Programación sobre Redes

**Trabajo Practico Teórico**

1. ¿Qué es una VLAN?

VLAN, o Virtual Local Area Network, es una red lógica que agrupa distintos dispositivos conectados físicamente a una misma red local. Segmentados para formar redes independientes permiten mejorar la seguridad, gestionar el tráfico de forma más eficiente y simplificar la administración de la red.

Al utilizar VLANs, es posible aislar diferentes departamentos o tipos de tráfico. De esta forma se evitaría que se interfieran entre sí y mejoraría el rendimiento general de la red.

1. ¿Qué es una VPN?

VPN, o Virtual Private Network, es una tecnología que permite crear una conexión segura y cifrada entre un dispositivo y un servidor remoto. Esto protege la información personal de filtraciones de datos, espías y ciberamenazas.

1. ¿Qué es una SAN?

SAN, o Storage Area Network, es una red de alta velocidad que conecta servidores con dispositivos de almacenamiento, utilizada principalmente por empresas para aplicaciones críticas que requieren alto rendimiento y una baja latencia.

Las SAN centralizan el almacenamiento en bloques, permitiendo a las organizaciones almacenar daros en un pool compartido, lo que facilita prácticas coherentes de protección de datos, seguridad y recuperación ante desastres.

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

Un hub es el dispositivo de red pasivo y el más básico y antiguo. Funciona como un repetidor simple que toma los datos que recibe por un puerto y los reenvía a todos los demás puertos conectados, sin ningún tipo de filtrado o gestión inteligente del tráfico. Por si mismo, no es capaz de conectarse a otras redes ni a internet. Puede ser útil en entornos muy pequeños y controlados donde la seguridad y el rendimiento no sean una prioridad. En la actualidad, los hubs están prácticamente obsoletos y no se recomiendan para nuevas instalaciones, ya que los switches ofrecen mejor rendimiento, seguridad y flexibilidad.

El switch es como una versión mejorada del hub ya que, a diferencia de este último, es un dispositivo capaz de aprender y recordar que dispositivos están conectados a cada puerto. Es decir, es un dispositivo de red activo, ya que tiene la capacidad de analizar el tráfico de red y tomar decisiones inteligentes sobre cómo dirigir los datos y enviarlos solamente a el o los dispositivos destinatarios (en lugar de repetirlos en todos). Son mucho más eficientes y seguros que los hubs, ya que reducen el tráfico innecesario en la red y proporcionan un mejor rendimiento general. Ideal para casas grandes u oficinas medianas donde varios equipos necesitan compartir recursos y comunicarse entre si.

Un router es un dispositivo de red activo que conecta múltiples redes y dirige el tráfico de datos entre ellas. Su función principal es determinar la mejor ruta para que los paquetes de datos lleguen a su destino. Es el aparato que normalmente nos proporciona el proveedor de Internet y que nos permite conectarnos a la misma. Los routers modernos suelen incluir funciones adicionales como Wi-Fi, firewall o control parental. Incluso, estos últimos pueden funcionar como switches o hubs, aunque con capacidades más limitadas que los dispositivos dedicados. Son excelentes para un departamento con pocos dispositivos o una pequeña oficina con varios empleados que necesitan compartir recursos y acceder a Internet.

Un repetidor lo único que hace es captar la señal de WiFi que ya tengas en tu hogar o trabajo, y la amplía para que llegue más lejos. Es una especia de puente que funciona en ambas direcciones.

1. ¿Qué es un protocolo de comunicaciones?

Un protocolo de comunicación es un conjunto de normas y reglas que permiten que los dispositivos se comuniquen entre sí. Son estándares que definen cómo se intercambian los datos.

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

TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP es un conjunto de reglas estandarizadas que permiten a los equipos comunicarse en una red como Internet. Pueden ser equipos de distintas marcas o incluso encontrarse en zonas del mundo diferentes. Y las personas y programas que los utilizan pueden hablar distintos lenguajes humanos e informáticos. TCP/IP fue desarrollado por el Departamento de Defensa de EE. UU. para especificar el modo en que los equipos transfieren datos de un dispositivo a otro. TCP/IP incide mucho en la precisión y dispone de varios pasos para garantizar la correcta transmisión de los datos entre ambos equipos.

Este es uno de los mecanismos que emplea para ello. Si el sistema enviara un mensaje entero en una pieza y se encontrara cualquier problema, sería necesario enviar de nuevo el mensaje completo. Lo que hace TCP/IP es descomponer cada mensaje en *paquetes* que se vuelven a ensamblar en el otro extremo. De hecho, cada paquete podría tomar una ruta distinta hasta el equipo de destino si la ruta deja de estar disponible o está muy congestionada.

Además, TCP/IP divide las distintas tareas de comunicación en *capas*. Cada capa tiene una función distinta. Los datos pasan por cuatro capas independientes antes de recibirse en el otro extremo. A continuación, TCP/IP recorre estas capas en orden inverso para reensamblar los datos y presentárselos al destinatario.

NetBIOS es un protocolo de red que viene activado por defecto en las tarjetas de red en Windows. Está algo obsoleto y hoy en día no es muy utilizado. Sin embargo puede tener vulnerabilidades que son aprovechadas por los piratas informáticos para llevar a cabo diferentes métodos de ataques. Básicamente lo que permite NetBIOS es que las aplicaciones se comuniquen con la red. Un equipo en una red local se comunica con otro a través de una conexión utilizando lo que se conoce como datagramas NetBIOS. Su función es establecer la sesión y mantener las conexiones. Hay que mencionar que este protocolo necesita de otros protocolos para transportar datos tanto en redes inalámbricas como en LAN.

Como todo, hay que tener en cuenta cuáles son los beneficios y los inconvenientes de tener activo este protocolo de red en particular en Windows. Por lo tanto, teniendo en cuenta los anteriores puntos de los que hemos hablado, NetBIOS sigue contando con algunas ventajas, algunas de ellas son:

* Resuelve nombres de sus dispositivos sin requerir configuración por parte del usuario.
* Se encuentra habilitado en todas las sesiones de Windows (Esto puede resultar un inconveniente también).
* Se convirtió en el fundamento básico de muchas aplicaciones de red.

Por la contra también nos podemos encontrar con algunos inconvenientes. Recordemos que estamos dejando de lado, que se trata de una función que poco a poco se está quedando obsoleta. Es por esto mismo por lo que podemos encontrar los siguientes aspectos en su contra:

* NetBIOS no proporciona ningún marco estándar o formato de datos para sus transmisiones.
* No resulta práctico para ser utilizado en redes de gran tamaño debido a que tiende a sobrecargar la red relativamente fácil.
* Actualmente, se trata de un protocolo que no resulta seguro. Además de que es un protocolo de red que se ha quedado ya anticuado. De ahí que resulte hasta beneficios desactivarlo.

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?

El proxy, o servidor proxy, en una red informática, es un servidor programa o dispositivo, este hace de intermediario entre las peticiones de recursos entre un cliente A a un servidor C.

Esta situacion estrategica de punto intermedio le permite ofrecer diversas funcionalidades:

* Control de acceso
* Registro del trafico
* Restricción a determinados tipos de trafico
* Mejora de rendimiento
* Anonimato de la comunicación
* Cache web
* Etc.

14- Explicar el protocolo Spanning tree.

El Spanning Tree Protocol o STP, es un protocolo que funciona en el nivel de la capa 2 en el modelo OSI (capa de enlace de datos) que crea una topología lógica sin bucles para redes ethernet. Al comprobar la red buscando rutas duplicadas y desactivarlas, el Spanning tree protocol impide que se creen dos o mas tramas paralelas que, de lo contrario, provocarían bucles. El procedimiento forma un árbol con la red física sin conexiones multiples entre el origen y el destino. STP se basa en un algoritmo inventado por Radia Perlman mientras trabajaba para Digital Equipment Corporation

En términos generales, lo que el STP hace es eliminar lógicamente caminos de comunicación. Para ello el protocolo crea un árbol de switches presentes en la red y elige el switch de referencia a partir del cual se creara el árbol.

El switch designado como el cual a partir del que se creara el árbol se llama root bridge. La elección del root bridge es hecha con base en una prioridad y también con base en la dirección MAC. Solo puede existir un root bridge en una red.

Cada switch, que no es el root bridge, se define como root port. Esta interfaz es elegida teniendo en cuenta el menor costo para el root bridge. Esta interfaz se coloca en modo de enrutamiento.

Por cada segmento, se establece un designated bridge. Este será el switch con el menor costo hasta el root bridge. La interfaz de conexión con el root bridge se encuentra en modo “reenvío”. El puerto de uno de los switches se coloca en modo de bloqueo, por lo tanto, bloquea los frames y evita los bucles (loops) en la red.

15- Explicar el protocolo de comunicaciones OSPF.

EL protocolo Open shortest Path First o OSPF es un protocolo de enrutamiento que marca cual es el camino que se debe seguir en la transmisión de los paquetes de datos en las conexiones de red.

Cada enrutador configurado con el protocolo OSPF intercambia información con los dispositivos vecinos sobre las rutas disponibles y su costo (OSPF Cost). El intercambio de datos se lleva a cabo según el principio de “todos con todos “. La información recibida se guarda en la base de datos LSDB y, sobre su base, los enrutadores determinan los vecinos y calculan las rutas. Lo importante es definir la ruta mas optima para el envió de paquetes.

Cada enrutador en OSPF elige de forma autónoma una ruta específica, y los mensajes sobre las rutas de red disponibles sirven solo como información de referencia.

16- Explicar el protocolo ARP.

El adress resolution protocol o ARP es un portocolo o procedimiento que conecta una IP que cambia constantemente a la direccion fija de una maquina tambien conocida como dirección Media Access Control o MAC, todo esto en un area de red local (LAN).

Cando una computadora se agrega a la red LAN recibira una direccion IP unicapara usarla para identificacion y comunicación.

Los paquetes de datos llegan a una puerta de enlace, con destino a una máquina host en particular. La puerta de enlace, o el dispositivo de hardware en una red que permite que los datos fluyan de una red a otra, solicita al programa ARP que encuentre una dirección MAC que coincida con la dirección IP. La caché de ARP mantiene una lista de cada dirección IP y su dirección MAC correspondiente. La caché de ARP es dinámica, pero los usuarios de una red también pueden configurar una tabla ARP estática que contenga direcciones IP y direcciones MAC.

Las cachés de ARP se mantienen en todos los sistemas operativos dentro de una red Ethernet IPv4. Cada vez que un dispositivo solicita una dirección MAC para enviar datos a otro dispositivo conectado a la LAN, primero verifica su caché de ARP para ver si la conexión IP-MAC ya ha sido establecida. Si existe, entonces no es necesario realizar una nueva solicitud. Sin embargo, si la traducción aún no se ha llevado a cabo, se envía la solicitud de direcciones de red y se ejecuta el proceso de ARP.

El tamaño de la caché de ARP está limitado por diseño, y las direcciones tienden a permanecer en la caché solo por unos pocos minutos. Se purga regularmente para liberar espacio. Este diseño también tiene fines de privacidad y seguridad, evitando que las direcciones IP sean robadas o suplantadas por atacantes cibernéticos. Mientras que las direcciones MAC son fijas, las direcciones IP se actualizan constantemente.

Durante el proceso de purga, se eliminan las direcciones no utilizadas, así como cualquier dato relacionado con intentos fallidos de comunicación con computadoras que no están conectadas a la red o que ni siquiera están encendidas.

17- ¿Qué es un Firewall?

El firewall es una de las herramientas de seguridad más efectivas y disponibles para la protección de los usuarios internos de la red contra las amenazas externas. El firewall reside entre dos o más redes y controla el tráfico entre ellas; de este modo, ayuda a prevenir el acceso sin autorización. Los productos de firewall usan diferentes técnicas para determinar qué acceso permitir y qué acceso denegar en una red.

* Filtrado de paquetes: evita o permite el acceso de acuerdo con las direcciones IP o MAC.
* Filtrado de aplicaciones evita o permite el acceso a tipos específicos de aplicaciones según los números de puerto.
* Filtrado de URL: evita o permite el acceso a sitios Web según los URL o palabras clave específicas.
* Inspección de paquetes con estado (SPI, Stateful Packet Inspection): los paquetes entrantes deben ser respuestas legítimas de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. La SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como los del tipo DoS

18- ¿Qué es una DMZ?

Una zona desmilitarizada o DMZ hace referencia a un área de la red que es accesible tanto para los usuarios internos como para los externos. Es más segura que la red externa, pero no tan segura como la red interna. Se crea a través de uno o más firewalls para separar las redes internas, externas o DMZ. Normalmente, en una DMZ se colocan servidores Web para acceso público.

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.: Accedo y configuro el router de mi casa como admin, en mi trabajo hago tareas relacionadas a networking, configuro una PAN hogareña para mi o mi familia, amigos/as etc (Personal Area Network, todo dispositivo Wireless o no), no tengo ninguna experiencia, etc.