Monografía

Tomás Vidal y Daniel Garzón
Sistemas Operativos y Redes
Facultad de Ingeniería, UNLP, La Plata, Argentina.
9 de Diciembre, 2024.

I. Introduction

Las redes de comunicaciones en la última era han protagonizado nuestra sociedad, gracias a la gran cantidad de información que se transmite diariamente a través de diferentes dispositivos, se ha requerido de disponer de diferentes protocolos que facilitan la transferencia eficiente, segura, organizada y en tiempo real de los datos.

El propósito de esta monografía es analizar el funcionamiento, las ventajas, los limitantes, y sus aplicaciones típicas describiendo sus características principales de los siguientes protocolos: DHCP, FTP, Telnet y RTP, además de abarcar la tecnología VoIP, esto a razon de que los previos protocolos tienen un papel fundamental en la asignación de direcciones ip, transferencia de archivos, administracion remota, manejo de flujo de datos o transmisión de voz y multimedia.

La importancia de este análisis radica en comprender cómo estos protocolos permiten que las redes operen de manera eficiente, optimizando recursos y garantizando la calidad del servicio, además de presentar una visión general que engloba el ecosistema tecnológico al que nos vemos sometidos hoy día.

II. DHCP

El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP), desarrollado a partir de 1985, es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

Este servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente.

A. Funcionamiento

El servicio tiene que existir en un servidor que sea capaz de proveer los datos a los dispositivos que lo requieran dentro de la red. El mecanismo de funcionamiento se basa en el ciclo conocido como **DORA**:

- **D**ISCOVER: El cliente que desea obtener una dirección IP envía un mensaje de difusión (*broadcast, 255.255.255.255*) al servidor DHCP en la red. Este mensaje se conoce como *DHCPDISCOVER* y tiene como objetivo localizar cualquier servidor DHCP disponible.
- **O**FFER: El servidor DHCP responde con un mensaje llamado *DHCPOFFER*, que contiene una dirección IP disponible, la máscara de subred, la puerta de enlace predeterminada y otros parámetros de configuración.
- **R**EQUEST: El cliente, tras recibir una oferta válida, envía un mensaje *DHCPREQUEST* al servidor para solicitar formalmente la asignación de la dirección IP y demás parámetros ofrecidos.
- **A**CKNOWLEDGE: Finalmente, el servidor confirma la asignación enviando un mensaje *DHCPACK*, tras lo cual el cliente puede empezar a usar la dirección IP y la configuración proporcionada.

B. Ventajas

El uso de DHCP presenta varias ventajas para la gestión de redes:

- **Automatización**: Los dispositivos obtienen automáticamente sus configuraciones de red sin intervención manual, reduciendo errores de configuración.
- **Eficiencia**: El administrador de red puede gestionar dinámicamente las direcciones IP, evitando conflictos y reutilizando direcciones en redes con muchos dispositivos.
- **Escalabilidad**: Facilita la administración de grandes redes, donde sería inviable configurar manualmente cada dispositivo.
- **Flexibilidad**: Es posible realizar cambios globales en la configuración de red desde el servidor DHCP sin necesidad de modificar cada dispositivo.

C. Limitaciones

A pesar de sus ventajas, DHCP también presenta algunas limitaciones:

- **Dependencia del servidor**: Si el servidor DHCP falla, los dispositivos nuevos o reiniciados no podrán obtener configuración de red.
- **Seguridad**: DHCP por sí mismo no incluye mecanismos de autenticación, lo que puede permitir ataques como la suplantación de servidor (*rogue DHCP*).
- **Pérdida de direcciones fijas**: Las direcciones asignadas dinámicamente pueden dificultar la administración en

escenarios donde algunos dispositivos requieren direcciones IP fijas.

D. Extensiones y Mejoras

Existen extensiones del protocolo DHCP para abordar algunos de sus desafíos, como:

- **DHCPv6**: Adaptado para redes IPv6, proporcionando soporte para el amplio rango de direcciones y características específicas de IPv6.
- **Opciones de seguridad**: Implementaciones avanzadas pueden incluir autenticación mediante 802.1X o configuración de servidores confiables.

E. Aplicaciones Típicas

DHCP es ampliamente utilizado en redes locales (LAN), como oficinas, hogares y campus universitarios. También se emplea en redes más grandes, como proveedores de servicios de Internet (ISP), para asignar direcciones IP dinámicamente a sus clientes.

F. Aplicación en CORE

Para implementar DHCP en CORE Network emulator, primero que todo se requiere ejecutar el siguiente comando en la terminal *"sudo apt-get install isc-dhcp-server apache2 libpcap-dev radvd at"* el cual configura e instala las utilidades de este emulador, sin él no se va a poder realizar la simulacion adecuadamente.

Una vez instalado y configurado las utilidades, a través del comando previo, se implementa una red sobre la cual se desea implementar DHCP como por ejemplo la que podremos ver en las figuras 1, 2 y 3 donde tendremos los clientes sin direccion ip asignada, el servidor y un router con su respectiva direccion, luego se configuran las utilidades en el dispositivo que va a actuar como servidor, asignandole cual va a ser la ip que actua como servicio y los routers a los que se conecta como sé ve a continuación:

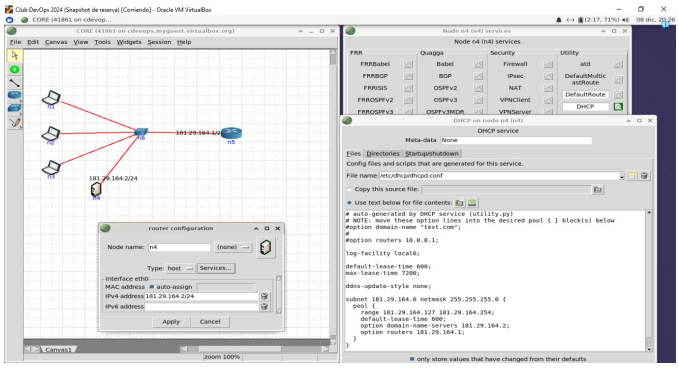

Fig. 1. Configuración de DHCP Servidor

luego, asignamos los dispositivos que deseamos como clientes y activamos la opción DHCP Client, sin modificar la configuración de este a diferencia de como se hizo con el servidor.

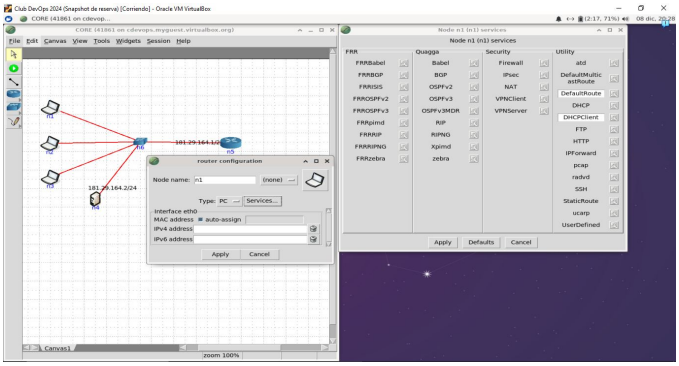

Fig. 2. Configuración de DHCP clientes

Una vez hecho esto, se corre la simuacion y se verifica su funcionamiento por medio del comando ping desde un cliente hacia el router como se ve a continuacion el cual responde de manera adecuada.

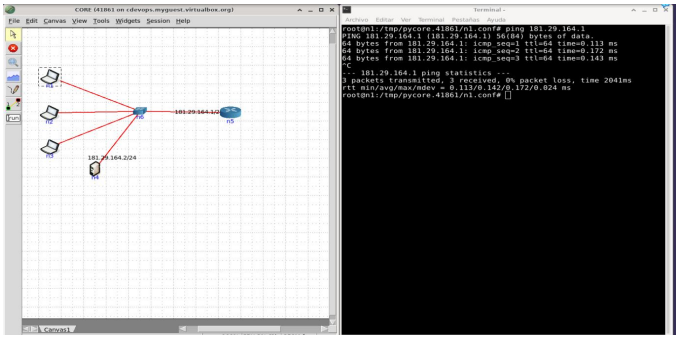

Fig. 3. Funcionamiento DHCP aplicado

III. FTP

El Protocolo de Transferencia de Archivos, nombrado FTP por sus siglas en inglés "File Transfer Protocol", es un protocolo de red que transfiere archivos conectados entre sistemas conectados a una red TCP/IP, que permite, desde un dispositivo cliente, enviar o descargar archivos de un servidor, el cual independientemente del tipo de sistema operativo que manejen ambos, se podrá subir o bajar información a alta velocidad.

Cabe aclarar que este protocolo opera en la capa de Aplicación del modelo TCP/IP de la capa de Red, predefinido generalmente para usar los puertos 20 y 21, a modo general su principal función consiste en definir el cómo se hace la transmisión de datos en la capa red y está compuesto por los siguientes elementos:

- **Servidor FTP:** Es el equipo al que deseamos conectarnos y que debe estar configurado para aceptar las conexiones de los clientes FTP. Este servidor debe estar activo el programa servicio FTP, compuesto por:
  1) **El Intérprete de Protocolo del Servidor (PI "protocol interpreter"):** El cual va a escuchar los comandos enviados por el intérprete de protocolo del cliente a través del puerto 21 generalmente, este gestionará el proceso de transferencia de datos en el servidor.

2) **El Servidor DTP (Data Transfer Process**):es quien se encarga de transmitir los datos entre el servidor y el cliente, como lo dice su propio nombre en español (Proceso de transferencia de datos), este tiene la capaciad de operar en modo pasivo, esperando conexiones entrantes en el puerto 20 para manejar las transferencias de datos de manera constante.

- **Cliente FTP:** Es el equipo que se conecta al servidor FTP el cual se compone por:
  1) **La interfaz de usuario:** esta nos ofrece un conjunto de comandos de alto nivel más fáciles de usar y memorizar que los comandos técnicos del protocolo FTP que se intercambian entre cliente y servidor de modo que facilita la interacción por parte del usuario.
  2) **Cliente PI (Intérprete de Protocolo):** este se encarga de iniciar la conexión de control con el servidor a través del puerto 21, de modo tal que, una vez establecida la conexión, codifica y envía los comandos FTP al servidor, además de supervisar el proceso de transferencia de archivos gestionado por el DTP.
  3) **Cliente DTP (Proceso de Transferencia de Datos):** este componente maneja la transferencia de archivos. Escucha el puerto 20 que se ha establecido como el puerto de datos y acepta conexiones para realizar el intercambio de archivos entre cliente y servidor.

A. Funcionamiento

El protocolo ftp utiliza dos canales principales: el canal de control (puerto 21 por defecto) y el canal de datos (puerto 20 por defecto), este funciona de la sigiente forma:

- **Establece la conexión:** El cliente FTP inicia una sesión, estableciendo una conexión con el servidor FTP por medio del puerto 21, el cual se utiliza para el control de la conexión, luego el usuario ingresa en el servidor mediante un nombre de usuario y contraseña. En algunos casos, se puede usar el acceso anónimo, (sin contraseña), sin embargo, solo se permitirá leer y descargar archivos que el administrador del servidor haya configurado como públicos.
- **Intercambio de comandos y respuestas:** Una vez se ha autenticado, el cliente envía comandos al servidor para realizar diversas operaciones, como listar directorios, descargar o subir archivos, para posteriormente ser responderle a cada comando con un código de estado que indica el resultado de la operación, es decir informa al usuario de la correcta asignacion para subida o bajada de datos.
- **Transferencia de datos:**Para transferir archivos o información de directorios, se establece un canal de datos independiente el cual se divide en 2 modos de uso, pasivo o activo, donde el primero hace una conexion en el servidor y el cliente de un puerto superior a 1024 incluido de modo que se pueda generar la transferencia en caso que haya un NAT o firewall de oir medio, mientras que el activo tiene la conexion del puerto 20 al generado por el cliente (superior a 1024 incluido).
- **Transferencia de archivos:** Como su nombre lo indica, el cliente puede descargar archivos del servidor o cargar archivos en él, donde la transferencia puede ser en modo binario (para imágenes, videos o programas) o en modo ASCII (para texto).
- **Finalización de la conexión:** Se cierra la sesión y finaliza la conexión despúes de haber transferido los archivos.

Es importante tener en cuenta que este protocolo para la transferencia de archivos no cifra los datos, sino que se transmiten en texto plano, lo que significa que, si un atacante logra interceptar alguno de estos archivos, podrá acceder a toda la información.

B. Ventajas

- **Transferencia rápida de archivos grandes:** FTP está diseñado para manejar grandes volúmenes de datos, permitiendo transferencias más eficientes en comparación con otros métodos como el correo electrónico.
- **Compatibilidad multiplataforma:** Funciona entre diferentes sistemas operativos, lo que facilita su uso entre diferentes dispositivos.
- **Soporte para reanudar transferencias interrumpidas:** Si una transferencia se interrumpe, FTP permite reanudarla desde el punto donde se detuvo.
- **Control de acceso:** Ofrece opciones de autenticación mediante usuarios y contraseñas, además de configuraciones específicas para accesos restringidos o anónimos.
- **Gestión remota de archivos:** Permite realizar operaciones como crear, eliminar, renombrar y mover archivos o carpetas en el servidor remoto por medio de la conexion por navegador web.
- **Transferencia de múltiples archivos:** FTP permite transferir varios archivos y directorios completos en una sola sesión, lo que optimiza el tiempo y la eficiencia.

C. Limitaciones

- **Seguridad insuficiente:** FTP transmite los datos en texto plano, inlcuyendo los nombres de usuario, contraseñas y archivos, sin cifrado, esto hace que los datos sean vulnerables si la conexión no es segura.
- **Falta de confidencialidad y protección de datos:** Dado que FTP no cifra la transferencia de datos, cualquiera que tenga acceso a la red podría obtener información.
- **Problemas con firewalls y NAT:** En el modo activo de FTP, el servidor necesita abrir una conexión hacia el cliente, lo cual puede ser bloqueado por firewalls o dispositivos NAT. Esto hace que FTP sea problemático en redes protegidas, lo que puede dificultar la conexión, incluso con el modo pasivo algunas redes aún pueden tener dificultades para configurar correctamente el puerto.

- **Falta de integridad de datos:** FTP no garantiza que los datos no se alteren durante la transferencia.
- **Limitación en la autenticación:** La autenticación en FTP generalmente se realiza con nombre de usuario y contraseña, pero ningun otro tipo de autentificación de por medio lo que genera que si llega a ser interceptada la contraseña y usuario, facilmente se puede ver afectado el cliente
- **Falta de manejo de archivos grandes en conexiones lentas:** FTP no está optimizado para conexiones de red muy lentas lo que puede volverlo ineficiente y propenso a interrupciones.
- **Uso de múltiples puertos:** FTP utiliza diferentes puertos para los comandos (puerto 21) y para la transferencia de datos (puerto 20 en modo activo o puertos dinámicos en modo pasivo), esto puede generar conflictos en redes restringidas o configuraciones complejas de seguridad.

D. Aplicaciones típicas

El protocolo FTP se emplea en diversas aplicaciones, como la gestión de servidores web, la transferencia de grandes volúmenes de datos y el acceso remoto a repositorios de archivos para descargar o subir información. Cuando los navegadores no tienen soporte para FTP o se necesitan funciones más avanzadas, se utilizan programas cliente FTP, que conectan el dispositivo del usuario con el servidor y permiten realizar transferencias eficientemente.

IV. Telnet

Telnet (abreviatura de *Telecommunication Network*) es un protocolo de red que permite a los usuarios establecer una conexión remota con un servidor para controlar un dispositivo o sistema como si estuvieran físicamente presentes. Desarrollado en los años 70, fue uno de los primeros protocolos diseñados para comunicación en redes IP.

A. Funcionamiento

Telnet utiliza el modelo cliente-servidor. Un cliente Telnet se conecta a un servidor Telnet a través del puerto TCP 23 (por defecto). Una vez establecida la conexión, los usuarios pueden interactuar con el sistema remoto mediante una interfaz de línea de comandos. El proceso típico es el siguiente:

- **Inicio de sesión**: El cliente inicia una conexión y proporciona las credenciales requeridas (nombre de usuario y contraseña).
- **Interacción remota**: El cliente envía comandos al servidor, que los ejecuta y devuelve los resultados al cliente.
- **Terminación**: La sesión se cierra cuando el usuario lo solicita o cuando ocurre un error.

Telnet no cifra las comunicaciones, por lo que tanto las credenciales como los datos transmitidos están expuestos a posibles interceptaciones.

B. Ventajas

- **Simplicidad**: Fácil de configurar y usar en redes pequeñas o controladas.
- **Versatilidad**: Permite interactuar con dispositivos remotos que solo tienen interfaz de línea de comandos.
- **Compatibilidad**: Es compatible con una amplia variedad de sistemas operativos y dispositivos.

C. Limitaciones

- **Falta de seguridad**: Todas las comunicaciones se transmiten en texto plano, lo que las hace vulnerables a ataques como el *sniffing*[1].
- **Obsolescencia**: En la actualidad, ha sido reemplazado en gran medida por protocolos más seguros, como SSH[2].
- **Uso limitado**: Su aplicación está restringida principalmente a redes seguras o controladas.

D. Aplicaciones Típicas

Telnet aún se utiliza en ciertos contextos, como:

- Configuración inicial de dispositivos de red, como routers y switches.
- Pruebas de conectividad y diagnóstico de servicios TCP.
- Acceso a sistemas heredados que no soportan protocolos más modernos.

V. VoIP

VoIP *"Voice over Internet Protocol"* o "Voz sobre Protocolo de Internet", es una tecnología que facilita la transmisión de voz a través de Internet a través del protocolo IP, VoIP trabaja en tocas las capas del modelo OSI ademas esta tecnología se diferencia de la telefonía tradicional en que, VoIP transforma la voz en paquetes de datos y la transporta a través de redes IP, como Internet o LAN, mientras que la telefonia clasica lleva la señal analógica a través de un cable de cobre.

A. Funcionamiento

- **Conversión de voz a datos digitales:** Se convierte la señal analógica de la voz en datos digitales utilizando un códec (codificador/decodificador).
- **Fragmentación y empaquetado:** Los datos digitales se dividen en paquetes, que llevan la información de audio, datos esenciales para su reensamblaje y enrutamiento.
- **Transmisión de datos:** Los paquetes de datos viajan a través de la red IP, utilizando protocolos como SIP para establecer, gestionar y terminar la llamada, y RTP (Real-Time Transport Protocol) para la entrega del contenido de audio en tiempo real.
- **Enrutamiento:** Los paquetes siguen rutas dinámicas a través de la red, dependiendo de las condiciones actuales, como la congestión.

[1]Un tercero captura el tráfico a través del hub o switch.

[2]SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación, el mismo es seguro porque la transferencia de información está encriptada.

- **Reensamblaje y reproducción:** Una vez que los paquetes llegan al destino, el códec los reensambla y convierte los datos digitales nuevamente en señales de audio analógicas.

B. Ventajas

- **Disminución de Gastos:** La telefonía IP permite reducir los costos de comunicación, viendose principalmente beneficiados en los casos de llamadas de larga distancia.
- **Ventaja Competitiva:** La adopción de VoIP puede proporcionar a las empresas una ventaja competitiva al permitir una comunicación más eficiente y rentable.
- **Máxima Movilidad:** Los sistemas VoIP permiten realizar y recibir llamadas desde cualquier lugar que tenga conexión a Internet.
- **Mensajería Unificada:** Integra diferentes métodos de comunicación en una sola plataforma, como puede ser mensajes, llamadas, videoconferencias, entre otros, mejorando así la eficiencia.
- **Servicios de Directorio:** Los sistemas VoIP permiten acceder fácilmente a directorios y bases de datos de contacto dentro de redes.
- **Migración Gradual y Segura:** La transición a VoIP puede realizarse de forma gradual y segura.
- **Seguridad y Calidad de Servicio:** Los sistemas VoIP ofrecen robustas medidas de seguridad y calidad en las llamadas, protegiendo los datos y asegurando una comunicación clara.

Nota: se recomienda leer [7], [9] y [10] para comprender esto a detalle

C. Limitaciones

- **Requiere de una Conexión de Banda Ancha:** Para tener una comunicacion estable y continua se requieren redes de banda ancha de calidad.
- **Requiere de una Conexión Eléctrica:** Los teléfonos VoIP requieren de una conexión eléctrica para operar, lo que puede ser un problema durante cortes de energía.
- **Problemas con Llamadas al 911:** VoIP usa direcciones IP para identificar números telefónicos, pero no es posible asociar una dirección IP con una ubicación geográfica, lo que complica que el 911 lo identifique.
- **Dependencia de la Calidad de la Red:** La calidad de la llamada VoIP depende de la estabilidad de la red, ya que problemas como alta latencia o pérdida de paquetes pueden distorsionar o interrumpir la conversación.

D. Aplicaciones típicas

Algunas de las aplicaciones típicas de VoIP se encuentran en aplicaciones como Messenger, Discord, Google Meet, Microsoft Teams, WhatsApp, Zoom, Skype, RingCentral, Vonage, Rebtel y muchos otras aplicaciones de llamadas y mensajería.

VI. RTP

El protocolo de transporte en tiempo real (*Real-Time Transport Protocol*, o RTP) es un protocolo diseñado para la transmisión de datos en tiempo real, como audio y video, a través de redes IP. Es ampliamente utilizado en aplicaciones de videoconferencia, VoIP y transmisión en vivo.

A. Funcionamiento

RTP trabaja en conjunto con otros protocolos para garantizar la calidad del servicio. Normalmente opera sobre UDP y no ofrece mecanismos de retransmisión, priorizando la entrega rápida de paquetes. Su funcionamiento incluye:

- **Encapsulación de datos**: Los datos (audio, video, etc.) se encapsulan en paquetes RTP, que incluyen información adicional como marcas de tiempo y números de secuencia.
- **Sincronización**: RTP utiliza marcas de tiempo para sincronizar diferentes flujos de datos, como audio y video.
- **Gestión de sesiones**: Trabaja junto con RTCP (*Real-Time Control Protocol*) para supervisar la calidad del servicio y sincronizar flujos en sesiones multimedia.

RTP utiliza números de puerto asignados dinámicamente, con un rango típico entre 1024 y 65535.

B. Ventajas

- **Baja latencia**: Ideal para aplicaciones en tiempo real, como llamadas de voz y transmisiones en vivo.
- **Compatibilidad**: Funciona con una amplia gama de protocolos y aplicaciones multimedia.
- **Extensibilidad**: Soporta diferentes tipos de datos y códecs.

C. Limitaciones

- **Falta de confiabilidad**: Al operar sobre UDP, no garantiza la entrega de los paquetes ni el orden de los mismos.
- **Complejidad**: Requiere configuraciones adicionales para manejar la calidad del servicio (QoS) en redes congestionadas.
- **Seguridad**: Por defecto, RTP no cifra los datos; se requiere SRTP (*Secure RTP*) para proteger las comunicaciones.

D. Aplicaciones Típicas

RTP es esencial en aplicaciones multimedia, tales como:

- **VoIP**: Utilizado en sistemas de telefonía por Internet.
- **Videoconferencias**: Herramientas como Zoom o Microsoft Teams.
- **Streaming en vivo**: Plataformas como YouTube Live o Twitch.

VII. Conclusiones

A través de esta monografía, se realizó un análisis detallado de diversos protocolos de comunicación en redes, explorando sus fundamentos, ventajas, limitaciones y aplicaciones. Este trabajo permitió no solo profundizar en el conocimiento técnico de herramientas esenciales como DHCP, Telnet, RTP, FTP y VoIP, sino también reflexionar sobre su impacto en el desarrollo y funcionamiento de los sistemas modernos de comunicación.

En el desarrollo de esta investigación, se destacaron algunos puntos clave:

1) Relevancia de los Protocolos: Cada protocolo cumple un rol específico dentro de las redes de comunicación, desde la automatización en la asignación de configuraciones de red (DHCP) hasta la gestión de datos en tiempo real (RTP) o la transmisión eficiente de archivos (FTP). Esto resalta la necesidad de una integración efectiva entre tecnologías para lograr redes funcionales y robustas.
2) Evolución Tecnológica: Protocolos como Telnet evidencian cómo las tecnologías inicialmente innovadoras pueden quedar obsoletas frente a opciones más seguras y eficientes, como SSH. Esto subraya la importancia de la constante innovación y actualización en el campo de las redes.
3) Impacto en Aplicaciones Prácticas: Desde entornos locales hasta plataformas globales, los protocolos estudiados son fundamentales para aplicaciones modernas como videollamadas, streaming, gestión de servidores y más. Esto refuerza la idea de que su correcto entendimiento e implementación son esenciales para garantizar servicios de alta calidad.
4) Reflexión sobre la Seguridad y la Confiabilidad: Un tema recurrente en los protocolos estudiados es la necesidad de mejorar la seguridad, especialmente en aquellos que transmiten información en texto plano, como FTP o Telnet. Este punto enfatiza el desafío constante de equilibrar simplicidad y funcionalidad con la protección de los datos.

Finalmente, este trabajo no solo permitió consolidar conocimientos técnicos, sino también reflexionar sobre la importancia de adoptar una visión crítica al analizar tecnologías, considerando sus fortalezas, debilidades y aplicaciones prácticas. En un mundo cada vez más interconectado, comprender estos fundamentos es esencial para abordar los retos de las redes del presente y del futuro.

REFERENCIAS

[1] www.ionos.es/digitalguide/servidores/configuracion/que-es-el-dhcp-y-como-funciona
[2] https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
[3] https://www.geeksforgeeks.org/introduction-to-telnet/
[4] https://esperanza7989.wordpress.com/wp-content/uploads/2012/02/tema5-ftp.pdf
[5] https://www.biblioinfo.com.ar/wp-content/uploads/2024/09/FTP-Y-TFTP.pdf
[6] https://static.hostalia.com/news/noviembre10/sabes-como-utilizar-el-protocolo-FTP.pdf
[7] https://ribuni.uni.edu.ni/1261/1/25717-MIIITIP.pdf
[8] https://www.mheducation.es/bcv/guide/capitulo/8448171330.pdf
[9] B. Hartpence *Packet Guide to Voice over IP* United States of America (2013)
[10] https://biblus.us.es/bibing/proyectos/abreproy/12135/fichero/Capítulo2.pdf
[11] https://www.publish0x.com/0fajarpurnama0/simple-introduction-to-computer-network-and-the-internet-xwpmdk?a=4oeEw0Yb0Btid=youtube
[12] https://coreemu.github.io/core/services/utility.html