Recursos de red.

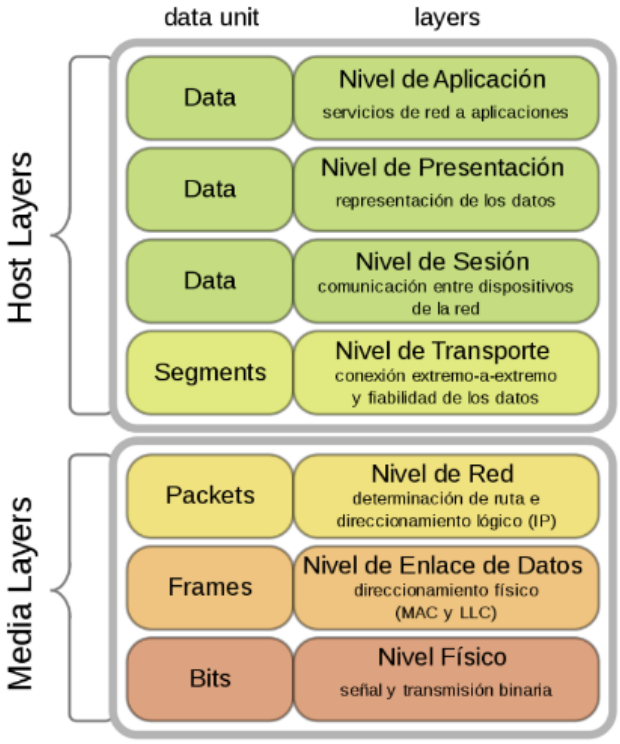
Índice

1. Introducción.

Una red es la unión de varios equipos conectados por medio de cables, señales ondas o cualquier método de transporte de datos que comparten información, recursos (impresoras, CD-ROM), servicios (e-mails, chats, juegos), etc.

Una red de comunicaciones es un conjunto de medios técnicos que permiten la conexión entre equipos autónomos. En este trabajo vamos a indagar sobre este tema y sus variantes.

2. Modelo OSI.



Este modelo, creado en el año 1980, es un estándar que tiene por objetivo conseguir interconectar sistemas de procedencia distinta para que esos puedan intercambiar información sin ningún tipo de impedimentos debido a los protocolos con los que estos operan de forma propia según su fabricante.

Este modelo se divide en 7 capas.

1. **Capa física**. Esta capa es la que se encarga de la topología de red y de las conexiones globales del ordenador hacia la red, se refiere tanto al medio físico como a la forma en la que se transmite la información
2. **Capa de enlace de datos**. Esta capa se ocupa del direccionamiento físico, del acceso al medio, la detección de errores, la distribución ordenada de tramas y el control de flujo
3. **Capa de red**. Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de datos se denominan paquetes, y se pueden clasificar en protocolos enrutables y de enrutamiento.
4. **Capa de transporte,** Como su nombre indica, efectúa el transporte de los datos de la maquina origen al destino.
5. **Capa de sesión.** Se encarga de mantener y controlar el enlace establecido entre dos ordenadores que están transmitiendo datos.
6. **Capa de presentación,** se encarga de la representación de la información, de manera que, aunque distintos equipos puedan tener diferentes representaciones los datos lleguen de manera legible.
7. **Capa de aplicación,** por último, esta capa es la que permite a los usuarios ejecutar acciones y comandos para volver a interactuar con la red.

Todos estos procesos son muy importantes, cada apartado puede tener varios protocolos o normas relativas a cada nivel.

3. MAC Address.

La dirección MAC es un identificador de 48 bits que corresponde de forma única a una ethernet de red. Es **individual**, cada dispositivo su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante(los primeros 24 bits) utilizando el OUI.

4. Dirección IP.

La dirección IP es un conjunto de números que identifica a un dispositivo en una red en concreto. La IP puede cambiar en un mismo dispositivo cada vez que entramos a una red, incluso local; por que solemos utilizar el protocolo DHCP el cual se encarga de asignarnos una IP al dispositivo y no tiene por qué ser siempre el mismo.

Podemos perfectamente generar una IP fija, si lo necesitamos. Normalmente en las empresas identifican a cada usuario con una IP fija.

Para saber nuestra IP en Windows simplemente debemos utilizar el comando IPCONFIG, y en Linux sería IFCONFIG.

Normalmente cuando creamos una red de clase C tenemos 256 partes disponibles.

Aunque realmente los hosts disponibles (dispositivos) que podemos utilizar son 254, esto se debe a que un registro debe estar reservado a la IP del *router* o Gateway y el otro a la IP BROADCAST, esta IP se puede comunicar con todas las demás.

En la capa del modelo OSI se encuentra en la 3 –RED.

5. Máscara de red.

Es una combinación de bits que sirve para delimitar el ámbito de una red.

Su función es indicar a los dispositivos que parte de la dirección IP es el número de red y que parte es la correspondiente al host.

Antes cuando me he referido a una red de clase C, me refería al estándar de la máscara de red 255.255.255.0

Los estándares son los siguientes.

- Clase A: 255.0.0.0
- Clase B: 255.255.0.0
- Clase C: 255.255.255.0

La clase C permite únicamente 254 hosts. Normalmente cuando se define una red

Clase	Bits	IP Subred	IP Broadcast	Máscara en decimal	CIDR
A	0000	0.0.0.0	127.255.255.255	255.0.0.0	/8
B	1000	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	1100	192.0.0.0	223.255.255.255	255.255.255.0	/24
D	1110	224.0.0.0	239.255.255.255	255.255.255.255	/32
E	1111	240.0.0.0	255.255.255.255	255.255.255.255	/64

La parte del CIDR equivale al número exponencial de la máscara.

Por ejemplo 255.0.0.0. únicamente tiene 256 bits en el (EL 0 EN REDES TAMBIÉN HAY QUE CONTARLO). Sería 2^8 = 256.

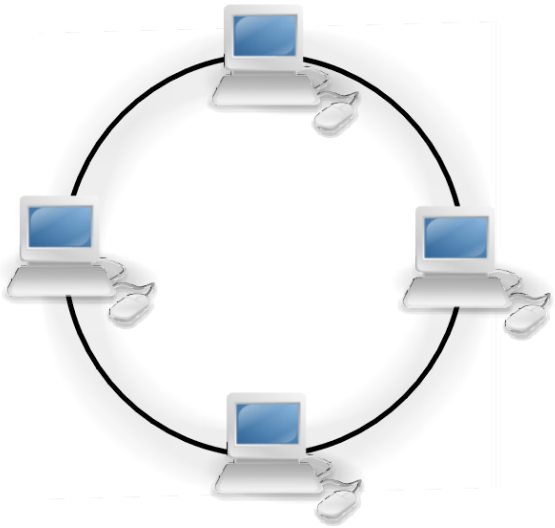
Éste último se utiliza para no necesariamente indicar la máscara de subred siempre que defines una. Ejemplo

192.168.0.10/24

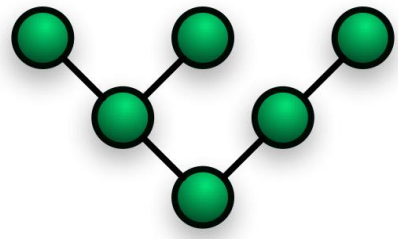
El 24 indicaría que es una de clase C.

6. Topologías de red.

Una topología de una red es la distribución física de la misma y existen varios tipos.



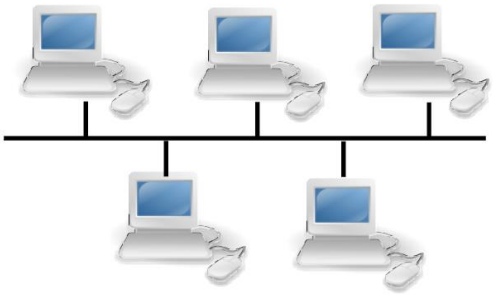
La **topología de anillo**, como se muestra en el dibujo se encuentran conectadas entre sí en forma de anillo.

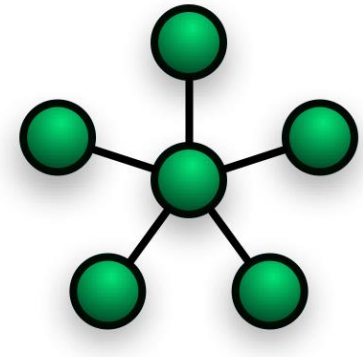


La topología de árbol es una conexión entre nodos y realiza la forma de un árbol. Cuenta con un cable principal llamado **Backbone**, el cual lleva la comunicación a todos los nodos de la red compartiendo un mismo canal de comunicación.

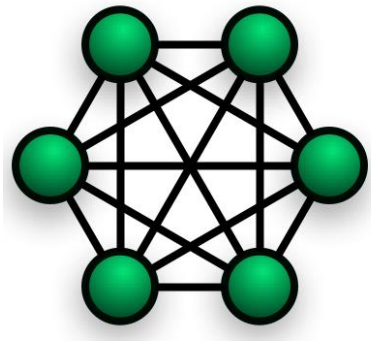
La red de topología de bus se basa en un cable central el cual lleva la información a todos los nodos de la red.

Su desventaja se basa en su distribución secuencial de datos, por lo que si se interrumpe el cable central la red queda inutilizada.



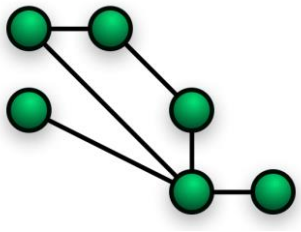


Topología de estrella, todos los nodos van a un punto central formando así una estrella como se ve en la imagen.



La topología de malla es parecida a la estrella en vez de un nodo central todas están conectadas entre sí. Su importancia radica en que la información puede viajar en distintos caminos.

La topología hibrida es una combinación de dos o más diferentes para adaptar la red a las necesidades del cliente, de este modo podemos combinar las topologías que deseemos obteniendo infinitas variedades.



7. Seguridad de redes.

Es un apartado muy importante que consiste en las prácticas que hay que realizar para prevenir el acceso no autorizado a nuestra red, la modificación o la denegación de una red informática.

Los algoritmos de seguridad han pasado por muchos cambios desde los años 90 para hacerse más seguros y eficaces.

Éstos son:

- **WEP** (Privacidad equivalente al cableado) Fue desarrollado para redes inalámbricas y aprobado como estándar en 1999. Pero actualmente es muy fácil de romper y difícil de configurar. No se utiliza ya.
- **WPA,** Fue una mejora temporal para el WEP, pero aun así dejo de utilizarse porque llego a romperse también.
- **WPA-2,** Este protocolo logro aguantar muchos años, pero en 2017 fueron capaces de atacarlo con KRACK Attacks.

Un vídeo que lo explica muy bien es este:

https://www.youtube.com/watch?v=QYrJ767S_TE

Un protocolo muy importante que está en WEB es el protocolo HTTPS (Protocolo de transferencia de hipertexto seguro), este protocolo se encuentra en la fase de aplicación. Cuando nosotros estamos en una web y queremos asegurarnos de que es segura debemos comprobarlo con el siguiente icono

El puerto asociado a este protocolo es el 443.

8. Servidor de archivos.

Un servidor de archivos es un tipo de servidor que almacena y distribuye archivos informáticos, su función es permitir el acceso remoto de otros modos a los archivos.

En principio cualquier ordenador conectado a la red y con un software apropiado puede utilizarlo.

Un servidor de archivos muy típico es Google Drive, o OneDrive.

Un protocolo muy importante y asociado a este tema es el protocolo FTP (File Transfer Protocol), este protocolo se encuentra en la rama de aplicación y los puertos asociados son el 20 y el 21.

9. Servidor de impresión.

Un servidor de impresión es un concentrador que conecta una empresora a una red, para que cualquier PC pueda acceder a ella e imprimir lo necesario.

Un protocolo asociado a este es IPP.

10. Servidor de conexión remota.

Un ordenador puede conectarse a otro de forma remota gracias al protocolo SSH, de la capa aplicación y el puerto 22; la función principal de este protocolo es un acceso remoto a otro equipo o servidor para poder utilizarlo.

También hay software que te lo permite como los siguientes.

- Teamviewer, muy utilizado de forma privada.
- SupRemo
- Ammyyy Admin
- AnyDesk
- Citrix, muy utilizado de forma empresarial.

Nos puede facilitar mucho este apartado y que haya software de este tipo, para por ejemplo trabajar desde casa o simplemente acceder desde otro lugar.

11. Herramientas de encriptación

La encriptación es algo necesaria para no facilitar los datos a alguien que no queramos que los tenga, o los consiga de forma ilícita. Para ello hay varios algoritmos como el RC4 o TKIP para por ejemplo redes inalámbricas.

La encriptación es una manera de codificar la información para protegerla a terceros, hay varias herramientas para ello.

Para proteger y cifrar los datos de un USB podemos utilizar AES Crypt.

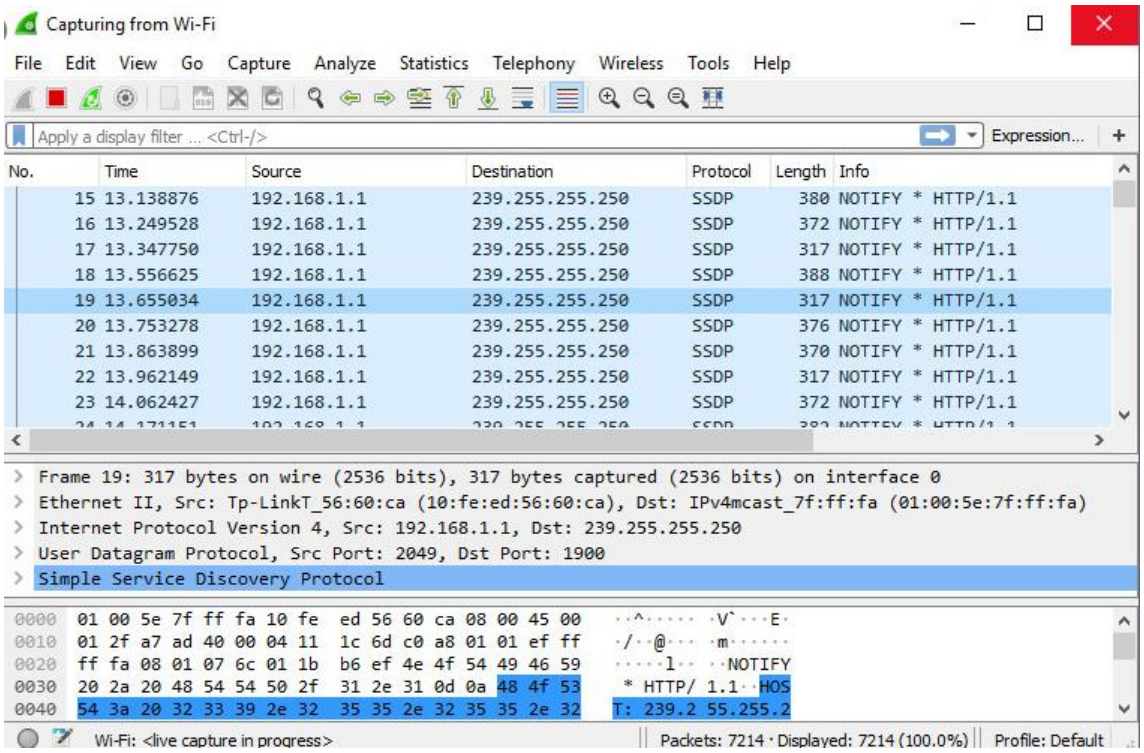
Para cifrar archivos de forma individual AxCrypt.

Hay muchas más herramientas para ello, esto solo han sido un par de ejemplos.

12. Herramientas de análisis de redes

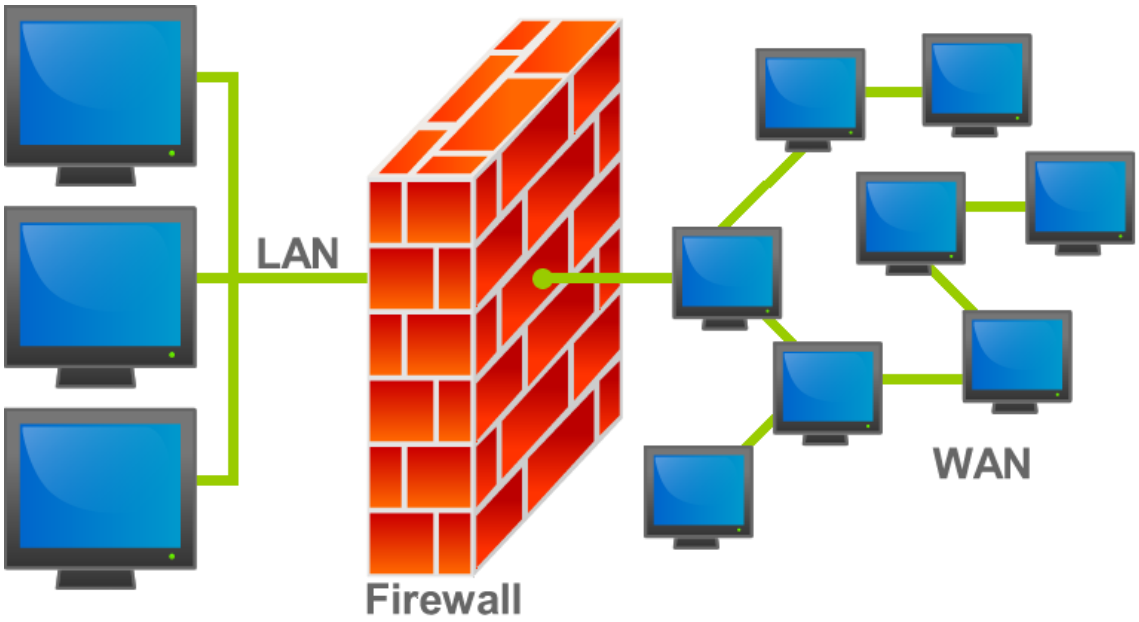
Todos los ejemplos que pondré a continuación pueden realizar la tarea de poder ver nuestra red de forma remota y paquetes que van llegando a los mismos. También tienes el acceso a los paquetes de WiFi e incluso Bluethooth. Los ejemplos son:

- Systems Lizard Remote Process Explorer
- Ontract EasyRecover
- PowerShell Sciptomatic
- Wireshark, el más utilizado.



13. Firewall / Cortafuegos.

Se trata de un dispositivo configurado para permitir, limitar, cifrar o descifrar el tráfico entre los diferente ámbitos.



Antiguamente no estaba integrado en el sistema operativo, pero a partir de los años se añadió. El firewall de Windows 10 ya es uno bastante bueno, y

14. Sistemas de detección de intrusiones(IDS).

Es un programa, que como su propio nombre indica; se encarga de comprobar si se encuentran IPs no deseadas en nuestra red. Realiza un análisis del tráfico de la red y si entra algo que no es conocido te lo detecta y genera una alerta.

15. Más ejemplos de protocolos

- DNS (Domain Name Service), Es el protocolo para modificar una IP a un nombre, utilizado para las propias páginas web, utiliza el puerto 53 y se encuentra en la capa de aplicación..
- HTTP, es el protocolo de transferencia de hipertexto; antes mencioné el seguro, éste utiliza el puerto 80 y se encuentra en la capa aplicación.
- UDP, Este protocolo se encuentra en la capa de transporte, permite enviar datos de una ip a otra sin necesidad de estar conectados.
- **SCP,** este protocolo permite a un programa ejecutar código sin necesidad tener que preocuparse por la comunicación entre ambos. Se encuentra en la capa de sesión.

16. Conclusión.

Las redes, tal y como las conocemos; es algo que ha llevado construirse muchos años sinceramente no es lo que más me apasione de la informática, pero sé que es algo necesario y toda empresa necesita a alguien que gestione la red y necesiten equipos de seguridad informática especializados en ello.

17. BIBLIOGRAFÍA

1. https://es.slideshare.net/tonatiuh2508/administracion-de-los-recursos-de-una-red
2. https://es.wikipedia.org/wiki/Servicio_de_red
3. https://es.wikipedia.org/wiki/Modelo_OSI
4. https://www.profesionalreview.com/2018/11/22/modelo-osi/
5. https://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red#En_bus
6. https://www.oas.org/juridico/spanish/cyber/cyb29_computer_int_sp.pdf
7. http://culturacion.com/topologia-de-red-malla-estrella-arbol-bus-y-anillo/
8. https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13790-8.html
9. https://es.wikipedia.org/wiki/M%C3%A1scara_de_red
10. https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP#IP_fija
11. https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto
12. https://es.wikipedia.org/wiki/Seguridad_de_redes
13. https://www.jmsolanes.net/es/servidor-de-archivos/
14. https://es.wikipedia.org/wiki/Protocolo_de_transferencia_de_archivos
15. https://www.netspotapp.com/es/wifi-encryption-and-security.html
16. https://www.xataka.com/basics/programas-escritorio-remoto
17. https://www.segurisoft.es/encriptacion/top-10-software-encriptacion/
18. https://www.redeszone.net/2018/04/23/protege-datos-importantes-herramientas-cifrado/
19. https://www.ontrack.com/es/blog/5-herramientas-que-deberias-utilizar-en-la-administracion-de-redes/
20. https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)
21. https://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos
22. Documentación AULACAMPUS.