**Trabajo Práctico Teórico de Programación sobre Redes**

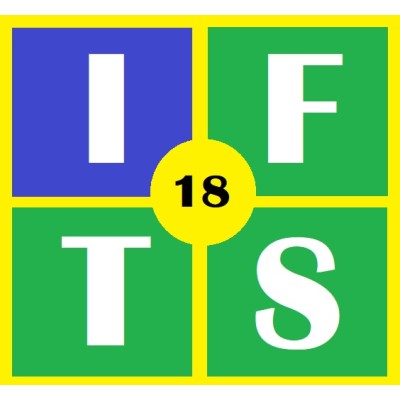
Grupo: Cecilia Calanna, Sheila Muñoz, Alejandra Senlle y Facundo Bartolome

Profesor: Lucas Rusatti

Materia: Programación sobre Redes

Institución: Instituto de Formación Técnica Superior n°18

Carrera: Tecnicatura en Desarrollo de Software



**Preguntas**

1) ¿Qué es una VLAN?

2) ¿Qué es una VPN?

3) ¿Qué es una SAN?

4) Diferencias entre un Hub, Repetidor, Router y SWITCH. Explicar las diferencias.

5) ¿Qué es un protocolo de comunicaciones?

6) Explique TCP/IP y NetBios, resuma sus diferencias. (Acá sí explicar cada uno y sus diferencias)

7) ¿Cómo está formado un paquete de datos en TCP/IP? ¿Qué es un “flag” en un paquete de TCP/IP?

8) Defina la red según su geografía. Explicar distintas variantes.

9) Defina una red según su topología. Explicar distintas variantes.

10) Explicar el servicio de DHCP.

11) Explicar el servicio de DNS.

12) Explicar las tecnologías Wireless, y sus estándares.

13) ¿Qué es un Proxy?

14) Explicar el protocolo Spanning tree.

15) Explicar el protocolo de comunicaciones OSPF.

16) Explicar el protocolo ARP.

17) ¿Qué es un Firewall?

18) ¿Qué es una DMZ?

19) ¿Qué es un Gateway?

20) Según Microsoft, ¿qué significa NBL?

21) Tipos de enlace: MPLS, LAN to LAN, microonda, VSAT. a. Explique cada uno de estos tipos de enlace. b. Agregue dos tipos de enlaces, no mencionados anteriormente. c. Ranking de enlaces según lo pedido (de uno a seis, siendo uno el mejor): Por económico, performance, mayor capacidad, mayor o mejor configuración de restricciones, soporte a mayor distancia, menor esfuerzo de configuración. d. Elija un tipo de enlace para los siguientes escenarios: 1 d. Conectividad de varios de call centers con un data center central. 2 d. Conectar los datos de los pozos petroleros durante 15 minutos por día. 3 d. Comunicar dos edificios enfrentados en la misma calle.

22) Describir la tecnología LTE.

23) Explique la solución de Microsoft Teams. Si quieren describir otra solución de otra empresa es también válido.

24) ¿Qué significa aplicar calidad en un enlace MPLS?

25) ¿Qué diferencias puede encontrar entre una conexión Coaxial, UTP o Fibra?

26) Según Cisco, ¿qué significa CCENT, CCNA y CCNP? Descripción breve del Track Routing & Switching y de algún otro a elección (ej. Wireless, Security, Cloud, etc).

27) Explique el modelo OSI.

28) Realizar cuestionario online y copiar el resultado: (1 por cada integrante) https://es.educaplay.com/es/recursoseducativos/706834/test\_de\_redes\_y\_comunicaciones.htm

29) Explicar el estándar IEEE 802.3 regula la red. Cómo se implementa, ventajas y desventajas.

30) Explicar el estándar IEEE 802.4 regula la red.

31) ¿Qué protocolos se usan para enviar y recibir correo?

32) ¿Qué protocolo puede usarse para leer correo recibido?

33) Diferencias entre IPV4 e IPV6

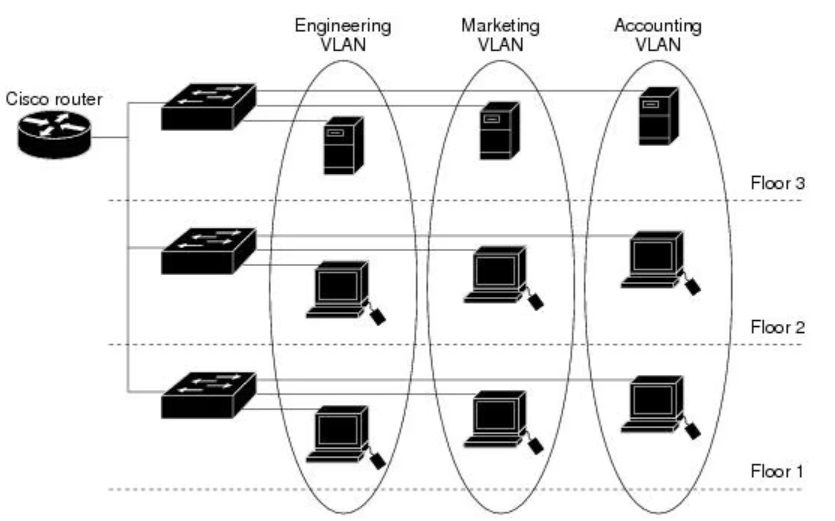
34) (Individual para cada integrante del grupo). ¿Qué experiencia tienen en redes? Ejemplos.: Acceder y configurar el router de mi casa como admin, en mi trabajo hago tareas relacionadas a networking, configuró una PAN hogareña para mi o mi familia, amigos/as etc (Personal Area Network, todo dispositivo Wireless o no), no tengo ninguna experiencia, etc.

R1:

Las VLAN (Virtual LAN), o también conocidas como redes de área local virtuales, es una tecnología de redes que nos permite una segmentación lógica en una red conmutada, permitiendo que grupos de dispositivos se comuniquen como si estuvieran conectados al mismo cable, independientemente del switch físico o la ubicación en una LAN del campus. Esto se traduce en una flexibilidad organizativa, ya que el administrador puede dividir la red en segmentos según la función, el proyecto o la aplicación, sin tener en cuenta la ubicación física del usuario o del dispositivo.

En una VLAN, los dispositivos comparten una misma infraestructura, pero se consideran parte de redes lógicas diferentes. Los paquetes de unidifusión, difusión y multidifusión se reenvían sólo a terminales dentro de la VLAN de origen. Esto mejora la seguridad y eficiencia de la red al evitar que dispositivos no pertenecientes a la VLAN reciban información no deseada.

Además, las VLAN crean dominios de difusión lógicos que pueden abarcar varios segmentos LAN físicos, mejorando el rendimiento al dividir grandes dominios de difusión en otros más pequeños. Los administradores pueden implementar políticas de acceso y seguridad específicas para grupos de usuarios, simplificando la administración de la red.

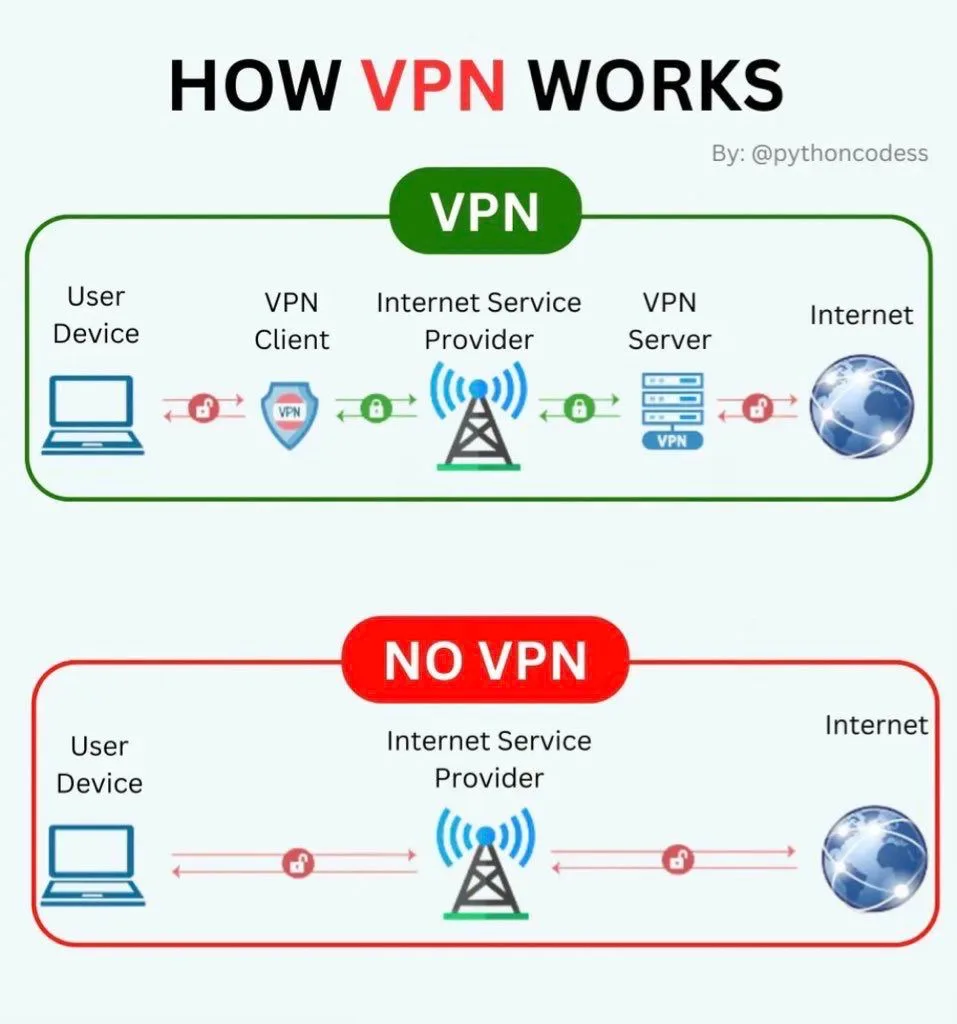


<https://eclassvirtual.com/descripcion-general-de-las-vlan/>

R2:

Una VPN es una "Virtual Private Network" (Red privada virtual) y describe la oportunidad de establecer una conexión protegida al utilizar redes públicas. Las VPN cifran su tráfico en internet y disfrazan su identidad en línea. Esto le dificulta a terceros el seguimiento de sus actividades en línea y el robo de datos. El cifrado se hace en tiempo real.

Una VPN oculta su verdadera dirección IP al permitirle a la red redireccionarla por un servidor remoto especial, alojado por el proveedor de una VPN. Esto significa que si navega en línea con una VPN, el servidor de la VPN se convierte en la fuente de sus datos. Esto significa que su Proveedor de servicios de internet (ISP) y otros terceros no pueden ver los sitios web que visita o qué datos envía y recibe en línea. Una VPN funciona como un filtro que convierte todos sus datos en texto incomprensible. Si alguien logra interceptar su información, de nada le sirve.

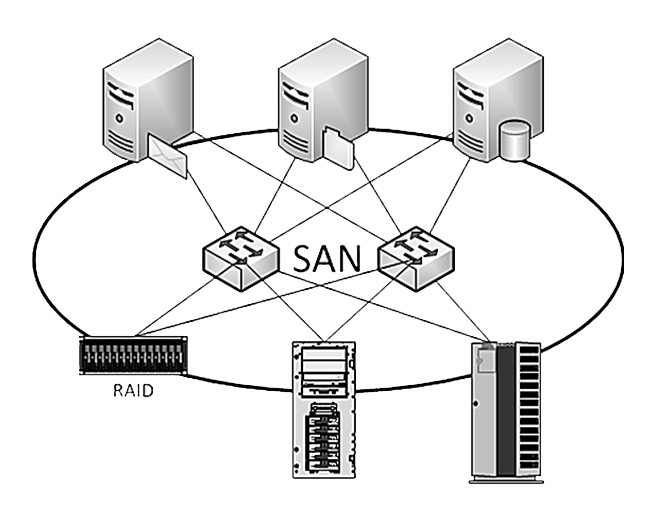


<https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn?srsltid=AfmBOopIVAPTAdh6cHpQHKL2k4QIP8BEWlhdXbBVS_TSzGqrJvmMppdY>

R3:

Una red de área de almacenamiento o Storage Area Network (SAN) es una red dedicada que se adapta a un entorno específico y combina servidores, sistemas de almacenamiento, conmutadores de red, software y servicios.

Es posible que la memoria del ordenador y los recursos de almacenamiento local no proporcionen suficiente almacenamiento, protección de almacenamiento, acceso de varios usuarios o velocidad y rendimiento para las aplicaciones empresariales. Por lo tanto, la mayoría de las organizaciones emplean algún tipo de SAN además del almacenamiento conectado a la red (NAS) para mejorar la eficiencia y la gestión de datos.



<https://www.ibm.com/es-es/topics/storage-area-network>

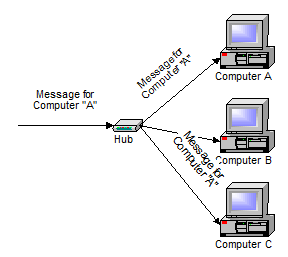
R4:

* HUB (Contenedor)

El Hub es un dispositivo simple con una única misión, la de interconectar los ordenadores de una red local. Su funcionamiento es sencillo, cuando alguno de los ordenadores de la red local que están conectados a él le envía datos, el Hub los replica y transmite instantáneamente al resto de ordenadores de esta red local.

Estamos por lo tanto ante un punto central de conexión de una red, y suele utilizarse para crear redes locales en las que los ordenadores no se conectan a otro sitio que al resto de ordenadores de la red. Por sí sólo no permite conectarse a Internet, y tampoco permite enviar los datos de información a determinados ordenadores, simplemente copia los que recibe de uno y los copia enviándolos al resto de la red por igual.

Sin embargo estos dispositivos tienen algunas desventajas. La primera es que gasta excesivo ancho de banda, ya que si le quieres enviar datos a un único ordenador no podrás hacerlo sin que cada bit se replique y se envíe también al resto que componen la red. Además, mientras se realiza esta transmisión ningún otro equipo puede enviar otra señal hasta que termine.



* Repetidor

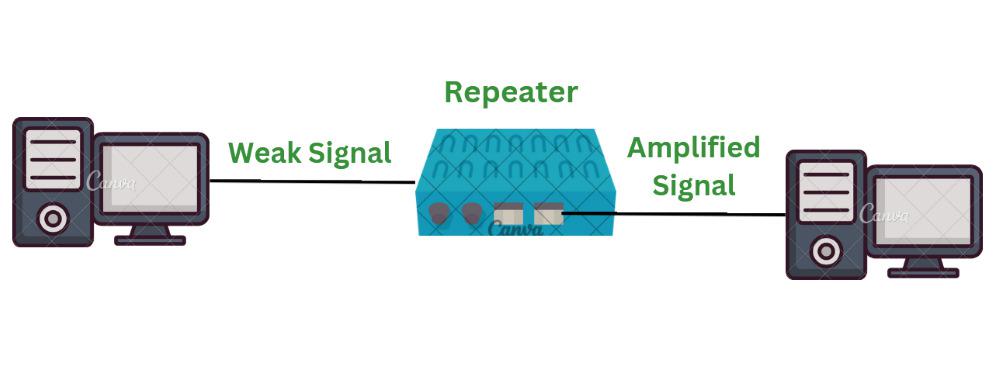
Es un dispositivo electrónico que conecta dos segmentos de una misma red, transfiriendo el tráfico de uno a otro extremo, bien por cable o inalámbrico.

Los segmento de red son limitados en su longitud, si es por cable, generalmente no superan los 100 M., debido a la pérdida de señal y la generación de ruido en las líneas.

Con un repetidor se puede evitar el problema de la longitud, ya que reconstruye la señal eliminando los ruidos y la transmite de un segmento al otro.

En la actualidad los repetidores se han vuelto muy populares a nivel de redes inalámbricas o WIFI.

El Repetidor amplifica la señal de la red LAN inalámbrica desde el router al ordenador. Un Receptor, por tanto, actúa sólo en el nivel físico o capa 1 del modelo OSI.

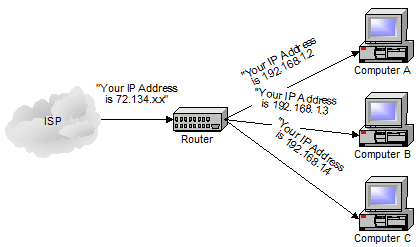


* Router

El Router se encarga de reenviar tus paquetes de datos entre distintas redes, por lo general una local o LAN y una externa con un puerto WAN que puedes utilizar, por ejemplo, para conectarse al ADSL o la fibra y de ahí a Internet.

A día de hoy los routers pueden cumplir las funciones de los otros dos dispositivos que hemos mencionado, ya que suelen incluir un Switch (o Hub) de entre 4 y 8 puertos Ethernet. De esta manera pueden hacer lo mismo, sólo que sin limitarse a las redes locales y abriendo las puertas a que los ordenadores puedan conectarse también a otras redes externas. De hecho de ahí viene su nombre, que "enruta" los paquetes de información a otras redes para llevarlos a su destino final.

Los routers también incorporan otras tecnologías como un Firewall basado en hardware, que protege tu red de forma inteligente y sin necesitar instalar nada más de posibles ataques DDoS y otros peligros.

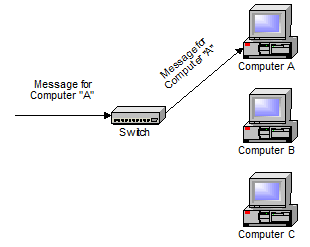


* Switch

Los Switch son los hermanos listos de los Hub, y también se utilizan para la creación de redes locales. La principal diferencia es que a través del Switch la información enviada por el ordenador de origen va directamente al ordenador de destino sin replicarse en el resto de equipos que estén conectados.

Por lo tanto la red ya no queda "limitada", y mientras le enviamos datos a un ordenador el resto de equipos de la red pueden enviarse también datos entre ellos. El límite está en que cuando dos o más ordenadores están enviando datos simultáneamente a la misma máquina entonces sí que no se pueden enviar más a ese mismo ordenador.

Este tipo de dispositivo nació para poder trabajar en redes con una mayor cantidad de máquinas conectadas que con el Hub. Como la comunicación a través de ellos es mucho más fluida, también disminuye los errores en las redes locales.



<https://www.xataka.com/basics/cuales-son-las-diferencias-entre-hub-switch-y-router>

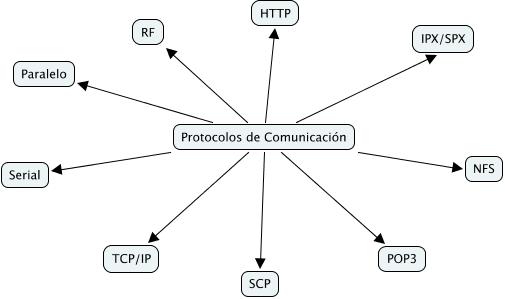
R5:

Los protocolos de comunicación son estándares formales que están formados por procedimientos, restricciones y formatos, que permiten el intercambio de un conjunto de información, lo cual puede lograr la correcta comunicación entre servidores o dispositivos a través de una red.

Para todo ello, los protocolos de comunicación incluyen ciertos mecanismos que permiten que los dispositivos se identifiquen y establezcan conexiones entre sí.

También se incluyen normas que especifican cómo son los paquetes y los datos en cada mensaje enviado y recibido.

En la actualidad, algunos protocolos de comunicación admiten el reconocimiento de mensajes y la compresión de datos, lo cual permite una comunicación de red muy confiable y con alto rendimiento.



<https://sdindustrial.com.mx/blog/protocolos-de-comunicacion-que-son/>

R6:

* TCP/IP

El Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) es el protocolo de comunicación principal utilizado en la red de Internet. Consiste en dos protocolos diferentes: el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP).

TCP se encarga de dividir los datos en paquetes más pequeños para que puedan ser transmitidos a través de la red de manera eficiente y confiable. Además, TCP garantiza que todos los paquetes lleguen al destino de manera ordenada y sin errores.

Por otro lado, IP se encarga de enrutar los paquetes de datos a través de la red hacia su destino final. IP utiliza una dirección IP única para identificar cada dispositivo conectado a la red, lo que permite que los paquetes de datos sean enviados y recibidos en el dispositivo correcto.

TCP/IP se utiliza para una amplia variedad de aplicaciones en línea, como la navegación web, el correo electrónico, la transmisión de archivos y la comunicación de voz y vídeo. También se utiliza en redes privadas, como redes de área local (LAN) y redes de área amplia (WAN).

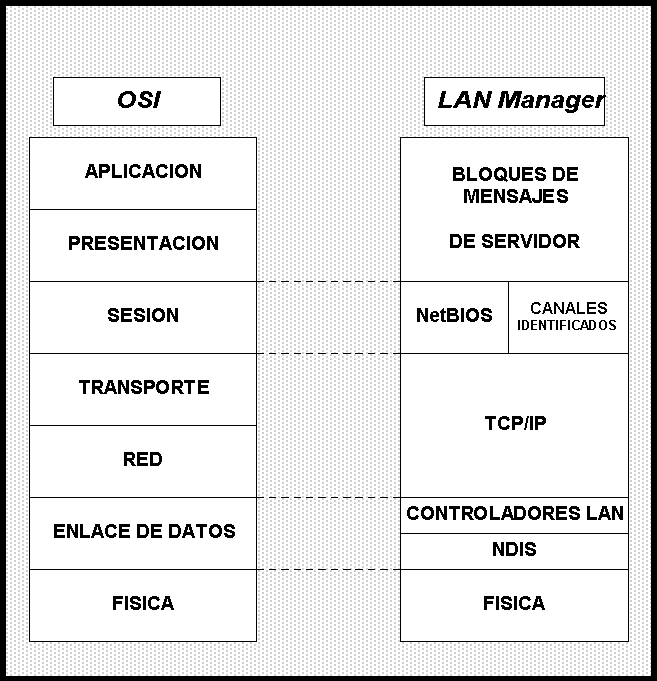
TCP/IP es un estándar abierto y ha sido adoptado por la mayoría de los sistemas operativos y dispositivos de red, lo que permite una comunicación efectiva y sin problemas en la red de Internet.

* NetBios

NetBIOS, o Sistema Básico de Entrada/Salida de Red, es un protocolo de red que permite que las aplicaciones en diferentes computadoras se comuniquen dentro de una red de área local (LAN). Proporciona servicios para la resolución de nombres, el establecimiento de sesiones y la distribución de datagramas.

NetBIOS permite que las computadoras se encuentren y se comuniquen entre sí en la misma red utilizando identificadores únicos llamados nombres NetBIOS. Este protocolo opera en la capa de sesión (capa 5) del modelo OSI y utiliza puertos UDP 137, 138 y el puerto TCP 139 para proporcionar sus servicios.

La siguiente figura muestra una relación entre los protocolos NetBios y TCP/IP en relación al modelo de las 7 capas.



<https://www.vpnunlimited.com/es/help/cybersecurity/netbios?srsltid=AfmBOooAjMfq7dLiEMDa1DQ393AGeOiJ6HN68XIBJ9VZf6t9ZL_Brfhw>

R7:

Cada paquete TCP/IP tiene una estructura básica compuesta por encabezados (headers).

El encabezado IP actúa como la columna vertebral, proporcionando las direcciones de origen y destino, así como información sobre cómo debe ser manejado el paquete en la red. Este encabezado es crucial para los routers, ya que les permite tomar decisiones basadas en la información contenida en él.

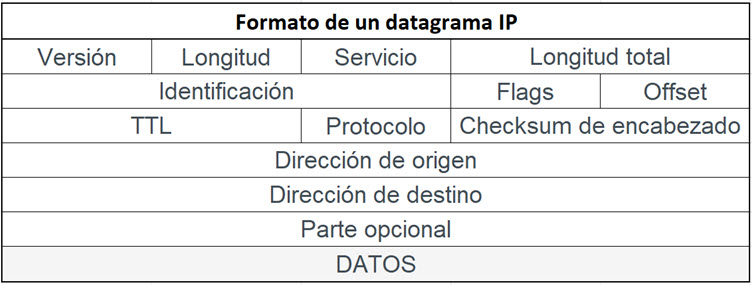
Dentro del encabezado IP, encontramos el encabezado TCP, que contiene detalles como los puertos de origen y destino, el número de secuencia y la suma de verificación hash. Esta última es esencial para verificar la integridad del paquete. Por ejemplo, los investigadores de seguridad vigilan estos encabezados en busca de anomalías que podrían indicar ataques como el escaneo de puertos o intentos de inyección de datos.

Consideramos que el encabezado es la columna vertebral, los datos y el payload representan el corazón de los paquetes TCP/IP. Aquí es donde se almacena la información valiosa que se transmite a través de la red.

Los flags de TCP indican los cambios de situación o condición que tienen que tener los peers entre ellos en su comunicación extremo a extremo.

En la formación clásica de TCP nos encontramos sólo 6 flags, por lo menos eso es lo que nos cuentan y son:

* SYN
* ACK
* FIN
* RST
* PSH
* URG



<https://www.welivesecurity.com/es/recursos-herramientas/tcp-ip-protocol-perspectiva-ciberseguridad/>

<https://www.eduardocollado.com/2020/03/13/flags-de-tcp/>

R8:

Las redes se configuran con el objetivo de transmitir datos de un sistema a otro o de disponer recursos en común, como servidores, bases de datos o impresoras. En función del tamaño y del alcance de la red de ordenadores, se puede establecer una diferenciación entre diversas dimensiones de red. Entre los tipos de redes más importantes se encuentran:

* Personal Area Networks (PAN) o red de área personal

Para llevar a cabo un intercambio de datos, los terminales modernos como smartphones, tablets, ordenadores portátiles o equipos de escritorio permiten asociarsea una red. Esto puede realizarse por cable y adoptar la forma de una Personal Area Network (PAN) o red de área personal, aunque las técnicas de transmisión más habituales son la memoria USB o el conector FireWire. La variante inalámbrica Wireless Personal Area Network (WPAN) se basa en técnicas como Bluetooth, Wireless USB, Insteon, IrDA, ZigBee o Z-Wave. Una Personal Area Network inalámbrica que se lleva a cabo vía Bluetooth recibe el nombre de Piconet. El ámbito de acción de las redes PAN y WPAN se limita normalmente a unos pocos metros y, por lo tanto, no son aptas para establecer la conexión con dispositivos que se encuentran en habitaciones o edificios diferentes.

* Local Area Networks (LAN) o red de área local

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.

* Metropolitan Area Networks (MAN) o red de área metropolitana

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. Para ello, entran en acción routers de alto rendimiento basados en fibra de vidrio, los cuales permiten un rendimiento mayor al de Internet y la velocidad de transmisión entre dos puntos de unión distantes es comparable a la comunicación que tiene lugar en una red LAN.

* Wide Area Networks (WAN) o red de área amplia

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.

En la mayoría de los casos, las Wide Area Networks suelen pertenecer a una organización determinada o a una empresa y se gestionan o alquilan de manera privada. Los proveedores de servicios de Internet también hacen uso de este tipo de redes para conectar las redes corporativas locales y a los consumidores a Internet.

* Global Area Networks (GAN) o red de área global

Una red global como Internet recibe el nombre de Global Area Network (GAN), sin embargo no es la única red de ordenadores de esta índole. Las empresas que también son activas a nivel internacional mantienen redes aisladas que comprenden varias redes WAN y que logran, así, la comunicación entre los ordenadores de las empresas a nivel mundial. Las redes GAN utilizan la infraestructura de fibra de vidrio de las redes de área amplia (Wide Area Networks) y las agrupan mediante cables submarinos internacionales o transmisión por satélite.

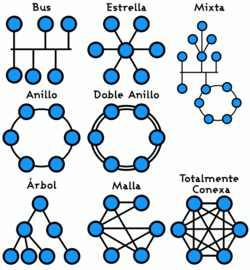


<https://www.ionos.com/es-us/digitalguide/servidores/know-how/los-tipos-de-redes-mas-conocidos/>

R9:

Las topologías de red se refieren a la forma en la que está dispuesta una red, es decir, a los esquemas de conexión en redes informáticas. Esto incluye sus nodos y las líneas utilizadas para asegurar la transmisión y recepción de datos de manera correcta y segura. En función de esta disposición se pueden evitar cortes innecesarios o incrementar el flujo de la información transmitida.

Para que todos los componentes vinculados funcionen de forma correcta es imprescindible que la red informática esté bien estructurada. La red debe adaptarse a todos los dispositivos, ya sean computadores, impresoras, servidores, hubs, switches, televisiones, cámaras de seguridad etc para que se cumplan los requerimientos y funcionen de forma correcta.



### Topología de Bus

También se le conoce como topología de red troncal, bus o línea. En esta red todos los dispositivos se conectan directamente a un canal y no existe otro vínculo entre nodos. Los datos fluyen a lo largo del cable a medida que viaja a su destino.

Se instala fácilmente, tiene poco cableado y es fácil aumentar o disminuir el número de aparatos que se adjuntan a la red. Algunos inconvenientes son problemas de congestión, colisión y bloqueo. Además, si existe un problema en el canal, todos los dispositivos quedarán desconectados.

### Topología de Anillo

En esta red cerrada los nodos se configuran en un patrón circular con estructura de anillo. Cada nodo se vincula a uno con los dos contiguos. Al llegar un mensaje a un dispositivo, esté comprueba los datos de envío y si no es el receptor, lo pasa al siguiente, y así sucesivamente hasta que lo recibe el destinatario.

Ofrece mejor rendimiento que la de bus, es fácil de instalar y localizar pero los nodos no pueden enviar mensajes al mismo tiempo. Es decir que no puede desconectarse ningún dispositivo o se perderá la conexión entre todos.

### Topología de Estrella

Es el tipo de topología más común En ella los dispositivos se conectan a un punto central (hub) que actúa a modo de servidor. Este hub gestiona la transmisión de datos a través de la red. Permite que todas las estaciones se comuniquen entre sí.

Sin embargo, si el nodo central tiene algún error, toda la red queda expuesta y puede provocar una desconexión. Existe también la topología de estrella extendida que funciona igual pero cada elemento que se conecta al nodo central se convierte en el centro de otra estrella. El cableado es más corto pero se conectan menos dispositivos.

### Topología de Árbol

Esta red tiene un punto de enlace troncal y a partir de este se ramifican los demás nodos. El eje central es como el tronco del árbol. Las ramas se conectan son los concentradores secundarios o los nodos de control y los dispositivos conectados se conectan a los branches. Puede ser de árbol binario en el que cada nodo se fragmenta en dos enlaces o árbol backbone , un tronco con un cable principal que lleva información al resto de nodos ramificados.

Entre las ventajas de esta tipología está que no se presentan problemas entre los subsiguientes dispositivos si falla uno, reduce el tráfico de red y es compatible con muchos proveedores de hardware y de software. Es aconsejable para redes de gran tamaño.

### Topología de Malla

En esta clase de red informática todos los componentes o nodos están interconectados y enlazados directamente mediante vías separadas. La ventaja es que si una conexión falla, existen caminos alternativos para que la información fluya por varias rutas alternativas. Eso sí, para ello debe haber una limitada cantidad de dispositivos que unir.

### Topología de mixta

Esa topología mezcla dos o más topologías de red diferentes. Adaptar su estructura a las necesidades físicas del lugar en el que se realiza la instalación, así como a los requerimientos de seguridad, velocidad e interconexión.

Es fiable porque permite detectar errores y resolver problemas de forma sencilla, es eficaz, escalable y flexible. Sin embargo, es difícil detectar fallas, tiene diseño complejo y difícil y el mantenimiento es caro.

### Topología totalmente conexa

En este caso existe un enlace directo entre todos los pares de sus nodos. Se trata de redes caras de configurar, pero siempre con un alto grado de confiabilidad. Existen muchas rutas para los datos que ofrecen la gran cantidad de enlaces redundantes entre nodos. Esta topología se usa sobre todo para aplicaciones militares.

<https://www.tokioschool.com/noticias/topologias-red/>