IFTS 18

Tecnicatura Desarrollo de software
Programación sobre redes
Prof. Lucas Rusatti

Trabajo Práctico - Programación sobre Redes

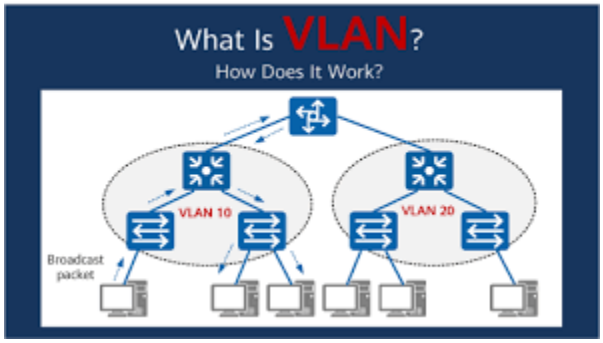
Integrantes:

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.

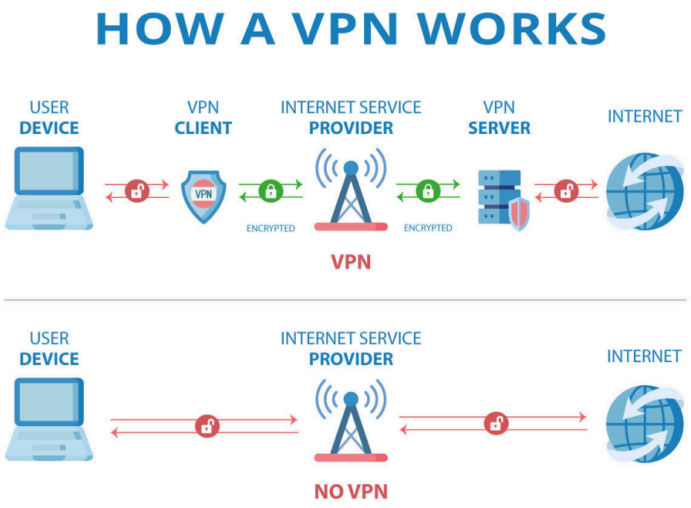
Una VLAN permite a los administradores de red crear grupos lógicos de dispositivos que pueden comunicarse como si estuvieran en la misma red física, incluso si están en diferentes ubicaciones físicas. Esto mejora la seguridad, el rendimiento y la gestión de la red al reducir el tráfico innecesario y aislar grupos de usuarios o aplicaciones.



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.

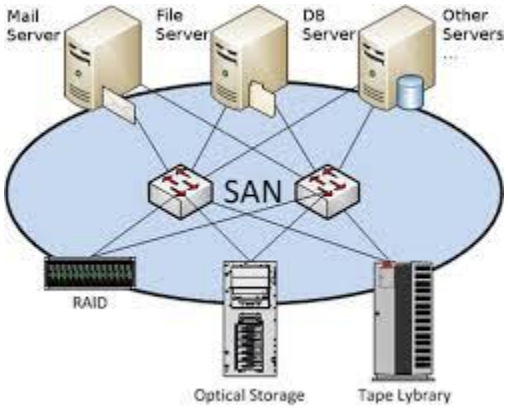
Las VPNs utilizan técnicas de encriptación y túneles seguros para proteger la información transmitida a través de redes públicas como Internet. Existen varios tipos de VPNs, incluyendo VPNs de acceso remoto, VPNs de sitio a sitio, y VPNs basadas en SSL/TLS. Las VPNs son esenciales para el teletrabajo seguro y para conectar oficinas remotas de manera 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.

Una SAN utiliza protocolos de red especializados como Fibre Channel o iSCSI para proporcionar acceso de bloque a nivel de disco. Esto permite una gestión centralizada del almacenamiento, mejora la utilización de recursos y facilita la implementación de estrategias de respaldo y recuperación de desastres.



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 aspectos como el formato de los datos, la secuencia de los mensajes intercambiados, y las acciones tomadas al transmitir o recibir un mensaje. Ejemplos comunes incluyen HTTP para la web, SMTP para correo electrónico, y TCP/IP para la comunicación básica en Internet.

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.

TCP/IP es fundamental para la comunicación en Internet y redes modernas, mientras que NetBIOS es más antiguo y se usa principalmente en entornos Windows para compartir recursos en redes locales pequeñas. TCP/IP es más escalable y versátil, mientras que NetBIOS es más simple pero limitado en alcance.

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 IP: Contiene direcciones IP de origen y destino, tipo de protocolo, etc.
- Cabecera TCP: Incluye puertos de origen y destino, número de secuencia, flags, etc.
- Datos: La carga útil del paquete.

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.

Los flags TCP más comunes son:

- SYN: Inicia una conexión
- ACK: Confirma la recepción de datos
- FIN: Finaliza una conexión
- RST: Reinicia una conexión
- PSH: Indica que los datos deben ser enviados inmediatamente

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

Según la geografía, las redes se pueden clasificar en:

- LAN (Red de Área Local): Típicamente cubre un edificio o un grupo de edificios cercanos. Ofrece altas velocidades y baja latencia.
- MAN (Red de Área Metropolitana): Cubre una ciudad o un área metropolitana. Puede ser propiedad de una organización o de un proveedor de servicios.
- WAN (Red de Área Amplia): Conecta LANs y MANs a través de grandes distancias geográficas, a menudo utilizando líneas arrendadas o conexiones satelitales.
- PAN (Red de Área Personal): Conecta dispositivos cercanos al usuario, como teléfonos móviles, tablets, o wearables.
- GAN (Red de Área Global): Abarca todo el globo, como Internet.

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

Según la topología, las redes se pueden clasificar en:

- Bus: Todos los nodos se conectan a un único cable. Simple pero vulnerable a fallos.
- Estrella: Todos los nodos se conectan a un punto central. Fácil de administrar pero dependiente del nodo central.

- Anillo: Cada nodo se conecta a dos nodos adyacentes formando un círculo. Eficiente pero puede ser complejo de implementar.
- Malla: Cada nodo se conecta a múltiples otros nodos. Altamente redundante pero costosa.
- Árbol: Combina características de topologías en estrella y bus. Escalable pero puede ser compleja.
- Híbrida: Combinación de dos o más topologías diferentes.

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.

El proceso típico de DHCP incluye:

- DHCP Discover: El cliente busca un servidor DHCP.
- DHCP Offer: El servidor ofrece una dirección IP.
- DHCP Request: El cliente solicita la dirección ofrecida.
- DHCP Acknowledge: El servidor confirma la asignación.

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.
El proceso de resolución DNS típicamente involucra:

- Consulta al servidor DNS local
- Si no se encuentra, consulta a servidores raíz
- Referencia a servidores TLD (Top-Level Domain)
- Consulta al servidor autoritativo del dominio
- Respuesta devuelta al cliente

DNS también maneja otros tipos de registros como MX para correo electrónico, TXT para verificación de dominio, etc.

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:

- Wi-Fi (IEEE 802.11): Incluye variantes como 802.11a/b/g/n/ac/ax, cada una con mejoras en velocidad y alcance.
- Bluetooth (IEEE 802.15.1): Ideal para conexiones de corto alcance, con versiones mejoradas como Bluetooth Low Energy (BLE).
- ZigBee (IEEE 802.15.4): Utilizado en domótica y redes de sensores por su bajo consumo energético.

- NFC (Near Field Communication): Para comunicaciones de muy corto alcance, comúnmente usado en pagos móviles.
- LoRaWAN: Para redes de área amplia de bajo consumo, útil en IoT.
- 5G: La última generación de tecnología celular, ofreciendo altas velocidades y baja latencia.

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.
Los proxies pueden ser de varios tipos:

- Forward Proxy: Actúa en nombre de los clientes, ocultando sus identidades.
- Reverse Proxy: Protege y balancea la carga de los servidores.
- Transparent Proxy: Intercepta y redirige el tráfico sin configuración del cliente.
- Caching Proxy: Almacena copias de contenido frecuentemente accedido para mejorar el rendimiento.

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.
Funciona así:

- Elección del puente raíz (root bridge)
- Identificación de puertos raíz en cada switch
- Identificación de puertos designados en cada segmento
- Bloqueo de puertos redundantes

Existen variantes como Rapid STP (RSTP) y Multiple STP (MSTP) que ofrecen convergencia más rápida y soporte para VLANs.

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.

- Construye una base de datos topológica completa de la red
- Utiliza el algoritmo Dijkstra para calcular las rutas más cortas
- Soporta áreas jerárquicas para mejorar la escalabilidad
- Converge rápidamente ante cambios en la topología
- Es más eficiente que protocolos de vector distancia como RIP en redes grandes

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.
El proceso incluye:

- Broadcast ARP request con la IP objetivo
- El dispositivo con esa IP responde con su MAC
- La información se almacena en la caché ARP

ARP también se usa en el proceso de detección de direcciones duplicadas. Existen variantes como Proxy ARP y Gratuitous ARP para casos de uso específicos.

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.
Los firewalls pueden ser:

- Stateless: Filtran basándose en reglas predefinidas sin considerar el contexto
- Stateful: Mantienen un registro del estado de las conexiones
- Application Layer: Analizan el tráfico a nivel de aplicación
- Next-Generation: Combinan múltiples funciones de seguridad

Los firewalls modernos a menudo incluyen funciones como IPS (Sistema de Prevención de Intrusiones), antivirus, y filtrado web.

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.
Una DMZ típicamente se implementa con:

- Firewall externo: Protege la DMZ de Internet
- Firewall interno: Protege la red interna de la DMZ
- Servidores en la DMZ: Web, correo, DNS públicos, etc.

La DMZ reduce el riesgo de que un compromiso en un servidor público afecte a la red interna.

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.

Los gateways pueden funcionar en diferentes niveles:

- Capa de aplicación: Traducen entre protocolos de aplicación
- Capa de transporte: Convierten entre TCP y UDP
- Capa de red: Conectan redes con diferentes protocolos de enrutamiento

Los gateways son esenciales en la conexión de redes IoT con redes IP tradicionales.

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.
NLB de Microsoft ofrece:

- Distribución de carga basada en reglas
- Afinidad de sesión para mantener conexiones a servidores específicos
- Detección de fallos y redistribución automática del tráfico
- Soporte para múltiples sitios y direcciones IP virtuales

NLB es particularmente útil para servicios web, FTP, y VPN.

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.

- Ofrece velocidades de descarga de hasta 300 Mbps y de subida de hasta 75 Mbps.
- Utiliza tecnologías como OFDMA, MIMO y modulación adaptativa.
- Reduce la latencia a menos de 10 ms para aplicaciones en tiempo real.
- Soporta handover entre celdas para movilidad continua.
- Es la base para el desarrollo de las redes 5G.

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.

- Integra chat, videoconferencias, almacenamiento de archivos y colaboración en aplicaciones.
- Permite la creación de canales para organizar conversaciones y archivos por temas.
- Ofrece integración con otras aplicaciones de Microsoft 365 y herramientas de terceros.
- Incluye funciones de seguridad y cumplimiento normativo empresarial.
- Soporta la personalización mediante bots y aplicaciones personalizadas.

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.
Aplicar QoS en MPLS implica:

- Clasificación del tráfico en diferentes clases de servicio.
- Marcado de paquetes con etiquetas que indican la prioridad.
- Configuración de políticas de encolamiento y descarte en los routers MPLS.
- Reserva de ancho de banda para aplicaciones críticas.
- Monitoreo y ajuste continuo para mantener los niveles de servicio acordados.

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.
    - Ancho de banda: Hasta 1 Gbps en versiones modernas.
    - Distancia máxima: Hasta 500 metros sin repetidores.
    - Inmunidad al ruido: Buena, debido a su blindaje.
- UTP (Par Trenzado sin Apantallar): Cable delgado y flexible que se usa comúnmente en redes Ethernet y telefonía.
    - Ancho de banda: Hasta 10 Gbps en Cat6a y superiores.
    - Distancia máxima: Típicamente 100 metros.
    - Inmunidad al ruido: Moderada, mejora en categorías superiores.
- 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.
    - Ancho de banda: Terabits por segundo en las mejores implementaciones.
    - Distancia máxima: Kilómetros sin repetidores.
    - Inmunidad al ruido: Excelente, inmune a interferencias electromagnéticas.

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. Capa Física: Maneja la transmisión de bits brutos a través del medio físico.
2. Capa de Enlace de Datos: Proporciona transferencia confiable de datos entre dos nodos.
3. Capa de Red: Maneja el enrutamiento y el envío de paquetes entre redes.
4. Capa de Transporte: Asegura la entrega confiable de segmentos entre puntos en una red.
5. Capa de Sesión: Establece, gestiona y termina las sesiones entre aplicaciones.

6. Capa de Presentación: Traduce datos entre el formato de la aplicación y el formato de red.
7. Capa de Aplicación: Proporciona servicios de red a las aplicaciones del usuario final.

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
- Configuración de routers:
    - Establecimiento de conexiones WAN (DSL, cable, fibra)
    - Configuración de redes LAN y WLAN
- Instalación de repetidores Wi-Fi:

- Análisis de cobertura y selección de ubicaciones óptimas
- Configuración de extensión de red (mismo SSID o red mesh)
- Optimización de canales para evitar interferencias