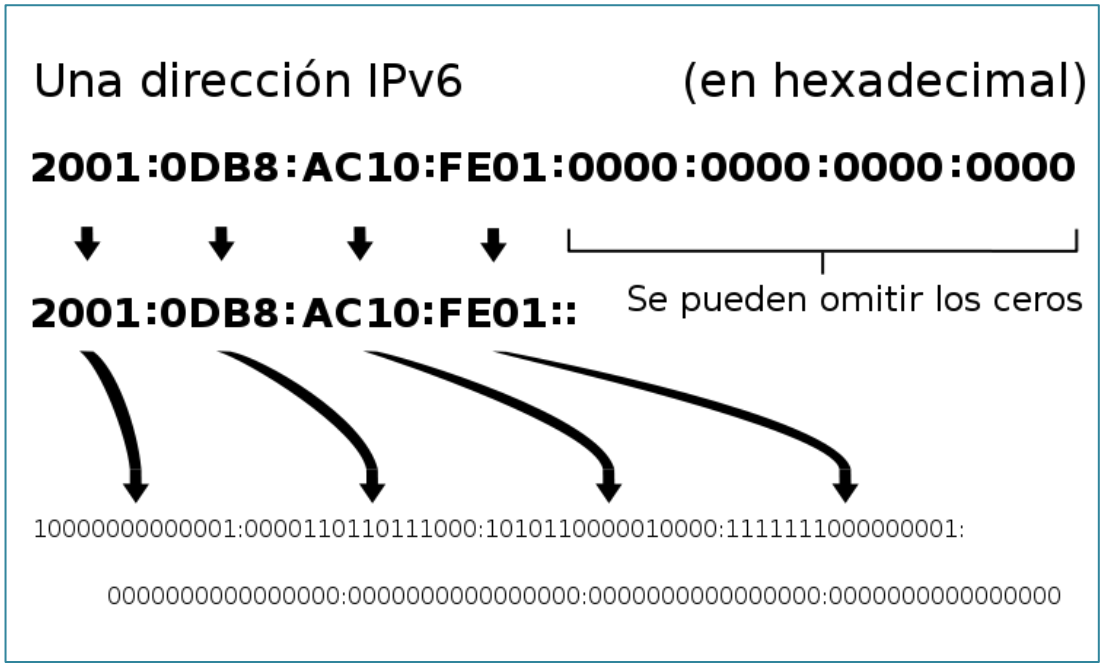
- Identificador de **red**, que determina la red en la que se encuentra el dispositivo.
- Identificador de estación (**host**) dentro de la red. Todos los host de una misma red comparten la parte de identificador de red.



Actualmente se está utilizando la versión **IPv4**, pero la demanda mundial de direcciones ha excedido las posibilidades de este formato. El rango debe incrementarse de alguna manera. En este sentido ha surgido **IPv6**.

Las direcciones IPv6 están basadas en **128 bits**, correspondientes a **32 dígitos hexadecimales**.

Estas IPs están compuestas por 8 secciones de 4 dígitos de 16 bits cada uno y cada sección está separada por dos puntos **(:)**. Debido a que cada sección es de **4** dígitos de **16** bits tendremos un total de **65.536** combinaciones posibles por sección.



Máscara de red

Indica, en una dirección IP, qué porción de bits forman parte de la red y cuáles identifican a la estación. También está formada por **32 bits** agrupados en **4 grupos** de **8 bits** cada uno.

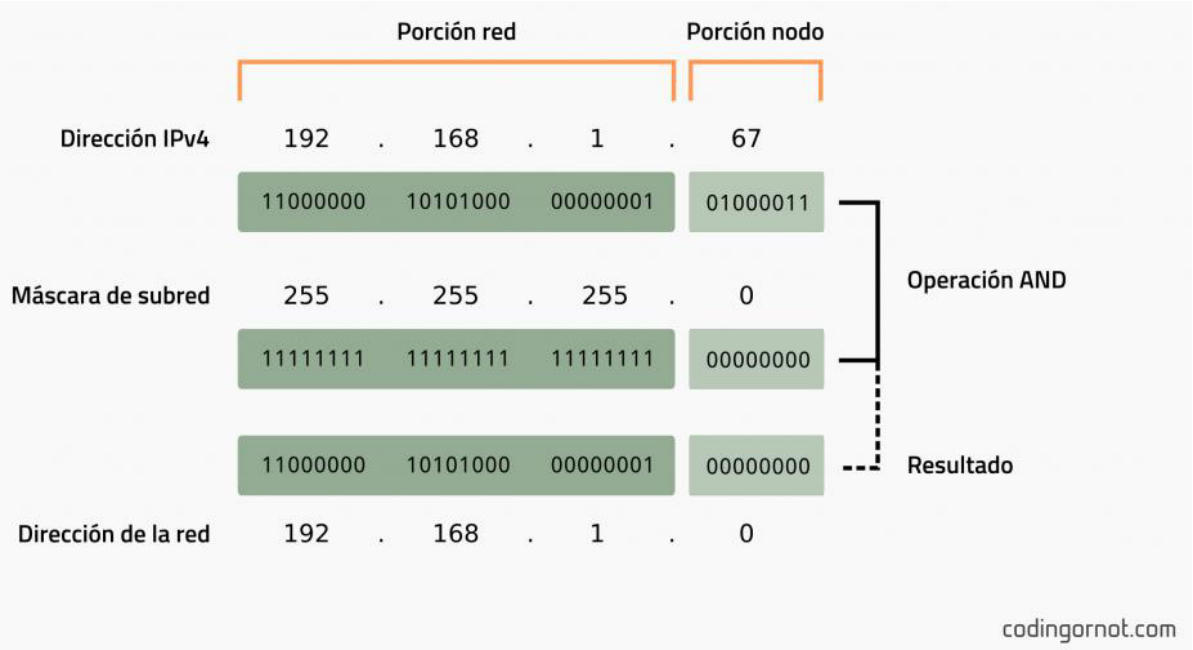
Las máscaras se crean, con notación binaria, poniendo todos los bits que identifican a la red a “1” y los bits que identifican a la estación a “0”.

El **router** usa la máscara de red para conocer la dirección de red de una IP dada y conseguir un encaminamiento eficaz. Es decir, enviar los paquetes de información que recibe a la dirección correcta.

La máscara de red no añade ninguna funcionalidad a una dirección IP. Simplemente se emplea para ayudar a conocer el número de bits que identifican a una red y el número de bits que identifican a la estación.



Máscara de red



El procedimiento que se utiliza para diferenciar una parte de otra es simple: nuestro sistema realiza una operación lógica **AND** sobre la dirección IP y la máscara de subred, bit por bit.

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

La máscara de red también puede expresarse mediante la notación **CIDR** (***C**lassless **I**nter-**D**omain **R**outing*) que sitúa un valor a continuación de la IP indicando cuantos bits de la máscara de red están a 1.

IP 192.168.0.1
MS 255.255.255.0 ⇒ 192.168.0.1/24

En ***Windows***, si se ejecuta el programa **cmd** (símbolo del sistema) y se escribe **ipconfig /all** podemos ver la configuración de red de nuestro equipo.
En ***Linux***, utilizaremos, desde la terminal, **ip** o ***ifconfig*** (obsoleto).

Clases de direcciones IP

El identificador de red puede tener una longitud en bits variable, aunque en un principio se predeterminaron una serie de máscaras de red concretas para facilitar el proceso de encaminamiento. Surge así el concepto de **clase de direcciones**.

- **Clase A**: un byte para el identificador de red y tres bytes para el identificador de host. La máscara de red predeterminada es **255.0.0.0** y su primer octeto está comprendido entre 0 y 127. Por ejemplo, la dirección 10.52.36.11 es de clase A. Se utiliza para redes grandes, ya que deja un gran número de bits para los host de la red.
- **Clase B**: dos bytes para el identificador de red y dos bytes para el identificador de host. La máscara de red predeterminada es **255.255.0.0** y su primer octeto está comprendido entre 128 y 191. Por ejemplo, la dirección 172.16.52.63 es de clase B. Se utiliza para redes medianas.
- **Clase C**: tres bytes para el identificador de red y un byte para el identificador de host. La máscara de red predeterminada es **255.255.225.0** y su primer octeto está comprendido entre 192 y 223. La dirección 192.168.123.132 es de clase C. Se utiliza para redes pequeñas.
- Existen también las clases **D** y **E**, pero los usuarios finales no suelen utilizarlas.

En algunos casos, los valores de la máscara de red predeterminada no cubren las necesidades de la organización debido a la topología física de la red o a que el número de redes o de hosts no encaja dentro de las restricciones de la máscara de subred predeterminada. En este caso se pueden dividir las redes utilizando **máscaras de subred**.

Clase de dirección	Rango del primer octeto (decimal)	Bits del primer octeto (los bits verdes no se modifican)	Partes de una dirección correspondientes a la red (R) y al host (H)	Máscara de subred por defecto (decimal y binaria)	Cantidad posible de redes y hosts por red
A	De 1 a 127	00000000 - 01111111	R.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 redes (2^7-2) 16 777 214 hosts por red (2^24-2)
B	De 128 a 191	10000000 - 10111111	R.R.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16 382 redes (2^14-2) 65 534 hosts por red (2^16-2)
C	De 192 a 223	11000000 - 11011111	R.R.R.H	255.255.255.0 11111111.11111111.11111111.00000000	2097,150 redes (2^21-2) 254 hosts por red (2^8-2)
D	De 224 a 239	11100000 - 11101111	No es para uso comercial como host		
E	De 240 a 255	11110000 - 11111111	No es para uso comercial como host		

^^ Las direcciones que tienen sólo ceros (0) y sólo unos (1) son direcciones host no válidas.

Direcciones especiales

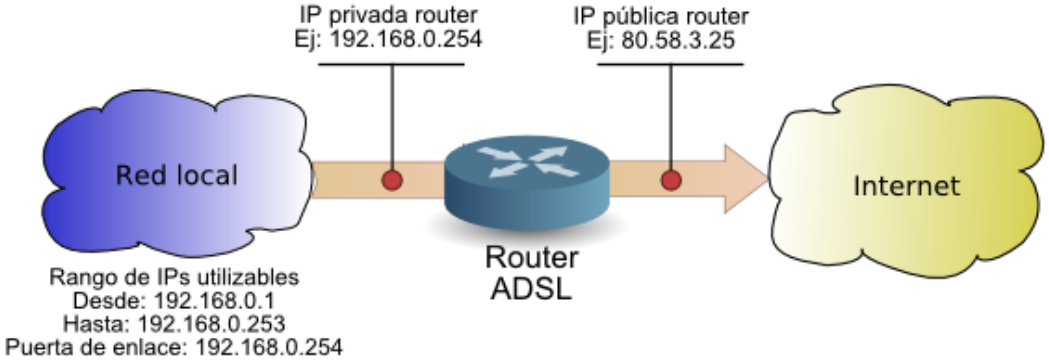
Es importante destacar que existen direcciones reservadas, y por tanto no asignables a un ordenador dentro de una red.

- **Dirección de red**: IP con número de estación todo a ceros (por ejemplo 192.168.1.0), se usa para indicar la red actual completa (una red debe tener también una IP por cuestiones de encaminamiento).
- **Dirección de bucle local**: se reserva para los procesos de comunicación a través de TCP/IP que se generan dentro del host. Se emplea cualquier dirección de la red 127.0.0.0/8. En particular la dirección 127.0.0.1 se llama **localhost** e identifica la tarjeta de red por defecto de cualquier dispositivo.
- **Dirección de broadcast**: sirve para comunicar con todos los host de la red en la que se ubica a la vez. Por ejemplo 192.168.1.255.
- **Dirección del router**: no tiene por qué ser una dirección concreta, aunque por comodidad se suele elegir la primera (o la última) dirección de la red. En este caso lo habitual es que el router tenga la dirección 192.168.1.1, aunque puede tomar otra.

Direcciones públicas y privadas

- **Direcciones públicas**: identifican a un dispositivo conectado a Internet. No se deben utilizar en un ordenador interno ya que podrían ocasionar conflictos al comunicarse con el exterior.
- **Direcciones privadas**: son rangos de direcciones reservados para redes privadas o intranets y no pueden emplearse en Internet. Conectan varios ordenadores y/o dispositivos dentro de una LAN.

Las direcciones IP de los PCs de una red local son direcciones privadas ya que los PCs no están directamente conectados a Internet. Solamente el router dispone de conexión directa a Internet y por eso es el único que dispone de una dirección IP pública.
Cuando los PCs de una misma red se quieren comunicar unos con otros, lo hacen directamente, pero si quieren comunicarse con Internet, deben hacerlo a través del router.



Los routers conectados a redes públicas (*internet*) descartan el tráfico dirigido a direcciones privadas como medida adicional de seguridad.

Los únicos rangos de direcciones (direcciones privadas) que se pueden utilizar en redes locales son:

Rangos Redes Locales	
Desde	Hasta
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Puerta de enlace

La puerta de enlace (***gateway***) es un dispositivo con el que podemos interconectar redes con protocolos y/o arquitecturas diferentes.

Traduce la información del protocolo utilizado en una red al protocolo usado en la red de destino, suele traducir las direcciones IP de ambas para que se comuniquen entre ellas.

Se utiliza para esto los *routers* o los ordenadores con al menos dos tarjetas de red. Cada puerta de enlace lleva asociada una dirección IP, las más comunes suelen ser por defecto: 192.168.1.1, 192.168.0.1, 10.0.0.1, etc.

Lo normal es que todos los PCs de nuestra red tengan configurada la misma puerta de enlace.

Aunque en la actualidad suelen coincidir casi siempre, no hay que confundir los conceptos de **router** y **gateway**.

Subredes

Los administradores de sistemas pueden dividir todavía más una red TCP/IP de clase A, B o C en **subredes**. El administrador del sistema que asigna un bloque de direcciones IP puede estar administrando redes que no se organizan de una forma que encaje fácilmente con estas direcciones.

*Por **ejemplo**, supongamos que tiene una red de área extensa con 150 hosts en tres redes de ciudades diferentes que se conectan mediante un enrutador TCP/IP. Cada una de estas tres redes tiene 50 hosts. Se le asigna la red de clase C 192.168.123.0. Esto significa que puede usar las direcciones entre 192.168.123.1 y 192.168.123.254 para los 150 hosts.*

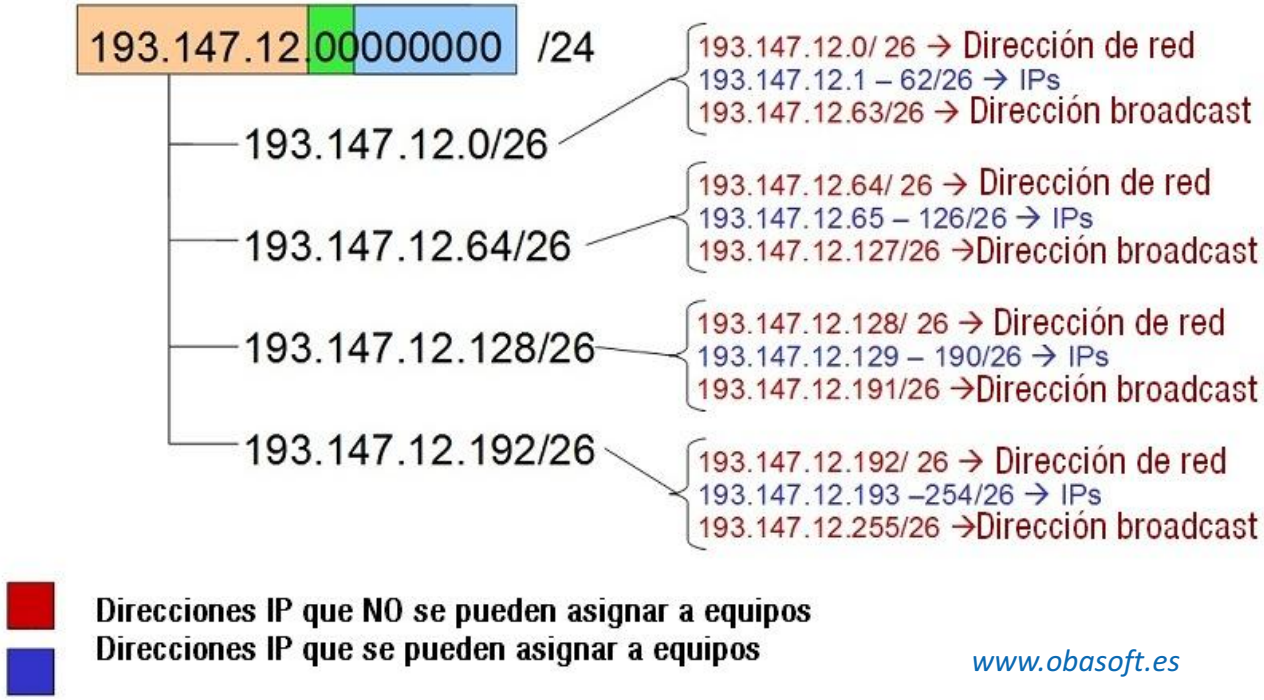
Recordemos que hay dos direcciones (la de red y la de broadcast) que no se pueden usar. En el ejemplo serían 192.168.123.0 y 192.168.123.255.
Ahora debería ser capaz de asignar direcciones IP a 254 hosts. Esto funciona correctamente si los 150 equipos están en una única red. Sin embargo, sus 150 equipos se hallan en tres redes físicas independientes. En lugar de solicitar más bloques de direcciones para cada red, divide su red en subredes, lo que le permite usar un bloque de direcciones en varias redes físicas.

*En este caso, divide la red en cuatro subredes mediante una máscara de subred que hace que la dirección de red sea más larga y que el intervalo posible de direcciones de host sea menor. En otras palabras, está "**tomando prestados**" algunos de los bits que se suelen usar para la dirección del host y los está usando para la parte correspondiente a la red.*

La máscara de subred 255.255.255.192 le da cuatro redes de 62 hosts cada una. Esto funciona porque, en notación binaria, 255.255.255.192 es lo mismo que 1111111.11111111.1111111.11000000. Los primeros dos dígitos del último octeto se convierten en direcciones de red, con lo que se obtienen las redes adicionales 00000000 (0), 01000000 (64), 10000000 (128) y 11000000 (192). En estas cuatro redes, los últimos seis dígitos binarios se pueden emplear para las direcciones de host.

Al utilizar la máscara de subred 255.255.255.192, la red 192.168.123.0 se convierte en las cuatro redes 192.168.123.0, 192.168.123.64, 192.168.123.128 y 192.168.123.192. Estas cuatro redes tendrían como direcciones de host válidas:

192.168.123.1-62
192.168.123.65-126
192.168.123.129-190
192.168.123.193-254



Se puede ver cómo funciona esto si examinamos las dos direcciones de host 192.168.123.71 y 192.168.123.133. Si se utilizó la máscara de subred predeterminada de clase C 255.255.255.0, ambas direcciones están en la red 192.168.123.0. Sin embargo, si utilizó la máscara de subred 255.255.255.192, se encuentran en redes diferentes: 192.168.123.71 se encuentra en la red 192.168.123.64 y 192.168.123.133 en la red 192.168.123.128.

Pasos para crear subredes

1. Identificar la máscara según la clase a la que pertenezca la red.
2. Resolver $2^n \geq$ **número de subredes** a obtener donde ***n*** será el número de unos que "*tomaremos prestados*" a la parte de dirección de host.
3. Obtener la nueva máscara.
4. Resolver 2^m **-2= número de host** por cada subred donde ***m*** será el número de ceros que quedaron en la parte de dirección de host.
5. Resolver **256-*valor_octeto_modificado_ms*=salto de red**. El "salto de red" es el valor en que se incrementa la dirección de red al pasar de una red a otra.

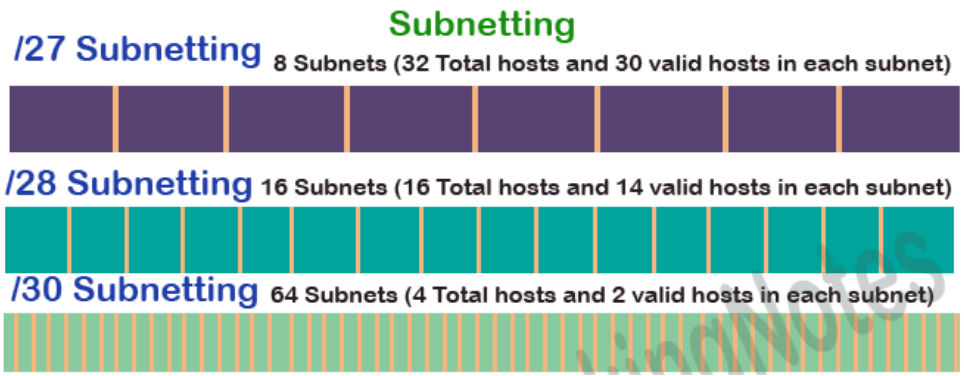
Subnetting

Se basa en la idea de no malgastar direcciones de red. La máscara y el subnetting permitieron multiplicar de forma eficiente los distintos tipos de subredes.

Por ***ejemplo***:

Si necesito una red donde sólo hacen falta 20 IPs, ¿Cuántas direcciones IP malgastamos al coger una dirección de Clase C? Pues malgastaríamos 2^8 - 2 – 20 = 234 IP's.

El subnetting permitió que las redes se pudieran dividir en redes más pequeñas llamadas subredes, haciendo variable las máscaras de las clases y aprovechando mejor el número de direcciones IP.



VLSM

•La máscara de subred de longitud variable (**VLSM**) se utiliza para crear esquemas de direccionamiento **eficientes** y **escalables**.

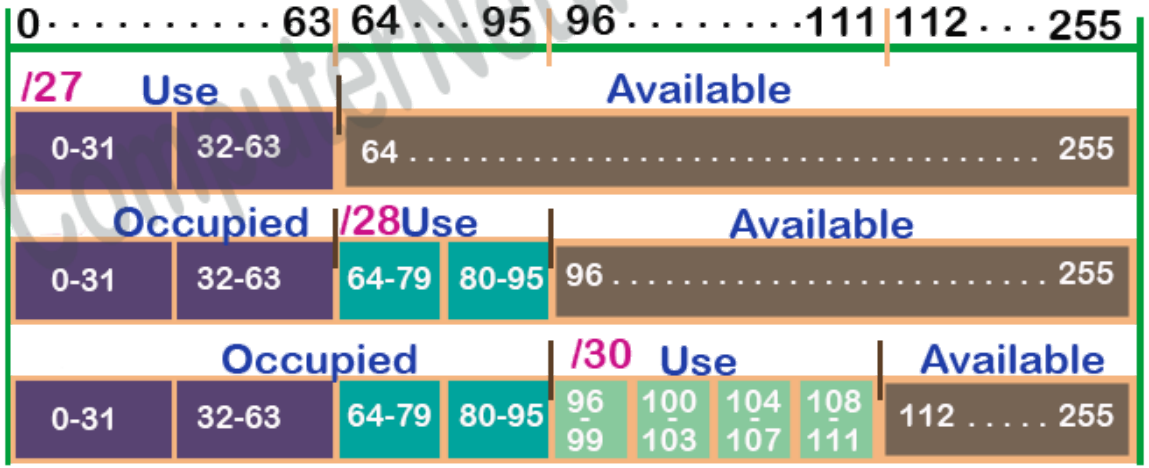
• VLSM se puede usar para dividir a su vez en subredes una dirección que ya está dividida en subredes.

• La utilización de VLSM permite a una organización tener subredes de diferentes tamaños, es decir, utilizar más de una máscara de subred dentro del mismo espacio de direccionamiento de red.

Permite adoptar un esquema de direccionamiento en **función de las necesidades de la red**, así un administrador de red puede usar una máscara larga en las redes con pocos hosts, y una máscara corta en las subredes con muchos hosts.

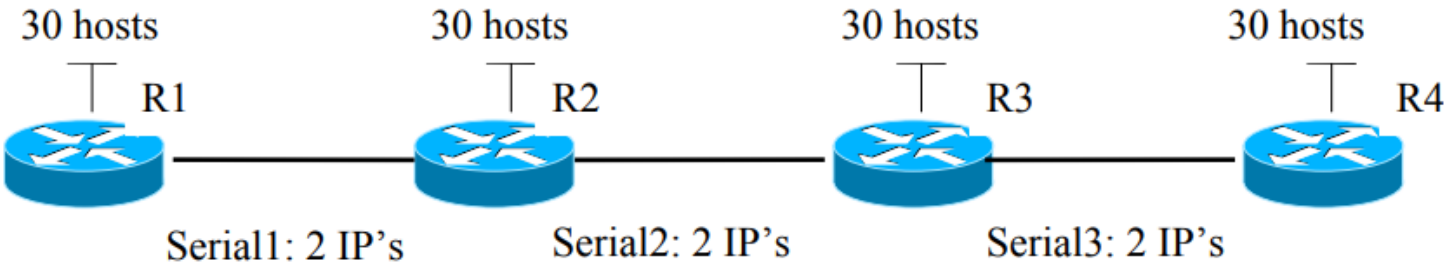
Máscaras de 30 bits → Conexiones seriales, con sólo dos direcciones de host válidas

Máscaras de 22-24 bits → Para 500-1000 usuarios.



Ejemplo

Partiendo de la dirección de red base 192.168.187.0/24, y según el esquema siguiente:



Realizar un esquema de direccionamiento IP que implique un mayor aprovechamiento de direcciones, evitando el desperdicio en los enlaces punto a punto y ajustándose a las necesidades de la red.

Con subnetting

30 hosts se pueden codificar con 5 bits → 2 5 -2 = 30 hosts

192.168.187.XXXXXXXX
192.168.187. 000 XXXXX → 192.168.187.0/27 → Ethernet R1
192.168.187. 001 XXXXX → 192.168.187.32/27 → Ethernet R2
192.168.187. 010 XXXXX → 192.168.187.64/27 → Ethernet R3
192.168.187. 011 XXXXX → 192.168.187.96/27 → Ethernet R4
192.168.187. 100 XXXXX → 192.168.187.128/27 → Serial 1
192.168.187. 101 XXXXX → 192.168.187.160/27 → Serial 2
192.168.187. 110 XXXXX → 192.168.187.192/27 → Serial 3
192.168.187. 111 XXXXX → 192.168.187.224/27 → Libre

Hemos agotado todas las direcciones disponibles y no habrá más espacio para el crecimiento.
Direcciones libres = 30 IP.
Direcciones desperdiciadas en enlaces punto a punto: 28 x 3 = 84
*Este direccionamiento implica un **desperdicio de 1/3 del espacio de direccionamiento** potencial ocasionado por direccionar 3 redes punto a punto con subredes /27.*

Con VLSM

Asignaremos subredes /30 a las conexiones punto a punto dividiendo una subred que antes asignábamos enteramente a un enlace WAN

192.168.187.XXXXXXXX
192.168.187. 000 XXXXX → 192.168.187.0/27 → Ethernet R1
192.168.187. 001 XXXXX → 192.168.187.32/27 → Ethernet R2
192.168.187. 010 XXXXX → 192.168.187.64/27 → Ethernet R3
192.168.187. 011 XXXXX → 192.168.187.96/27 → Ethernet R4

192.168.187. 100 000 XX → 192.168.187.128/30 → Serial 1
192.168.187. 100 001 XX → 192.168.187.132/30 → Serial 2
192.168.187. 100 010 XX → 192.168.187.136/30 → Serial 3

192.168.187. 100 …….→ se pueden obtener direcciones IP para 8 enlaces series 3

192.168.187. 101 XXXXX → 192.168.187.160/27 → Libre
192.168.187. 111 XXXXX → 192.168.187.192/27 → Libre
192.168.187. 111 XXXXX → 192.168.187.224/27 → Libre

Fuente: personals.ac.upc.edu



Subnetting



Subnetting con VLSM

Supernetting

Una **superred** o **supernet** es una red IP que está formada por la combinación de dos o más redes o subredes con un prefijo CIDR común. El prefijo de enrutado de la superred comprende los prefijos de las redes que la constituye.

Se trata de resumir varias redes utilizando para ello la sumarización de sus bits comunes.

El Supernetting (o uso de **Superredes**) sirve para aligerar las tablas de enrutamiento, pues en lugar de varias entradas apuntando a varias subredes , podemos **resumir todas ellas en una superred que será el resultado de la sumarización de las anteriores**.

¿Qué es Sumarizar?

Sumarizar" es resumir los bits comunes de varias redes. De esa forma obtenemos una red con prefijo (el cual indicará los bits comunes, que forman la parte de red).

Por supuesto hemos de tener en cuenta que para usar **Supernetting** tendremos que implementar un protocolo de enrutamiento dinámico sin clase que soporte VLSM y CIDR , como por ejemplo OSPF, RIP v2, IS-IS…

Recordemos que los protocolos sin clase envían la máscara de subred en las actualizaciones de enrutamiento.

Ejemplo de Sumarización de Redes

172	30	4	0
10101100	00011110	00000100	00000000
172	30	5	0
10101100	00011110	00000101	00000000
172	30	6	0
10101100	00011110	00000110	00000000
172	30	7	0
10101100	00011110	00000111	00000000

Resultado de la sumarización:

172	30	4	0
10101100	00011110	00000100	00000000

Con Prefijo de Red ----> /22 (22 bits en común)



Superredes

9. Traducción de direcciones de red. NAT y PAT

La idea básica que hay detrás de **NAT** (Net Address Translation) es traducir las IPs privadas de la red en una IP publica para que la red pueda enviar paquetes al exterior; y traducir luego esa IP publica, de nuevo a la IP privada del pc que envió el paquete, para que pueda recibirlo una vez llega la respuesta.

Esta técnica reduce el número de direcciones IP públicas además de proporcionar un mayor grado de seguridad para los ordenadores de la red interna ya que permite ocultar las direcciones originales al circular por el exterior.

PAT (Port Address Translation) es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet.

NAT

Conjunto de direcciones globales internas	Dirección local interna
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Dirección global interna	Dirección local interna
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

www.sapalomera.cat

¿Cómo conocer nuestra IP pública? Lo más sencillo es utilizar alguna web, como por ejemplo ***miip.es***



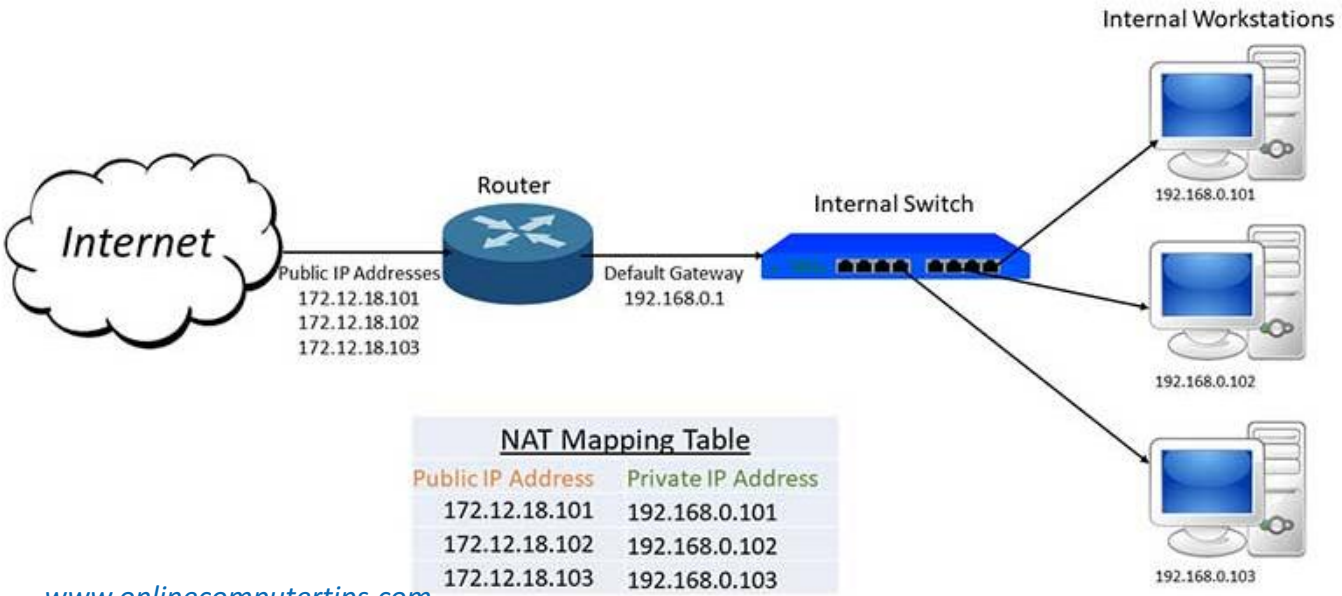
Traducción de direcciones de red – NAT

***Por ejemplo**:*

Tenemos la siguiente red (casera) con dos PCs que salen a Internet a través del router. Cada PC tiene asignada una IP privada. El router tiene su IP privada (puerta de enlace) y su IP pública (que es la IP de Internet).

*Cuando uno de los PCs de la red local quiere enviar un paquete a Internet, se lo envía al router (o a la puerta de enlace o gateway), y éste hace lo que se conoce como **SNAT** (SourceNAT) y cambia la dirección de origen por si IP pública. Así, el host remoto sabrá a qué IP pública ha de enviar sus paquetes.*

Cuando una respuesta o un paquete pertenecientes a esa conexión llegue al router, éste traducirá la dirección IP de destino del paquete (que ahora es la IP del router) y la cambiará por la dirección privada del host que corresponde, para hacer la entrega del paquete a la red local.



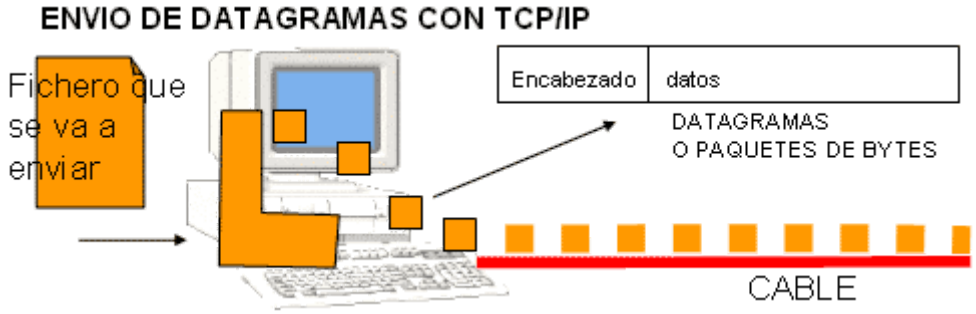
www.onlinecomputertips.com

Para que funcione el encaminador que da acceso a Internet debe reescribir algunos datos en los ***datagramas*** que encamina. En función de la información que se modifique tenemos varios tipos de NAT.

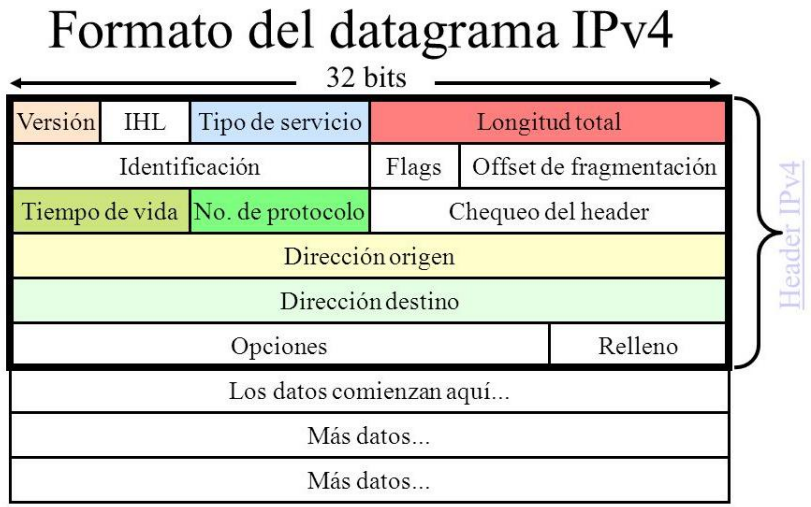
- **NAT** básico: sólo se modifica la IP.
- **NAPT/PAT**: además se modifican los puertos empleados en la comunicación (IP de origen, puerto de origen, IP de destino, puerto de destino.

El encaminador NAT dispondrá de una tabla NAT con los cambios que se realizan en el tráfico saliente para poder deshacer dichos cambios en el tráfico entrante

Datagrama: es una unidad de datos que se encuentra asociada a una red de conmutación de paquetes. Es habitual que estos se encuentren estructurados en secciones de cabecera y datos



informaticafrida.blogspot.com



REFERENCIAS

Bibliografía

Servicios de red e internet. García Sánchez, Álvaro. Sanz Rodríguez, Javier. González Sotillo, Álvaro. Enamorado Sarmiento, Luis. Garceta Grupo Editorial.

Webgrafía

Wikipedia

Otros…

