TRABAJO PRÁCTICO TEÓRICO

Programación sobre Redes

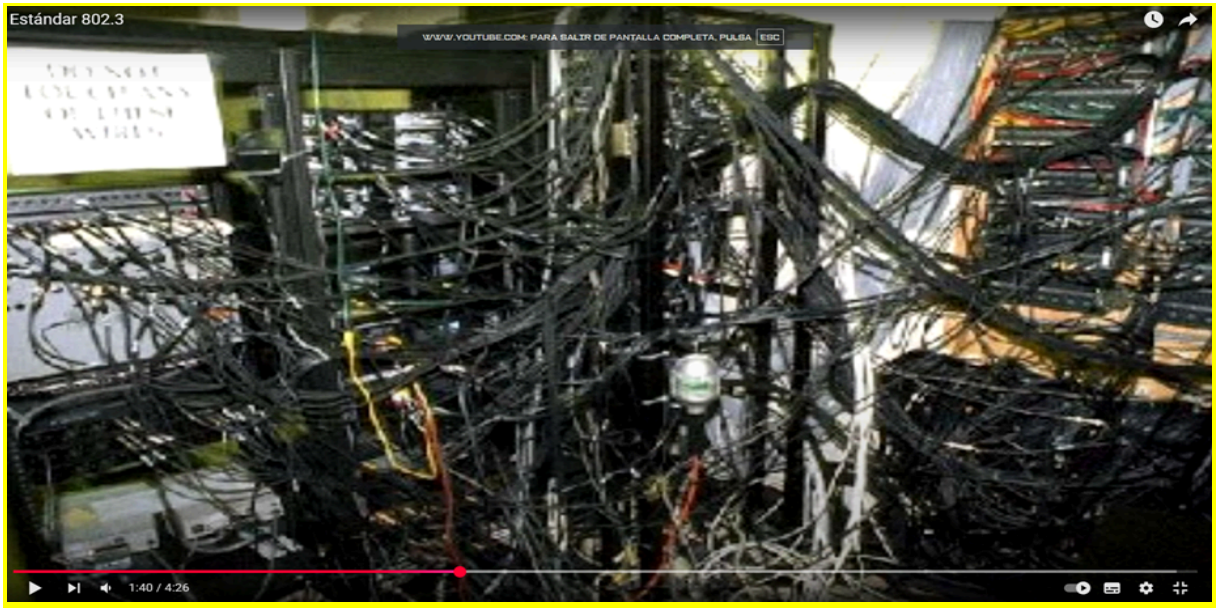
Grupo A

Uriel Leikis

Melvin Farías

Belén Martín

Guadalupe Pereyra



[Enlace a presentación creativa]

1- ¿Qué es una VLAN?

Una VLAN (Virtual Local Area Network) es una red de área local virtual que permite agrupar dispositivos de red de manera lógica, independientemente de su ubicación física. Funciona dividiendo un solo switch físico en varios switches virtuales más pequeños, lo que mejora la seguridad, la gestión de la red y el rendimiento. Por ejemplo, en una oficina, puedes separar los ordenadores del departamento de contabilidad de los de marketing, incluso si están conectados al mismo switch, evitando que se comuniquen directamente entre sí.

2- ¿Qué es una VPN?

Una **VPN** (**V**irtual **P**rivate **N**etwork) es una tecnología que crea una conexión de red segura y cifrada sobre una red pública, como Internet. Al usar una VPN, tu tráfico de datos se encapsula y se enruta a través de un servidor remoto, lo que oculta tu dirección IP y protege tu privacidad. Es muy útil para acceder de forma segura a redes corporativas desde ubicaciones remotas o para navegar de forma anónima y privada en Internet.

3- ¿Qué es una SAN?

Una **SAN** (**S**torage **A**rea **N**etwork) es una red de alta velocidad diseñada para conectar servidores a dispositivos de almacenamiento de datos. En lugar de que los servidores accedan al almacenamiento a través de una red local (LAN) tradicional, una SAN crea una red dedicada para el tráfico de almacenamiento. Esto permite que múltiples servidores accedan a un mismo conjunto de dispositivos de almacenamiento, como si estuvieran conectados localmente, mejorando el rendimiento y la escalabilidad del almacenamiento.

4- ¿Diferencias entre hub, repetidor, router y switch?

- **Hub:** Un conector básico que envía datos a todos los dispositivos.
- **Repetidor:** Amplifica una señal para extender la distancia de la red.
- **Router:** Conecta redes diferentes y dirige el tráfico usando direcciones IP.
- **SWITCH:** Un conector inteligente que envía datos a un destino específico.

5- ¿Qué es un protocolo de comunicaciones?

Un **protocolo de comunicaciones** es un conjunto de reglas y estándares que rigen la forma en que los dispositivos de una red intercambian datos. Es como un lenguaje común que todos los equipos deben entender para poder comunicarse de manera efectiva. Los protocolos definen el formato, la sincronización y el orden de los datos, así como el manejo de errores. Sin protocolos, la comunicación entre dispositivos de diferentes fabricantes sería imposible.

6- Explicar TCP/IP y NetBios; resuma sus diferencias.

- TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol): Es un conjunto de protocolos de red fundamental que forma la base de Internet. El protocolo IP se encarga de direccionar y enrutar los paquetes de datos entre redes, mientras que el protocolo TCP garantiza que los datos se entreguen de manera confiable, completa y en el orden correcto. Es un estándar abierto, escalable y universal.
- NetBIOS (**N**etwork **B**asic **I**nput/**O**utput **S**ystem): Es un protocolo de sesión que permite a las aplicaciones en diferentes computadoras comunicarse a través de una red local. Es una API (Interfaz de Programación de Aplicaciones) que proporciona servicios de nombre, sesión y datagramas. Históricamente, fue muy utilizado en las primeras redes de Microsoft, pero actualmente ha sido reemplazado casi por completo por TCP/IP.

La diferencia se puede resumir en que TCP/IP es un conjunto de protocolos de red completo que puede enrutar datos a través de grandes distancias (WAN), mientras que NetBIOS es principalmente una API de red que opera en redes locales (LAN) y no es enrutable a través de Internet sin tecnologías adicionales. TCP/IP es un estándar global y abierto, mientras que NetBIOS es un protocolo más antiguo y específico de las redes de Microsoft.

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**, conocido como segmento TCP, está compuesto por dos partes principales:

1. **Cabecera (Header):** Contiene información de control como las direcciones IP de origen y destino, puertos de origen y destino, números de secuencia y de acuse de recibo, y los "flags".
2. **Cuerpo (Payload):** Es la porción de datos que se está transmitiendo, es decir, la información real que se quiere enviar.

Un **"flag"** en un paquete de TCP/IP es un bit de control en la cabecera que indica una característica o estado específico del segmento TCP. Por ejemplo, los flags SYN (Sincronización) y ACK (Reconocimiento) se utilizan para establecer una conexión, mientras que el flag FIN (Finalizar) se usa para cerrar una conexión. Estos flags son esenciales para el control de flujo y la confiabilidad de la comunicación.

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

La clasificación de una red según su geografía se basa en el área que abarca:

- PAN (**P**ersonal **A**rea **N**etwork): Conecta dispositivos en un área muy pequeña, como una persona o un escritorio. Ejemplos: Bluetooth, NFC.
- LAN (**L**ocal **A**rea **N**etwork): Cubre un área limitada, como una casa, oficina o un edificio. Ejemplos: la red de tu hogar o la de tu empresa.
- MAN (**M**etropolitan **A**rea **N**etwork): Abarca un área urbana, como una ciudad o un campus universitario. A menudo está formada por la interconexión de varias LANs.
- WAN (**W**ide **A**rea **N**etwork): Se extiende por grandes distancias geográficas, conectando ciudades, países o continentes. Internet es el ejemplo más grande de una WAN.
- GAN (**G**lobal **A**rea **N**etwork): Red global, como una red de comunicación satelital o, de manera más amplia, Internet.<

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

La **topología de red** es la forma en que se organizan y conectan los dispositivos (hosts, switches, routers) dentro de una red, tanto desde el punto de vista **físico** (cómo están dispuestos los cables y nodos) como **lógico** (cómo circula la información). La elección de la topología afecta la **eficiencia, costo, escalabilidad y tolerancia a fallos** de la red.

Podemos enumerar los siguientes tipos de redes:

- **Bus:** todos los nodos comparten un único canal; simple, pero si el canal falla toda la red cae.

- **Estrella:** todos los nodos se conectan a un dispositivo central (hub o switch). Si falla un nodo, los demás siguen funcionando; pero si cae el nodo central, se cae toda la red. Es la más usada.

- **Anillo:** cada nodo se conecta al siguiente, formando un círculo. Los datos viajan en una única dirección (o doble, en versiones más modernas). Tiene un desempeño predecible, pero una falla en un nodo puede afectar a toda la red.

- **Malla:** cada dispositivo está conectado con varios otros. Puede ser **parcial** (algunos nodos interconectados) o **total** (todos con todos). Es altamente tolerante a fallos, pero costosa por la cantidad de enlaces requeridos.

- **Árbol (jerárquica):** combina características de estrella y bus. Existe un nodo raíz (servidor o switch principal) y a partir de él se ramifican otros niveles. Es escalable y organizada, pero depende del nodo raíz.

Topologías adicionales:

- **Mixta o híbrida:** es la combinación de dos o más topologías (por ejemplo, estrella + bus; estrella + malla). Se utiliza en redes grandes donde diferentes sectores requieren distintas estructuras. Es flexible y escalable, pero puede ser compleja de gestionar.

- **Doble anillo:** variante de la topología en anillo que incorpora un segundo anillo paralelo. Esto permite que, si uno falla, el tráfico circule por el otro. Se utiliza en redes metropolitanas (MAN) y ofrece redundancia.

- **Totalmente conexa:** todos los nodos se conectan directamente entre sí (malla completa). Ofrece la máxima redundancia y tolerancia a fallos, pero el costo y la complejidad crecen exponencialmente a medida que aumenta el número de nodos.

10- Explicar el servicio de DHCP.

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite asignar automáticamente configuraciones IP a los dispositivos de una red. Su función principal es **evitar la configuración manual de cada host**, reduciendo errores y facilitando la administración.

Funciones principales de DHCP:

- Asignación automática de direcciones IP.

- Provisión de máscara de subred.

- Configuración de la puerta de enlace predeterminada (gateway).

- Indicación de servidores DNS y, en algunos casos, servidores WINS u opciones adicionales.

Componentes principales:

- **Servidor DHCP:** equipo (servidor dedicado, router, firewall, etc.) que contiene un "pool" o rango de direcciones IP para asignar.

- **Cliente DHCP:** dispositivo que solicita una dirección IP (PC, smartphone, impresora, etc.).

- **Mensajes DHCP:** la comunicación cliente-servidor se realiza mediante un proceso de cuatro fases conocido como DORA.

Proceso **DORA** (Discover, Offer, Request, Acknowledge)

- **Discover:** el cliente que recién entra a la red envía un broadcast preguntando: "¿Hay un servidor DHCP disponible?".

- **Offer:** el servidor responde ofreciendo una IP disponible junto con otros parámetros.

- **Request:** el cliente solicita formalmente la dirección IP que le fue ofrecida.

- **Acknowledge:** el servidor confirma la asignación y el cliente ya puede usar esa configuración.

Tipos de asignación DHCP

- **Automática:** la IP se asigna de forma permanente al cliente, hasta que deje de existir en el pool.

- **Dinámica:** la IP se asigna con un tiempo determinado llamado *lease* (concesión); una vez expirado, puede renovarse o asignarse a otro dispositivo.

- **Manual (reserva):** se asigna siempre la misma IP a un cliente específico, identificado por su dirección MAC.

11- Explicar el servicio de DNS.

El **DNS (Domain Name System)** es un sistema jerárquico y distribuido que traduce nombres de dominio legibles por humanos (ejemplo: www.google.com) en direcciones IP (ejemplo: 142.250.184.132), necesarias para que los equipos puedan comunicarse en Internet o en una red privada. De allí la importancia que tiene este servicio: los usuarios recuerdan más fácilmente palabras que números. Sin DNS, tendríamos que escribir direcciones IP en lugar de nombres de dominio. DNS actúa como una “agenda telefónica” de Internet.

Estructura jerárquica del DNS - está organizado en forma de árbol:

- **Raíz (root)**: representada como un ".", contiene los servidores principales de Internet.
- **Dominios de nivel superior (TLD – Top Level Domains)**: como .com, .org, .net, .ar, .edu.
- **Dominios de segundo nivel**: definidos por organizaciones o empresas, ej. google.com.
- **Subdominios**: subdivisiones dentro de un dominio, ej. mail.google.com.

Tipos de servidores DNS

- **Servidor recursivo (resolver)**: recibe la petición del cliente y hace todo el recorrido hasta conseguir la IP.
- **Servidor raíz**: primer nivel de la jerarquía DNS.
- **Servidor TLD**: maneja dominios como .com, .org, .ar.
- **Servidor autoritativo**: tiene la información definitiva de un dominio (ej. registros de Google).

Funcionamiento de una consulta DNS

Ejemplo: cuando un usuario ingresa www.google.com

1. **Consulta al resolver local**: el sistema operativo primero revisa su caché DNS.
2. **Servidor DNS recursivo**: si no lo tiene en caché, pregunta a los servidores raíz.
3. **Servidores raíz:** indican dónde encontrar los servidores del TLD .com.
4. **Servidor TLD:** indica el servidor autoritativo de google.com.
5. **Servidor autoritativo:** responde con la dirección IP exacta.

6. El resolver guarda la respuesta en caché y el navegador se conecta a esa IP.

Registros más importantes en DNS

- **A**: nombre de dominio → dirección IPv4.
- **AAAA**: nombre de dominio → dirección IPv6.
- **CNAME:** alias
- **MX**: servidores de correo electrónico.
- **NS**: servidores autoritativos de un dominio.
- **PTR**: resolución inversa (IP → nombre).

12- Explicar las tecnologías Wireless, y sus estándares.

Las **tecnologías inalámbricas (Wireless)** permiten la transmisión de datos sin cables, utilizando ondas de radio, infrarrojas o microondas. La más conocida es **Wi-Fi**, basada en la familia de estándares **IEEE 802.11**.

Evolución de los estándares principales:

- **802.11b (1999)**: hasta 11 Mbps, en 2.4 GHz, económico pero sensible a interferencias.
- **802.11g (2003)**: hasta 54 Mbps, en 2.4 GHz, más rápido y compatible con 11b.
- **802.11n (2009)**: hasta 600 Mbps, opera en 2.4 y 5 GHz, usa tecnología MIMO (múltiples antenas).
- **802.11ac (2013)**: hasta varios Gbps, solo en 5 GHz, introduce MU-MIMO (múltiples usuarios).
- **802.11ax (2019, conocido como Wi-Fi 6)**: hasta 9.6 Gbps, mejora eficiencia en entornos densos con OFDMA y mejor administración de canales.

Otros tipos de tecnologías Wireless:

- **Bluetooth (IEEE 802.15)**: comunicación de corto alcance entre dispositivos.
- **WiMAX (IEEE 802.16)**: Internet inalámbrico de largo alcance, hoy en desuso.
- **NFC (Near Field Communication)**: comunicaciones de proximidad, usado en pagos móviles.

En la práctica, Wi-Fi (802.11n/ac/ax) es el estándar dominante en redes locales.

13- ¿Qué es un Proxy?

Un **Proxy** es un servidor intermediario entre el cliente (ej. tu computadora) y el servidor final (ej. un sitio web). El tráfico pasa primero por el proxy antes de llegar al destino.

Funciones principales:

- **Caché**: almacena copias de páginas para responder más rápido y reducir consumo de ancho de banda.
- **Control de acceso**: permite o bloquea accesos a determinados sitios.
- **Anonimato**: oculta la IP real del cliente, brindando privacidad.
- **Filtrado de contenido**: utilizado en empresas y escuelas para restringir navegación.

Tipos de proxy:

- **Proxy directo o transparente**: el cliente no nota su existencia.
- **Proxy anónimo**: oculta la IP del cliente.
- **Proxy inverso**: se coloca frente a servidores, distribuye tráfico y protege aplicaciones web.

Es una herramienta útil para **optimizar, controlar y proteger** la navegación.

14- Explicar el protocolo Spanning Tree.

STP (Spanning Tree Protocol, IEEE 802.1D) es un protocolo usado en redes de switches para **evitar bucles de capa 2**.

Problema que resuelve:

Si existen múltiples caminos redundantes entre switches, pueden generarse bucles infinitos que saturan la red con *broadcast storms*.

Cómo funciona STP:

- Elige un switch raíz (root bridge).
- Calcula el camino más corto hacia el root.
- Los enlaces redundantes quedan en estado bloqueado.
- Si un enlace activo falla, STP reconfigura la topología habilitando un enlace alternativo.

Versiones mejoradas:

- **RSTP (Rapid STP, IEEE 802.1w)**: convergencia más rápida.
- **MSTP (Multiple STP, IEEE 802.1s)**: soporta múltiples instancias de spanning tree para distintas VLANs.

STP es clave en redes con switches redundantes, garantizando estabilidad sin bucles.

15- Explicar el protocolo de comunicaciones OSPF.

OSPF (Open Shortest Path First) es un protocolo de **enrutamiento dinámico** de tipo *link-state*. Permite a los routers intercambiar información y calcular automáticamente las mejores rutas dentro de una red IP.

Características principales:

- Usa el **algoritmo de Dijkstra** para calcular la ruta más corta.

- Divide la red en **áreas jerárquicas**:
    - **Área 0 (backbone):** núcleo de la red.
    - Otras áreas se conectan siempre al backbone.
- Soporta **VLSM y CIDR** (subneteo avanzado).
- Convergencia rápida: adapta rutas rápidamente ante caídas de enlaces.

Ventajas sobre RIP (protocolo más antiguo):

- Soporta redes grandes.
- Menos tráfico de actualización.
- Rutas más óptimas y confiables.

OSPF es el protocolo de enrutamiento más usado en redes empresariales y proveedores de Internet junto con BGP.

16- Explicar el protocolo ARP.

ARP (Address Resolution Protocol) funciona en la capa de enlace (capa 2), y se utiliza para traducir direcciones **IP (lógicas)** en direcciones **MAC (físicas)** dentro de una red local.

Funcionamiento:

1. Un host quiere enviar datos a una IP dentro de la LAN.
2. Envía un mensaje de broadcast: “¿Quién tiene la IP 192.168.1.20?”.
3. El host con esa IP responde con su dirección MAC.
4. El remitente guarda la relación IP ↔ MAC en su **tabla ARP**.

Problemas de seguridad:

- **ARP Spoofing/Poisoning:** un atacante envía respuestas ARP falsas para asociar su MAC a la IP de otro host (ej. la puerta de enlace), permitiendo interceptar tráfico (ataque *Man-in-the-Middle*).

ARP es fundamental para la comunicación en redes locales Ethernet, aunque requiere medidas de seguridad (como inspección dinámica ARP en switches).

17- ¿Qué es un Firewall?

Un Firewall es un sistema de seguridad de red que monitorea y controla el tráfico de red entrante y saliente basándose en reglas de seguridad predeterminadas. Actúa como una barrera entre una red interna confiable y redes externas no confiables (como Internet).

Las funciones principales incluyen filtrar paquetes de datos según reglas configuradas, bloquear accesos no autorizados, permitir o denegar tráfico según políticas de seguridad, y registrar actividad de red para auditorías. Los tipos pueden ser hardware, software, o híbridos, y pueden clasificarse como stateful o stateless.

18- ¿Qué es una DMZ?

Una **DMZ (Zona Desmilitarizada)** es un segmento de red física o lógica que actúa como una zona buffer entre la red interna privada de una organización e Internet.

Sus características incluyen alojar servicios que deben ser accesibles desde Internet (servidores web, email, DNS), proporcionar una capa adicional de seguridad, aislar servicios públicos de la red interna, y estar generalmente protegida por dos firewalls (uno externo y uno interno). Su propósito es permitir acceso controlado a servicios específicos sin comprometer la seguridad de la red interna.

19- ¿Qué es un Gateway?

Un **Gateway** es un dispositivo o software que actúa como punto de entrada y salida entre dos redes diferentes, especialmente aquellas que utilizan diferentes protocolos de comunicación.

Sus funciones incluyen traducir protocolos entre redes diferentes, enrutar tráfico entre redes, realizar conversión de formatos de datos, y actuar como punto de control de acceso. Los tipos incluyen gateway de red, gateway de aplicación, gateway de protocolo, y gateway por defecto (default gateway).

20- Según Microsoft, ¿qué significa NBL?

NBL significa **Network Buffer List**. Es una estructura de datos utilizada en el stack de red de Windows (NDIS - Network Driver Interface Specification).

Sus características principales incluyen representar una lista de buffers de red, ser utilizada para el manejo eficiente de paquetes de red, permitir el procesamiento en lotes de múltiples paquetes, y mejorar el rendimiento al reducir overhead de procesamiento.

21- Tipos de enlace

a. Explicación de cada tipo:

MPLS (Multiprotocol Label Switching):

- Tecnología de enrutamiento que utiliza etiquetas cortas para dirigir paquetes
- Proporciona QoS (Quality of Service) garantizada
- Ideal para redes empresariales con múltiples sitios
- Ofrece VPNs privadas y seguras

LAN to LAN:

- Conexión directa entre dos redes de área local
- Puede utilizar diversos medios (fibra, cable, wireless)
- Típicamente para distancias cortas a medianas
- Alta velocidad y baja latencia

Microonda:

- Comunicación inalámbrica punto a punto usando ondas de radio
- Requiere línea de vista directa
- Ideal para terrenos difíciles donde el cableado es complicado
- Susceptible a condiciones climáticas

VSAT (Very Small Aperture Terminal):

- Comunicación satelital bidireccional
- Utiliza antenas parabólicas pequeñas
- Ideal para ubicaciones remotas
- Cobertura global pero con latencia alta

b. Dos tipos adicionales:

Fibra Óptica Dedicada:

- Conexión directa por fibra óptica entre dos puntos
- Muy alta velocidad y confiabilidad
- Inmune a interferencias electromagnéticas

VPN sobre Internet:

- Túnel encriptado sobre conexiones de Internet públicas
- Económico y flexible
- Calidad dependiente de la conexión a Internet subyacente

c. Ranking de enlaces (1-6, siendo 1 el mejor):

Criterio	MPLS	LAN to LAN	Microonda	VSAT	Fibra Dedicada	VPN/Internet
Económico	4	2	3	6	5	1
Performance	2	1	3	6	1	4
Mayor capacidad	3	1	4	6	1	5
Configuración restricciones	1	3	4	5	2	6
Soporte distancia	2	6	4	1	3	2
Más fácil de configurar	3	2	4	5	4	1

d. Elección por escenario:

1. Conectividad call centers con data center central:

La mejor opción sería MPLS, porque garantiza QoS, permite gestión centralizada, escalable para múltiples sitios.

2. Conectar pozos petroleros:

La mejor opción sería VSAT, ya que permite ubicaciones remotas, transmisión esporádicay no requiere alta velocidad constante.

3. Comunicar dos edificios enfrentados:

Recomendaría Microonda, porque ofrece línea de vista directa, sin necesidad de infraestructura física, y rápida implementación.

22- Describir la tecnología LTE.

LTE (Long Term Evolution) es un estándar de comunicación inalámbrica de alta velocidad para teléfonos móviles y terminales de datos.

Las características principales de LTE incluyen velocidades de descarga hasta 300 Mbps (teóricas), velocidades de subida hasta 75 Mbps, baja latencia (menos de 10ms), tecnología completamente IP, utilización de OFDMA (Orthogonal Frequency

Division Multiple Access), y soporte para handover entre diferentes tecnologías. En términos de evolución, es sucesor de 3G (UMTS/HSPA) y precursor de 5G, con variantes como LTE-A (Advanced) y LTE-A Pro.

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

Microsoft Teams es una plataforma de comunicación y colaboración empresarial que integra chat, videoconferencias, almacenamiento de archivos y integración de aplicaciones.

Las características principales de Teams incluyen comunicación mediante chat individual y grupal, llamadas de voz y video; colaboración a través de compartir archivos y co-autoría en tiempo real; integración con Office 365 y aplicaciones de terceros; organización por canales por equipos y proyectos; y seguridad mediante cifrado, cumplimiento normativo y administración centralizada. Una alternativa es Slack, que ofrece una plataforma similar con enfoque en canales de comunicación, excelente integración con herramientas de desarrollo, e interfaz intuitiva y personalizable.

24- Calidad en enlace MPLS

Aplicar **calidad (QoS)** en un enlace MPLS significa implementar mecanismos para priorizar, gestionar y garantizar el rendimiento de diferentes tipos de tráfico.

Los componentes de QoS en MPLS incluyen clasificación para identificar y marcar tráfico según tipo/prioridad, policing para controlar la velocidad de entrada de tráfico, shaping para suavizar ráfagas de tráfico, queuing para gestionar colas de transmisión con diferentes prioridades, y marking para usar etiquetas MPLS indicando el tratamiento requerido. Los beneficios incluyen garantía de ancho de banda para aplicaciones críticas, baja latencia para aplicaciones en tiempo real, control de jitter para voz y video, y diferenciación de servicios según SLA.

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

Medio de transmisión:

- Coaxial: señales eléctricas de cobre
- UTP: señales eléctricas en pares de hilos trenzados, más económica
- Fibra: mediante pulsos de luz a través de finos filamentos de vidrio, más rápida y costosa

	UTP	coaxial	Fibra
Tecnología Ampliamente probada	si	si	si
Ancho de banda	Medio	Medio	Muy alto
Hasta 1 Mhz	Si	Si	Si
Hasta 10 Mhz	Si	Si	Si
Hasta 20 Mhz	Si	Si	Si
Hasta 100 MHZ	si	Si	Si
Canal video	no	Si	Si
Canal Full Duplex	Si	Si	Si
Distancia medida	100 m 65 Mhz	500 (Ethernet)	2 km (Multi.) 100 km (Mono.)
Inmunidad Electromagnética	Limitada	Media	Alta
seguridad	Baja	Media	Alta
Costo	Bajo	Medio	Alto

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): certificado de nivel de entrada ofrecido por Cisco Systems, para personas que estén comenzando la carrera en redes.

- CCNA (Cisco Certified Entry Networking Technician): certificado de nivel intermedio, ofrece una base sólida de redes, preparando a profesionales para roles más avanzados

- CCNP (Cisco Certified Network Professional): certificado para profesionales con experiencia, es un certificado que valida los conocimientos de diseño, implementación, verificación y resolución de problemas de redes empresariales.

- Track Routing: proceso de selección de una ruta a través de una o más redes.

- Switching: elemento que hace posible la conexión entre varios dispositivos.

- Wireless: toda tecnología que sea inalámbrica.

27- Explique el modelo OSI.

OSI: Modelo conceptual que divide la comunicación y la interoperabilidad de la red en siete capas abstractas

Capa 7: La capa de aplicación inicia la comunicación con la red, incluidos los protocolos y los procesos de manipulación de datos que convierten los datos de red legibles por ordenador en respuestas legibles por el usuario.

Capa 6: La capa de presentación prepara los datos para la capa de aplicación, incluyendo la traducción de datos, la compresión y el cifrado.

Capa 5: La capa de sesión inicia y termina las conexiones entre dos dispositivos que interactúan en la red, asegurándose de que los recursos no se utilicen en exceso ni se infrautilizan.

Capa 4: La capa de transporte transmite datos de extremo a extremo entre dos dispositivos que interactúan en la red, asegurándose de que los datos no se pierdan, no estén mal configurados ni se dañen.

Capa 3: La capa de red gestiona los procesos de dirección, enrutamiento y reenvío de datos para los dispositivos que interactúan en diferentes redes. Si los dispositivos están en la misma red, no necesitan la capa de red para interactuar.

Capa 2: A diferencia de la capa de red, la capa de enlace de datos gestiona el enrutamiento de datos entre dos dispositivos que interactúan en la misma red.

Capa 1: La capa física comprende los activos físicos, como enrutadores y cables USB, que convierten los datos en cadenas de 1 y 0 para su transmisión a capas superiores.

Se centra en proporcionar una lista de tareas para que los ingenieros completen la construcción de cada capa de una arquitectura de red, en lugar de especificar protocolos para la comunicación entre capas.

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

- Qué es: protocolo de detección de colisiones de acceso múltiple por detección de portadora (CSMA/CD). proporciona direccionamiento MAC (Capa 2), dúplex, servicios diferenciales y atributos de control de flujo, así como diversas definiciones físicas (Capa 1), con atributos de medios, reloj y velocidad. También proporciona una definición LAG (similar a EtherChannel) para proporcionar mayor capacidad y disponibilidad del enlace.

- Implementación:

    - Hardware:
        - Tarjetas de interfaz de red (NIC):
            - Gestionar el acceso
            - Codificar y decodificar datos
            - Manejar direcciones MAC
        - Switches y routers:
            - Dispositivos que tienen puertos y circuitos que cumplen con las especificaciones de la capa física (Capa 1) para conectar cables correctamente
            - Especificaciones de la capa de enlace de datos (Capa 2) para gestionar las tramas de datos
        - cables y conectores:
            - define los tipos de cables y conectores asegurándose que las señales eléctricas viajan correctamente entre dispositivos
    - software:
        - firmware:
            - ejecuta funciones de la capa de enlace
            - manejo de tramas ethernet
            - control de flujo
        - controladores del sistema operativo:
            - Permite que la NIC se comunique con el resto del sistema.
    - Ventajas y desventajas
    - Ventajas:
        - La seguridad depende de los dispositivos conectados en la red
        - Permite velocidades de transmisión de 10 GB por segundo o superiores

        - Las transmisiones son individuales (no transmites por el mismo canal)
    - Desventajas:
        - Menor conectividad
        - Instalación de una red local

29- Explicar el estándar IEEE 802.4 regula la red.

El estándar IEEE 802.4 también conocido como el estándar Token Bus, fue desarrollado para proporcionar un medio confiable de comunicación en redes de área local (LAN) que operan en entornos industriales y de automatización. Centrándose en la transmisión de datos de manera determinista y predecible, lo que lo hace especialmente adecuado para aplicaciones que requieren tiempos de respuesta consistentes y controlados.

30- ¿Qué protocolos se usan para enviar y recibir correo?

- Protocolos:
    - SMTP : Protocolo simple de transferencia de correo, y es responsable de enviar mensajes de email. Este protocolo es utilizado por clientes de email y servidores de correo para intercambiar emails entre computadoras.
    - POP3 (Post Office Protocolo versión 3): proporciona acceso a una bandeja de entrada almacenada en un servidor de email. Ejecuta las operaciones de descarga y eliminación de mensajes
    - IMAP: permite acceder y administrar sus mensajes de email en el servidor de email. Este protocolo le permite manipular carpetas, eliminar permanentemente y buscar eficientemente a través de mensajes. También te da la opción de establecer o eliminar banderas de email, o buscar atributos de correo electrónico de forma selectiva.

- puertos
    - SMTP:
        - 25
        - 2525
        - 587
        - 465
    - POP3:
        - 110
        - 995
    - IMAP:
        - 143

        - 993

31- ¿Qué protocolo puede usarse para leer correo recibido?

Protocolos: POP3 y IMAP

32- Diferencias entre IPV4 e IPV6

- Espacio de dirección:
    - Ipv4: 2^{32} o 4 294 967 296 direcciones IP
    - Ipv6: 2^{128}, o 3403×10^{38}, o 340 282 366 920 938 000 000 000 000 000 000 000 000 000 direcciones IP
- Nomenclatura:
    - Ipv4: dirección numérica de cuatro números decimales (en el rango de 0 a 255), cada uno de los cuales representa ocho bits, separados por tres puntos: 197.0.0.1
    - Ipv6: dirección se representa mediante ocho números hexadecimales compuestos de números (0-9) y letras (A-F), cada uno de los cuales representa cuatro bits, separados por dos puntos: 2600:1400:d:5a3::3bd.
- Tipos de comunicación:
    - Ipv4: admite el direccionamiento uno a uno (mono difusión), uno a todos (transmisión) y uno a muchos (multidifusión) con enrutamiento de paquetes múltiples
    - Ipv6: admite el direccionamiento de monodifusión, multidifusión y difusión por proximidad con enrutamiento de paquetes múltiples.

33- (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.

Uriel - Tuve como experiencia en la configuración de una red personal (PAN) al vincular unos auriculares inalámbricos a mi teléfono y una vez accedí al router de mi casa para cambiar la contraseña.

Melvin - En mi caso no he tenido ninguna experiencia práctica con la materia, si conocía algunos de los términos de los que se desarrollaron en el TP.

Guadalupe - Honestamente no tengo experiencia práctica personal en redes en casa o en mi trabajo. Aunque sí escuché a uno de mis jefes hablar sobre el tema un par de veces, ya que es quien suele resolver los problemas de conexión que puedan surgir, ya sea entre equipos o con el servidor, y también se encarga del cableado.

Belén - En mi caso mi experiencia en redes es básica, principalmente a nivel hogareño. Conecté distintos dispositivos como Smart TV, notebook y celular. Más allá de eso, no tengo experiencia configurando redes ni usando programas como Packet Tracer, pero me interesa aprender más sobre el tema.