GOBIERNO DE LA CIUDAD DE BUENOS AIRES

Ministerio de Educación

Dirección de Formación Técnico Superior

Instituto de Formación Técnico Superior N°18

Mansilla 3643 - C1425BBW - Capital Federal

Programación sobre Redes

“Trabajo practico teorico”

Modalidad de trabajo: grupal hasta 5 integrantes.

Docente: Lucas Russatti

Año de Cursado: 3ro (5to cuatrimestre)

Modalidad de trabajo: grupal hasta 5 integrantes.

Fecha de entrega: Viernes 26 de septiembre de 2025

Forma de presentación de los ejercicios:

- Un documento + un recurso creativo relacionado al proyecto

Integrantes del Grupos:

- Diaz, Nestor
- Iha, Ariel
- Luiso, Ricardo
- Orihuela Torres, Elias
- Otero, Matias

Link de Github:

- https://github.com/teotronic5438/grupoE.git

Recurso Creativo:

- https://create.kahoot.it/share/programacion-sobre-redes-grupo-e/c82a81c7-facc-4d9b-927a-fbc4dbf535ba

Bonus Track:

- **Conexiones:** https://youtu.be/F-FmK9MXJY4?si=a87l_O64l5nRRUsO
- **Protocolos de red:** https://app.animaker.com/video/KGOEMD7EXAQX6F55

1- ¿Qué es una VLAN?

El término viene de una lan virtual, una red de área local virtual. Es una segmentación de una red, que puede ser en menor o mayor medida dependiendo la cantidad de direcciones de hosts disponibles que desearíamos obtener.

2- ¿Qué es una VPN?

Es una red privada virtual, mediante encriptación se cifra el tráfico proveniente de una red y un cliente.

3- ¿Qué es una SAN?

Es una red área de almacenamiento. Diferentes tipos de almacenamiento discos, cintas, se encuentran conectados a dispositivos que su vez comparten los recursos permitiendo el acceso en conjunto. Teniendo caminos y discos redundates con un rápido acceso (canales de fibra) mejorando la fiabilidad y la baja latencia.

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

Hub, repetidor trabajan en la capa 1 del modelo OSI. No tiene una conexión lógica, la señal se repite mediante una señal eléctrica.

Switch, trabaja en la capa 2 del modelo OSI, se encarga de la conmutación de paquetes mediante direcciones MAC. Posee una conexión lógica.

Router, trabaja en la capa 3 del modelo OSI (Red), se encarga de enrutar el tráfico por diferentes redes mediantes el protocolo IP. El router posee tablas de enrutamiento permitiendo el acceso a las redes con protocolos de enrutamiento, que pueden estáticos o dinámicos (rip, ospf).

5- ¿Qué es un protocolo de comunicaciones?

Es un lenguaje mediante el cual los dispositivos logran entablar una comunicación con éxito.

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

Tcp/Ip: Protocolo de control de transmisión / Protocolo Internet.

Es un conjunto de protocolos de transmisión que permite la comunicación entre redees incluídas LAN e internet definiendo como se envía, direccionan, transmiten y enrutan y reciben datos entre dispositivos.

NetBios: Network Basic Input Output System

Es una api desarrollada por IBM en los 80 que facilita la comunicación entre aplicaciones en una red local. Provee nombres lógicos como ej (pc_oficina) en lugar de direcciones ip para equipos que puedan encontrarse y compartir recursos.

7- ¿Cómo está formado un paquete de datos en TCP/IP? ¿Qué es un "flag" en un paquete de TCP/IP?

En una red basada en TCP/IP, los datos viajan encapsulados en paquetes, y cada capa del modelo agrega su propia cabecera (header).

La estructura general de un paquete típico cuando se usa TCP/IP es así:

Capa de Enlace (Ethernet, Wi-Fi, etc.)

Cabecera de enlace: contiene las direcciones físicas (MAC de origen y destino) y el tipo de protocolo de red.

Trama: este nivel incluye también un campo de control de errores (CRC).

Capa de Red (IP)

Cabecera IP: incluye dirección IP de origen, dirección IP de destino, TTL (tiempo de vida), protocolo (ej: 6 = TCP, 17 = UDP).

Capa de Transporte (TCP o UDP)

Cabecera TCP: incluye puerto de origen, puerto de destino, número de secuencia, número de confirmación, flags, ventana de recepción, checksum, etc.

Aquí es donde se maneja el control de la comunicación (fiabilidad, orden de entrega, control de congestión).

Capa de Aplicación

Datos: el contenido real que envía la aplicación (por ejemplo, una página web HTTP, un correo electrónico SMTP, un archivo FTP, etc.).

Entonces, el paquete completo está formado por:

[Cabecera Enlace] + [Cabecera IP] + [Cabecera TCP] + [Datos de Aplicación]

El flag en un paquete TCP es un bit de control que indica que se está haciendo en la comunicación (iniciar, confirmar, enviar urgente, cerrar, resetear).

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

Pan: personal area network, muy pequeña dista unos pocos metros, en un entorno personal.

Lan: local area network, dentro de una casa, oficina, o edificio.

Can: campus area network, red entre varios edificios cercanos, como un campus o parque tecnológico.

Man: metropolitan area network, cubre una ciudad o área metropolitana.

Wan: wide area network, cubre un pais, continente o es global.

Gan: global area network, extiende la conectividad a nivel mundial con enlaces satelitales.

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

Bus: todos los dispositivos companten un mismo canal de comunicación.

Estrella: todos los dispositivos se conectan a un dispositivo central, puede se un hub o switch.

Anillo: todos los dispositivos se conectan unos con otros de forma circular, cada uno enlazado con el siguiente.
Malla: cada nodo se conectan con varios otros, formando múltiples rutas.
Árbol: es una combinación de varias estrellas conectadas en forma jerárquica.
Híbrida: es un combinación que puede surgir entre una topología de estrella y bus por ejemplo.

10- Explicar el servicio de DHCP.

Dinamic host configuration protocol, es un servicio dentro de una red que asigna direcciones ip. Un dispositivo al conectarse a una red, se le asigna dinámicamente una dirección de red, máscara de subred, una dirección DNS y un gateway con un tiene un tiempo de concesión (lease time).

11- Explicar el servicio de DNS.

El DNS es un sistema que conecta los nombres de los sitios con las direcciones que usan las computadoras para encontrarse en la red.
Cuando alguien escribe un nombre de página, se hace una consulta a un servicio que busca la dirección correspondiente. Si no la tiene guardada, va preguntando en distintos niveles hasta llegar al lugar que tiene la información correcta. Una vez que obtiene esa dirección, la devuelve para que se pueda establecer la comunicación.

Video complementario: https://app.animaker.com/video/KGOEMD7EXAQX6F55

12- Explicar las tecnologías Wireless, y sus estándares.

Las tecnologías Wireless son las que permiten transmitir información sin necesidad de cables, usando ondas de radio, infrarrojas o microondas. Gracias a esto, los dispositivos pueden conectarse entre sí o a una red sin estar físicamente unidos, lo que da más movilidad y flexibilidad.
Con el tiempo se fueron creando estándares que definen cómo deben comunicarse estos dispositivos. Los más conocidos son los de la familia Wi-Fi (IEEE 802.11), que empezaron con 802.11b y g, luego pasaron a 802.11n, y más tarde a 802.11ac y 802.11ax (conocido como Wi-Fi 6). Cada nueva versión fue mejorando la velocidad, el alcance y la capacidad de manejar más dispositivos al mismo tiempo.
Existen también otros estándares dentro del mundo inalámbrico, como Bluetooth para conexiones de corto alcance entre equipos, WiMAX (802.16) para cubrir áreas más amplias, o las redes móviles como 3G, 4G y 5G que se usan en la telefonía celular.

13- ¿Qué es un Proxy?

Un proxy es un intermediario entre un dispositivo y el destino al que quiere conectarse en la red. Cuando se hace una petición, en lugar de ir directo al servidor final, primero pasa por el proxy, que luego la reenvía y devuelve la respuesta al usuario.
Puede usarse para distintas funciones: mejorar la seguridad al ocultar la dirección real del usuario, controlar o filtrar el acceso a ciertos contenidos, guardar en caché información para acelerar el acceso a páginas frecuentes, o incluso balancear la carga entre varios servidores.
Es un punto intermedio que gestiona y controla el tráfico entre el cliente y el servidor.

14- Explicar el protocolo Spanning tree.

El Spanning Tree Protocol (STP) es un protocolo de red que se usa para evitar bucles en redes de área local (LAN) que tienen múltiples caminos entre switches. Los bucles pueden causar que los paquetes se repitan infinitamente, saturando la red.
STP funciona identificando un switch raíz y calculando la mejor ruta hacia él desde cada dispositivo de la red usando un costo asociado a cada enlace, que generalmente depende del ancho de banda: a mayor velocidad, menor costo. El protocolo mantiene activas las rutas con menor costo y bloquea las demás para evitar bucles. Si alguna ruta activa falla, STP puede reactivar uno de los caminos bloqueados para mantener la conectividad.
El Spanning Tree Protocol organiza la red de forma que siempre haya una única ruta activa entre dispositivos, evitando problemas por bucles sin desconectar físicamente cables.

Video complementario: https://app.animaker.com/video/KGOEMD7EXAQX6F55

15- Explicar el protocolo de comunicaciones OSPF.
El OSPF (Open Shortest Path First) es un protocolo de enrutamiento interior que se utiliza para que los routers dentro de una misma red intercambien información sobre las rutas disponibles y puedan determinar la mejor forma de enviar los paquetes de datos. Es un protocolo de tipo link-state, lo que significa que cada router tiene conocimiento completo del estado de los enlaces de la red y construye un mapa de toda la topología.
Cada router comparte su información a través de mensajes llamados LSA (Link State Advertisements). Estos mensajes contienen detalles sobre los enlaces que tiene el router y sus costos asociados, generalmente basados en ancho de banda o métricas de rendimiento. Con esa información, cada router ejecuta el algoritmo de Dijkstra para calcular la ruta más corta hacia cada destino, asegurando que los paquetes tomen caminos eficientes y evitando bucles de enrutamiento.
El OSPF también organiza la red en áreas, lo que permite manejar redes grandes de forma más eficiente y reducir la cantidad de información que cada router necesita procesar. Además, es

capaz de adaptarse rápidamente a cambios en la red, como fallas de enlaces o la adición de nuevos routers, actualizando su mapa y recalculando rutas en tiempo real.

Video complementario: https://app.animaker.com/video/KGOEMD7EXAQX6F55

16- Explicar el protocolo ARP.

El ARP (Address Resolution Protocol) es un protocolo de red que se utiliza para mapear direcciones IP a direcciones MAC dentro de una misma red local (LAN) . Cada dispositivo en una red tiene una dirección física única llamada MAC , que se usa para el envío de tramas a nivel de enlace , mientras que las direcciones IP operan a nivel de red . ARP actúa como un traductor entre estos dos niveles.

Cuando un dispositivo necesita enviar un paquete a otro en la misma red, pero solo conoce su dirección IP, envía un mensaje ARP de solicitud (ARP Request) en broadcast, preguntando “Quién tiene esta IP?”. Todos los dispositivos de la red reciben la solicitud, pero solo aquel que posee la IP consultada responde con un mensaje ARP de respuesta (ARP Reply) indicando su dirección MAC. El remitente guarda esta información en una tabla ARP o caché, para no tener que consultar de nuevo en futuras comunicaciones.

Existen también variantes y mecanismos relacionados, como ARP inverso (RARP), que permite obtener una dirección IP a partir de una MAC, y protocolos de seguridad que ayudan a evitar ataques como ARP spoofing, donde un dispositivo malicioso envía respuestas ARP falsas para interceptar o redirigir tráfico.

El ARP es un componente crítico en redes locales, porque permite que los dispositivos identifiquen correctamente a sus vecinos y transmitan datos a nivel de enlace de manera eficiente.

17- ¿Qué es un Firewall?

Un firewall es un sistema de seguridad de red que filtra y controla el tráfico de red entrante y saliente según un conjunto de reglas predefinidas. Puede ser hardware, software o una combinación de ambos.

Su función principal es proteger los recursos internos de accesos no autorizados, ataques externos o malware. Puede trabajar en diferentes niveles (filtrado de paquetes, inspección profunda, cortafuegos de aplicaciones).

Ejemplo: bloquear puertos no usados, permitir solo tráfico HTTP/HTTPS, detectar conexiones sospechosas.

18- ¿Qué es una DMZ?

Una DMZ (Demilitarized Zone o Zona Desmilitarizada) es un segmento de red intermedio que separa la red interna de confianza (LAN) de redes externas no seguras (como Internet).

En esta zona suelen colocarse servidores públicos (correo, web, DNS) que deben ser accesibles desde el exterior, pero que al mismo tiempo no deben tener conexión directa a la red interna.
La DMZ actúa como un “colchón de seguridad”: si un servidor de la DMZ es comprometido, la red interna permanece protegida.

19- ¿Qué es un Gateway?

Un gateway es un dispositivo que actúa como punto de entrada y salida entre dos redes que pueden usar protocolos o arquitecturas diferentes.
A diferencia del router (que conecta redes con el mismo protocolo IP), el gateway puede hacer traducciones de protocolos.
Ejemplo: un gateway de VoIP convierte tráfico IP en señal telefónica tradicional; un gateway IoT traduce protocolos industriales a TCP/IP.

20- Según Microsoft, ¿qué significa NBL?

En entornos de Microsoft y Windows, NBL significa Net Buffer List.
Es una estructura de datos usada por el NDIS (Network Driver Interface Specification) para manejar buffers de red de forma eficiente.
El NBL permite que los controladores de red y el sistema operativo gestionen paquetes de datos sin tener que copiar información constantemente, mejorando el rendimiento de la pila de red en Windows.

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.

a. Explique cada uno:

MPLS (Multiprotocol Label Switching): Tecnología de red que enruta paquetes usando etiquetas en lugar de direcciones IP. Es rápido, seguro y muy usado en redes corporativas.
LAN to LAN: Conexión directa entre dos redes locales remotas mediante VPN o enlaces dedicados, permite trabajar como si fueran una sola red.

Microonda: Enlace inalámbrico punto a punto que utiliza ondas electromagnéticas de alta frecuencia. Ideal para distancias medianas-grandes con línea de vista.
VSAT (Very Small Aperture Terminal): Tecnología satelital que permite acceso a Internet y datos en áreas remotas mediante antenas pequeñas.

b. Dos tipos adicionales:
Fibra óptica dedicada: Conexión física de alta velocidad y gran capacidad, con baja latencia.
4G/5G móvil: Uso de redes móviles para conexión de datos con buena cobertura y movilidad.

c. Ranking de enlaces según criterio (1 = mejor, 6 = peor):
Económico: 1. LAN to LAN, 2. 4G/5G, 3. Microonda, 4. VSAT, 5. Fibra dedicada, 6. MPLS.
Performance: 1. Fibra dedicada, 2. MPLS, 3. LAN to LAN, 4. 5G, 5. Microonda, 6. VSAT.
Mayor capacidad: 1. Fibra dedicada, 2. MPLS, 3. LAN to LAN, 4. 5G, 5. Microonda, 6. VSAT.
Mayor configuración de restricciones: 1. MPLS, 2. Fibra dedicada, 3. LAN to LAN, 4. VSAT, 5. 5G, 6. Microonda.
Soporte a mayor distancia: 1. VSAT, 2. MPLS, 3. Fibra dedicada, 4. 5G, 5. Microonda, 6. LAN to LAN.
Menor esfuerzo de configuración: 1. 5G, 2. LAN to LAN, 3. Fibra dedicada, 4. Microonda, 5. VSAT, 6. MPLS.

d. Escenarios:
Conectividad de varios call centers con un data center central: MPLS (seguridad, calidad de servicio, estabilidad).
Conectar datos de pozos petroleros durante 15 minutos por día: VSAT (cubre zonas remotas sin infraestructura terrestre).
Comunicar dos edificios enfrentados en la misma calle: Microonda o LAN to LAN con fibra (enlace directo, bajo costo).

22- Describir la tecnología LTE.

Long-Term Evolution o LTE es un estándar inalámbrico de cuarta generación (4G) que proporciona mayor capacidad de red y velocidad para teléfonos móviles y otros dispositivos celulares en comparación con la tercera generación (3G), pero con menor rendimiento (velocidad, retardo de propagación, etc.) que la tecnología 4G pura. LTE ofrece velocidades máximas de transferencia de datos de hasta 100 Mbps de bajada y 30 Mbps de subida. Proporciona latencia reducida, capacidad de ancho de banda escalable y compatibilidad con versiones anteriores de la tecnología existente del Sistema Global para Comunicaciones Móviles (GSM) y del Servicio Universal de Telecomunicaciones Móviles (UMTS). La evolución LTE-Advanced (LTE-A) consigue tasas de hasta 300 Mbps.

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

Microsoft Teams es un espacio de trabajo pensado para la colaboración en tiempo real y la comunicación, las reuniones, el uso compartido de archivos y aplicaciones, e incluso para los ocasionales emoji. Todo en un único lugar, en equipo, y con todo a disposición de todos. stá diseñado para fomentar la colaboración en tiempo real entre miembros de un equipo, ofreciendo un espacio unificado para todas las actividades de colaboración. Sus funcionalidades principales son la mensajería, reuniones y llamadas, intercambio de archivos, integración de aplicaciones y centros de trabajo para organizar las actividades en equipos y canales.

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

Aplicar calidad a un enlace MPLS significa asegurar una experiencia de comunicaciones predecible y confiable, lograda a través de la Calidad de Servicio (QoS). Esto implica priorizar ciertos tipos de tráfico (como VoIP o video) sobre otros (como la navegación web), mediante la asignación de etiquetas a los paquetes de datos. Como resultado, se garantiza que las aplicaciones críticas reciban el ancho de banda y el rendimiento necesarios, manteniendo baja latencia, reduciendo la pérdida de paquetes y asegurando un flujo de datos ininterrumpido

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

Las diferencias radican en varios aspectos. En medio de transmisión, coaxial utiliza una señal eléctrica por un conductor central de cobre, UTP una señal eléctrica por pares de hilos de cobre trenzados y fibra Pulso de luz (fotones) a través de un filamento de vidrio/plástico. En velocidades de transmisión, coaxial posee la velocidad más lenta (hasta 10Gbps), seguido por UTP (hasta 40 Gbps),mientras que Fibra llega hasta terabits por segundo. En ancho de banda, coaxial se encuentra en segundo lugar, UTP en ultimo lugar, y finalmente Fibra como la mejor opción ya que admite decenas de THz. En materia de seguridad, el Coaxial ofrece un grado medio de seguridad ya que la señal puede ser interceptada, UTP ofrece el nivel más bajo de seguridad por la facilidad en la intercepción de la señales, y Fibra ofrece el nivel más alto de seguridad (cortar el cable interrumpe la señal, es muy difícil interceptarla sin ser detectado). En cuanto a costos, Coaxial se encuentra en un grado medio, UTP como la infraestructura de costos más baja, y Fibra como el nivel de costos más 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 Era la certificación de nivel de entrada. Demostraba que una persona tenía las habilidades fundamentales para instalar, operar y solucionar problemas de una pequeña red empresarial. CCNA, o Cisco Certified Network Associate, es una certificación de nivel básico que

acredita las habilidades esenciales en redes, como la instalación, configuración y resolución de problemas en redes medianas. Por otro lado, CCNP, o Cisco Certified Network Professional, es una certificación de nivel profesional que requiere que el candidato demuestre conocimientos avanzados en planificación, implementación y resolución de problemas en redes empresariales complejas. El routing es la capacidad de buscar la ruta correcta para mover o transferir paquetes de información entre una o varias redes de Internet.
El switching es un elemento que hace posible la conexión entre varios dispositivos como ordenadores, servidores o sensores. Todos estos operan en una misma red empresarial o dentro de una estructura física determinada. Un router permite que la información de la red se pueda compartir entre varios equipos, con el nivel de protección adecuado ante potenciales amenazas externas.Mientras que el switch tiene como misión generar una red de recursos compartidos en el ámbito interno de una organización. El track security se centra en proteger los activos de información de un a organización. Su misión es garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas frente a amenazas constantes. Un especialista en seguridad no solo pone barreras (firewalls), sino que también monitorea, detecta anomalías y responde a incidentes.

27- Explique el modelo OSI.

El modelo Open Systems Interconnection (OSI) es un modelo conceptual creado por la Organización Internacional para la Estandarización, el cual permite que diversos sistemas de comunicación se conecten usando protocolos estándar. En otras palabras, el OSI proporciona un estándar para que distintos sistemas de equipos puedan comunicarse entre sí.
El modelo OSI se puede ver como un lenguaje universal para la conexión de las redes de equipos. Se basa en el concepto de dividir un sistema de comunicación en siete capas abstractas, cada una apilada sobre la anterior.

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

El estándar IEEE 802.3 regula Ethernet, la tecnología más usada en redes LAN cableadas. Define cómo se transmiten los datos por cobre o fibra, el formato de las tramas (direcciones MAC, cabeceras, control de errores), las velocidades (10 Mbps hasta cientos de Gbps) y el método de acceso al medio (antes CSMA/CD, hoy reemplazado por switches que evitan colisiones).

Implementación

* Se aplica en redes LAN con topología en estrella, conectando PCs, routers y switches mediante tarjetas de red (NICs) con direcciones MAC únicas. Funciona tanto sobre cables de cobre (UTP/STP) como fibra óptica, según la velocidad y distancia necesarias.

Ventajas

* Estándar mundial, compatible entre fabricantes.
* Escalable en velocidad (de 10 Mbps a 400 Gbps).
* Confiable y económico.
* Fácil de instalar y configurar.
* Mayor seguridad física frente a redes inalámbricas.

Desventajas

* Limitada movilidad al ser cableado.
* Costoso en grandes distancias por el tendido de cable.
* En versiones antiguas (hubs) había colisiones.
* No es ideal para redes WAN de larga distancia.

29- Explicar el estándar IEEE 802.4 regula la red.

El estándar IEEE 802.4 describe una red en bus que funciona mediante token. El token indica qué estación tiene permiso para transmitir. Ninguna estación puede enviar datos si no tiene el token. Físicamente, la red se organiza como la topología bus, pero lógicamente funciona con la topología de anillo. Cada estación tiene un número único que la identifica. Al iniciar la red, la estación con el número más alto genera el token, que luego se pasa a la estación con el siguiente número más bajo. La estación que recibe el token puede transmitir sus datos y, al terminar o cuando se cumple un tiempo límite, pasa el token a la siguiente estación. Este proceso se repite hasta que todas las estaciones hayan tenido su turno, permitiendo que cada una transmita de manera ordenada y periódica. Así, la red implementa un sistema organizado de acceso al medio llamado multiplexación en el tiempo.

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

Para enviar correo se utiliza el protocolo SMTP (Simple Mail Transfer Protocol), que se encarga de transferir los mensajes desde el cliente hacia el servidor de correo o entre servidores hasta que llega al destinatario.

Para recibir correo existen dos protocolos principales:

* POP (Post Office Protocol): descarga los mensajes desde el servidor hacia el dispositivo local, y por defecto los elimina del servidor (aunque puede configurarse que deje copias).
* IMAP (Internet Message Access Protocol): mantiene los mensajes en el servidor y permite sincronizarlos en varios dispositivos, facilitando el acceso desde diferentes lugares.

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

El protocolo IMAP (Internet Message Access Protocol) permite leer y organizar tus correos directamente en el servidor. Con él puedes mover mensajes entre carpetas, eliminar correos,

buscar información dentro de los mensajes y marcar correos con banderas. Por defecto, los correos se quedan en el servidor hasta que tú decidas borrarlos.

32- Diferencias entre IPV4 e IPV6

IPv4 consta de 32 bits dividido en 4 octetos donde cada octeto es un número decimal entre 0 y 255. Los octetos están separados por puntos. Mientras que en una dirección IPv6 consta de 128 bits, representados en 8 grupos de 16 bits expresados en hexadecimal separados por dos puntos. IPv4 ofrece millones de direcciones e IPv6 tiene prácticamente un sin fin de posibles direcciones.

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.

Ariel Iha: he configurado router hogareño para conectar dispositivos ip, como cámaras, impresoras, servidores de archivos, configurado ip estáticas basadas en direcciones mac desde la página del router, cambié la contraseña de una red wifi. He armado cables con fichas rj45, testeado cables de red.

Nestor Diaz: No tengo experiencia en redes, el mayor acercamiento que tuve fue cuando investigué un poco sobre como poder tener internet en mi PC, y aprendí que se puede utilizar placas wifi o usar un cable Ethernet conectado directamente al router.

Matias Otero: Trabajo en el área de Telecomunicaciones – Estoy mas en la parte de Ups y sistemas de alimentación segura, configuro ocasionalmente algún puerto de un Switch , cambio vlan y realizo algún troubleshooting básico, armo algún cable o conectores ,alguna vez fusione fibra, pero básicamente los conocimientos adquiridos fueron de manera informal.

Elias Orihuela Torres: He trabajado como soporte técnico y revisado habitualmente la configuración de router, computadoras e impresoras. Armado de cables de red básicos en LAN. No tengo experiencia con fibra óptica, pero si hice un curso de administración de redes pero fue hace más de 10 años.