IFTS 18

Tecnicatura Desarrollo de software
Programación sobre redes
Prof. Lucas Rusatti

Trabajo Práctico - Programación sobre Redes

Integrantes:

Santiago Valenzuela

1. ¿Qué es una VLAN?
Una VLAN (Virtual Local Area Network) es una red lógica que se crea dentro de una red física. Permite segmentar una red en múltiples redes lógicas independientes, cada una con su propio espacio de direccionamiento.

2. ¿Qué es una VPN?
Una VPN (Virtual Private Network) es una tecnología de red que permite establecer una conexión segura entre un dispositivo y una red remota a través de Internet. Permite a los usuarios acceder a recursos de la red de forma privada y segura.

3. ¿Qué es una SAN?
Una SAN (Storage Area Network) es una red de almacenamiento que permite compartir y gestionar recursos de almacenamiento entre servidores. Proporciona una infraestructura de almacenamiento dedicada y escalable.

4. Diferencias entre un Hub, Repetidor, Router y SWITCH:
- Hub: Dispositivo que conecta múltiples dispositivos en una red y transmite datos de manera indiscriminada a todos los puertos.
- Repetidor: Dispositivo que amplifica o regenera una señal digital para extender el alcance de la red.
- Router: Dispositivo que interconecta redes y dirige el tráfico entre ellas, basándose en la dirección IP de destino.
- Switch: Dispositivo que conecta múltiples dispositivos en una red y envía datos de manera selectiva sólo a los puertos destino.

5. ¿Qué es un protocolo de comunicaciones?
Un protocolo de comunicaciones es un conjunto de reglas y formatos estandarizados que permiten la comunicación entre dispositivos en una red. Definen cómo se inicia, mantiene, negocia y finaliza una conexión de red.

6. Explicar TCP/IP y NetBios, resuma sus diferencias:
TCP/IP (Transmission Control Protocol/Internet Protocol) es un conjunto de protocolos de comunicación que define cómo se transmiten los datos a través de redes de computadoras. Permite la interconexión de redes.
NetBIOS (Network Basic Input/Output System) es un protocolo de comunicación que permite a las aplicaciones acceder a los servicios de red, como compartir archivos y recursos. A diferencia de TCP/IP, NetBIOS opera a nivel de capa de sesión y no de red.

7. ¿Cómo está formado un paquete de datos en TCP/IP? ¿Qué es un "flag" en un paquete de TCP/IP?
Un paquete de datos en TCP/IP está compuesto por:
- Cabecera: Información de control, como dirección IP de origen y destino, puertos, números de secuencia, etc.

- Carga útil: Datos que se transmiten.

Un "flag" en un paquete TCP/IP es un bit de control que indica el estado o el tipo de segmento TCP, como SYN, FIN, ACK, etc. Estos flags se utilizan para el establecimiento, mantenimiento y finalización de la conexión.

8. Defina la red según su geografía. Explicar distintas variantes.
Según la geografía, las redes se pueden clasificar en:

- Redes de área local (LAN): Redes limitadas a un área geográfica pequeña, como un edificio o campus.
- Redes de área metropolitana (MAN): Redes que cubren un área geográfica más amplia, como una ciudad.
- Redes de área amplia (WAN): Redes que abarcan grandes extensiones geográficas, como entre ciudades o países.

9. Defina una red según su topología. Explicar distintas variantes.
Según la topología, las redes se pueden clasificar en:

- Topología en bus: Todos los dispositivos comparten un mismo canal de comunicación.
- Topología en estrella: Los dispositivos se conectan a un dispositivo central (como un switch o hub).
- Topología en anillo: Los dispositivos se conectan formando un círculo.
- Topología en malla: Cada dispositivo se conecta directamente a los demás.

10. Explicar el servicio de DHCP.
DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los dispositivos obtener automáticamente una dirección IP y otra información de configuración de red, como máscara de subred, puerta de enlace, servidores DNS, etc.

11. Explicar el servicio de DNS.
DNS (Domain Name System) es un servicio de red que traduce nombres de dominio (como www.example.com) a direcciones IP, permitiendo que los usuarios accedan a sitios web y otros recursos de red de manera más intuitiva.

12. Explicar las tecnologías Wireless, y sus estándares.
Las tecnologías wireless (inalámbricas) permiten la comunicación entre dispositivos sin necesidad de cables. Algunos de los principales estándares wireless son:
- WiFi (IEEE 802.11): Permite la conexión de dispositivos a una red local inalámbrica.
- Bluetooth (IEEE 802.15.1): Permite la conexión de dispositivos de corto alcance, como auriculares o teclados.
- ZigBee (IEEE 802.15.4): Tecnología para redes de sensores y automatización del hogar.

13. ¿Qué es un Proxy?

Un proxy es un servidor intermediario que se ubica entre un cliente y un servidor. Actúa como un intermediario, recibiendo las solicitudes del cliente, procesando las y re-enviándolas al servidor correspondiente. Esto puede mejorar el rendimiento, seguridad y control del tráfico de red.

14. Explicar el protocolo Spanning tree.
El protocolo Spanning Tree (STP) es un protocolo de red que evita la formación de bucles en topologías de red redundantes, como en redes con múltiples switches. Selecciona un único camino activo entre dos puntos de la red, bloqueando los demás caminos para evitar bucles.

15. Explicar el protocolo de comunicaciones OSPF.
OSPF (Open Shortest Path First) es un protocolo de enrutamiento dinámico que utiliza el algoritmo de Dijkstra para calcular la ruta más corta entre los diferentes nodos de una red. Es un protocolo de estado de enlace que permite a los routers intercambiar información sobre la topología de la red.

16. Explicar el protocolo ARP.
ARP (Address Resolution Protocol) es un protocolo de red que permite asociar una dirección IP con una dirección MAC (capa de enlace). Esto es necesario para que un dispositivo pueda enviar datos a otro dispositivo en una misma red local.

17. ¿Qué es un Firewall?
Un firewall es un dispositivo de seguridad de red que monitoriza y controla el tráfico entrante y saliente de una red, aplicando reglas de seguridad predefinidas. Su función es proteger la red de accesos no autorizados y bloquear tráfico sospechoso o malicioso.

18. ¿Qué es una DMZ?
DMZ (Zona Desmilitarizada) es una subred aislada dentro de una red, utilizada para alojar servidores que deben estar accesibles desde Internet, como servidores web o de correo electrónico. Esto permite separar estos servidores de la red interna, aumentando la seguridad.

19. ¿Qué es un Gateway?
Un gateway (puerta de enlace) es un dispositivo de red que permite interconectar redes con diferentes tecnologías o protocolos. Actúa como un punto de entrada y salida entre redes, permitiendo que los dispositivos de una red se comunique con dispositivos de otras redes.

20. Según Microsoft, ¿qué significa NBL?
Network Load Balancing (NLB) permite gestionar varios servidores como un único clúster virtual, distribuyendo el tráfico entrante para mejorar la disponibilidad y escalabilidad de aplicaciones críticas. Es útil para aplicaciones sin estado, como servidores web, y permite agregar hosts dinámicamente para manejar cargas crecientes.

21. Tipos de enlace: MPLS, LAN to LAN, microonda, VSAT.

A. Explique cada uno de estos tipos de enlace:

a. MPLS (Multiprotocol Label Switching): Es una tecnología de conmutación de etiquetas que permite el transporte eficiente de tráfico de diferentes protocolos sobre una infraestructura de red compartida.
b. LAN to LAN: Es una conexión de red entre dos o más redes locales (LAN) a través de una red de área amplia (WAN).
c. Microonda: Es una tecnología de comunicación inalámbrica que utiliza ondas electromagnéticas de alta frecuencia para transmitir datos a distancias relativamente largas.
d. VSAT (Very Small Aperture Terminal): Es una tecnología de comunicación por satélite que utiliza antenas parabólicas pequeñas para la transmisión y recepción de datos a través de un satélite.

B. Agregue dos tipos de enlaces, no mencionados anteriormente:

a. Fibra óptica: Es un medio de transmisión que utiliza fibras de vidrio o plástico para enviar datos en forma de señales de luz.
b. Conexión Ethernet: Es una tecnología de red cableada que utiliza cables UTP (par trenzado sin blindaje) para conectar dispositivos a una red local.

C. Ranking de enlaces según lo pedido (de uno a seis, siendo uno el mejor):

1. Fibra óptica
2. MPLS
3. Microonda
4. LAN to LAN
5. VSAT
6. Conexión Ethernet

D. Elija un tipo de enlace para los siguientes escenarios:

a. Conectividad de varios call centers con un data center central: MPLS
b. Conectar los datos de los pozos petroleros durante 15 minutos por día: VSAT
c. Comunicar dos edificios enfrentados en la misma calle: Conexión Ethernet

22. Describir la tecnología LTE.

LTE (Long-Term Evolution) es un estándar de comunicaciones móviles 4G que ofrece mayores velocidades de transmisión de datos, menor latencia y mayor capacidad en comparación con las redes 3G. Permite el acceso móvil a Internet de alta velocidad y la transmisión de servicios multimedia.

23. Explique la solución de Microsoft Teams.

Microsoft Teams es una solución de colaboración y comunicación unificada. Permite a los usuarios realizar videoconferencias, chat, compartir archivos, realizar tareas y colaborar en proyectos de manera integrada dentro del ecosistema de aplicaciones de Microsoft 365.

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

Aplicar calidad en un enlace MPLS se refiere a la posibilidad de configurar y gestionar la calidad de servicio (QoS) en una red MPLS. Esto permite priorizar y garantizar el rendimiento de determinados tipos de tráfico, como voz, video o aplicaciones críticas, a través de la asignación de diferentes niveles de prioridad y ancho de banda.

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

- Coaxial: Cable grueso y rígido que se utiliza principalmente para transmisión de señales de televisión y cable.
- UTP (Par Trenzado sin Apantallar): Cable delgado y flexible que se usa comúnmente en redes Ethernet y telefonía.
- Fibra óptica: Cable que utiliza señales de luz para transmitir datos a altas velocidades y con menor pérdida de señal, especialmente útil para largas distancias.

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).

- CCENT (Cisco Certified Entry Networking Technician): Certificación de nivel de entrada que demuestra conocimientos básicos de redes.
- CCNA (Cisco Certified Network Associate): Certificación de nivel asociado que acredita habilidades en la implementación y administración de redes.
- CCNP (Cisco Certified Network Professional): Certificación de nivel profesional que demuestra experiencia avanzada en el diseño, implementación y solución de problemas de redes.

➔ Track Routing & Switching: Certifica conocimientos y habilidades en la configuración y administración de routers y switches Cisco.
➔ Track Wireless: Certifica conocimientos y habilidades en la implementación y administración de redes inalámbricas Cisco.

27. Explique el modelo OSI.

El modelo OSI (Open Systems Interconnection) es un marco de referencia conceptual que describe cómo deben comunicarse los diferentes dispositivos en una red. Está compuesto por 7 capas:

1. Física
2. Enlace de datos
3. Red
4. Transporte
5. Sesión
6. Presentación
7. Aplicación

Cada capa desempeña funciones específicas para permitir la comunicación entre sistemas.

28. Realizar cuestionario online y copiar el resultado: (1 por cada integrante)

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

El estándar IEEE 802.3 define las especificaciones para Ethernet, la tecnología de redes LAN más ampliamente utilizada.

Implementación:

- Utiliza cables de par trenzado, fibra óptica o conexiones inalámbricas.
- Emplea el método de acceso al medio CSMA/CD (Acceso Múltiple por Detección de Portadora con Detección de Colisiones).

Ventajas:

- Amplia adopción e interoperabilidad.
- Bajo costo de implementación.
- Velocidades de transmisión cada vez más altas.

Desventajas:

- Susceptible a colisiones en redes congestionadas.
- Limitaciones de distancia y ancho de banda.

30. Explicar el estándar IEEE 802.4 regula la red.

El estándar IEEE 802.4 definía las especificaciones para redes de token bus, un tipo de topología de red LAN que utilizaba un token pasado secuencialmente entre los dispositivos

para controlar el acceso al medio. Sin embargo, este estándar ya no es ampliamente utilizado, ya que ha sido superado por Ethernet (IEEE 802.3) como la tecnología de LAN dominante.

31. ¿Qué protocolos se usan para enviar y recibir correo?
Los principales protocolos utilizados para el envío y recepción de correo electrónico son:

- SMTP (Simple Mail Transfer Protocol): Utilizado para el envío de mensajes de correo.
- POP3 (Post Office Protocol versión 3) e IMAP (Internet Message Access Protocol): Utilizados para la recepción y descarga de mensajes de correo.

32. ¿Qué protocolo puede usarse para leer correo recibido?
Los protocolos que se pueden utilizar para leer el correo electrónico recibido son:

- POP3 (Post Office Protocol versión 3)
- IMAP (Internet Message Access Protocol)

Ambos protocolos permiten a los clientes de correo acceder y descargar los mensajes desde un servidor de correo.

33. Diferencias entre IPV4 e IPV6
Las principales diferencias entre IPv4 (Internet Protocol versión 4) e IPv6 (Internet Protocol versión 6) son:

- Espacio de direccionamiento: IPv4 tiene un espacio de 32 bits (4.3 mil millones de direcciones), mientras que IPv6 tiene 128 bits (aproximadamente 340 sextillones de direcciones).
- Formato de la dirección: IPv4 utiliza notación decimal con puntos, mientras que IPv6 usa notación hexadecimal con dos puntos.
- Mejoras de seguridad: IPv6 incluye funciones de seguridad integradas, como IPsec.
- Calidad de servicio (QoS): IPv6 tiene un mejor soporte para QoS y priorización de tráfico.
- Fragmentación de paquetes: IPv6 elimina la fragmentación de paquetes en los nodos intermedios.

34. (Individual para cada integrante del grupo) ¿Qué experiencia tienen en redes?
Instalacion y configuracion de repetidores y router