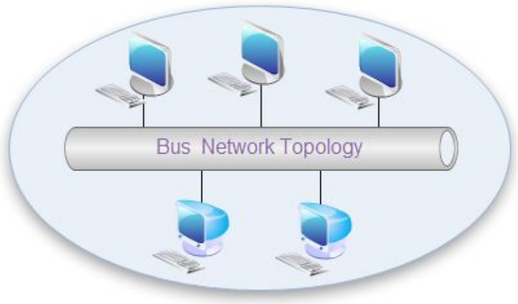
THE BRIDGE

CYBER SECURITY

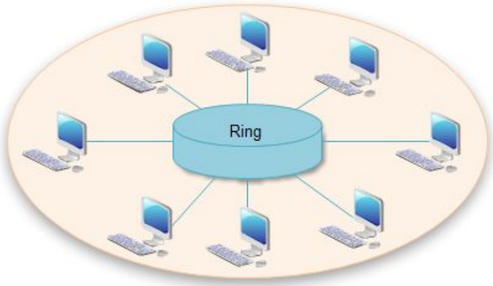
Fundamento de Redes

Topologías

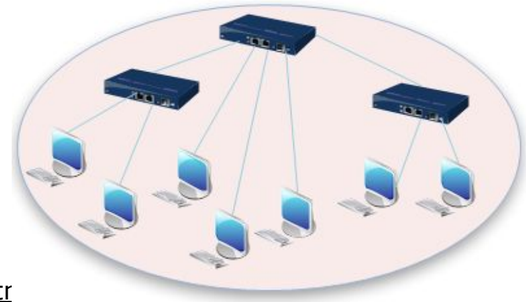
- La topología de red se define como un mapa físico o lógico de una red para intercambiar datos.
- El concepto de red puede definirse como «**conjunto de nodos interconectados**».
- Los tipos de Topología son:
  - **Bus**: todos los nodos están conectados a un único cable de comunicación, llamado bus. Los datos se transmiten en ambas direcciones a través del bus.



  - **Anillo**: los nodos están conectados en un círculo cerrado. Los datos se transmiten en una dirección a través del anillo



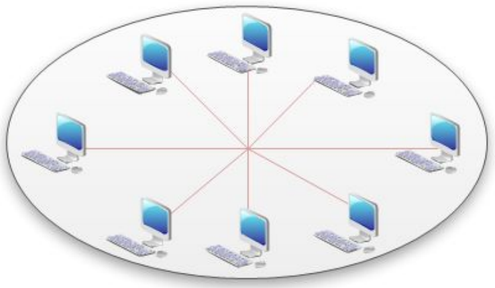
  - **Topología de Árbol:** Pueden enlazarse varios dispositivos en una topología de árbol como si fueran ramas. Estas topologías se utilizan mucho para enlazar equipos en el sistema de una empresa.



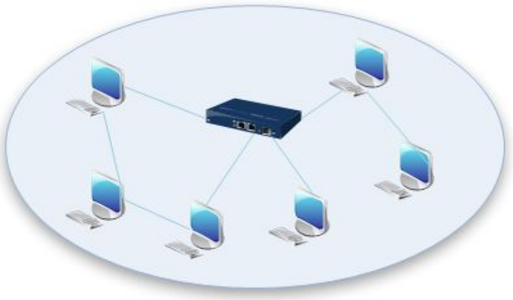
https://www.edrawsoft.com/es/network-topologies.htr

Diferentes Topologías

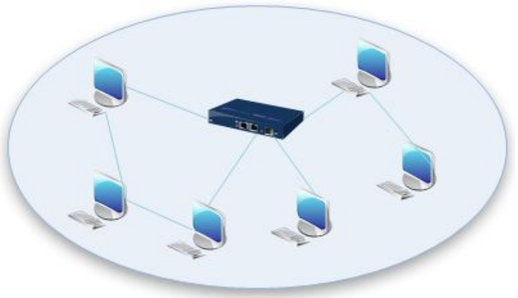
- **Topología en estrella**: todos los nodos están conectados a un nodo central, llamado concentrador o switch. Los datos se transmiten desde el nodo fuente al nodo central y luego al nodo de destino.



- **Topología en malla**: cada nodo está conectado a todos los demás nodos de la red. Los datos se transmiten directamente de un nodo a otro.



- **Topología híbrida:** es una combinación de dos o más topologías de red. Por ejemplo, una topología de estrella que se conecta a otras topologías de estrella.



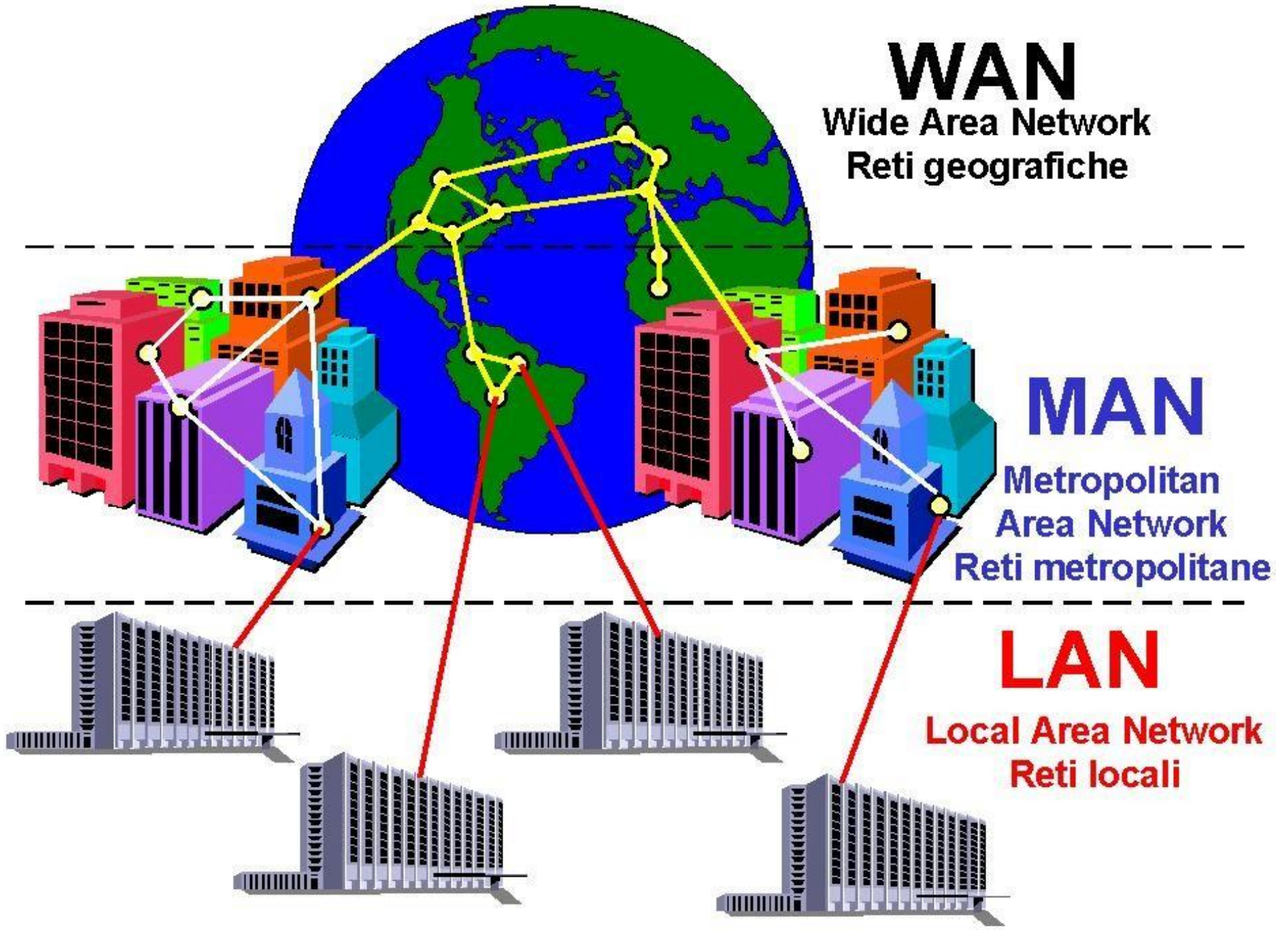
https://www.edrawsoft.com/es/network-topologies.html

Tipo de redes

- **Wide Area Network (WAN)**
  - Las Wide Area Networks (WAN) o redes de área amplia se extienden por zonas geográficas como países o continentes.
  - El número de redes locales o terminales individuales que forman parte de una WAN es, en principio, ilimitado

- **Metropolitan Area Network (MAN)**
  - La Metropolitan Area Network (MAN) o red de área metropolitana es una red de telecomunicaciones de banda ancha que comunica varias redes LAN en una zona geográficamente cercana.
  - Por lo general, se trata de cada una de las sedes de una empresa que se agrupan en una MAN por medio de líneas arrendadas.

- **Local Area Network (LAN)**
  - Si una red está formada por más de un ordenador, esta recibe el nombre de Local Area Network (LAN).
  - Una red local de tales características puede incluir a dos ordenadores en una vivienda privada o a varios miles de dispositivos en una empresa.
  - Asimismo, las redes en instituciones públicas como administraciones, colegios o universidades también son redes LAN.
  - Un estándar muy frecuente para redes de área local por cable es Ethernet.



https://sites.google.com/site/nenixtkm/-tipo-de-redes

NIC

- La **NIC** (del inglés **Network Interface Card**), la tarjeta de red; componente de hardware que conecta una computadora a una red informática. También llamada Tarjeta de Red.

- **Tipos de NIC**
  - **Según el BUS**: PCI, USB, etc.
  - **Según el tipo de puerto**: Coaxial, RJ45 (Categoría 4, 5,6 etc.)
  - **Según la velocidad**: 10Mbps, 100Mbps, 10/100Mbps, 1000Mbps, etc.

- Al funcionar como una interfaz en la capa TCP/IP, una tarjeta NIC puede transmitir señales en la capa física y paquetes de datos en la capa de red

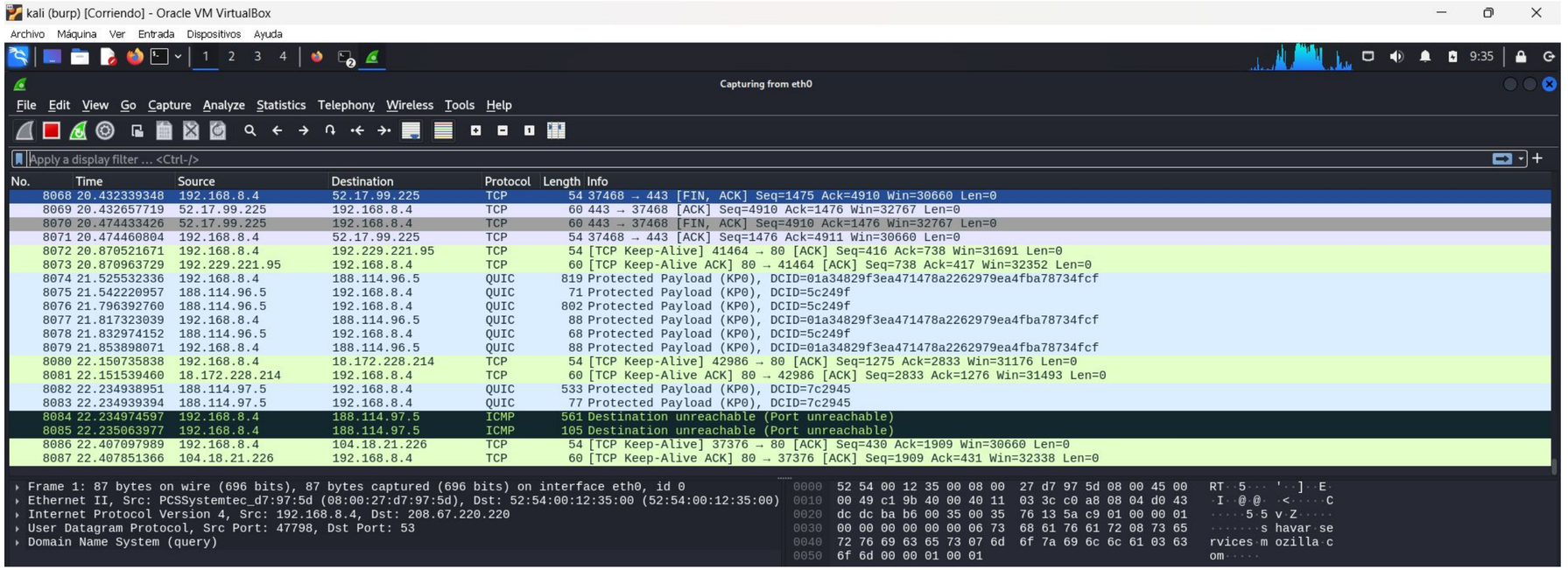
  - Cuando un usuario solicita una página web, la tarjeta LAN obtiene datos del dispositivo del usuario y los envía al servidor en Internet, y luego recibe los datos requeridos de Internet para mostrárselos a los usuarios

- **Modos de funcionamiento**
  - Gestionado o normal
  - Monitor o promiscuo

https://www.tecnologia-informatica.com/tarjeta-de-red/

Modo Promiscuo

- **Modo Monitor o promiscuo**
  - Es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella.
  - Este modo está muy relacionado con los **sniffers** que se basan en este modo para realizar su tarea
  - El modo promiscuo resulta muy útil para ver qué paquetes atraviesan tu red.
  - Su utilidad se basa en que todos los paquetes que pasan por una red tienen la información de a qué protocolo pertenece y las opciones de reensamblado. Incluso, si están cifrados, tienen la información en claro, es decir, que es posible saber qué contiene el paquete.



MAC

- La Mac Address o dirección Mac (siglas en inglés de Media Access Control) es un identificador único de 48 bits para identificar los dispositivos de NIC, WIFI, Impresoras, etc.
  - Son identificadores únicos a nivel mundial para cada dispositivo.
  - Los fabricantes graban la Mac en la memoria ROM del dispositivo en formato binario, por lo que no se puede modificar.
  - Las primeras 3 partes identifica al fabricante.
  - Las siguientes 3 identifican al dispositivo

https://computerhoy.com/reportajes/tecnologia/direccion-mac-ordenador-movil-sirve-317181

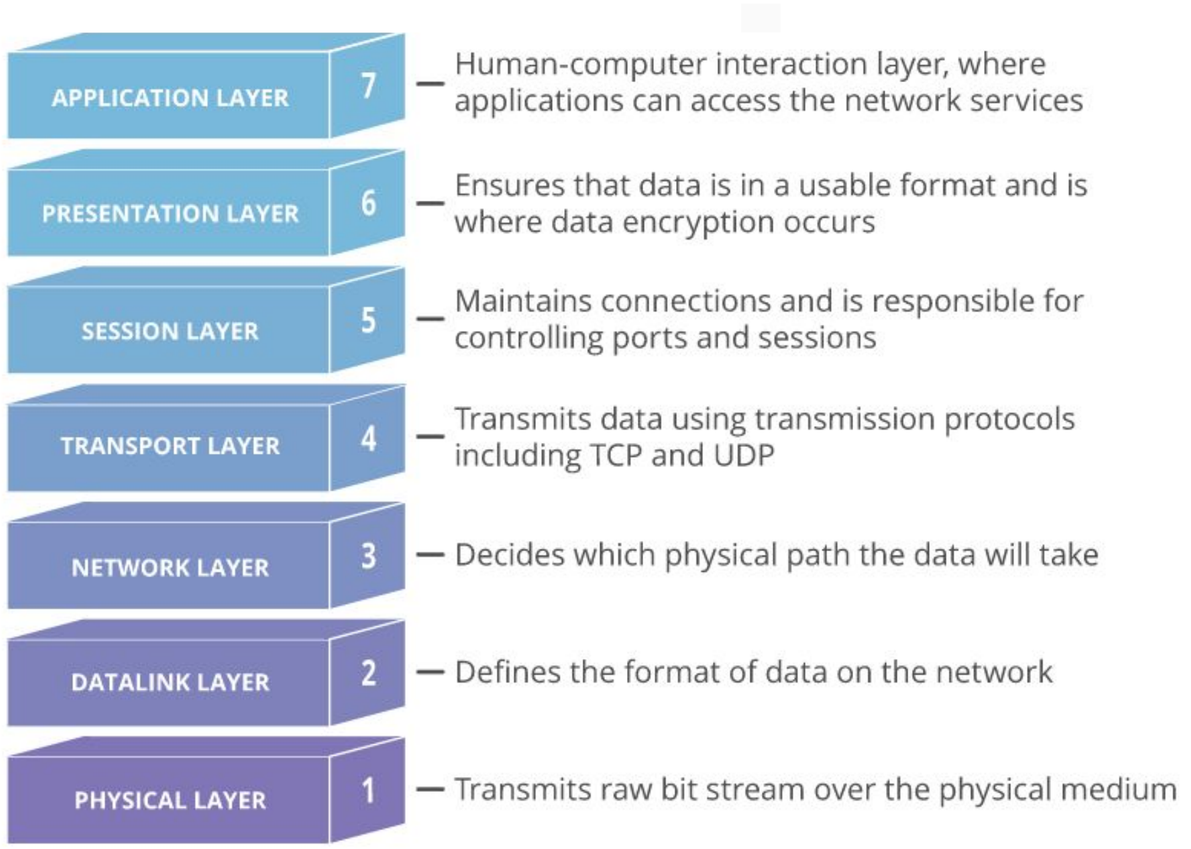
Modelo OSI

- El modelo OSI es un modelo de referencia para los protocolos de la red. Fue creado en el año 1980 por la Organización Internacional de Normalización (ISO) y publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT). El modelo OSI está conformado por 7 capas o niveles de abstracción. Cada uno de estos niveles tendrá sus propias funciones para que en conjunto sean capaces de poder alcanzar su objetivo final.
- A continuación, se detallan las 7 capas del modelo OSI, de arriba hacia abajo:

  - **Capa de aplicación**: Es la capa que interactúa directamente con los datos del usuario, como navegadores web o correo electrónico. En resumen, es responsable de la traducción, el cifrado y la compresión de datos.

  - **Capa de presentación**: Esta capa es responsable de la presentación de los datos. Es deciº, se encarga de la representación de los datos para que puedan ser interpretados por la capa de aplicación. En resumen, es responsable de la codificación y decodificación de los datos.

  - **Capa de sesión**: Esta capa es responsable de crear la sesión, o la instancia de comunicación, entre los dos dispositivos. Esta capa garantiza que se puedan transferir todos los datos que se intercambian y luego se encarga de cerrar la sesión. En resumen, las tareas de esta capa incluyen la configuración, coordinación y terminación de una sesión.



https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/

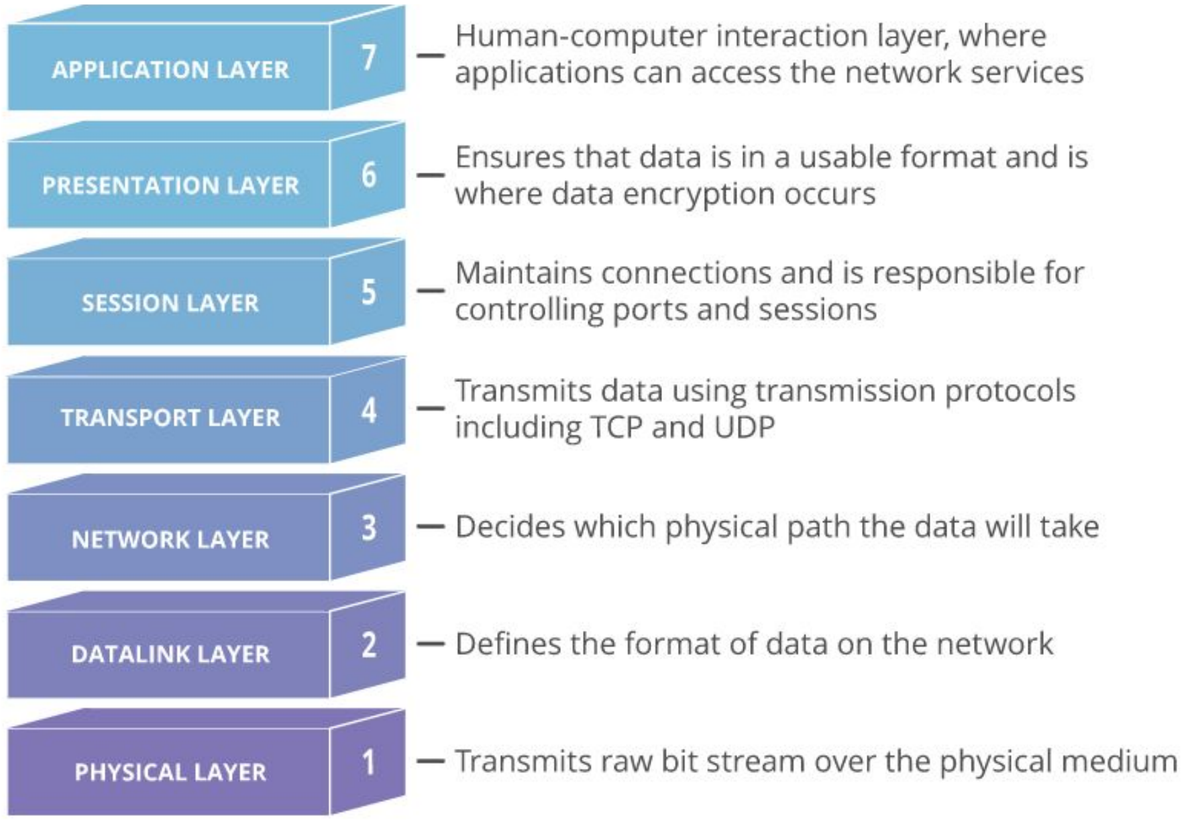
Modelo OSI

- **Capa de transporte**: Esta capa es la responsable de la comunicación de extremo a extremo entre los dos dispositivos. Es decir, de tomar datos de la capa de sesión y dividirlos en segmentos, antes de enviarlos a la capa 3.

- **Capa de red**: Esta capa es responsable de la transferencia de datos entre redes diferentes. Es decir, de tomar los datos de la capa de transporte y enviarlos a través de la red. La capa de red también es responsable de la identificación de la mejor ruta para que los datos lleguen a su destino.

- **Capa de enlace de datos**: Esta capa es responsable de la transferencia de datos entre dispositivos conectados directamente. Es decir, de tomar los datos de la capa de red y dividirlos en tramas antes de enviarlos a la capa física. La capa de enlace de datos también es responsable de la detección y corrección de errores en la transmisión de datos.

- **Capa física**: Esta capa es responsable de la transmisión de datos a través del medio físico. Es decir, de tomar los datos de la capa de enlace de datos y convertirlos en señales eléctricas, ópticas o de radio para su transmisión a través del medio físico. La capa física también es responsable de la detección de errores en la transmisión de datos .



https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/

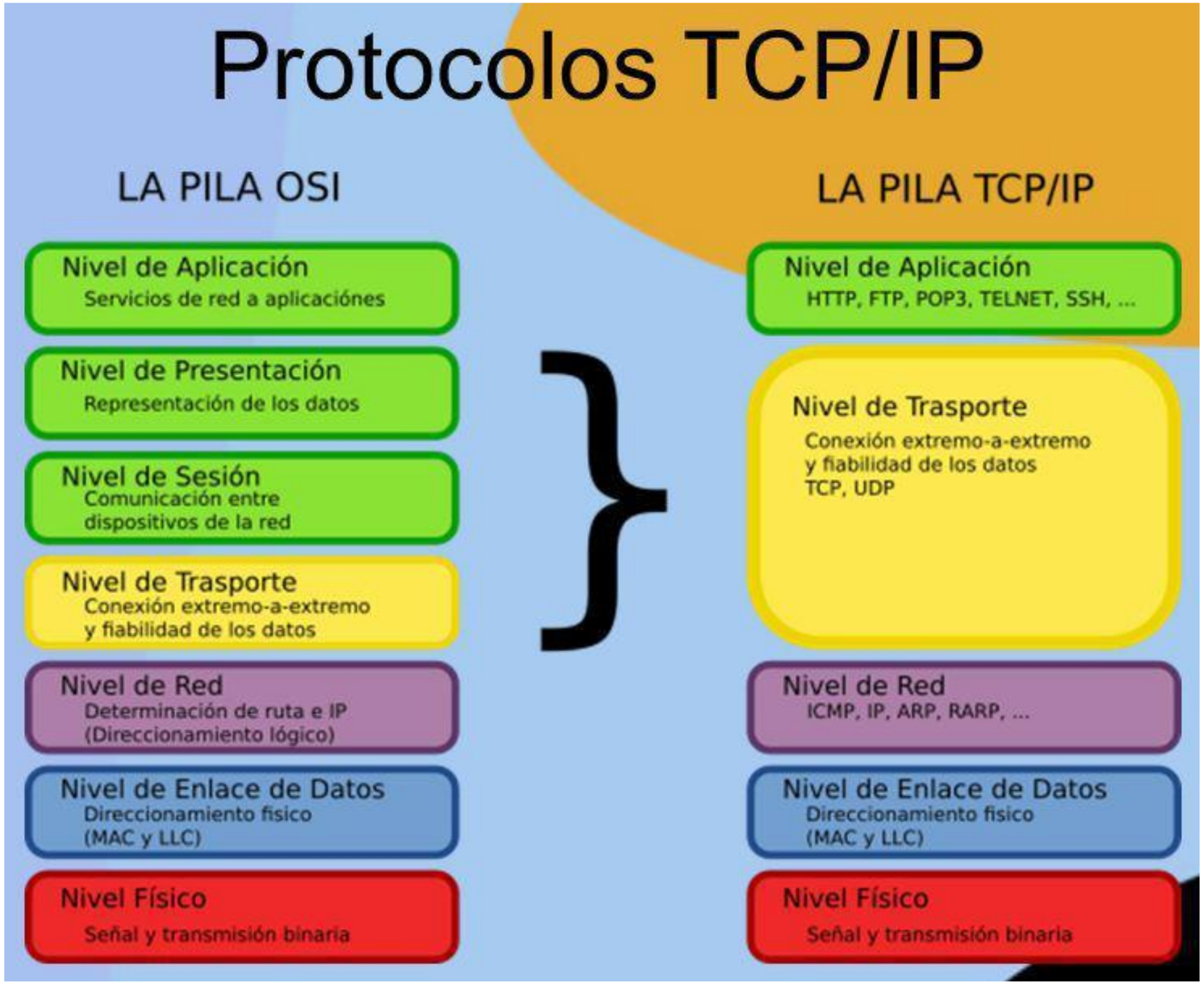
Protocolo TCP/IP

- La definición de TCP/IP es la identificación del grupo de protocolos de red que hacen posible la transferencia de datos en redes, entre equipos informáticos e internet.

- Este protocolo hace que la capa de transporte haga las funciones de la capa de presentación, sesión y transporte.

- Las siglas TCP/IP hacen referencia a este grupo de protocolos:
  - **TCP** es el Protocolo de Control de Transmisión que permite establecer una conexión y el intercambio de datos entre dos anfitriones. Este protocolo proporciona un transporte fiable de datos.

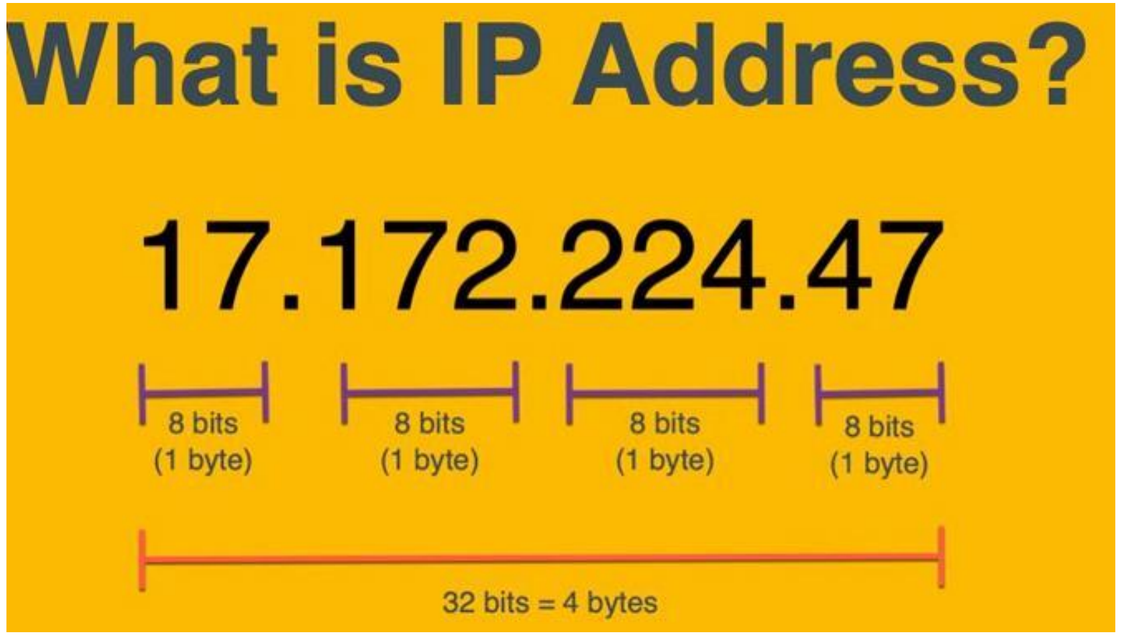
  - **IP** o protocolo de internet, utiliza direcciones series de cuatro octetos con formato de punto decimal (como por ejemplo 75.4.160.25). Este protocolo lleva los datos a otras máquinas de la red.



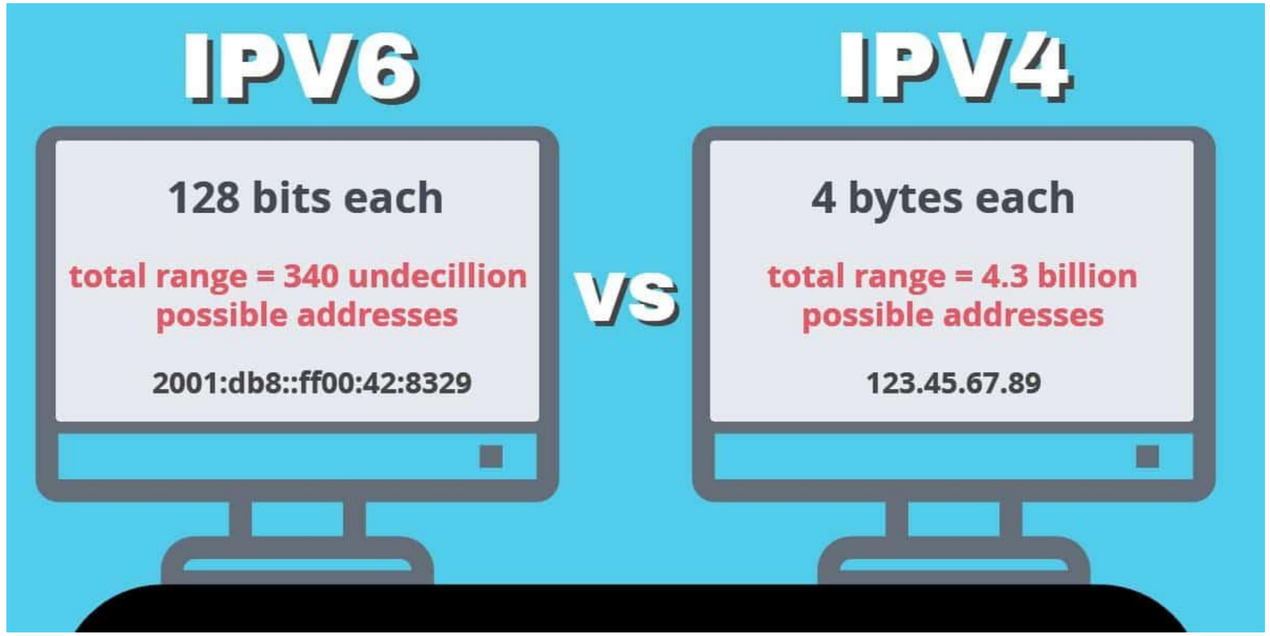
https://slideplayer.es/slide/39823/

Dirección IP

- «Dirección IP» significa «dirección del Protocolo de Internet».
- Una dirección IP identifica una red o dispositivo en Internet
- Como se compone una dirección IP
- Esta la versión 4 y la versión 6 actualmente.



https://operavps.com/what-is-an-ip-address/



https://www.kaskus.co.id/thread/5edc5f2f09b5ca5c2a76b00e/situs-yang-cuma-bisa-diakses-dengan-ipv6

Mascara de Subred

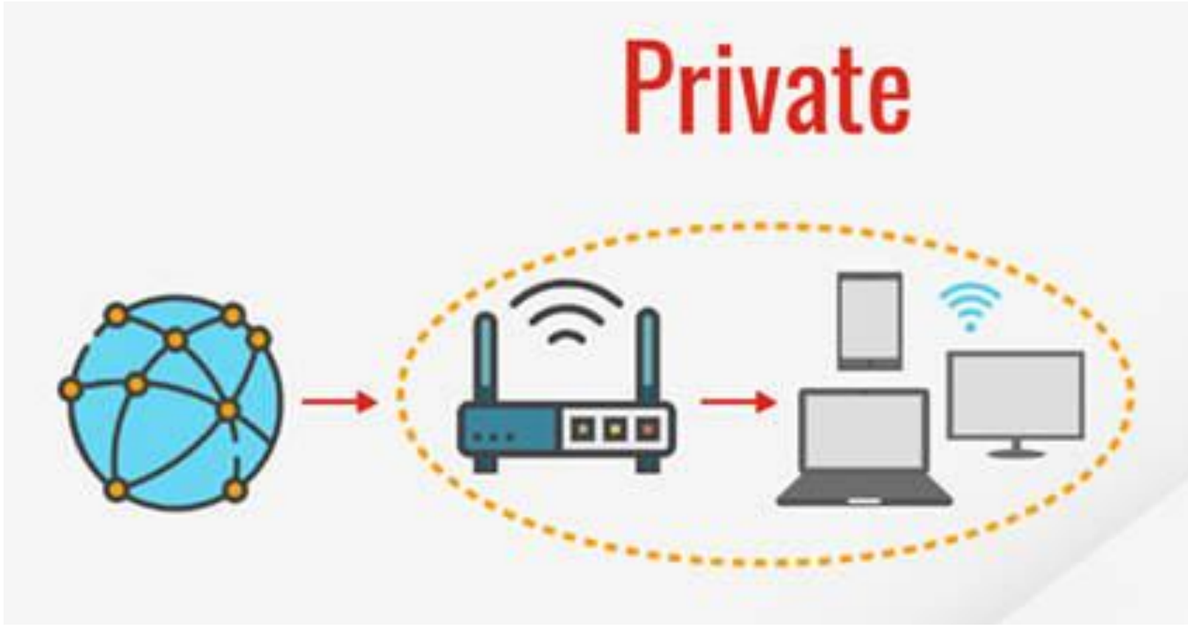
- La subred se refiere al proceso de división de la red más grande en subredes más pequeñas (subnets).
- Siempre se asigna una dirección IP para identificar la subred y otra para identificar la dirección de difusión dentro de la subred.
- Es más eficiente y permite guardar una gran cantidad de direcciones.
- Genera menos tráfico de emisión y se simplifica la localización de fallos aislando los problemas.
- Una máscara de subred es un número del 1 al 32.

255.255.255.0

https://community.fs.com/es/blog/know-ip-address-and-subnet-mask.html

Tipos de IP

- Una dirección **IP pública** es la dirección IP de puertas afuera (de cara al público) que asigna a su router su proveedor de servicios de Internet (ISP).
  - El router utiliza esta IP pública para poder acceder a Internet.
  - Otros ordenadores en Internet utilizan su dirección IP pública para comunicarse con los dispositivos de su red.
- Una dirección **IP privada** permite al router dirigir correctamente el tráfico de Internet dentro de la red, además de permitir a los dispositivos dentro de una red comunicarse entre ellos.



https://www.fortinet.com/resources/cyberglossary/what-is-ip-address

Tipos de IP

- Una **IP estática** es una dirección IP fija y permanente que se asigna manualmente a un dispositivo.
  - Imagina que es como tener un número de teléfono personal que nunca cambia.
  - Es decir, con una IP estática tu dispositivo siempre tendrá la misma dirección cuando se conecte a internet.
- Una **IP dinámica** es una dirección IP que se asigna automáticamente a tu dispositivo cuando te conectas a internet.
  - Siguiendo el ejemplo anterior, imagina que es como tener un número de teléfono temporal que cambia cada vez que te conectas a la red.
  - Esto es muy útil en la mayoría de los casos, ya que las direcciones IP están limitadas y se pueden reutilizar

https://www.fortinet.com/resources/cyberglossary/what-is-ip-address

Rango de IP

- Ciertas direcciones IP están reservadas para uso público y otras para uso privado.
- Esto es lo que hace que las direcciones IP privadas no puedan llegar a Internet pública, porque ni siquiera pueden comunicarse correctamente a menos que existan detrás de un router.
- Los siguientes rangos están reservados por la Autoridad de números asignados de Internet (IANA)

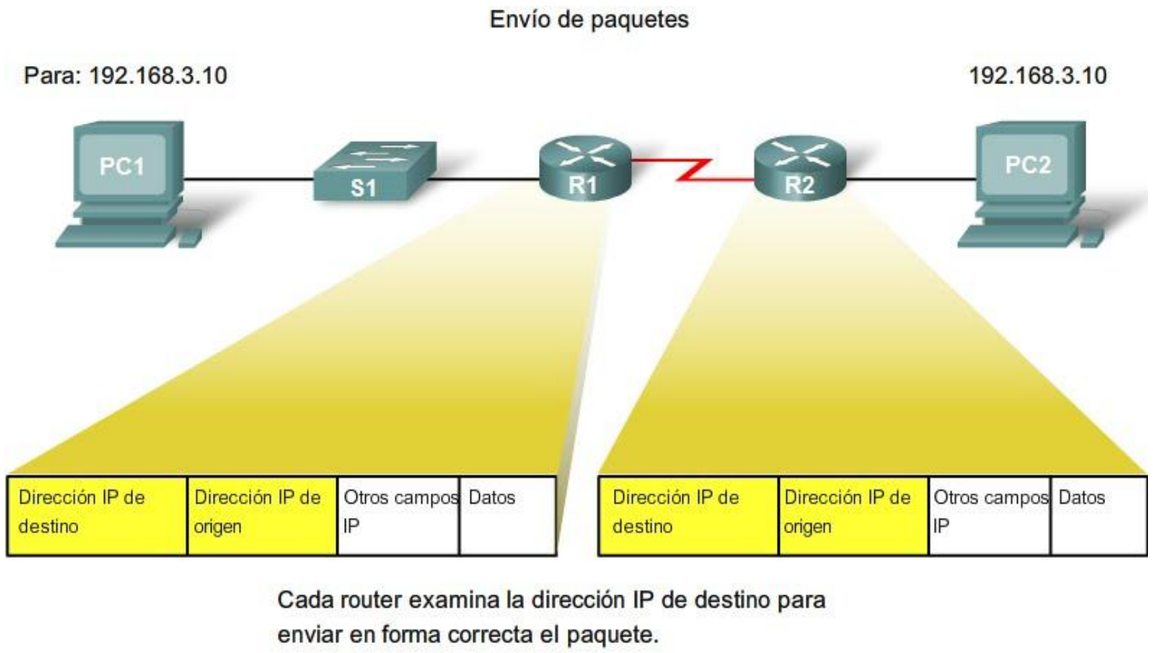
CLASE	DIRECCIONES DISPONIBLES		CANTIDAD DE REDES	CANTIDAD DE HOSTS	APLICACIÓN
	DESDE	HASTA			
A	0.0.0.0	127.255.255.255	128*	16.777.214	Redes grandes
B	128.0.0.0	191.255.255.255	16.384	65.534	Redes medianas
C	192.0.0.0	223.255.255.255	2.097.152	254	Redes pequeñas
D	224.0.0.0	239.255.255.255	no aplica	no aplica	Multicast
E	240.0.0.0	255.255.255.255	no aplica	no aplica	Investigación

* El intervalo 127.0.0.0 a 127.255.255.255 está reservado como dirección loopback y no se utiliza.

https://sites.google.com/site/redesdecomunicacionenlaudi/rangos-y-clases-de-la-ip

Paquete

- Paquete de red o paquete de datos es cada uno de los bloques en que se divide la información para enviar, en el nivel de red.
- En todo sistema de comunicaciones resulta interesante dividir, la información a enviar, en bloques de un tamaño máximo conocido.
- Esto simplifica el control de la comunicación, las comprobaciones de errores, la gestión de los equipos de encaminamiento (routers), etc.
- Los paquetes están formados por una cabecera, una parte de datos y una cola.
- En la cabecera estarán los campos que pueda necesitar el protocolo de nivel de red;
- En la cola, si la hubiere, se ubica normalmente algún mecanismo de comprobación de errores.



https://www.sites.google.com/site/redesccna2cisco/envio-de-paquetes

Socket

- Cuando dos procesos que están en hosts diferentes necesitan intercambiar información a través de la red, ya sea la red local o Internet, es necesario que abran un socket para establecer la comunicación y también para intercambiar cualquier flujo de datos
- Para cada una de las conexiones que realizamos fuera de nuestro equipo, necesitamos de un socket para que podamos intercambiar información entre los diferentes procesos
- Usamos el comando **netstat** para ver los sockets.

En el siguiente ejemplo, podemos ver los socket creados en un servidor web, mirando estos socket desde el propio servidor web.

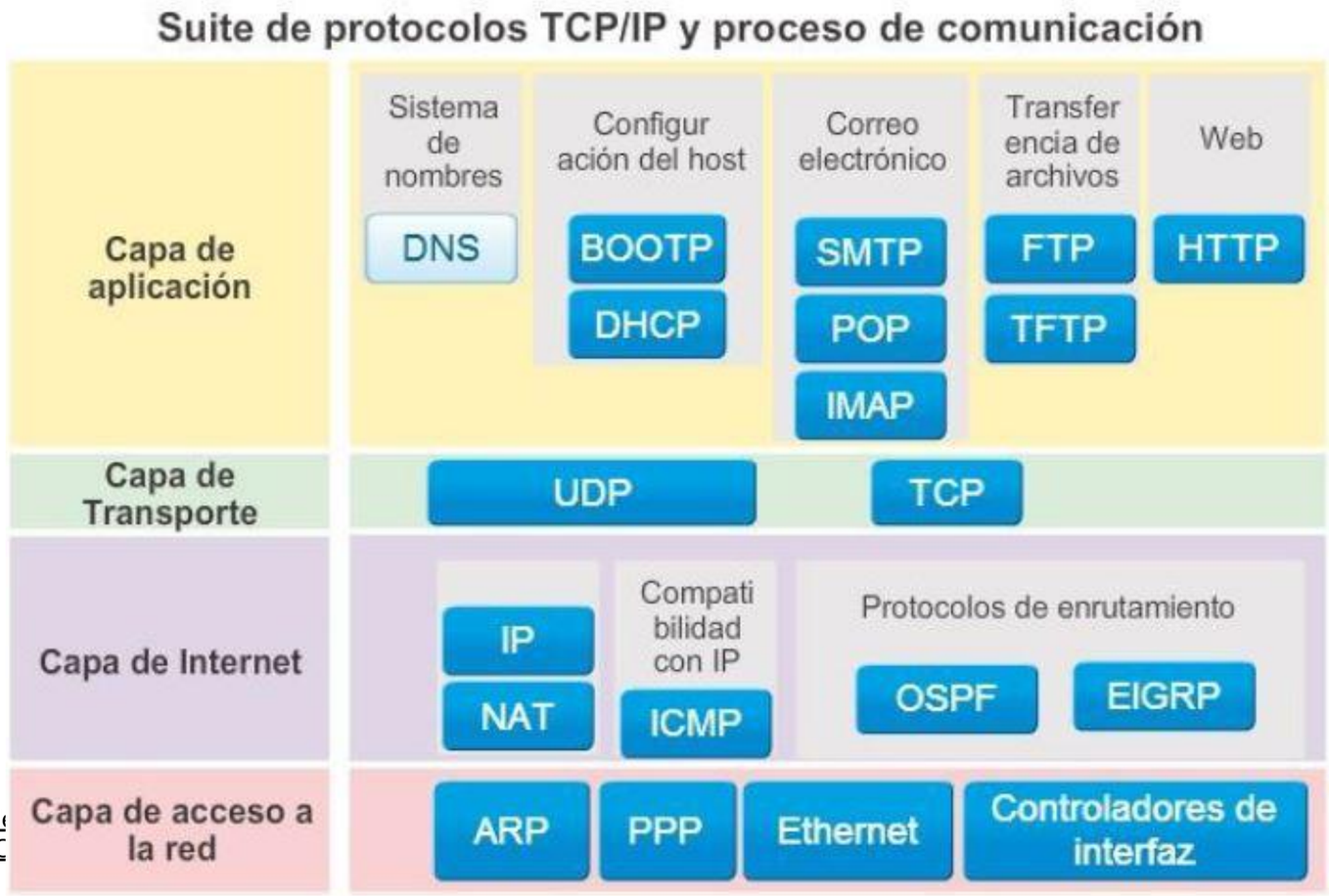
- Usuario 1
- Protocolo: TCP.
- IP origen: 77.77.77.77 (el cliente).
- IP destino: 88.88.88.88 (nosotros).
- Puerto origen o local: 49152 (el cliente).
- Puerto destino o remoto: 443 (nosotros, usamos HTTPS).

En el caso del segundo usuario, tendríamos:

- Usuario 2
- Protocolo: TCP.
- IP origen: 71.71.71.71 (el cliente).
- IP destino: 88.88.88.88 (nosotros).
- Puerto origen o local: 49152 (el cliente).
- Puerto destino o remoto: 443 (nosotros, usamos HTTPS).

Servicio

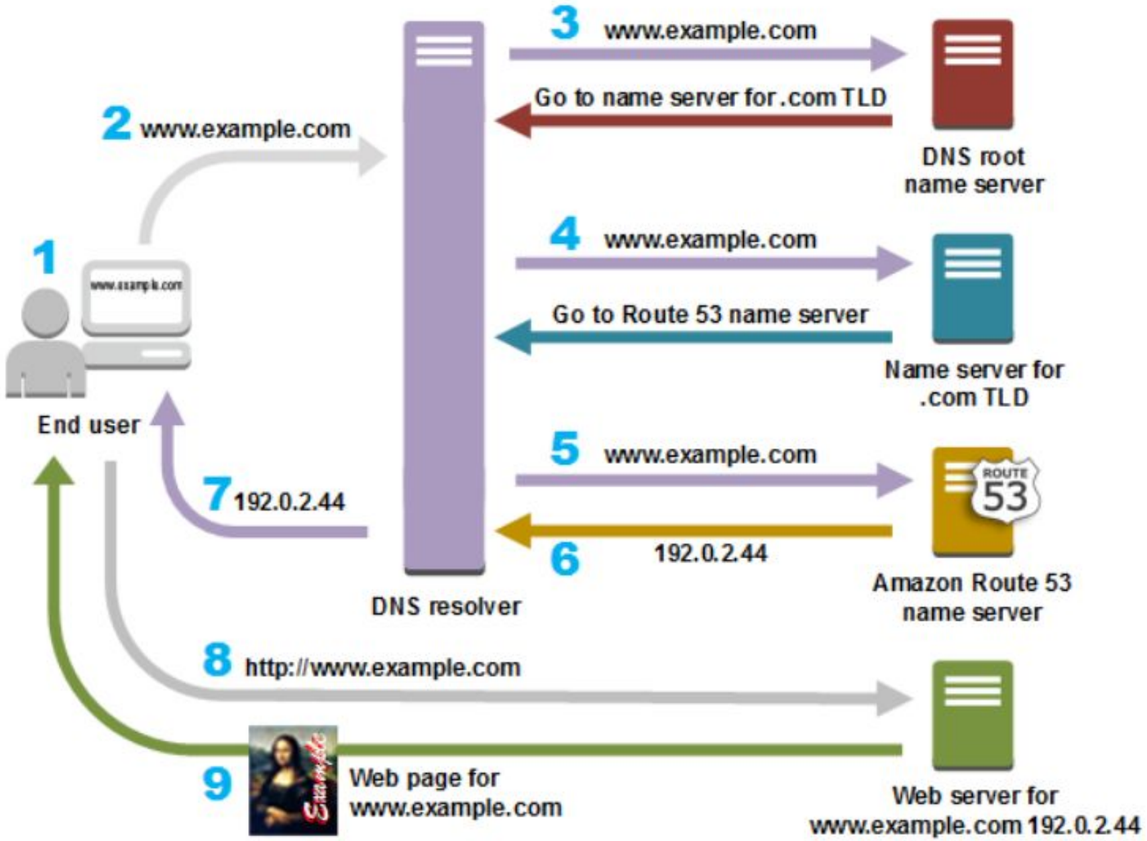
- Un servicio de red es la creación de una red de trabajo en un ordenador. Generalmente los servicios de red son instalados en uno o más firewalls del servidor seleccionado. Eso facilita el uso y el fallo de muchos usuarios.
- Los servicios de red son configurados en redes locales corporativas para mantener la seguridad y la operación amigable de los recursos.
- También estos servicios ayudan a la red local a funcionar sin problemas y eficientemente.
- Las redes locales corporativas usan servicios de red como:
  - DNS
  - DHCP
  - FTP
  - WEB Server.



https://www.ingenieriasystems.com/2016/10/Creacion-de-Internet-y-desarrollo-d
-TCPIP-Suite-de-protocolos-TCPIP-y-proceso-de-comunicacion-CCNA1-V5-CISCO-C
3.html

Servidor de DNS

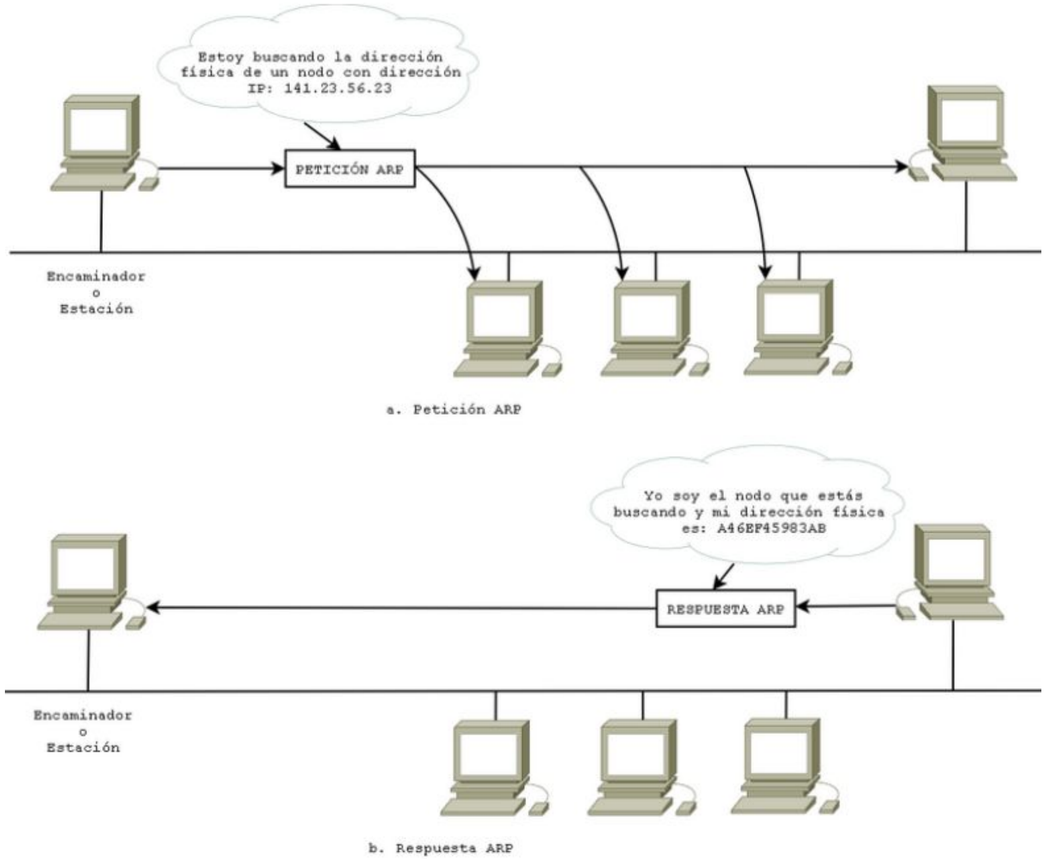
- El sistema de nombres de dominio (DNS) es el directorio telefónico de Internet.
- Las personas acceden a la información en línea a través de nombres de dominio como nytimes.com o google.com.
- Los navegadores web interactúan mediante direcciones de Protocolo de Internet (IP).
- El DNS traduce los nombres de dominio a direcciones IP para que los navegadores puedan cargar los recursos de Internet.



https://aws.amazon.com/es/route53/what-is-dns/

ARP

- El Protocolo de Resolución de Direcciones (ARP, por sus siglas en inglés)
- es un protocolo de comunicaciones de la capa de enlace de datos que se utiliza para descubrir la dirección de hardware (MAC) asociada a una dirección IP en una red.
- En otras palabras, el **ARP** se encarga de vincular una dirección **MAC** o **dirección física**, con una dirección **IP** o **dirección lógica**.
- Este protocolo es fundamental para el buen funcionamiento de las redes y permite que los dispositivos conectados a una red puedan obtener una ruta MAC de otro equipo que está conectado a esa misma red, es decir, se encarga de "localizar" donde están los demás dispositivos cableados o inalámbricos en la red, preguntando por la dirección MAC de cada uno de ellos enviando un paquete a la dirección de broadcast que es FF:FF:FF:FF:FF:FF.
- El Comando en Kali para acceder a la tabla es **arp**



https://geekytheory.com/redes-el-protocolo-arp/

Puertos

- Se utilizan para permitir que una máquina realice varias conexiones simultáneas a otras máquinas de modo que los datos contenidos en los paquetes entrantes se dirijan al proceso que los está esperando (**Multiplexación de conexiones**).

- Los puertos se identifican por un número comprendido entre 0 y 65.535.

  - **Puertos bien conocidos**: Los puertos inferiores al 1.024 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.

  - **Puertos registrados**: Los comprendidos entre 1.024 y 49.151 pueden ser usados por cualquier aplicación. Existe una lista pública en la web del **IANA**.

  - **Puertos dinámicos o privados**: Los comprendidos entre los números 49.152 y 65.535 son denominados dinámicos o privados, normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Se usan en conexiones peer to peer (P2P).

- **FTP**: 20 y 21
- **SSH**: 22
- **Telnet**: 23, 95 y 107
- **SMTP (Correo)**: 25
- **Oracle SQLNet**: 66
- **DHCP**: 67 y 68
- **HTTP (web sin seguridad)**: 80
- **POP3 (Correo)**: 110
- **IMAP (Correo)**: 143, 220, 993
- **HTTPS (web con seguridad)**: 443
- **SMTPS (Correo con seguridad)**: 465
- **SQL Server**: 1433
- **Oracle Listener**: 1521

https://www.mundodeportivo.com/urbantecno/windows/principales-puertos-red


THE
BRIDGE