



Universidad Autónoma del Estado de México

Centro Universitario UAEM Valle de Chalco

**IMPLEMENTAR TFTP EN ESCUELAS DE MEDIA SUPERIOR EN
SITUACIONES DE CATASTROFE UTILIZANDO CISCO**

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERA EN COMPUTACIÓN

P R E S E N T A

ITZEL AIRAM GARCÍA RAMÍREZ

ASESOR:

M. EN C.C. RICARDO JAVIER BUCIO LÓPEZ

Revisor: I. EN C. JOSÉ ANTONIO VILLARRUEL TÉLLEZ

Revisora: DRA. ANABELEM SOBERANES MARTÍN

VALLE DE CHALCO SOLIDARIDAD, MÉXICO

OCTUBRE 2025.



CUVCH

**IMPLEMENTAR TFTP EN ESCUELAS DE MEDIA
SUPERIOR EN SITUACIONES DE CATASTROFE
UTILIZANDO CISCO**

ÍNDICE

I	RESUMEN.....	8
II	ANTECEDENTES	10
	2.1 Justificación.....	18
III.	IMPORTANCIA DEL PROBLEMA.....	20
IV.	PLANTEAMIENTO DEL PROBLEMA.....	22
	4.1 Pregunta de Investigación	23
V.	MARCO TEORICO.....	24
	5.1 Protocolos de comunicación de datos	24
	5.1.1 Protocolos a nivel de aplicación de Internet.....	24
	5.1.2 Tipos de Protocolos de Comunicación	26
	5.2 APIs	27
	5.2.1 Tipos de APIs	27
	5.2.2 Arquitectura de APIs	29
	5.3 Comunicación de datos basados en TCP/IP para redes	29
	5.4 Modelo de arquitectura del protocolo TCP/IP	30
	5.4.1 Capa de Interfaz de Red	31
	5.4.2 Capa de Internet	43
	5.4.3 Capa de Transporte	46
	5.4.4 Capa de Aplicación	49
	5.5 Transmisión de Datos.....	58
	5.6 Software de uso para la simulación y uso del protocolo TFTP	58
	5.6.1 Cisco Packet Tracer	59
VI	MÉTODO Y TÉCNICAS DE INVESTIGACIÓN.....	60

VII.	PRESENTACIÓN Y DISCUSIÓN DE RESULTADOS	64
7.1	Análisis de Requerimientos	64
7.1.1	Requerimientos Funcionales.....	64
7.1.2	Requerimiento no Funcionales.....	64
7.2	Herramientas y tecnologías a utilizar	65
7.2.1	Para entorno de software y simulación.....	65
7.2.2	Para entorno físico	65
7.3	Diseño en Cisco Packet Tracer.....	66
7.4	Implementación (Desarrollo del funcionamiento de la simulación del uso de protocolo TFTP en Cisco Packet Tracer)	69
7.5	Verificación del funcionamiento del protocolo TFTP	75
7.6	Representación de forma Física	78
7.6.1	Implementación y Verificación del funcionamiento del protocolo TFTP con software tftp32.....	80
VIII.	CONCLUSIONES Y SUGERENCIAS.....	91
8.1	Conclusiones.....	91
8.2	Sugerencias	92
IX.	REFERENCIAS.....	93

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Vint Cerf y Robert Kahn.	11
Ilustración 2. Modelo Protocolo TCP/IP.	12
Ilustración 3. Diferencia entre TCP y UDP.	13
Ilustración 4. Comparación entre modelo OSI y TCP/IP.	14
Ilustración 5. Protocolos en capa de Aplicación (Modificado de (Meza, 2024)).	14
Ilustración 6. FTP y TFTP	15
Ilustración 7. Conjunto de protocolos TCP/IP. Fuente: https://www.ibm.com/docs/es/aix/7.2.0?topic=protocols-internet-application-level	25
Ilustración 8. Esquema representativo de las API.	28
Ilustración 9. Funcionamiento de APIs.	29
Ilustración 10. Modelo TCP/IP.	31
Ilustración 11. Redes involucradas.	32
Ilustración 12. Esquema de Red LAN.	33
Ilustración 13. Modelo OSI.	35
Ilustración 14. Capa Física modelo OSI.	36
Ilustración 15. Conexiones LAN y WAN en router.	37
Ilustración 16. Posiciones Estandarizadas.	37
Ilustración 17. Capa 2 del modelo OSI.	37
Ilustración 18. Capa de Red modelo OSI.	38
Ilustración 19. Capa de Red.	39
Ilustración 20. Formato de datos en Bits.	40
Ilustración 21. Enrutamiento función.	41
Ilustración 22. Representación gráfica de redes informáticas principales.	42
Ilustración 23. Diagrama representativo de una red WLAN.	43
Ilustración 24. Representación gráfica de ARP.	45
Ilustración 25. Representación gráfica de funcionamiento de ICMP.	46
Ilustración 26. Capa de Transporte.	47

Ilustración 27. Proceso de una conexión cliente-servidor.	48
Ilustración 28. Función gráfica del UDP.	49
Ilustración 29. Diferencia de búsqueda de sitio web.	50
Ilustración 30. Función DHCP.	51
Ilustración 31. Función de puertos FTP.	53
Ilustración 32. Modo activo.	54
Ilustración 33. Modo pasivo.	55
Ilustración 34. Demostración gráfica de la Transferencia de datos.	58
Ilustración 35. Logo software de Cisco Packet Tracer.	59
Ilustración 36. Modelo de cascada.	62
Ilustración 37. Abriendo la aplicación.	66
Ilustración 38. Servidor virtual TFTP de Cisco.	67
Ilustración 39. Switch virtual de Cisco.	67
Ilustración 40. PC virtual de Cisco.	68
Ilustración 41. Router virtual de Cisco.	68
Ilustración 42. Diseño de escenario virtual.	69
Ilustración 43. Servicios/Protocolos apagados.	70
Ilustración 44. Protocolo TFTP activo.	71
Ilustración 45. IP Configuration.	71
Ilustración 46. Asignación de Dirección IP.	72
Ilustración 47. Asignación de Dirección IP.	73
Ilustración 48. Preconfiguración de la Interfaz Fa0/0 a utilizar.	74
Ilustración 49. Asignación de IP en CLI.	75
Ilustración 50. Demostración de lista de Ayuda usando (?).	75
Ilustración 51. Uso de comando TFTP.	76
Ilustración 52. Archivo correctamente copiado.	76
Ilustración 53. Archivo Transferido correctamente.	77
Ilustración 54. Software tftp32 Download.	78
Ilustración 55. Historia de Descargas.	79
Ilustración 56. Interfaz de software tftp32.	79

Ilustración 57. Ventana del CMD.....	80
Ilustración 58. Dirección IP de pc Servidor.....	81
Ilustración 59. Dirección IP de pc Cliente. Fuente: Propia.....	81
Ilustración 60. Muestra de paquetes enviados de servidor a cliente.....	82
Ilustración 61. Muestra de paquetes enviados de cliente a servidor.....	83
Ilustración 62. Sección de "tftp client". Fuente: Propia.....	83
Ilustración 63. Campos a llenar.....	84
Ilustración 64. Puerto 69 de TFTP.....	85
Ilustración 65. Carpeta con solo archivos determinados del software tftp32.....	86
Ilustración 66. Demostración del equipo sin archivo recibido aún.....	86
Ilustración 67. Transferencia del archivo.....	87
Ilustración 68. Transferencia en curso en pc cliente.....	87
Ilustración 69. Archivo transferido al cliente exitosamente.....	88
Ilustración 70. Archivo funcionando en Pc cliente después de la transferencia.....	89
Ilustración 71. Escenario Virtual Final.....	90
Ilustración 72. Escenario Físico Final Servidor-Cliente.....	90

I. RESUMEN

Las escuelas de media superior del Estado de México ubicadas dentro del municipio de Ixtapaluca no cuentan con un respaldo de información para salvar la información importante de todo el alumnado y personal de la institución. Ya que estas se encuentran vulnerables y propensas a una inundación causada en los tiempos de lluvias y estas pueden causar el desborde del canal ubicado a algunos metros que genera inundaciones en las calles, casas y por supuesto en las escuelas.

En el presente trabajo se diseñó e implemento una simulación del uso del protocolo TFTP (Trivial File Transfer Protocol) para tener un respaldo del sistema y de datos ante alguna situación de catástrofe. Esto con la finalidad de no llegar a la pérdida total de los archivos y datos de información de cada uno de los alumnos y trabajadores de la institución.

El protocolo TFTP es una buena opción ya que este, es un protocolo de conexión y solo se necesita saber el nombre o archivo a transferir, aunque no es muy seguro, es un protocolo que facilita su manipulación ya que este no requiere de una contraseña para autenticar al usuario.

La simulación para representar la funcionalidad de protocolo TFTP se desarrolló haciendo uso de materiales de software como Cisco Packet Tracer en su versión 8.2.1.

Como herramientas a utilizar para la representación del uso del protocolo y mostrar el resguardo y transferencia de sistema, archivos o datos se utilizaron los siguientes dispositivos: servidor TFTP, router y computadora. Esto para una manera simulada.

También se puede realizar utilizando una computadora principal que es donde se encuentran ubicados los datos o archivos de los cuales se pretende hacer su transferencia a otro dispositivo de almacenamiento, en este caso una segunda computadora para así tener un respaldo de información seguro. Se puede hacer en la segunda computadora de forma nativa o creando una máquina virtual para su representación física.

Al finalizar la representación simulada dentro de Cisco Packet Tracer o de forma física y haber demostrado la función del protocolo tftp (Trivial File Transfer Protocol) se llevó a cabo la implementación de exponerlo ante las autoridades de la zona de escuelas de Ixtapaluca, principalmente en la escuela Preparatoria Oficial No. 122 para las áreas de control escolar y dirección general ubicadas en la planta baja del edificio, ya que es una institución más vulnerable a casos de inundación por desborde de canal que se encuentra ubicado a algunos metros de ella y esta propensa a poder llegar a pérdidas totales de los archivos y equipos de cómputo.

Palabras clave: Información, Transferencia, Implementación, Simulación, Tecnología y Redes.

II. ANTECEDENTES

A continuación, se presentan los datos más relevantes que existen de acuerdo con las investigaciones encontradas, relacionados con el proyecto de investigación presentado en la tesis.

Una computadora es como una mente que puede apilar, jugar, guardar y dar datos. Lo hace siguiendo serie de instrucciones, como un mapa siguiendo instrucciones. A estos pasos se les llama programas (software).

El software, es la zona más rara de las computadoras o dispositivos donde se puede comunicar y observar datos de manera gráfica. Si no hay programas, las máquinas de hoy no serán tan normales y casi nadie las entendería bien para usarlas fácilmente.

A inicios de los mandatos de internet allá por la década de 1970, se hizo clara la falta de un conjunto estandarizado de reglas fijas para facilitar la comunicación entre todos sin tanto problema.

TFTP es un sistema antiguo creado por primera vez en 1980 a través de IEN 133 (Nota Experimental de Internet 133), algo así como una nota de pruebas de internet. Se hizo oficial al año siguiente en el RFC 783 en ese momento. Hoy en día, el modo de actuar esta en el RFC 1350 señala el andar estandarizado de Internet. Con su actualización aparecido en el año 1992, provocó sobre todos los cambios en el rato de espera y en el archivo transferido (Villanueva, 2025).

Vinton G. Cerf es vicepresidente y principal promotor de internet de Google, un defensor líder de la red. Buscar nuevas tecnologías y programas raros para el “Padre de Internet”. Vint, con Robert Kahn, ideó los protocolos TCP/IP y el diseño base de Internet.

El Dr. Robert E. Kahn concibió la idea de las redes de arquitectura abierta. Es coinventor de los protocolos TCP/IP y tuvo que ver con el Programa de Internet de DARPA. El CNRI es como el ayudante del equipo de la Secretaría del Grupo de Trabajo de Ingeniería de Internet (IETF) Ilustración 1 (Bush, 2024).



Ilustración 1. Vint Cerf y Robert Kahn.

Fuente: <https://georgewbush-whitehouse.archives.gov/government/cerf-kahn-bio.html>

¿Qué son los Protocolos TCP/IP?

El TCP/IP son conjuntos de normas para formatos de mensaje y procedimientos que permiten a las computadoras y los programas intercambiar información, dentro de los protocolos TCP/IP hay identificación del grupo de protocolos de red que hacen posible esa transferencia de datos dentro de las redes. El termino de protocolos se puede interpretar en términos de niveles o capas (IBM, 2021).

Las siglas TCP/IP hace referencia al grupo de protocolos TCP: es el Protocolo de Control de Transmisión que deja establecer conexión para el intercambio de dato o información entre los equipos anfitriones. Este protocolo proporciona un transporte confiable de los datos.

Y el IP o Protocolo de Internet, usa direcciones en serie de cuatro octetos con un formato de punto decimal (como ejemplo 75.4.160.25). este protocolo lleva los datos a otras computadoras en la red.

Este cuenta con las capas del modelo TCP/IP las cuales se muestran en la Ilustración 2.

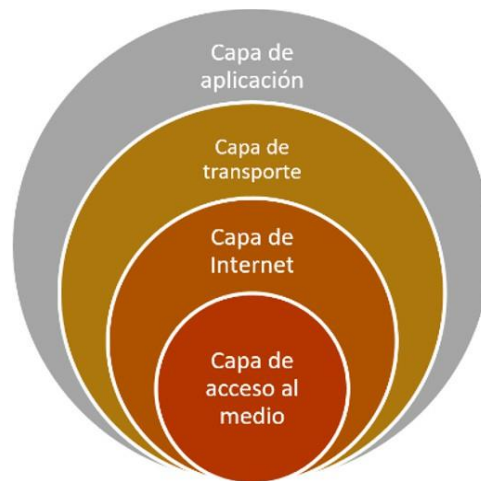


Ilustración 2. Modelo Protocolo TCP/IP.

Fuente: <https://www.profesionalreview.com/2020/03/21/protocolo-tcp-ip/>

En estas capas/niveles se ve justo en la parte de usar la Capa de Aplicación está el protocolo TFTP. Este protocolo es la base de la simulación para las cosas que pasan en la escuela.

Capa o nivel de Aplicación

Esta arriba del TCP/IP, el cual le da alas redes FTP, TFTP, Telnet o SMTP, que hablan con las capas de abajo (con TCP o UDP).

El TCP (Protocolo de Control de Transmisiones) usa enlaces como si tuviera lazos invisibles y el UDP (Protocolo de Datagramas de Usuario) no usa, va sin conexiones, como si fuera libre, ahí lo que los hace diferentes.

Este modelo tiene capas que se parecen a las del modelo OSI, aunque hace más cosas diferentes.

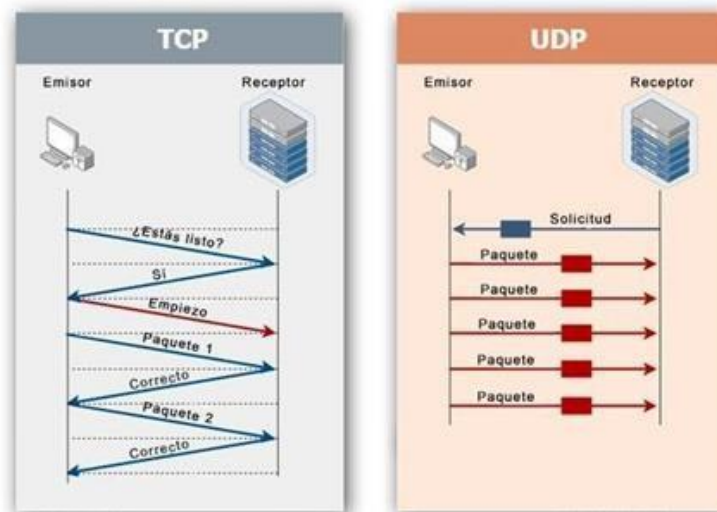


Ilustración 3. Diferencia entre TCP y UDP.

Fuente: <https://carballar.com/que-es-tcp-y-udp>

¿Qué es un Modelo OSI?

Es un esquema conceptual hecho por la Organización Internacional para la estandarización, ayuda a varios modos de comunicación se junten usando reglas fijas para todos. OSI decide un estándar para varios sistemas de equipos puedan comunicación entre ellos (Cloudflare, 2024).

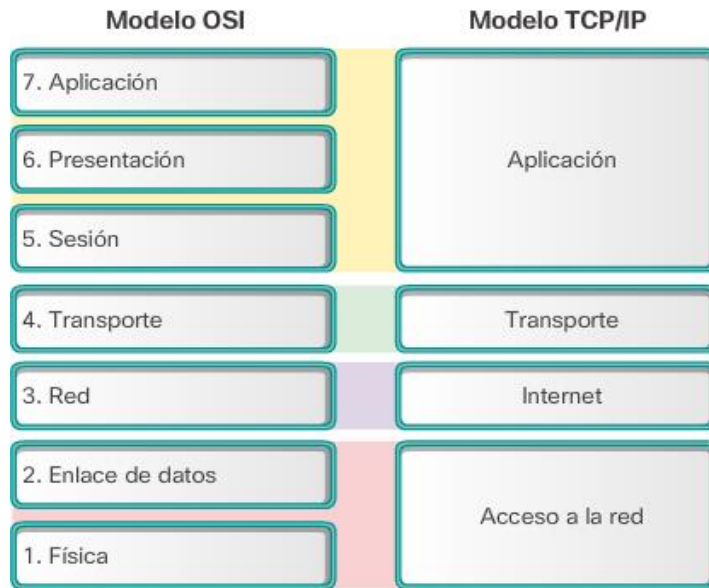


Ilustración 4. Comparación entre modelo OSI y TCP/IP.

Fuente: <https://interpolados.wordpress.com/2017/03/01/comparacion-entre-el-modelo-osi-y-el-modelo-tcpip/>

Tal como se mira en la Ilustración 4, dentro de la capa de Aplicación del modelo TCP/IP incluye tres pisos cinco, seis y siete los cuales constan en la Sesión, Presentación y la Aplicación del modelo OSI. Dentro de este nivel de aplicación hay diversos tipos de protocolos.



Ilustración 5. Protocolos en capa de Aplicación (Modificado de (Meza, Platzi, 2024)).

TFTP se unió al grupo de los protocolos que ya existían dentro de la capa de aplicación, hecho para ser algo simple, liviano y fácil de usar, por lo cual no es tan seguro como los otros protocolos.

El protocolo TFTP es fácil, como pasar los archivos sin tanto lío. Está diseñado para ser pequeño y de fácil de usar, así que solo lee y guarda archivos desde o hacia un servidor lejano, no puede mostrar carpetas y en la actualidad no pide clave de autenticación de usuarios para entrar (Oracle, 2014).

TFTP salió como un protocolo FTP más fácil, pero este no permite ver una lista de archivos en una carpeta, no puedes borrar cosas, ni cambiarles el nombre, tampoco hace otras acciones que lo hace versátil que FTP.

Algunas máquinas, como las computadoras sin disco, clientes ligeros y routers pueden prenderse desde la red en lugar de hacerlo desde un disco duro de la zona. Ya que TFTP usa UDP, su código de protocolo es básicamente chico si lo comparamos con el protocolo de FTP (Villanueva, 2025).

Como ya se mencionó el protocolo TFTP salió de FTP así que va dentro del desarrollo donde se encuentra este, en la capa de aplicación, ambos son protocolos y hacen la función de una transferencia de archivos, datos e información.

Diferencia entre los protocolos FTP y TFTP:

FTP	TFTP
<ul style="list-style-type: none">• Se basa en TCP durante la transferencia.• Utiliza los puertos 21 y 20.• Requiere de una contraseña para autenticar al usuario.	<ul style="list-style-type: none">• Se basa en UDP ya que es un protocolo sin conexión.• Utiliza el puerto 69.• Solo necesitas saber el nombre del archivo que estás intentando descargar

Ilustración 6. FTP y TFTP

(Elaborado a partir de (PC Solución, 2025)).

¿Qué es Autenticación?

Es el proceso que usan las empresas para confirmar que solo las personas, servicios y aplicaciones adecuados con los permisos correctos pueden acceder a los recursos de la organización. En la autenticación es fundamental de la ciberseguridad porque la prioridad de los infiltrados es obtener accesos a los sistemas no autorizados (Microsoft, 2024).

Entonces, la autenticación es un parámetro o filtro de seguridad como la contraseña que colocan los usuarios para poder acceder a la computadora y obtener la información de una manera más segura, confiable y así fortalecer la integridad del propietario, ordenador, información, etc.

Confidencialidad de la información: es tener la autorización únicamente al usuario permitido para acceder a los datos sin forzar ni sobrepasar la seguridad del equipo y la información.

Aplicación de TFTP en ambientes Cisco.

En Cisco, usa servidores de Internet , como los de protocolo trivial de transferencia de archivos (TFTP). Hacen cambios de archivos y apoyan el cuidado de los equipos Cisco, así como otras cosas más:

- Cosas nuevas del software: los servidores TFTP se usan para darles a los aparatos de red, como los switch o los routers, arreglos o en cómo funcionan los protocolos.
- Configuración de dispositivos de red: los servidores tftp se utilizan para almacenar archivos de configuración de los dispositivos de red.

- Recolección de datos y registros: centralizan la recopilación de los registros, capturas de red u otros datos, esto simplifica el proceso de recuperación y administración de datos con fines de análisis.
- Pruebas y resolución de problemas de red: ayudan a los escenarios de pruebas y resolución de problemas de red, permite que los usuarios transfieran los archivos para comprobar conectividad, velocidad o simplemente verificar que la red funcione (Cisco, 2025).

El protocolo tftp trae un avance tecnológico por el cual viene a lograr la transferencia de estos archivos importantes que la escuela maneja con gran información confidencial de cada alumno inscrito en la institución educativa.

Ya que, tftp es un protocolo con una versión renovada al protocolo FTP, aunque le falte tener muchos privilegios de los que tiene el FTP, TFTP puede llegar a ser un protocolo seguro y utilizado con cotidianidad en lugares conectados en una misma red local.

2.1 Justificación

La razón de llevar a cabo esta implementación acerca del protocolo TFTP es porque puede servir de mucho aprender el uso de este, para la transferencia, resguardo y recuperación de la información llevando a cabo un buen uso y manejo de toda la información que se encuentra dentro de la institución de media superior llevando de un punto de partida hasta el punto de llegada de esa información de cada uno de los alumnos con un valor significativo para la escuela brindando disponibilidad de la información personal de cada uno de las personas.

Este protocolo es el encargado de recuperar la información o simplemente de transferirla de un lado a otro, para después hacer un respaldo seguro y así implementar el registro de cada información personal de una manera digital.

Se pretende que en el momento de que la institución se encuentre en una situación de catástrofe natural como lo puede ser una inundación de factor más probable a suceder por la ubicación en la que esta se encuentra y se pueda llevar a cabo el uso de protocolo TFTP, dando solución pronta de poder extraer los datos e información ubicada en uno o varios ordenadores del área encargada dentro de la escuela como lo es control escolar por medio de la implementación de simulación en Cisco, en donde la situación presentada no se permita el acceso a la institución, entonces para no perder tiempo esto se puede hacer solo teniendo la dirección ip de la computadora y el nombre del archivo a transferir para así poder llevar a cabo dicha implementación y marcha de la función del protocolo sin necesidad de estar presente en el lugar dando la demostración a través de la simulación.

Haciendo ya la implementación de una simulación con el uso del protocolo se espera obtener de manera satisfactoria los datos e información requerida al momento sin necesidad de perder tiempo para uno mismo y para los involucrados

teniendo en cuenta que pueden presentarse dificultades como puede llegar a ser la pérdida de dicha información, errores de enlace, caída por interferencia de datos, errores humanos entre otros. Tratando de evitar justamente este tipo de anomalías.

Si dentro de la institución donde se lleve a cabo la implementación del protocolo TFTP se haría de una forma simulada en la plataforma de Cisco Packet Tracer esto dejando a criterios y requerimientos del usuario. Pero hay una posibilidad de hacer una representación simulada dentro de esta plataforma con la finalidad de que se aprenda el uso correcto a llevarse a cabo, de igual forma esta investigación está destinada a ser implementada en base a la realización de una simulación en Cisco para ver su función y alcance de este protocolo.

La finalidad de tener herramientas donde se pueden hacer simulaciones es para por supuesto simular una situación en la vida real y centralizar más la perspectiva de las cosas reales a las cuales después si se van a tener que presentar ya de forma física donde ya no puedo haber errores sino soluciones completamente acertadas, más que nada para la ayuda de la institución quien apliqué este protocolo.

Esta es una forma de empezar a informarse y adentrarse a practicar el uso, manejo y función del protocolo TFTP, para así obtener resultados satisfactorios a la hora de ejecución y así mismo el personal a usar este método de transferencia de archivos tenga el conocimiento claro y bien aprendido para que sin ningún problema. Al igual llevar este uso a los alumnos y darles un enfoque a que se involucren con las redes.

III. IMPORTANCIA DEL PROBLEMA

Las escuelas ubicadas dentro del municipio de Ixtapaluca la gran mayoría de ellas no cuentan con un respaldo de información segura para salvar guardar los datos e información importante de todo el personal y alumnado de dicha institución.

La falta de respaldo de información en las escuelas ubicadas en el municipio de Ixtapaluca representa un riesgo crítico, especialmente en instituciones de nivel medio superior, una de ellas se encuentra cerca de un canal de aguas negras propenso a desbordamiento en temporadas de lluvias quedando fuera de los alcances de las personas, que al igual por un error humano todo tipo de información igual queda en riesgo a posibles pérdidas. Esta vulnerabilidad compromete directamente la integridad de datos fundamentales, como los registros administrativos, calificaciones, historial académico y datos personales del alumnado y personal de trabajo.

Por otro lado, la ubicación de las áreas administrativas en la planta baja del edificio principal de la institución aumenta significativamente el riesgo de daños directos a los equipos y por supuesto a los expedientes físicos, engrandeciendo la vulnerabilidad de la institución.

Implementar un método de respaldo eficiente y accesible es crucial para garantizar la continuidad operativa y la protección de los datos críticos ante eventos catastróficos o simplemente errores humanos.

Teniendo en cuenta la importancia de realizar este tipo de respaldo de información evitarían algunas cuestiones, como pudieran ser :

La interrupción de operaciones: pérdida de datos administrativos afectaría toda la gestión y control de la escuela, dificultando procesos esenciales como la reinscripción, certificación y tramites académicos.

Afectar al alumnado: podrían enfrentar procesos complicados para tramites, solicitudes en su trayectoria académica e incluso retrasos con sus estudios y así tener problemas para continuar su educación en siguientes instituciones.

Problemas legales y administrativos: la falta de respaldos puede llevar a conflictos legales por la incapacidad de demostrar registros oficiales o cumplir con regulaciones educativas.

Pérdida de confianza: los padres, alumnos y docentes podrían perder la confianza en la institución por irregularidades o falta de seguridad a la integridad de su información, lo que impactaría en la reputación de la institución.

IV. PLANTEAMIENTO DEL PROBLEMA

El protocolo TFTP se emplea en aquella problemática que pueda presentarse para la escuela y esta pueda enfrentarse a situaciones provocadas por una catástrofe natural hablando de inundaciones, desborde de canal cerca de la escuela o simplemente errores humanos, y donde se pueda ver afectada con la interrupción de la corriente eléctrica, daños en la infraestructura de red, no tener accesos a la escuela o computadoras y hasta pérdidas totales de los equipos de cómputo dentro de las áreas de mayor importancia para la concentración de la información importante y general.

Ya que estas áreas y equipos se encuentran en una zona de planta baja quedando vulnerables a que suceda este tipo de situaciones o no llegar a esos extremos y simplemente un error humano por cualquier personal a cargo del uso de dicha información.

Ante este problema que puede volver a llegar a situarse mayormente en las temporadas de lluvia en la escuela de media superior, el uso del protocolo TFTP puede ser una oportunidad de llevarse a cabo y este haga la recuperación de datos importantes como los son, expedientes médicos de cada alumno inscrito en dicha institución, baucher de pago ante cualquier trámite solicitado ya sea de pagos de inscripción o reinscripción, de credencial, tramites, etc. Aunque de entrada se sabe que este protocolo es algo arriesgado en su uso basándose en la seguridad ya que, no es un método muy confiable ni seguro por llevar a cabo pero que puede cumplir con lo requerido de una transferencia de archivo. Se necesita dar un buen curso de inducción al uso del protocolo en simulación para aquellos responsables a cargo de las áreas donde se manipule todo tipo de información ya que se trata de información confidencial e importante del plantel.

4.1 Pregunta de Investigación

Por lo planteado en este trabajo se propone las siguientes preguntas de investigación:

¿Cómo se podrá implementar una simulación de transferencia de archivos en la plataforma Cisco de una escuela de media superior utilizando TFTP garantizando el resguardo de información?

¿Cómo es posible llevar a cabo el protocolo TFTP para la obtención de archivos en una situación real?

¿Por qué la implementación facilitaría y disminuiría tiempos de recolección de archivos o información en caso de situaciones de catástrofe natural para escuelas de media superior?

V. MARCO TEORICO

En el presente trabajo se realiza la simulación del uso del protocolo TFTP para la demostración de cómo llevar a cabo la transferencia de archivos utilizando este protocolo dentro de la escuela de media superior o escuelas dentro del municipio de Ixtapaluca, así estas empiecen a implementar a un respaldo de resguardo de su información de una forma de situación real.

Por lo tanto, es necesario mencionar algunos conceptos de protocolos de comunicación de datos comprender la lectura.

5.1 Protocolos de comunicación de datos

Un protocolo de comunicación abarca diversas normas que deben cumplir los equipos y softwares que intervienen en la comunicación de los datos entre las computadoras. Si los equipos no tienen las normas es imposible que la comunicación se realice. Hoy en día los protocolos de comunicación admiten el reconocimiento de mensajes y compresión de datos, lo cual la comunicación de red puede ser confiable y con un buen rendimiento (SDI Industrial, 2025).

Los protocolos de comunicación son estándares formados por restricciones, formatos y procedimientos que permiten el intercambio de información para lograrse una correcta comunicación entre servidor y dispositivo a una red.

5.1.1 Protocolos a nivel de aplicación de Internet

Cuando una aplicación necesita enviar datos a otra aplicación, envían la información primero a los protocolos de nivel de transporte para ahí preparar la información para la transmisión.

Los protocolos de nivel de Internet abarcan cosas como:

- Protocolo de nombre de terreno virtual.
- Plan para mover expedientes.
- Puerta de enlace libre.
- Protocolo de transferencia de archivos sin importancia.

La gran mayoría en las que utilizamos los equipos ya sea para enviar correos, mensajes, ver alguna plataforma de streaming u obtener alguna indicación para llegar a un sitio, todas esas acciones por decir algunas solamente, ellas dependen de la comunicación entre ellos. Pueden ser equipos de distintas marcas o inclusive encontrarse en zonas del mundo diferentes. Los programas que los utilizan pueden hablar distintos lenguajes humanos e informáticos.

TCP/IP implementan protocolos de internet de nivel superior en el nivel de programa de aplicación. La Ilustración 7 muestra distintas capas del conjunto de protocolos TCP/IP. El entendimiento de la ilustración es iniciando de la parte superior a la inferior (IBM, 2024).

- La capa de aplicaciones consta de la Aplicación.
- La capa de transporte contiene el UDP y TCP.
- La capa de red contiene la Interfaz de red (hardware).
- Finalmente, la capa de hardware contiene la red física.

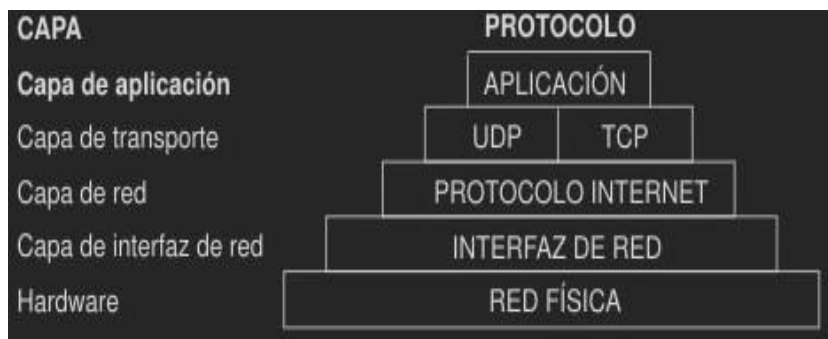


Ilustración 7. Conjunto de protocolos TCP/IP. Fuente:

<https://www.ibm.com/docs/es/aix/7.2.0?topic=protocols-internet-application-level>

En ningún protocolo del nivel de aplicación se proporciona las API ya que TCP/IP no las suministra

5.1.2 Tipos de Protocolos de Comunicación

Comunicación punto a punto

Estos métodos son vistos los mas antiguos y básicos, son usados para la comunicación por línea de datos entre dos puntos. En la primera máquina se le llama orden y en la máquina dos, respuesta.

Protocolo de comunicación TCP/IP

Transfer Control Protocol / Internet Protocol (TCP/IP), es un modelo de envío de paquetes que tiene un conjunto de reglas de transporte y un idioma preestablecido para la red de Internet. Cuando una maquina quiere mandar un archivo a otra máquina, primero separa en pedazos chicos sin rebasar los 5 Kb (SDI Industrial, 2025).

La información se transporta por la red en cada uno de esos paquetes de forma independiente y llegará a la dirección de red que debe llegar y también la dirección del remitente quien recibirá la respuesta. Cada paquete toma la mejor ruta entre las estaciones de red, esto dependerá de los caminos o los obstáculos.

Protocolos de Trasmisión de paquetes

Dentro de estos protocolos se basan en la información contenida en aquellos datos que pasan por la red de comunicación, eliminando la responsabilidad de los equipos y las líneas de datos.

Aquí los datos se parten y luego se organizan en paquetes con datos de origen a destino y van pasando de equipo en equipo y así hasta llegar al destino.

Por lo siguiente, los dispositivos que forman las redes solo se restringen a leer direcciones medidas de los paquetes y luego seguir la entregar a la máquina indicada y así en secuencia hasta que el archivo termine su camino y llegue al final (SDI Industrial, 2025).

Protocolos para interactuar entre redes

Los nodos que desean comunicarse se encontraran conectados únicamente a una red de área local (LAN) y cada nodo tendrá asignado un valor propio.

Este protocolo suele administrar los sistemas de consulta que se encargan de controlar las comunicaciones y ordenarlas de alguna forma, ningún componente de la red toma iniciativa de la comunicación por eso sale de ahí el proceso consecutivo que ejerce cada paquete de la red.

5.2 APIs

API o Application Programming Interface, en español quiere decir Interfaz de Programación de Aplicaciones, son funciones y procedimientos que permiten integrar sistemas permitiendo que las funcionalidades puedan ser recicladas por otras aplicaciones o softwares.

Una API sirve para el intercambio de datos entre distintos tipos de aplicación y así automatizar los procedimientos y desarrollar nuevas funcionalidades.

5.2.1 Tipos de APIs

Básicamente hay cuatro tipos en lo que se refiere a sus políticas de uso compartido y son clasificadas por su arquitectura como de su uso, a continuación, se mencionan:

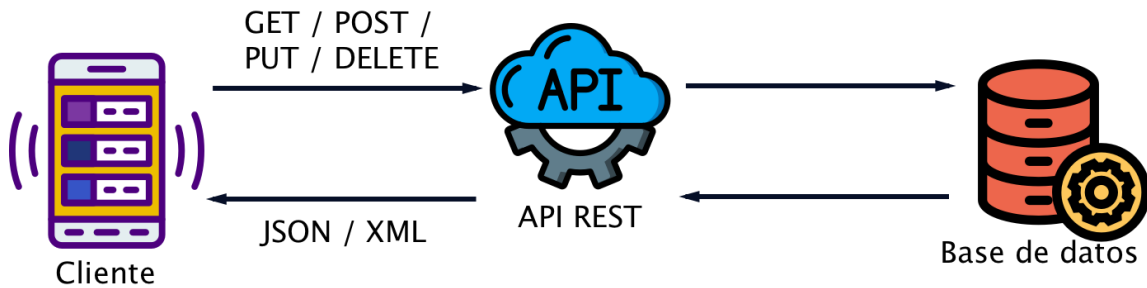


Ilustración 8. Esquema representativo de las API.

Fuente: <https://dossetenta.com/que-es-una-api-rest/>

API privadas:

Se ubican en las empresas de una manera interna y se usan para conectar datos y sistemas solo dentro de la empresa.

API públicas:

Son abiertas al usuario y cualquiera puede utilizarlas sin ninguna dificultad se tenga permiso o no.

API de socios:

Los desarrolladores externos autorizados tienen permitido entrar a aportar ayuda a la empresa.

API compuestas:

Son combinadas de dos o más API diferentes para llevar conductas o requisitos de alta complejidad del sistema.

5.2.2 Arquitectura de APIs

La construcción de las API suele explicarse en términos de cliente-servidor y la aplicación que manda la solicitud es desde el cliente y la que devuelve la respuesta se llama servidor.

Las API pueden funcionar de cuatro maneras distintas, según su motivo de creación y su momento, como ejemplo, el tiempo, la base meteorológica de la institución es el servidor y a donde llega la información es en la aplicación móvil se define como el cliente mostrado en la Ilustración 9 (AWS, 2024).

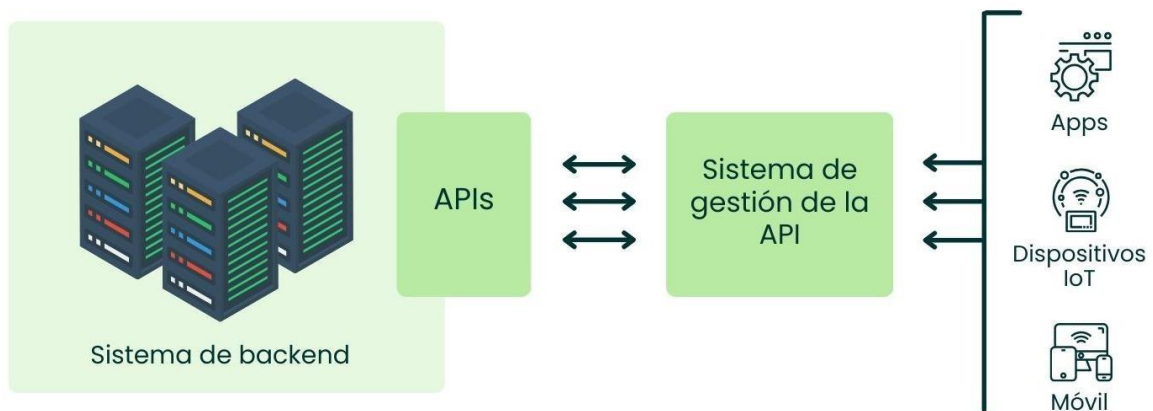


Ilustración 9. Funcionamiento de APIs.

Fuente: <https://dazzet.co/que-es/api/>

5.3 Comunicación de datos basados en TCP/IP para redes

Como se ha venido explicando, dentro de los protocolos tcp/ip hay distintas capas y en la que está enfocada este trabajo es en la capa de aplicación sin más, no dejando de lado las demás capas que componen al modelo TCP/IP.

5.4 Modelo de arquitectura del protocolo TCP/IP

Los Protocolo de Internet (IP) y TCP (Protocolo de Control de Transmisión) iniciaron a principios de 1980 y ARPANET los admitió en 1983, involucrada por cantidades de computadoras, centros de investigación militar y algunas empresas (Corona, 2004).

La arquitectura de los protocolos tcp/ip está basada en un modelo conceptual de cuatro pisos conocido como sistema DARPA, nombre del centro gubernamental de EE.UU. que desarrolló principalmente al TCP/IP.

Cada una de las capas de la estructura de protocolos corresponde a una o varias capas de modelos de siete niveles como el sistema OSI (Open Systems Interconnection) en español Interconexión de sistema abierto.

Del sistema DARPA las cuatro capas corresponden a: Aplicación, Transporte, Internet e Interfaz de Red, cada nivel corresponde a su categoría como se observa en la Ilustración 10.

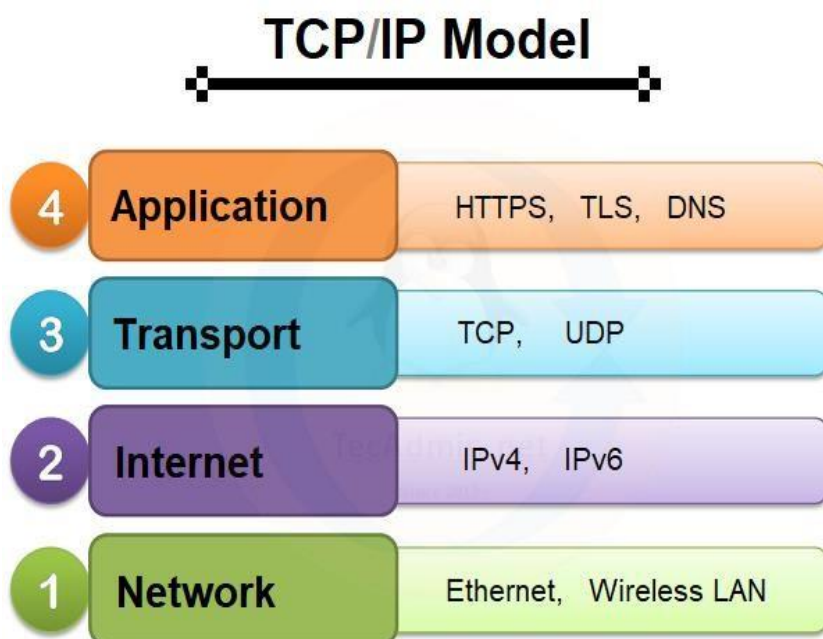


Ilustración 10. Modelo TCP/IP.

Fuente: <https://www.linkedin.com/pulse/what-tcp-ip-mohit-panchal-scq9c/>

5.4.1 Capa de Interfaz de Red

Primer nivel del protocolo TCP/IP pero la integra la capa física y la capa de enlace de datos dentro del modelo OSI. La Interfaz de Red también es nombrada por la capa de acceso a la red, encargado de poner los paquetes en el plano de la red y recibir los paquetes TCP/IP desde de la red.

Diversos tipos de red

Dentro de la capa de Interfaz de Red hay distintos tipos de redes involucradas en esta función de la capa, estas son utilizadas para conectar varios tipos de red. Abarca tecnologías LAN y WAN, tales como Ethernet o Token Ring y frame relay, es una tecnología cambio de paquetes para redes amplias, se permite la trasmisión de datos de forma eficiente y conectado a una red LAN.

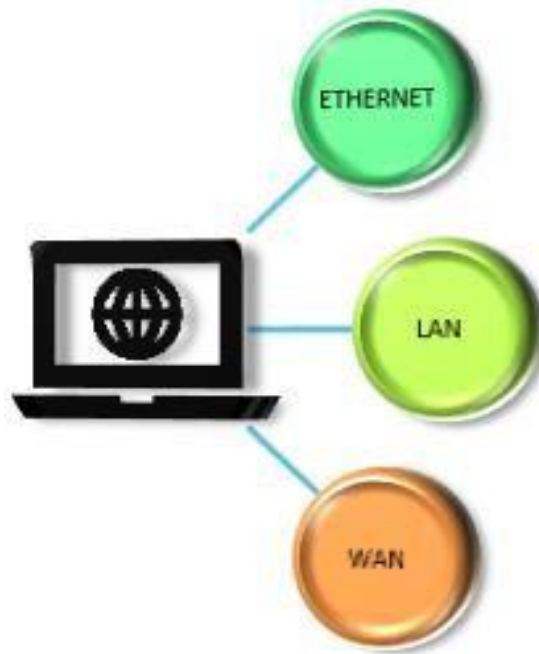


Ilustración 11. Redes involucradas.

Fuente: Propia.

Red de Área Local (LAN)

La red de área local es un conjunto de computadoras y dispositivos que están conectados en un área determinada como una escuela, un edificio, oficinas, etc. Es una red fácil y útil para unir en la misma red, así poder compartir archivos y hacer otras acciones.

Las LAN sirven como si una impresora está conectada con una computadora dentro de la misma casa u edificio, pero ubicadas en diferentes zonas sencillamente un envío de impresión resulta exitoso.

Como se muestra en la Ilustración 12, el esquema es que la impresora está conectada a la computadora PC1, la PC3 y las laptops 2 y 4 están conectadas en la misma red local a través del router (UsuarioDebian, 2008).

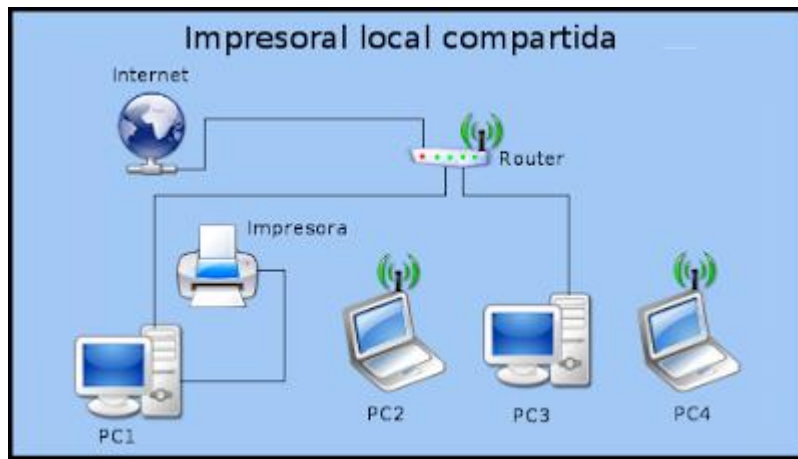


Ilustración 12. Esquema de Red LAN.

Fuente: <https://usuariodebian.blogspot.com/2008/03/impresora-local-compartida.html>

Características de LAN

- ✓ Son de red privada, la cual no puede ser controlada por un espacio externo.
- ✓ Opera con velocidad alta a comparación de redes WAN.
- ✓ Hay varios métodos de control de acceso como los token y ethernet.

Ventajas

- Compartir archivos y programas.
- Posibilidad de usar software de red.
- Seguridad.
- Compartir los recursos de la red.
- Gestión centralizada (Wordpress, 2025).

Desventajas

- Las computadoras deben encontrarse cerca geográficamente, sino el intercambio de información se dificulta.
- Alto riesgo de seguridad en aspectos de virus o hackers.
- Si no existe servidor puede ocasionar sobrecarga de máquinas.
- Si el servidor deja de funcionar la red se pierde (Wordpress, 2025).

Red Área Amplia (WAN)

Wide Area Network (WAN) conecta computadoras que se ubican a distancias considerables, permiten a los dispositivos se conectan de forma remota entre sí a través de una extensa red para su comunicación incluso cuando estén a distancia de km.

WAN es una red pública o podrían ser gestionadas por la empresa para conectar varias localidades a distancias grandes. El internet es un ejemplo básico para este tipo de red ya que conecta dispositivos de acceso a él a lo largo y ancho del mundo, sin en cambio a nivel técnico cualquier red que se expande en un área geográfica larga se le puede considerar una WAN aun su acceso sea privado (Fernández E. C., 2025).

Las WAN públicas son controladas por los proveedores de servicios de Internet que permitir a sus clientes su acceso a este. Las redes privadas amplias son usadas principalmente por las empresas, por ejemplo, permiten servicios en la nube y conexión a la red de las diferentes sedes de la empresa (IONOS, 2020).

Una WAN está funcionando dentro de las capas uno, dos y tres del modelo de referencia OSI como se muestra la Ilustración 13.

Modelo OSI

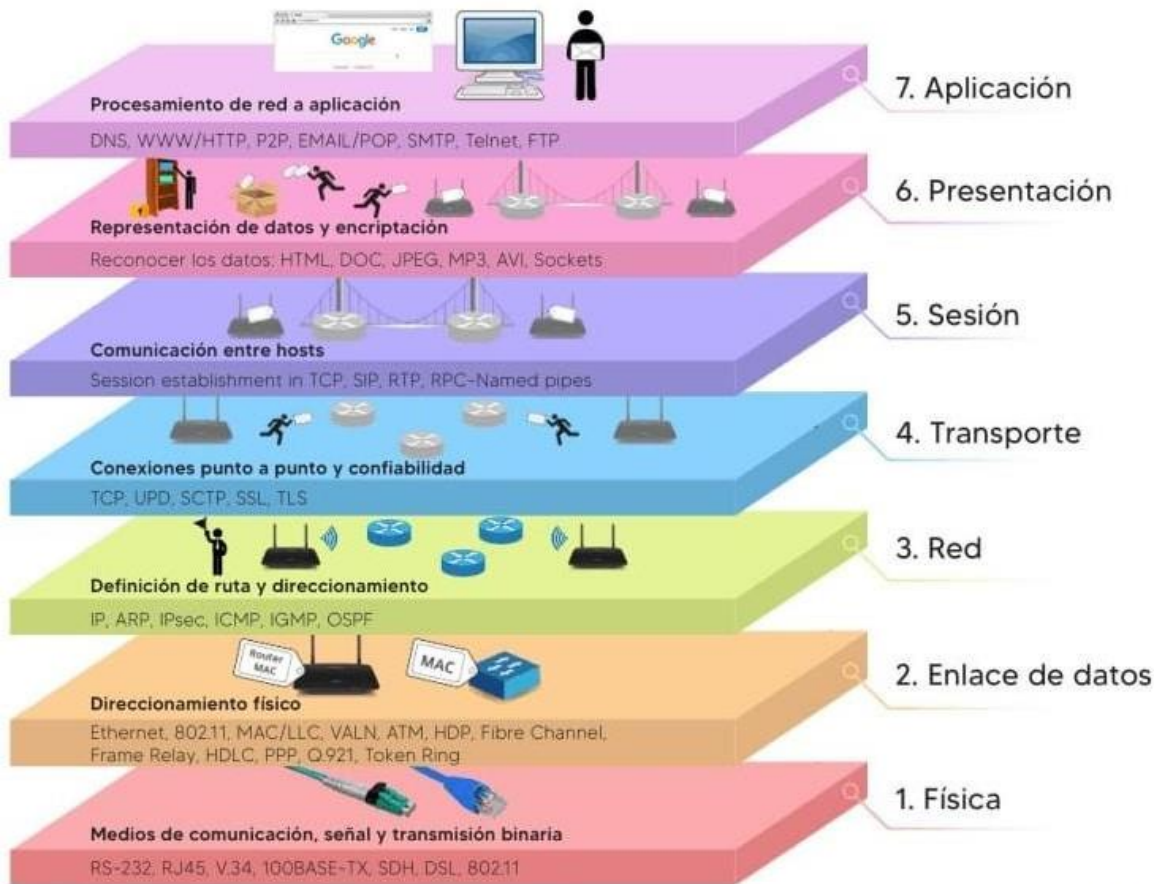


Ilustración 13. Modelo OSI.

Fuente: (Meza, 2018).

Desglosando los tres primeros niveles de OSI, en cada una de las capas en las cuales funciona la red WAN para tener un poco más de conocimiento y se entienda su función de está.

Dentro del protocolo TCP/IP la capa 1 corresponde al piso físico y el nivel 2 a la de Enlace de datos están abarcadas por nivel de Acceso a la red del mismo protocolo TCP/IP y la capa 3 de Red correspondiente al sistema OSI es abarcada dentro del TCP/IP por la capa de Red.

Capa 1 Física



Ilustración 14. Capa Física modelo OSI.

Fuente: (Meza, 2018).

El nivel uno hace la conexión física entre los dispositivos como ejemplo, en el paso de datos por un cable de cobre o fibra óptica (electricidad, hardware, cables) con tipo de entradas RJ45, RS-232, DLS, etc. (Meza, Platzi, 2018).

Por mencionar algunas de las funciones que tiene esta capa son:

- El tipo de medio de transmisión es especificado.
- El flujo de datos es controlado.
- Los datos se cambian en señales físicas.
- Mantiene y establece una conexión física entre dispositivos.

Se observa en la Ilustración 14 un ejemplo de la diferencia que existe entre las entradas de conexión del router para la red LAN y WAN. La apariencia del puerto WAN en el router puede ser tipo ADSL2+ o VDSL2 está señalado mayormente de color gris, tiene un puerto para WAN de Internet que es la conexión ADLS y cuatro puertos correspondientes a LAN para conectar diferentes dispositivos por vía cable de entrada rj45 (Luz, 2025).

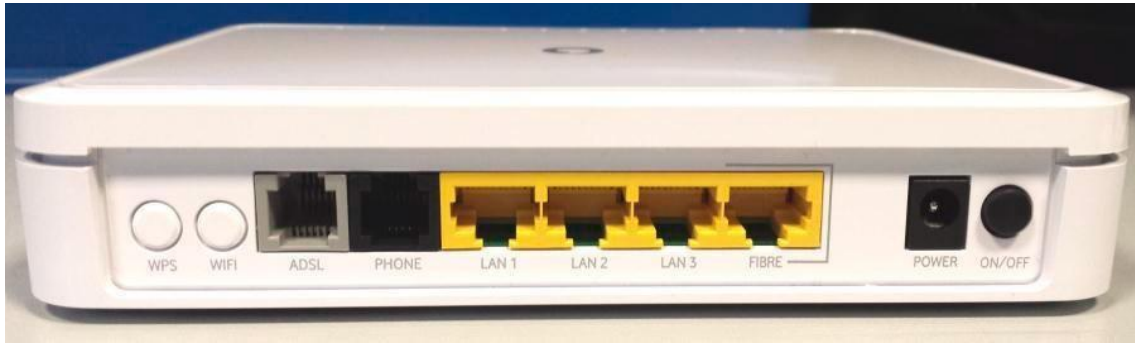


Ilustración 15. Conexiones LAN y WAN en router.

Fuente: (Luz, 2025).



Ilustración 16. Posiciones Estandarizadas.

Fuente: (Luz, 2025).

Capa 2 Enlace de Datos



Ilustración 17. Capa 2 del modelo OSI.

Fuente: (Meza, 2018).

Aquí se establece y encarga de un enlace entre los dispositivos asegurando que la transmisión de datos sea precisa y eficiente, hace que con la verificación y corrección de errores garantice de manera correcta los datos.

Los datos dentro de esta capa se envían convertidos en bits esto con la finalidad de hacerlos llegar a la capa de red, que viene siendo el piso tres del sistema OSI y del protocolo TCP/IP.

La capa de enlace de datos tiene el rol clave de agarrar datos fuertes y cambiarla en una cosa sin fallas al pasarla a la capa de red. Se hace al separar los datos básicos en bytes, los manda poco a poco y revisa el estado del cuadro que manda el computador final (Universidad del Azuay, 2025).

Capa 3 Red

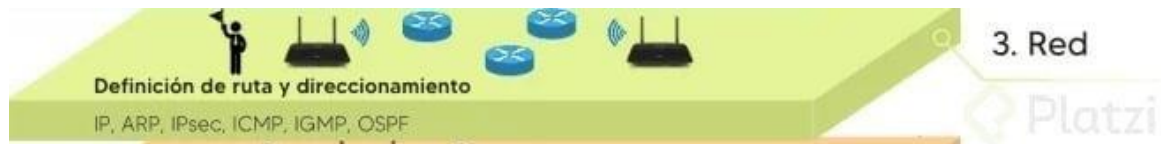


Ilustración 18. Capa de Red modelo OSI.

Fuente: (Meza, 2018).

Como ya se mencionó en esta capa de red cada uno de los paquetes enviados se divide en cuatro pedazos en forma de bits, para así facilitar el envío de paquete de una forma segura. La Ilustración 19 describe gráficamente el funcionamiento de esta capa y cómo es que se secciona el paquete al momento de su transferencia de un punto a otro.

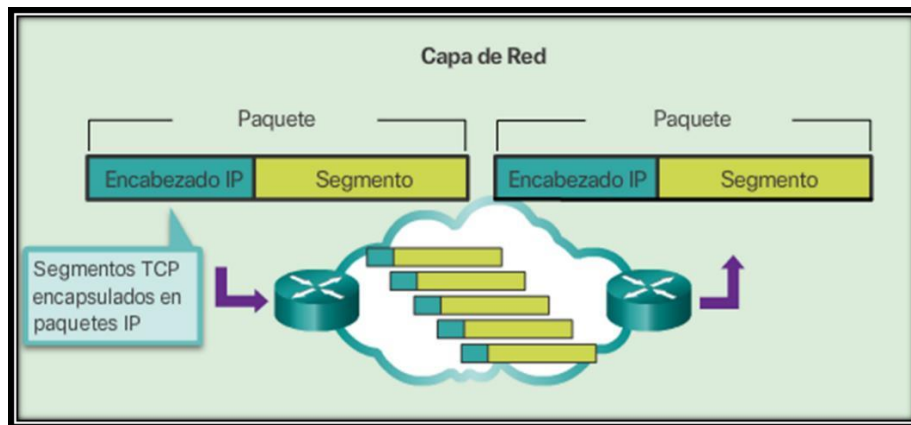


Ilustración 19. Capa de Red.

Fuente: https://irasema.neocities.org/Fundamentos_Netes/Tem1Sub2

¿Que son los Bits?

Un bit es la unidad mínima de información, usada para representar la contraposición entre dos valores verdaderos o falsos. Bit es el acrónimo de “binary digit” traducido al español “dígito binario” solo 0 y 1. Entonces, en base a esta definición un bit es un sistema de numeración binaria representada en solo dos valores ceros y unos. Los bits que hay en un byte por lo general tienen ocho bits, pero dependerá de la estructura de la computadora (Lenovo, 2025).

El funcionamiento de los bits se puede ver en la Ilustración 20, donde se visualiza el comportamiento de ellos en cada paquete o datos enviados.

Formateo de datos para la transmisión

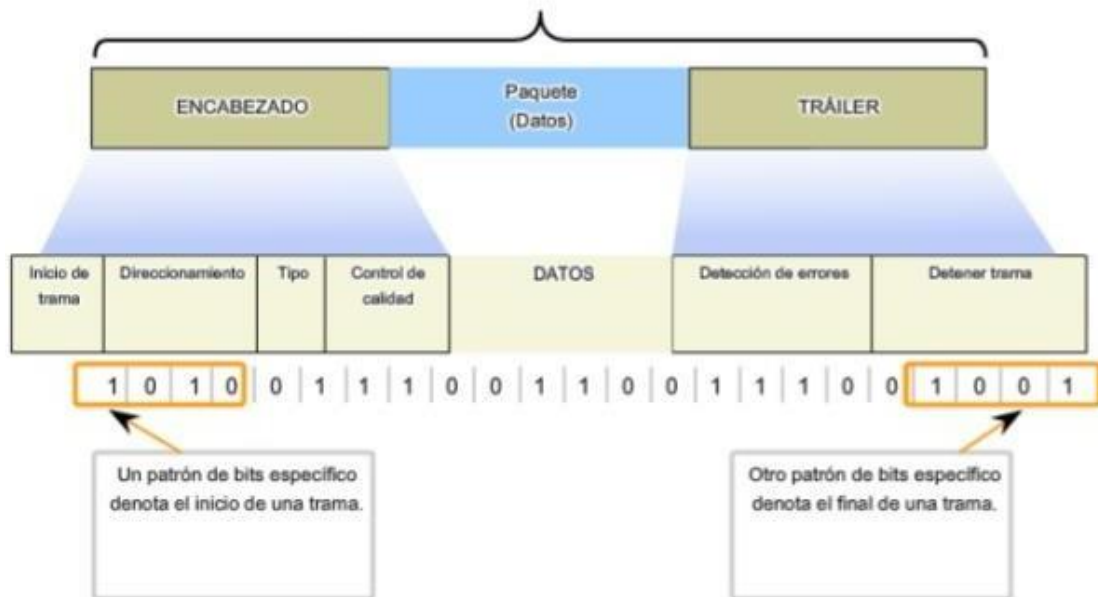


Ilustración 20. Formato de datos en Bits.

Fuente: <https://tododeredes.com/modelo-osi/capa-2/>

La capa de red es encargada de dirigir los datos en una red entre los dispositivos y selecciona la ruta más simple para que viajen los datos y se garantice la entrega al final.

Algunos de sus funcionamientos de la capa de res son los siguientes:

- Control de paquetes.
- Enrutamiento de datos.
- Direccionamiento de dispositivos.
- Reensamblaje de paquetes.

Enrutamiento

Según la página de Cisco, el direccionamiento es el proceso de elegir y definir el camino para el tránsito de los paquetes IP dentro de las redes, así como el proceso de gestión del tráfico de red en general. Es importante el enrutamiento ya que hay miles de rutas posibles entre destinos dentro de una gran red autónoma o internet, la claridad de esas rutas de transmisión de red para el tráfico interno y externo ayuda a los administradores a identificar fuentes de latencia y brindar resolverlas (Cisco, 2025).

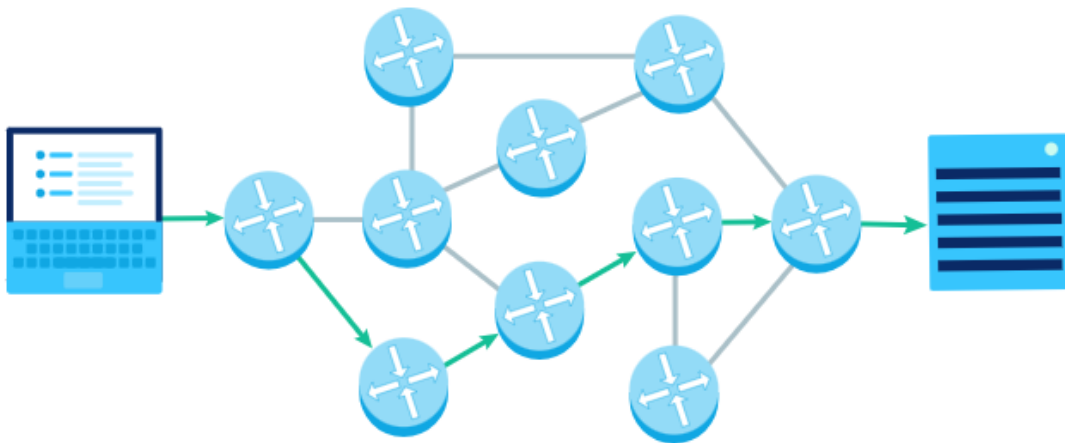


Ilustración 21. Enrutamiento función.

Fuente: <https://es.khanacademy.org/computing/ap-computer-science-principles/the-internet/x2d2f703b37b450a3:routing-with-redundancy/a/internet-routing>

El protocolo IP es el servicio del nivel de red implementado por el conjunto de protocolos TCP/IP. IP se diseñó como protocolo de baja sobrecarga, brinda solo funciones indispensables para mandar paquetes origen a un destino.

Características del protocolo IP

- Operación independiente a los medios que transporta los datos.
- No establece conexión con el destino antes de enviar los paquetes.
- La entrega de paquetes no está garantizada (Sapalomera, 2025).

Red Área Metropolitana (MAN)

Red de área metropolitana (MAN), sus siglas en inglés Metropolitan Area Network red informática conecta a las máquinas del área metropolitana. MAN es una red más grande que una LAN, pero chica que una red WAN.

Metropolitano involucra el tamaño de red, no el tamaño de una población de la zona en la que se vive (Cloudflare, 2025).

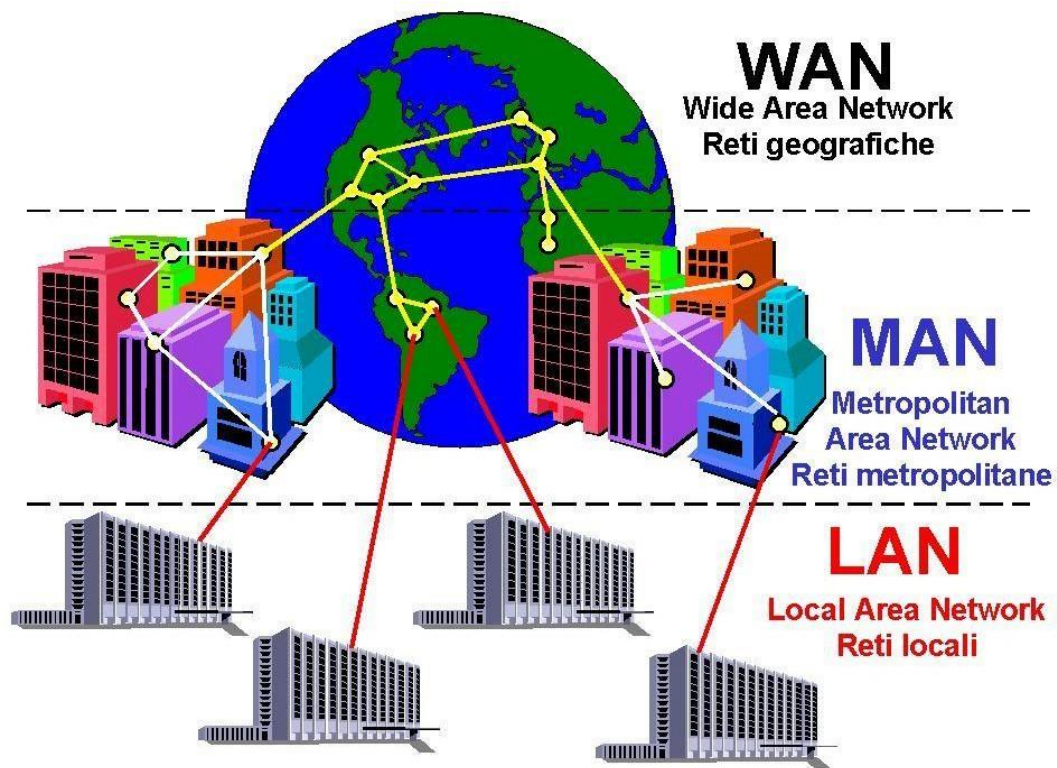


Ilustración 22. Representación gráfica de redes informáticas principales.

Fuente: <https://significado.com/red-man/>

Red de Área Local Inalámbrica (WLAN)

Una red WLAN (Red de Área Local Inalámbrica) una forma de repartir inalámbricamente de conectividad de red a diversos dispositivos dentro de un área localizada. Las WAN manejan ondas de radio con alta frecuencia y seguido

insertan un punto de acceso (AP) a internet, esto sin ninguna necesidad de conexión por cable físico. Esta permite a los usuarios moverse por el área con cobertura mientras hay una conexión de red (Beal, 2024).



Ilustración 23. Diagrama representativo de una red WLAN.

Fuente: Propia.

5.4.2 Capa de Internet

En esta parte hay un método muy común, es el IP, pues él pone la ruta a los datos entre equipos, dando claves IP diferentes a cada aparato para que la información llegue bien, sin problema.

La capa de Internet, llamada IP, toma y mueve paquetes para la red. Abarca el idioma de la red IP, el traductor de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP) (Oracle, 2010).

Protocolo IP

Sus caminos de red son los que se usan para mirar y decir cuáles son las rutas de red, tal vez sean lo más importante del conjunto de protocolos TCP/IP. El protocolo IP supervisa esto:

- Direcciones IP: pieza clave del plan, como sistema de direccionamiento usado desde que inicio el internet, se llaman IPv4, aunque hoy existe un nuevo direccionamiento que es IPv6.

IPv4 se está cambiando ya que el internet se está quedando sin espacio de direcciones IP, pero IPv6 tiene un montón de direcciones IP.

- Espacio total de IPv4: 4,294,967,296 direcciones.
- Espacio total de IPv6: 340,282,366,920,938,463,374,607,431,768,211,456 direcciones.
 - Comunicación entre equipos: elige el camino que debe seguir un paquete viendo la dirección IP del equipo que lo recibe.
 - Formato de paquetes: los paquetes se unen en grupos llamados paquetes de datos. Los datagramas los veremos más adelante ya que pertenecen a la capa de transporte del protocolo TCP/IP, se está observándola desde abajo hacia arriba.
 - División: si el paquete es muy amplio para mandarse por la red, el protocolo IP lo parte en pedazos más chicos (Oracle, 2010).

Protocolo ARP

Es un protocolo para encontrar direcciones (Address Resolution Protocol), conecta una dirección de internet que se mueve todo el tiempo a una dirección de máquina que siempre está en el mismo lugar dentro de una zona de computadoras cercana. Al ingresar a la red local, la PC nueva recibe un código IP, distinto a los que andan dando vueltas, como su identificación única para hablar solo entre ellas (Fortinet, 2025).

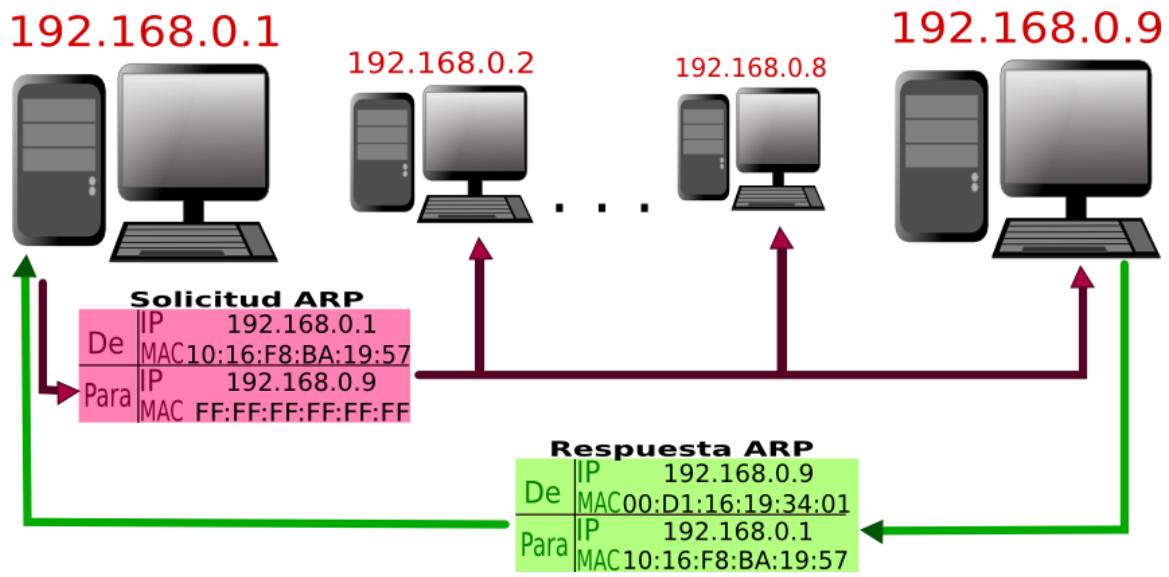


Ilustración 24. Representación gráfica de ARP.

Fuente: <https://mundosica.com/que-es-el-protocolo-arp-y-como-acceder-a-sus-tablas-desde-android/>

Protocolo ICMP

El protocolo de mensajes de control de internet se asegura de decirle al que manda si algo malo ha pasado cuando su recado está en camino. Este no solo avisa de fallos, también lleva mensajes de control. Este plan se parece a UDP, aunque más fácil y no lleva datos, sino que avisa si su envío se pierde en el camino (Estrada, 2025).

Así que, el sistema de mensajes de control de internet solo ve llegando datos demasiado rápido, imposible procesarlos a esto se le conoce como paquetes sueltos, no se puede alcanzar un destino entra como fallas de conectividad y busca otro camino nuevo para un nuevo envío.

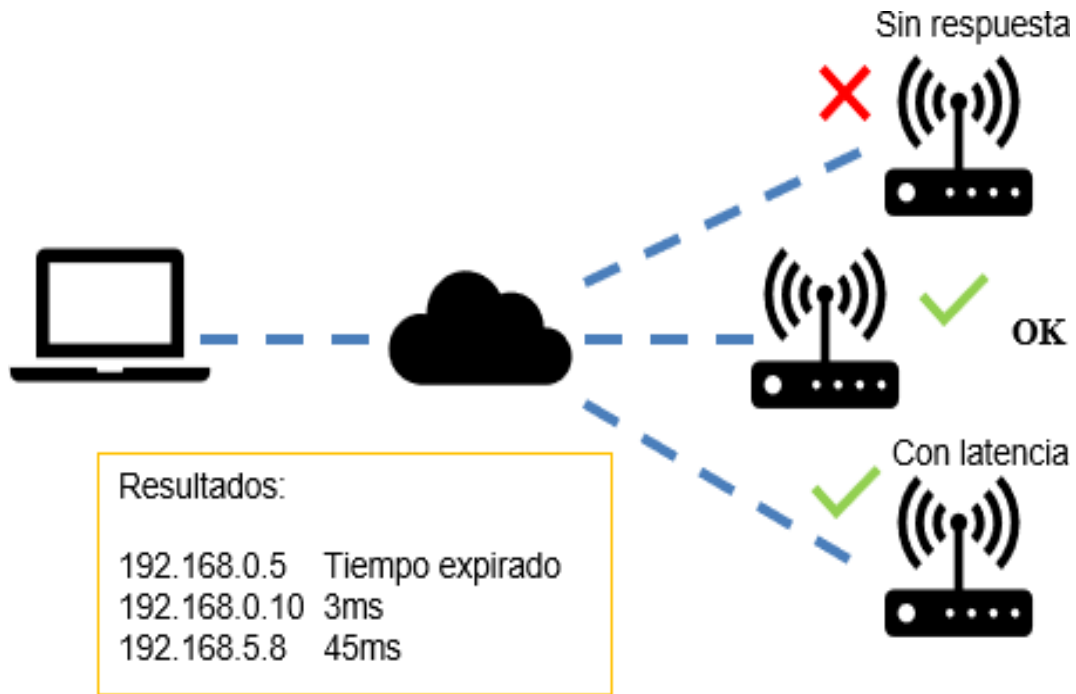


Ilustración 25. Representación gráfica de funcionamiento de ICMP.

Fuente: Propia.

Para entender un poco, el anfitrión es un aparato que se conecta a una red y que puede mandar y recibir información.

5.4.3 Capa de Transporte

La parte de transporte se ocupa de las comunicaciones entre las aplicaciones entre los muchos ordenadores que hay.

Como se aprecia en la Ilustración 26, la capa que traslada los datos es un puente entre la capa de aplicación y las capas de abajo que se encargan de mandar la información por la red.

La capa de transporte mueve los datos entre aplicaciones en dispositivos conectados en la red. En esta parte, los programas generan datos que se cambian entre el lugar de inicio y el final.

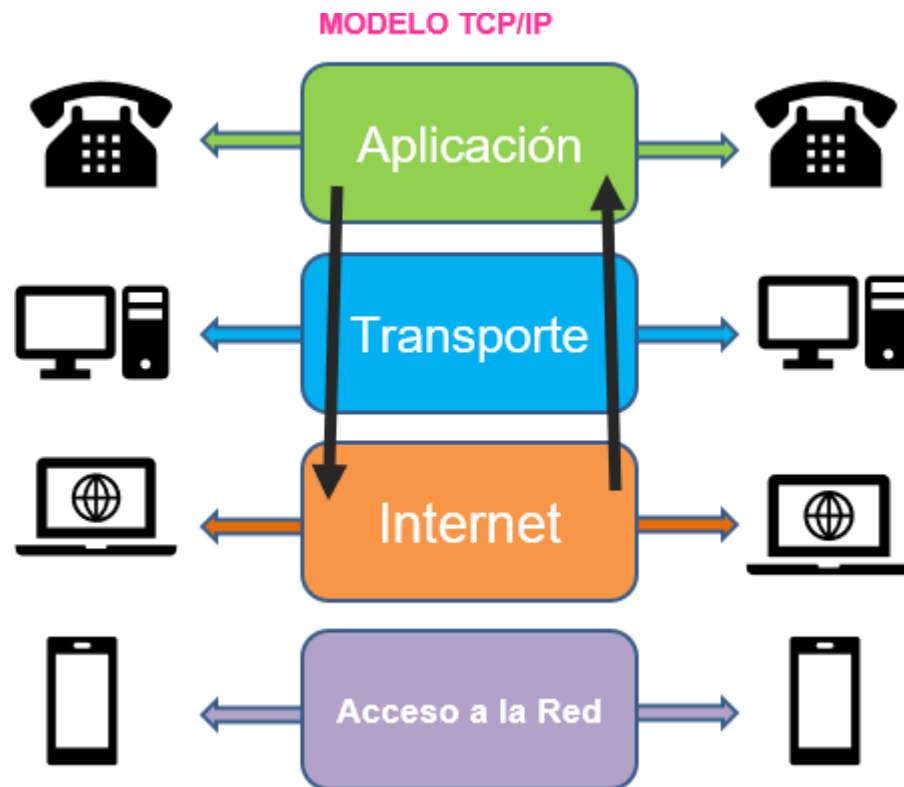


Ilustración 26. Capa de Transporte.

Fuente: Propia.

La capa de transporte ignora qué clase de servidor recibe, cómo los datos deben moverse, la ruta que escogen los datos o que tan grande es la red (CCNA, 2025).

Se incluyen dos protocolos:

- Protocolo de Control de Transmisión: TCP (Transmission Control Protocol).
- Protocolo de Datagramas de Usuario: UDP (User Datagram Protocol).

Protocolo TCP

Se usa para enviar datos a través de redes. Este protocolo separa los datos antes de mandarlos lejos, sus funciones avanzadas dan una llegada confiable a

diferencia de otros protocolos. Al deshacer los datos los devuelve a la capa de protocolo de internet (IP) cuidando que cada recado termine en su destino. Los paquetes quizás viajen por varias rutas si es que la ruta actual está muy llena o no esté disponible, hacerlo así mejora el funcionamiento de la red (Hostinger, 2025).

El vínculo entre quien envía y quien recibe aguanta hasta que todo se pasa bien. Cada vez que se manda un paquete de datos se necesita un acuse de quien recibe, si no dice nada, los datos se mandan de nuevo.

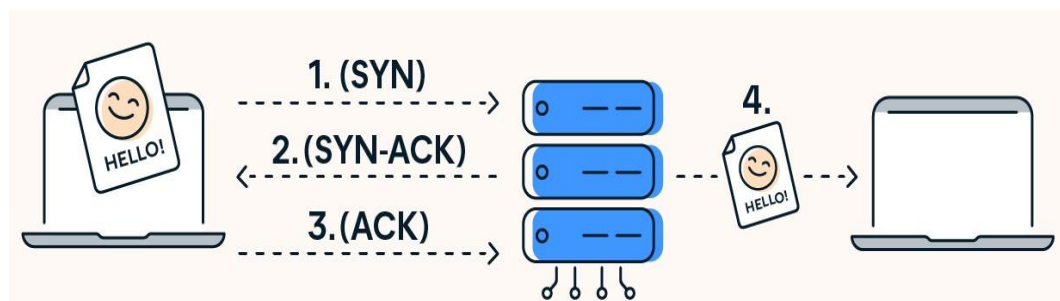


Ilustración 27. Proceso de una conexión cliente-servidor.

Fuente: (Gorman, 2023).

Protocolo UDP

El UDP actúa mandando los paquetes directo a quien los pidió, hasta que la transmisión esté finalizada. UDP manda información al destinatario sin confirmar la entrega de la información, ni ver si todo llegó bien (Gorman, 2023).

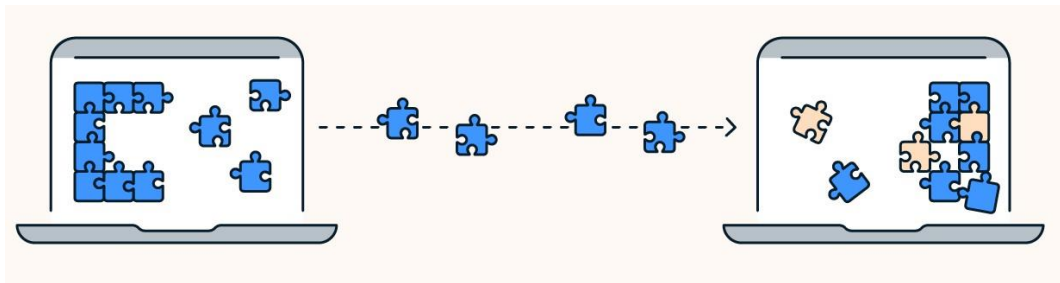


Ilustración 28. Función gráfica del UDP.

Fuente: (Gorman, 2023).

5.4.4 Capa de Aplicación

Esta capa es la más cercana al usuario final, ya que es la capa que proporciona la interfaz entre aplicaciones usadas para su comunicación y la red subyacente a través de la cual se transmiten todos los mensajes, los protocolos de la capa de aplicación son utilizados para el intercambio de datos que se ejecutan en las computadoras origen y destino.

Basado en el modelo TCP/IP este ocupa las tres capas superiores del modelo OSI que vienen siendo (aplicación, presentación y sesión), existen muchos protocolos los cuales serán vistos a continuación algunos de ellos, pero el protocolo por el cual se encuentra enfocado este trabajo es el protocolo TFTP.

Nombres de Dominio

Las siglas DNS se refiere a Domain Name System (Sistema de Nombres de Dominio) esta nomenclatura jerárquica para las redes, además de ser distribuido hace el traductor para los nombres de dominio (Videgain, 2019).

El DNS es un software de servidor especial para responder las consultas relativas a una base de datos DNS, suelen estar alojados en host dedicados, los equipos que contienen programas son denominados servidores DNS.

Se conectan a internet nuestro proveedor de servicio de internet (ISP) nos asigna una dirección IP única de 12 dígitos que corresponde a una IPv4 o una de 32 caracteres de formato hexadecimal que ya entraría como una IPv6, para ambos tipos de direcciones IP asignada a una máquina es capaz de manejar estos formatos de direcciones (Videgain, 2019).

Un ejemplo claro es notar la diferencia de estar escribiendo la dirección IP del sitio a solo buscar el sitio con su nombre ya que la función del dominio es justamente evitar escribir toda la dirección.

No es igual escribir Google.com en el buscador a escribir la dirección IP que le corresponde 172.217.3.78. Aquí el .com es utilizado para sitios web comerciales, en la siguiente ilustración 29 muestra la diferencia de búsqueda del sitio, pero que al final abre el sitio web al que corresponde ya sea escribiendo la IP o el nombre de este

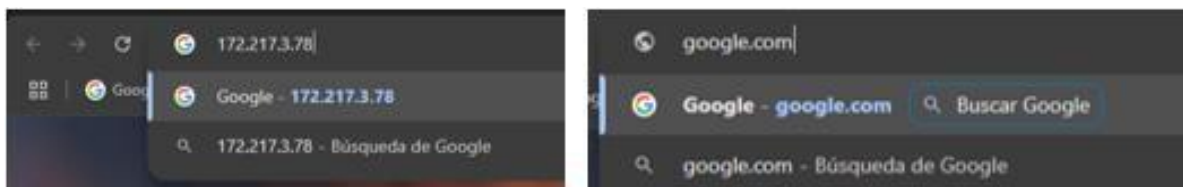


Ilustración 29. Diferencia de búsqueda de sitio web.

Fuente: Propia.

Protocolo de Configuración Dinámica de Host

DHCP es un protocolo cliente-servidor que brinda automáticamente una dirección IP a la computadora y otra información de configuración como con la máscara de subred unida con la puerta de enlace predeterminada. Al centralizar estas tareas, el servidor DHCP reduce el esfuerzo manual, minimiza los errores y garantiza el uso eficaz de los recursos de direcciones IP en toda la red (Microsoft, 2025).

Este protocolo es uno de los más utilizado por los routers, el protocolo tiene distintas formas de asignar IP siempre y cuando el tipo de configuración realizará y del tipo de circunstancia en el que nos encontramos. Una de ellas es asignación de dirección IP Automática, Manual o Estática o finalmente una asignación dinámica.

- **Automática:** proporciona una dirección IP al cliente que realiza la solicitud y estará disponible a ese cliente hasta que la libere.
- **Manual o Estática:** nos permitirá configurar un listado de parejas IP-MAC con el objetivo de que siempre se le proporcione a un cliente una dirección IP determinada y esta dirección no se cambie nunca.
- **Dinámica:** este método permite reutilización dinámica de las direcciones IP (Luz, 2025).

Se observa en la Ilustración 30 una pequeña representación de cómo es el funcionamiento del protocolo DHCP.



Ilustración 30. Función DHCP.

Fuente: <https://www.infoteknico.com/que-es-dhcp-y-como-funciona/>

FTP (Protocolo de Transferencia de Archivos)

Los orígenes de este protocolo son desde el año de 1971 por Abhay Bhusban y como lo dicen sus siglas en inglés es File Transfer Protocol y aunque con paso del tiempo ha ido evolucionado es un protocolo de los más antiguos y que sigue siendo utilizado hasta hoy día.

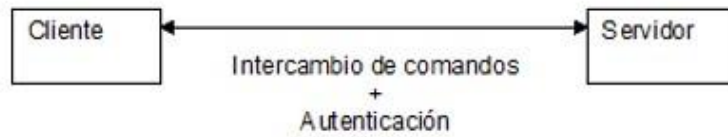
FTP es un protocolo cliente/servidor que permite a los usuarios transmitir archivos con las computadoras en la red. Su propósito principal es este protocolo es realizar el intercambio de archivos entre los equipos remotos de manera segura, eficaz e independiente (Fernández Y. , 2024).

La utilización que se le da a este tipo de protocolo es principalmente para mantener información guardada en los servidores domésticos. Una de sus importancias de este protocolo es que aquí se pueden descargar ficheros de modo binario directamente sin necesidad de ser codificados.

En el protocolo FTP se guarda la información en carpetas y subcarpetas ubicadas en el servidor y sirve en algún sistema operativo, esto lo hace un protocolo multiplataforma. Una de las características principales de FTP es que utiliza TCP para su transferencia y se requiere de una contraseña para la seguridad de los archivos transferidos.

En las computadoras los datos del FTP se mandan mediante los puertos 20 y 21, son los puertos fijos ya asignados en todos los dispositivos para llevar a cabo su envío de archivos. Cuál el puerto 21 se usa para fijar una conexión de control y el puerto 20 para la transferencia de los datos (Fernández Y. , 2024).

Puerto 21:



Puerto 20:

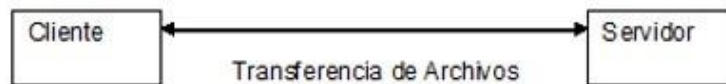


Ilustración 31. Función de puertos FTP.

Fuente: <https://miguegongon.blogspot.com/2011/11/respuesta-servidor-ftp-ante-las.html>

En la unión de control se mantiene conectado mientras toda la sesión FTP, esto por el puerto 21. Y en la conexión de datos está abierto y luego cerrado para cada actividad de transferencia de los archivos en el puerto 20 en su modo activo. Mientras la conexión de control está abierta, la conexión de datos se puede abrir y cerrar varias veces si se transfieren varios archivos.

El protocolo FTP tiene dos modos de funcionamiento el modo activo y el modo pasivo, ambos modos se utilizan en el puerto 21 del servidor como canal de control.

Modo activo: en este modo el cliente y el servidor son FTP y establecen conexiones de la siguiente manera: normalmente el usuario se conecta a un servidor FTP en el puerto 21 desde un puerto aleatorio desde su cliente de transferencia de archivos, el cliente envía el comando PORT especificando a que puerto debe conectarse el servidor.

Después el servidor se conecta desde el puerto 20. En modo activo, FTP inicia la conexión de datos, una vez establecida las transferencias de archivos y los listados de directorios se realizan a través de esta conexión (Villanueva, 2025).

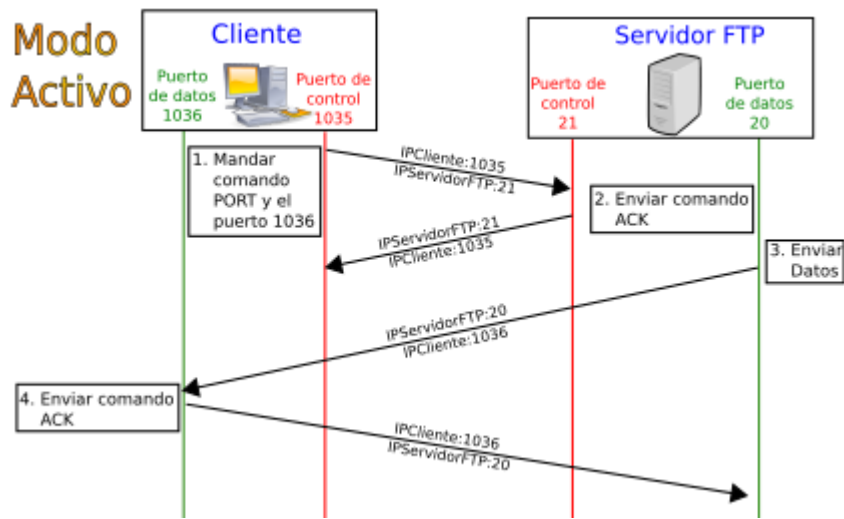


Ilustración 32. Modo activo.

Fuente: <https://miguegongon.blogspot.com/2011/11/respuesta-servidor-ftp-ante-las.html>

Modo pasivo: modo de conexión de datos más reciente, los clientes FTP modernos basados en interfaz gráfica de usuario o línea de comandos también lo admiten. Para establecer conexiones pasivas se requiere lo siguiente: el cliente inicia la conexión del canal de comandos, FTP cliente se conecta al puerto TCP 21 del servidor FTP en vez de enviar el comando PORT manda PASV, esto indicando al servidor que desea transferir archivos en modo pasivo y ahora el servidor selecciona un puerto aleatorio de su propio conjunto de puertos y notifica al cliente. Cuando el cliente determina el puerto del servidor al que conectará para el canal de datos inicia la conexión (Villanueva, 2025).

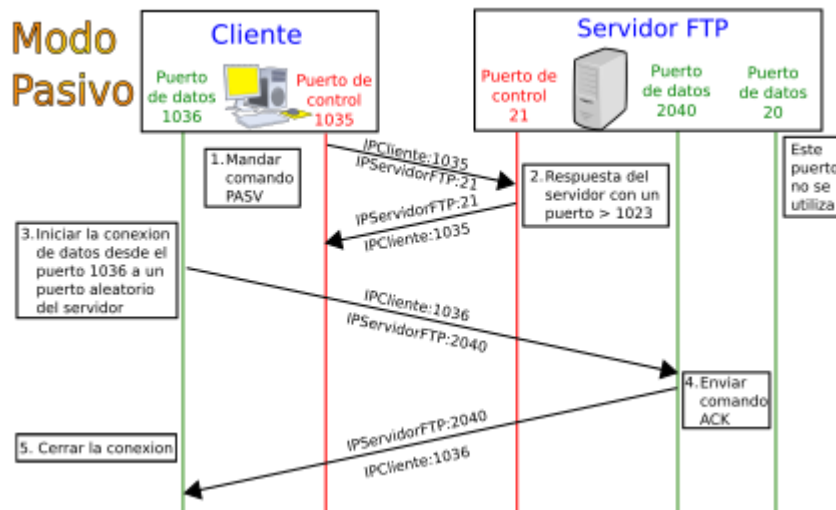


Ilustración 33. Modo pasivo.

Fuente: <https://miguegongon.blogspot.com/2011/11/respuesta-servidor-ftp-ante-las.html>

TFTP (Protocolo Trivial de Transferencia de Archivos)

Profundizando al protocolo de interés en este trabajo de investigación se empieza hablando del protocolo TFTP (Protocolo Trivial de Transferencia de Archivos).

TFTP es de transferencia de archivos simple desarrollado en la década de 1970 solo para dispositivos que sufrían de insuficiente espacio en disco duro. Aunque este protocolo fue desarrollado antes que el FTP, se terminó definiendo originalmente en el año 1981.

Hoy en día no es tan utilizado TFTP ya que mayormente se usa el FTP, porque fue el protocolo que se implementó primero y por el tipo de seguridad que tiene la hora de transferencia de los archivos de cliente-servidor ya que TFTP es un protocolo que no brinda seguridad a los archivos transferidos pero que si se usa de la manera adecuada puede salir la ejecución correcta.

En este protocolo no se usa para transferencia de datos a través del Internet, se manejó para mandar los archivos dentro de la red área local (LAN). El protocolo TFTP utiliza el puerto 69 es UDP como protocolo de transporte.

TFTP es especificado en la RFC 1350, tiene un diseño simple y requiere poca memoria y también tiene una funcionalidad limitada. Solo se usa para leer o escribir un archivo. No se puede cambiar el nombre, eliminar o incluso enumerar archivos. Tampoco proporciona ninguna forma de autenticación o cifrado de usuario (Cohen, 2023).

¿Qué es RFC 1350?

Se puede utilizar para mover archivos entre máquinas en diferentes redes que implementan UDP y es diseñado para ser pequeño y fácil de implementar, por eso mismo carece de la mayoría de características de un FTP normal este no excluye la posibilidad de implementar TFTP sobre otros protocolos de datagramas (Sollins, 1992).

La computadora funciona como un servidor TFTP, en este modo se debe instalar el software del servidor TFTP en la computadora, comparado con FTP, TFTP es más fácil de configurar, pero ofrece menos seguridad y velocidad de transmisión (Huawei, 2025).

Diferencia entre FTP vs TFTP

DIFERENCIAS	
FTP	TFTP
<ul style="list-style-type: none"> • Las aplicaciones FTP tradicionales ofrecen una gran cantidad de funciones, incluida la visualización y manipulación de archivos existentes en un servidor FTP remoto. • Requieren algún tipo de autenticación, como cuentas de usuario o contraseñas. • FTP no incluye ningún tipo de cifrado integrado para su transferencia de datos. 	<ul style="list-style-type: none"> • No administra archivos. • Solo brinda la posibilidad de subir (put) y descargar (get). • No utiliza pérdida de tiempo en procesos rigurosos de autenticación. • TFTP es pequeño y fácil de usar. • El protocolo es liviano lo que lo hace útil para dispositivos con poca capacidad de almacenamiento o procesamiento.

Tabla 1. Diferencia FTP vs TFTP. Fuente: (Garn, 2024).

El protocolo TFTP debido a su falta de seguridad y autenticación, es utilizado solo para circunstancias especiales como las que se mencionan a continuación:

- Arranque en red con estaciones de trabajo sin disco.
- Arranque de red con implementaciones de entorno de ejecución de un pre arranque.
- Realizar copias de seguridad de las carpetas de configuración del dispositivo de red.
- Transferencia de imágenes de firmware.
- Realizar envíos de archivos tradicionales desde dispositivo cliente a servidor de red (Garn, 2024).

5.5 Transmisión de Datos

La transmisión de datos, es el proceso de transferencia de datos digitales o analógicos entre dos o más dispositivos a través de un medio de comunicación, como lo es cables de cobre, fibra óptica o señales inalámbricas. Implica que los datos en señales eléctricas, ópticas o de radio se pueda transmitir a través de redes o canales (Spasojevic, 2024).

Dentro de las aplicaciones los usuarios buscan experiencias digitales con respuesta inmediata, las aplicaciones pueden utilizar y procesar datos mejorando rendimiento y la satisfacción de los clientes.

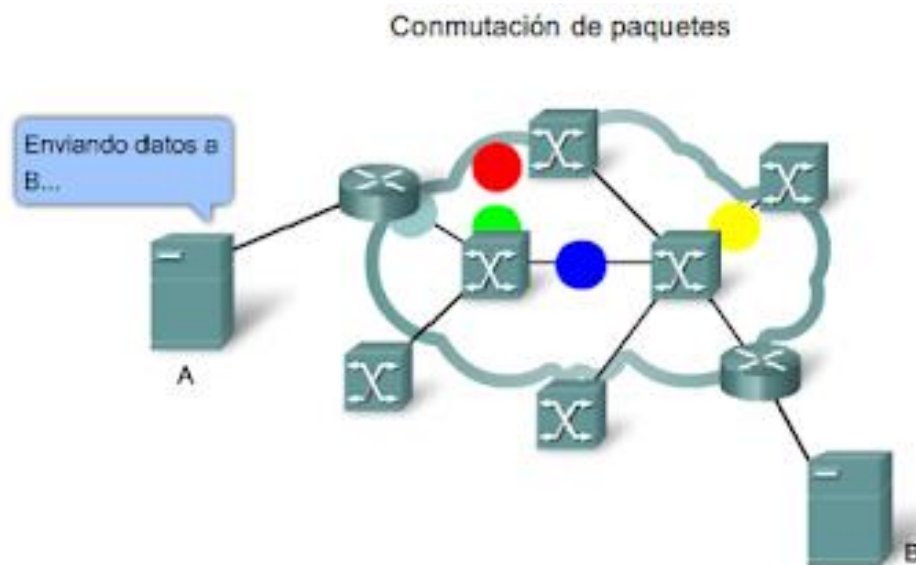


Ilustración 34. Demostración gráfica de la Transferencia de datos.

Fuente: <https://telecomunicaciones02.blogspot.com/2016/11/redes-de-conmutacion-de-datos.html>

5.6 Software de uso para la simulación y uso del protocolo TFTP

5.6.1 Cisco Packet Tracer

Es una aplicación de uso gratuito que sirve para simulaciones de escenarios virtuales en redes sin la necesidad de tener el escenario de forma física, es utilizado por estudiantes para su desarrollo académico y por los profesionales también.

El objetivo principal de Cisco Packet Tracer es utilizarlo para la creación de redes y ver su funcionamiento, además de poder practicar y conocer equipos de redes como switch, rack, cableado, router, etc. También aprender a integrar IoT o automatización de la red (IPData, 2025).



Ilustración 35. Logo software de Cisco Packet Tracer.

Fuente: Propia.

VI. MÉTODO Y TÉCNICAS DE INVESTIGACIÓN

En este trabajo se aplicará el método de investigación experimental y documental para el desarrollo de simulación de transferencia de archivos mediante el protocolo TFTP esto para el traspaso, resguardo y recuperación de la información llevando a cabo un buen uso y manejo de toda la información que se encuentra dentro de la institución de media superior cuando se encuentre en una situación de catástrofe natural que este fuera de alcance de las personas responsables del área.

El motivo por el que se utilizará la investigación documental es porque nos permite obtener información mediante la recolección de antecedentes o situaciones de catástrofe natural que se han presentado en las escuelas de media superior, con la finalidad de llegar a una solución óptima para los responsables de la institución y que en situaciones como esas al no poder ingresar a las instalaciones ellos puedan hacer una transferencia de archivos de manera segura usando el protocolo TFTP.

A continuación, se presentará una definición breve de cada tipo de investigación que se usaran en este trabajo:

- La investigación experimental es un enfoque sistemático de la investigación científica busca investigar las relaciones causa y efecto y promover el conocimiento en diversos campos (Research, 2024).
- La investigación documental es un método curioso en la investigación cualitativa que se ocupa de juntar, ordenar y elegir datos de lo que se lee en documentos, libros, revistas, estudios hechos, etc. Allí, esta mirar en el

fondo del análisis de datos, más la búsqueda, escoger pegarlo todo con el objetivo de estudiar algo (Dávila, 2015).

Con base en simulación que se desarrolla se considera importante llevar a cabo un método analítico de los antecedentes obtenidos, esto con el fin de analizar los obstáculos más generales que se presentan en el lugar para empezar con la solución adecuada y correcta al hacer uso del protocolo TFTP.

Una vez diseñada la simulación de manera correcta el uso del protocolo que se implementará, se utilizará en la metodología de cascada (waterfall model), este es un seguimiento en secuencia y partido en procesos del desarrollo de cada una de las etapas secuenciales del proyecto. Los resultados de cada etapa sirven como hipótesis de inicio para la siguiente.

En 1970 en el artículo de Winston W. Royce salió la primera descripción formal de la metodología de cascada sobre la gestión de desarrollo de software. El método de cascada se considera que surgió en la fabricación y construcción, de ahí viene el acuerdo que con este modelo no se puede volver a la fase anterior, pero con la condición de que cada fase tiene que estar completa sino no se puede pasar a la siguiente (Stepanets, 2024).

El modelo de cascada es un proceso sencillo es importante ejecutar cada una de sus fases e ir comprendiendo las implicaciones que tiene para cada proceso por el que va pasando.

Como se sabe el método de cascada funciona con un proceso de 5 etapas las cuales son las siguientes: requisitos, diseño, implementación, verificación y mantenimiento en un calendario previsto de un proyecto.

La metodología tiene bien definidas las fases secuenciales, cada fase está debidamente monitorizada como se muestra en la Ilustración 36.

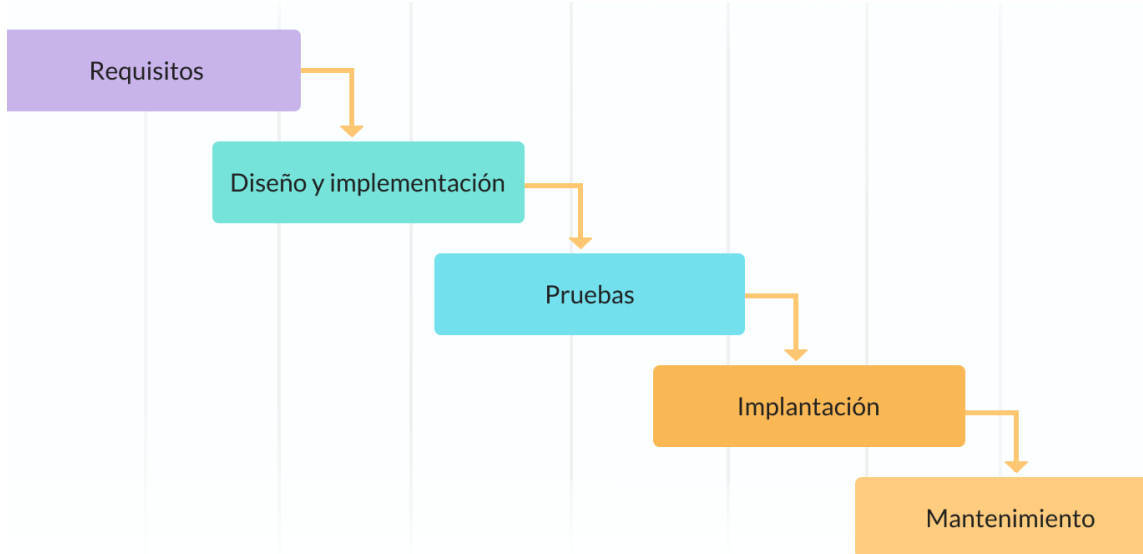


Ilustración 36. Modelo de cascada.

Fuente: (Stepanets, 2024).

El tipo de metodología planteada en esta investigación fue empezando por:

Análisis: básicamente es en averiguar y recopilar toda aquella información que les permita plantear soluciones eficientes que la institución educativa requiera.

Diseño: después de haber obtenido toda la información como el análisis de riesgos en la zona, permisos, entre otras. Se continua con el diseño de la simulación planteando que se llegue a encontrar en una situación de inundación y recreando el cómo podría ser para la problemática real. Se selecciona el software a utilizar como herramienta para realizar el diseño de dicha simulación del funcionamiento del protocolo TFTP, en este caso es Cisco Packet Tracer.

Implementación: llevar a cabo la implementación del protocolo TFTP, puede ser relevantemente sencillo utilizando el tipo de software de Cisco para su modo simulado y el software tftp para su modo físico, haciendo para ambos casos el uso del funcionamiento del protocolo.

Verificación: verificar que la simulación realice la acción y función del protocolo TFTP de forma satisfactoria para así brindar una buena capacitación al personal.

Mantenimiento: esta fase se omite para esta demostración del uso del protocolo, por lo mencionado al ser solo demostración de su uso que es de lo que trata este trabajo final, este no requiere tener mantenimientos a menos que el protocolo ya este en ejecución y en uso para su totalidad dentro de la institución, todo dependerá del permiso de la escuela.

Siguiendo esos pasos, se puede implementar el protocolo de una forma fácil y útil en la red de una escuela de media superior, proporcionando una solución eficiente para la transferencia de archivos dentro de la institución educativa.

VII. PRESENTACIÓN Y DISCUSIÓN DE RESULTADOS

En esta sección se explican todos los pasos que se realizan para la simulación del protocolo TFTP dentro del software demostrativo, así como la herramienta que se utiliza para el diseño, simulado y desarrollo de uso y función de este protocolo al momento de hacer una transferencia de archivo, esto con la finalidad de llevarlo a las escuelas de media superior del municipio de Ixtapaluca.

Lo primero que se realizó fue obtener y analizar los beneficios de usar el protocolo TFTP dentro de la institución para cualquier tipo de soluciones rápidas o de cualquier situación de catástrofe natural o error humano.

7.1 Análisis de Requerimientos

7.1.1 Requerimientos Funcionales

- Permitir una configuración de transferencia de archivos.
- Debe permitir carga y descarga de archivos.
- Función en redes locales (LAN).
- Compatibles con servidores, router y switch de respaldo utilizados en la escuela.

7.1.2 Requerimiento no Funcionales

- El protocolo TFTP debe ser capaz de operar en entornos con conexión inestables.
- La transferencia de archivos debe ser rápida y ligera, evitando el uso de ancho de banda.

- No requiere de conocimientos avanzados para su uso personal, administrativo y docente.
- El protocolo debe ser capaz de ejecutarse si conexión a internet siempre y cuando este dentro de una red local.
- Debe resistir a fallos de desconexión repentina y debe reanudar la transferencia sin reiniciar el proceso desde cero.

7.2 Herramientas y tecnologías a utilizar

Considerando los aparatos tecnológicos para el desarrollo de la simulación del uso del protocolo TFTP se hará uso de la o las siguientes herramientas y tecnologías:

7.2.1 Para entorno de software y simulación

- Software Cisco Packet Tracer 8.2.1.
- Pc (computadoras).
- Servicio TFTP virtual.
- Router virtual.
- Configuración de comandos CLI en Packet Tracer.

7.2.2 Para entorno físico

- Servicio TFTP (una computadora como servidor TFTP con el software instalado llamado tftp32 o tftp64).
- Cliente TFTP (pc, switch, router).
- Software TFTP (tftp32 o tftp64).
- Router físico con soporte TFTP.
- Switch ethernet.

- Cables ethernet (UDP).
- Consola de administración (PuTTY).
- Configuración de direcciones IP y Subnetting.

7.3 Diseño en Cisco Packet Tracer

Para empezar a realizar el diseño del escenario de simulación se inició abriendo el software de Cisco Packet Tracer y a colocar los componentes y dispositivos.

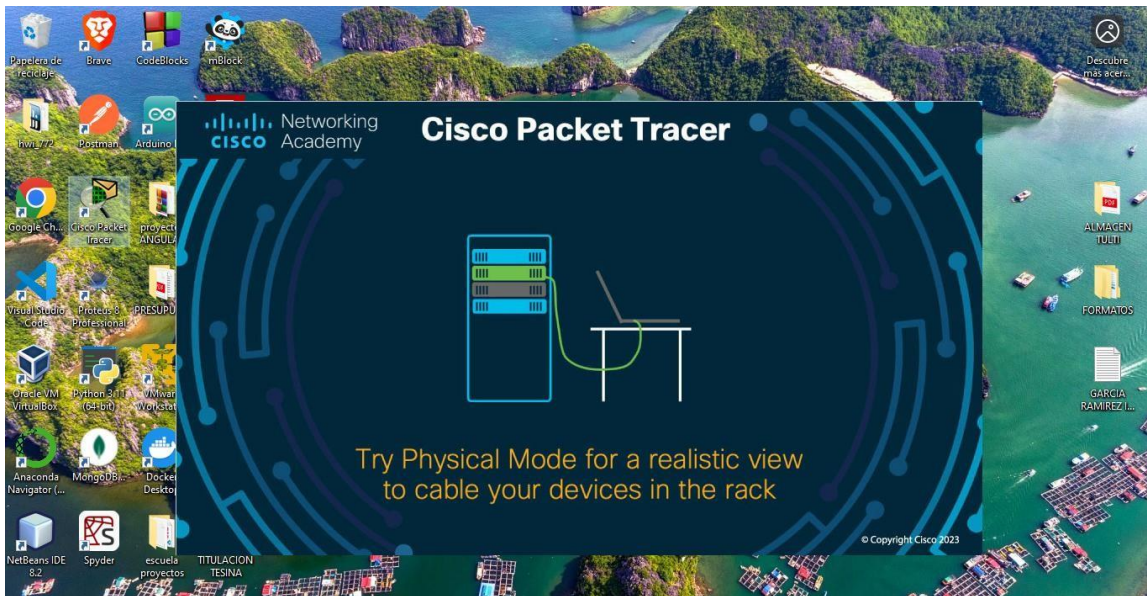


Ilustración 37. Abriendo la aplicación.

Fuente: Propia.

Dentro de la aplicación que se manipula para la creación del escenario de simulación dentro de Packet Tracer encontramos y ocupamos los siguientes componentes tecnológicos que la propia aplicación ofrece.

Servicio Virtual TFTP

Un servidor TFTP permite transferir archivos entre el servidor y el dispositivo cliente (PC) conectados en una misma red local.

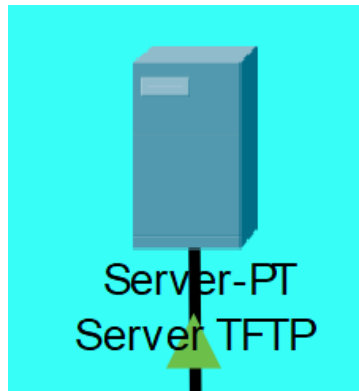


Ilustración 38. Servidor virtual TFTP de Cisco.

Fuente: Propia.

Switch-PT virtual

Un switch-PT es un conmutador que conecta dispositivos a una red generando conectividad Fast Ethernet y Gigabit Ethernet.

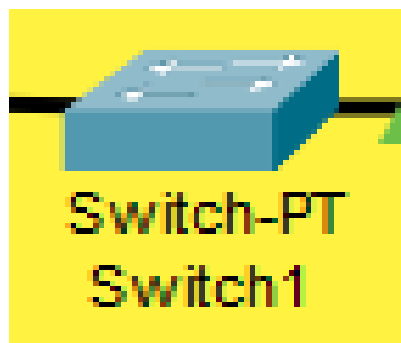


Ilustración 39. Switch virtual de Cisco.

Fuente: Propia.

PC Virtual

Un PC son aquellos que se utilizan para crear topologías de redes virtuales y experimentar con diferentes escenarios. Estas computadoras pueden fungir como cliente-servidor y manejar tareas y solicitudes.



Ilustración 40. PC virtual de Cisco.

Fuente: Propia.

Router virtual

Equipo utilizando en las redes para controlar el tráfico de uno o varios servicios virtuales dentro de la red, este puede dirigir las solicitudes entrantes a diferentes nodos (computadoras).

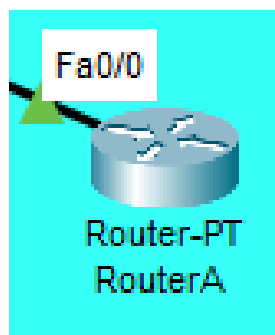


Ilustración 41. Router virtual de Cisco.

Fuente: Propia.

Diseño de escenario virtual

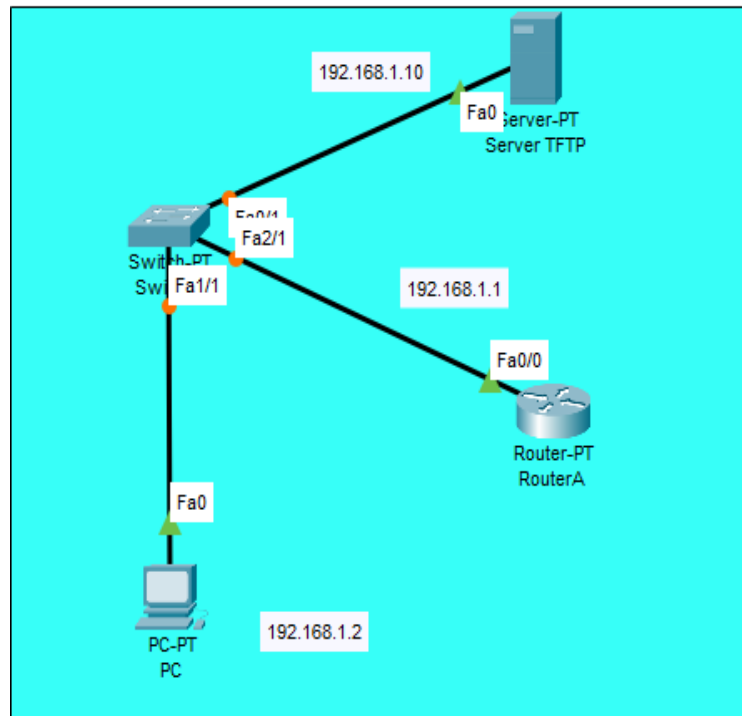


Ilustración 42. Diseño de escenario virtual.

Fuente: Propia.

7.4 Implementación (Desarrollo del funcionamiento de la simulación del uso de protocolo TFTP en Cisco Packet Tracer)

Configuración de servidor TFTP virtual

Se empezó realizando las configuraciones del servidor dejando en modo OFF (apagado) a todos los demás servicios para que no haya un choque de interferencia entre los servicios conocidos como protocolos.

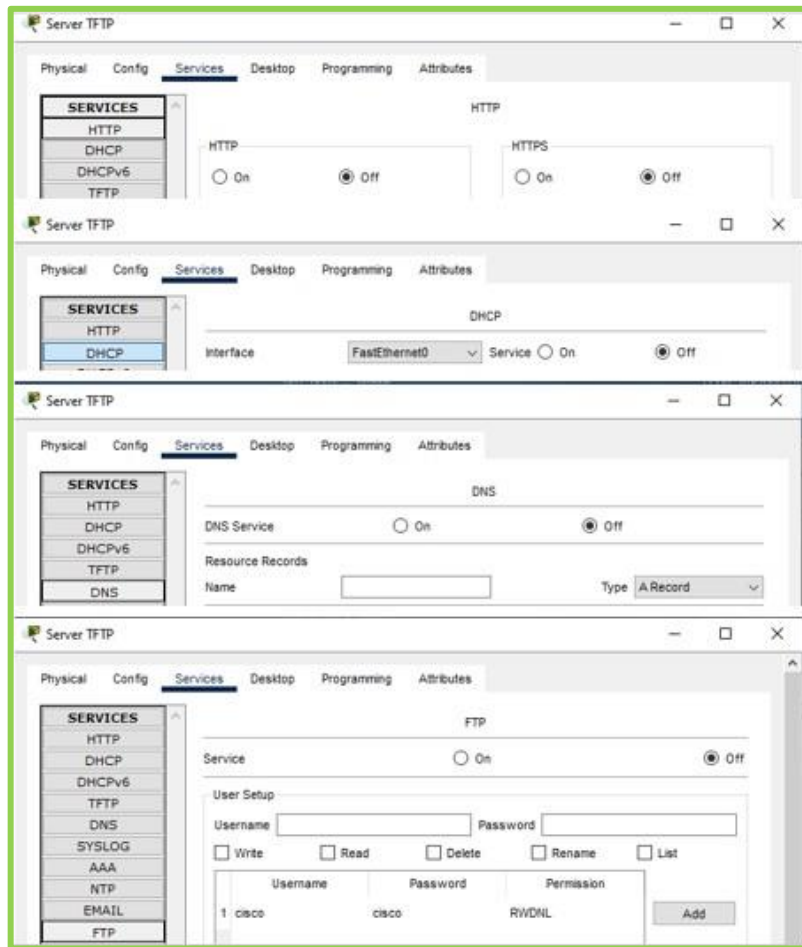


Ilustración 43. Servicios/Protocolos apagados.

Fuente: Propia.

El único protocolo que se queda encendido es el protocolo TFTP para así convertir el servidor en uno de tipo TFTP exclusivamente.

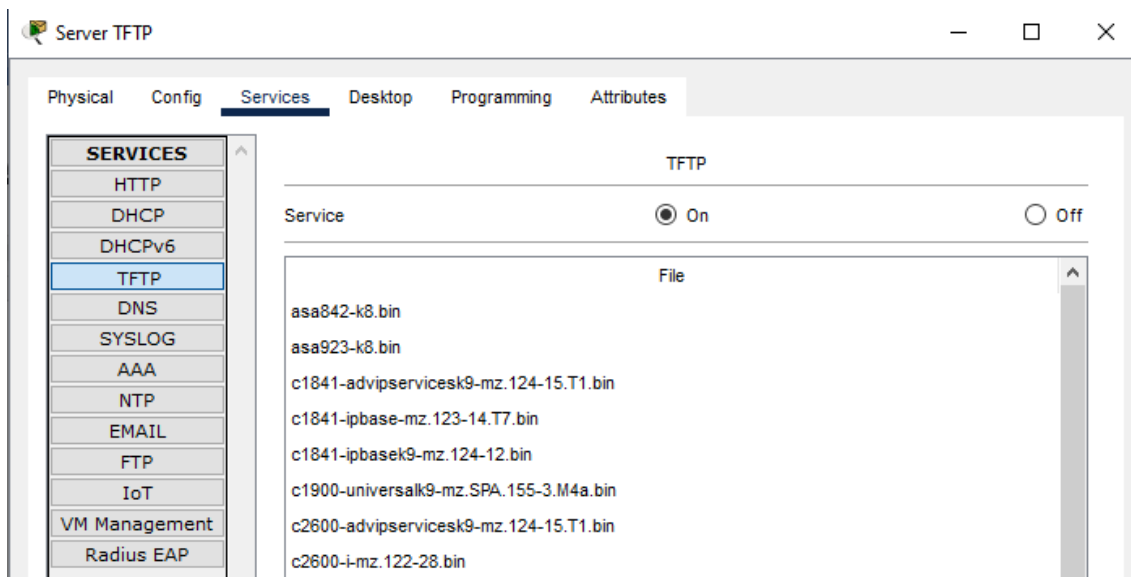


Ilustración 44. Protocolo TFTP activo.

Fuente: Propio.

Después se le asigno una dirección IP al servidor principal ya que a este se estará enlazando la petición de solicitud de transferencia. Esto se hace en el apartado “Desktop”, y en la opción que esta remarcada de color amarillo (IP Configuration) mostrando en la siguiente Ilustración 45.

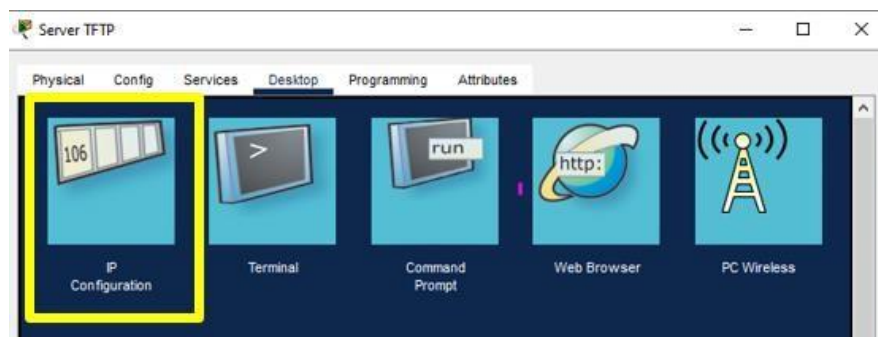


Ilustración 45. IP Configuration.

Fuente: Propia.

La dirección IP que se va a usar para el servidor TFTP es la 192.168.1.10 con una máscara de red 255.255.255.0 y su Default Gateway 192.168.1.1 como se mira en la Ilustración 46.

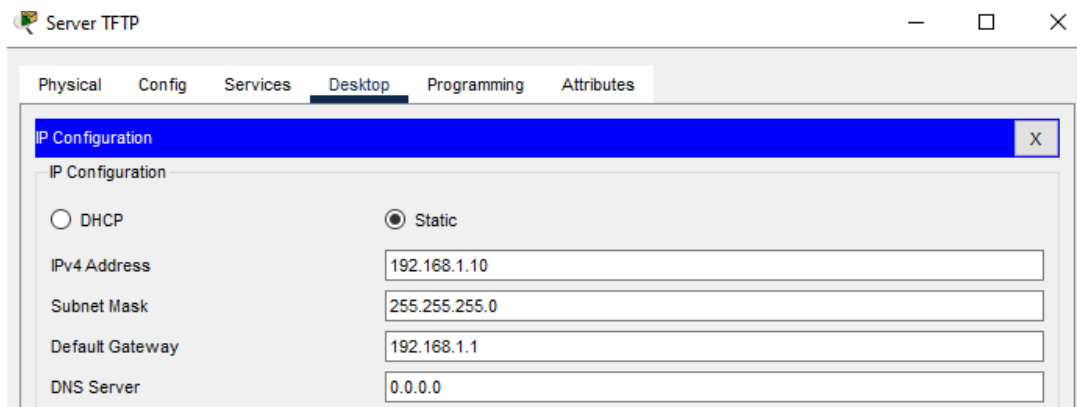


Ilustración 46. Asignación de Dirección IP.

Fuente: Propia.

¿Qué es la Máscara de Subred (Subnet Mask)?

Una máscara de subred segmenta una dirección IP existente en una red TCP/IP, entre la dirección IP y la máscara de subred constituyen una parte importante de las redes informáticas. La máscara de subred es un número de 32 o 128 bits (Castelán, 2022).

¿Qué es el Default Gateway?

La puerta de enlace pre fija, es la dirección IP de un dispositivo (enrutador) conectado a una red, donde la subred se comunica con otros dispositivos de la red, los datos que no se dirigen al dispositivo la subred la renvía a la puerta de enlace predeterminada.

Configuración computadora virtual

La configuración de la PC le asignamos una dirección IP (192.168.1.2) y su puerta de enlace misma que la del servidor para que así pueda haber comunicación entre los dispositivos.

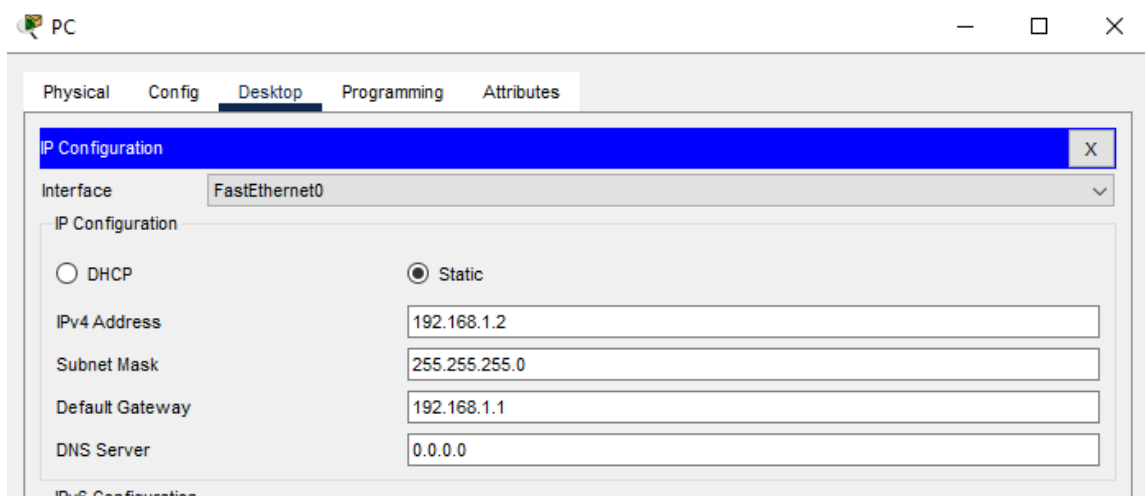
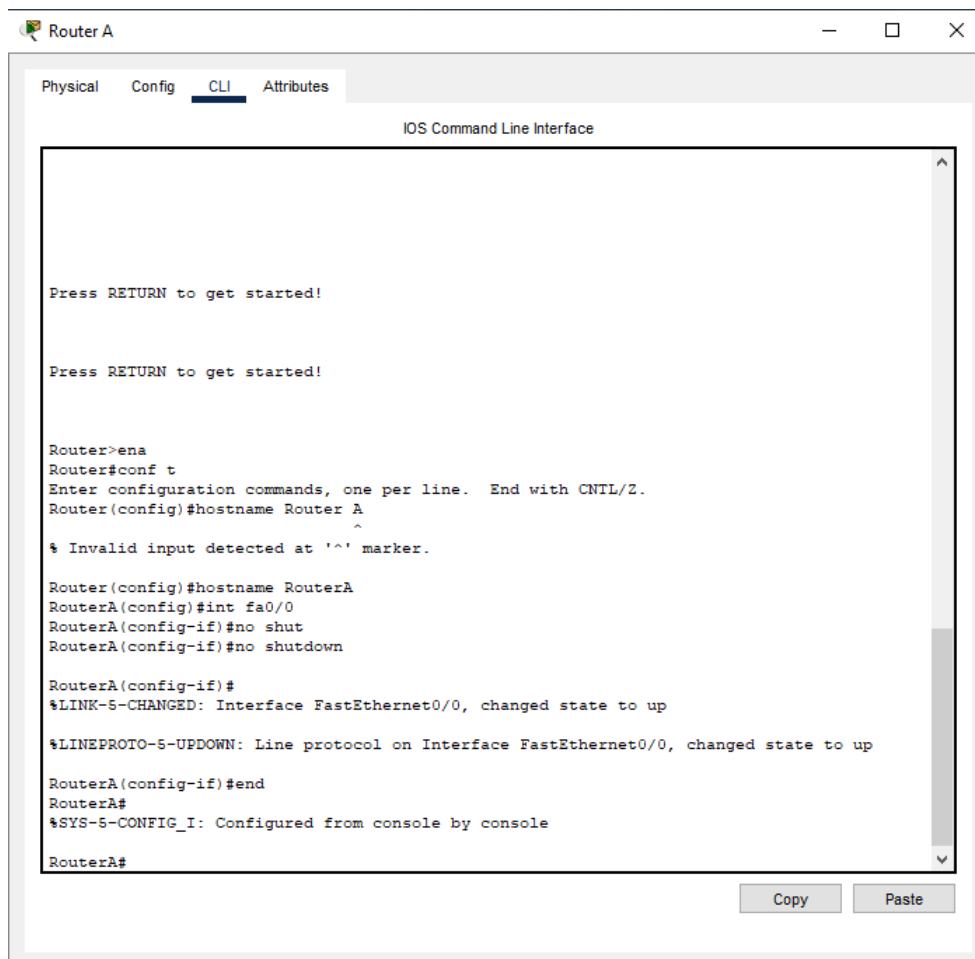


Ilustración 47. Asignación de Dirección IP.

Fuente: Propia.

Configuración de router virtual

Posteriormente se realizó la configuración del router dentro de la línea de comandos CLI, se le proporciono un hostname al "RouterA" y con el código "no shutdown" activamos la interfaz por la cual está conectado en este caso por la interfaz de salida Fast Ethernet 0/0.



The screenshot shows a window titled "Router A" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
Press RETURN to get started!

Press RETURN to get started!

Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Router A
RouterA(config)#hostname RouterA
RouterA(config)#int fa0/0
RouterA(config-if)#no shut
RouterA(config-if)#no shutdown

RouterA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

RouterA(config-if)#end
RouterA#
%SYS-5-CONFIG_I: Configured from console by console

RouterA#
```

At the bottom right of the terminal window, there are "Copy" and "Paste" buttons.

Ilustración 48. Preconfiguración de la Interfaz Fa0/0 a utilizar.

Fuente: Propia.

Y se le asignó igual una IP y una de enlace para que la transferencia de los archivos sea de manera exitosa y llegue al destino correspondiente. En la Ilustración 49 se muestra la configuración por medio de línea de comandos.

```

RouterA>enable
RouterA#
RouterA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#interface FastEthernet0/0
RouterA(config-if)#ip address 192.168.1.10 255.255.255.0
RouterA(config-if)#ip address 192.168.1.10 255.255.255.0
RouterA(config-if)#ip address 192.168.1.1 255.255.255.0
RouterA(config-if)#ip address 192.168.1.1 255.255.255.0
RouterA(config-if)#

```

Ilustración 49. Asignación de IP en CLI.

Fuente: Propia.

7.5 Verificación del funcionamiento del protocolo TFTP

Una vez que ya se tiene la configuración básica de los componentes a utilizar, ahora se empieza a hacer uso de los comandos adecuados para el uso del protocolo TFTP y poder hacer la demostración de transferencia de archivos.

Necesitamos acceder al modo privilegiado del router para posteriormente hacer la copia de la configuración actual del router a un servidor TFTP de red. La ventaja que el software de Packet Tracer tiene es que tenemos manuales de ayuda solo colocando el signo de interrogación cerrado (?) dentro de la línea de comando, esto para mostrar la lista de ayuda y poder seleccionar el comando deseado a utilizar, como se ve en la Ilustración 50.

```

RouterA>ena
RouterA>enable
RouterA#copy run
RouterA#copy running-config ?
  flash:          Copy to flash file
  ftp:            Copy to current system configuration
  scp:           Copy to scp: file system
  startup-config Copy to startup configuration
  tftp:          Copy to current system configuration
RouterA#copy running-config

```

Ilustración 50. Demostración de lista de Ayuda usando (?).

Fuente: Propia.

Se visualiza en la Ilustración 50 dentro la lista de apoyo aparece el protocolo TFTP, comando que se utiliza para poder hacer la transferencia de archivo y del cual se habla en este documento.

Después de que ya sabemos que si se puede hacer uso del comando TFTP al comando que ya habíamos pre escrito lo a completamos con el tftp, luego introducimos la dirección IP que corresponde al servidor de TFTP que ya previamente se le había asignado y colocamos el nombre destino a esta transferencia que esta a punto de realizarse.

Le nombraremos como ejemplo “PRUEBATESIS”, como se ve en la Ilustración 51.

```
RouterA#copy running-config tftp
Address or name of remote host []? 192.168.1.10
Destination filename [RouterA-config]? PRUEBATESIS
```

Ilustración 51. Uso de comando TFTP.

Fuente: Propia.

La Ilustración 52 señalada a continuación, se observa que la copia del archivo se realizó correctamente.

```
RouterA>ena
RouterA#copy run
RouterA#copy running-config tftp
Address or name of remote host []? 192.168.1.10
Destination filename [RouterA-config]? PRUEBATESIS

Writing running-config...!!
[OK - 730 bytes]

730 bytes copied in 0.598 secs (1220 bytes/sec)
RouterA#
```

Ilustración 52. Archivo correctamente copiado.

Fuente: Propia.

Para comprobar la copia correctamente realizada. Dentro de las configuraciones del servidor TFTP en la sección de “Services” > TFTP aparecerá el archivo al cual se le asigno el nombre de PRUEBATEISIS, si ya se encuentra dentro del servidor indica que el archivo fue correctamente transferido y guardado en el server como se visualiza en la Ilustración 53.

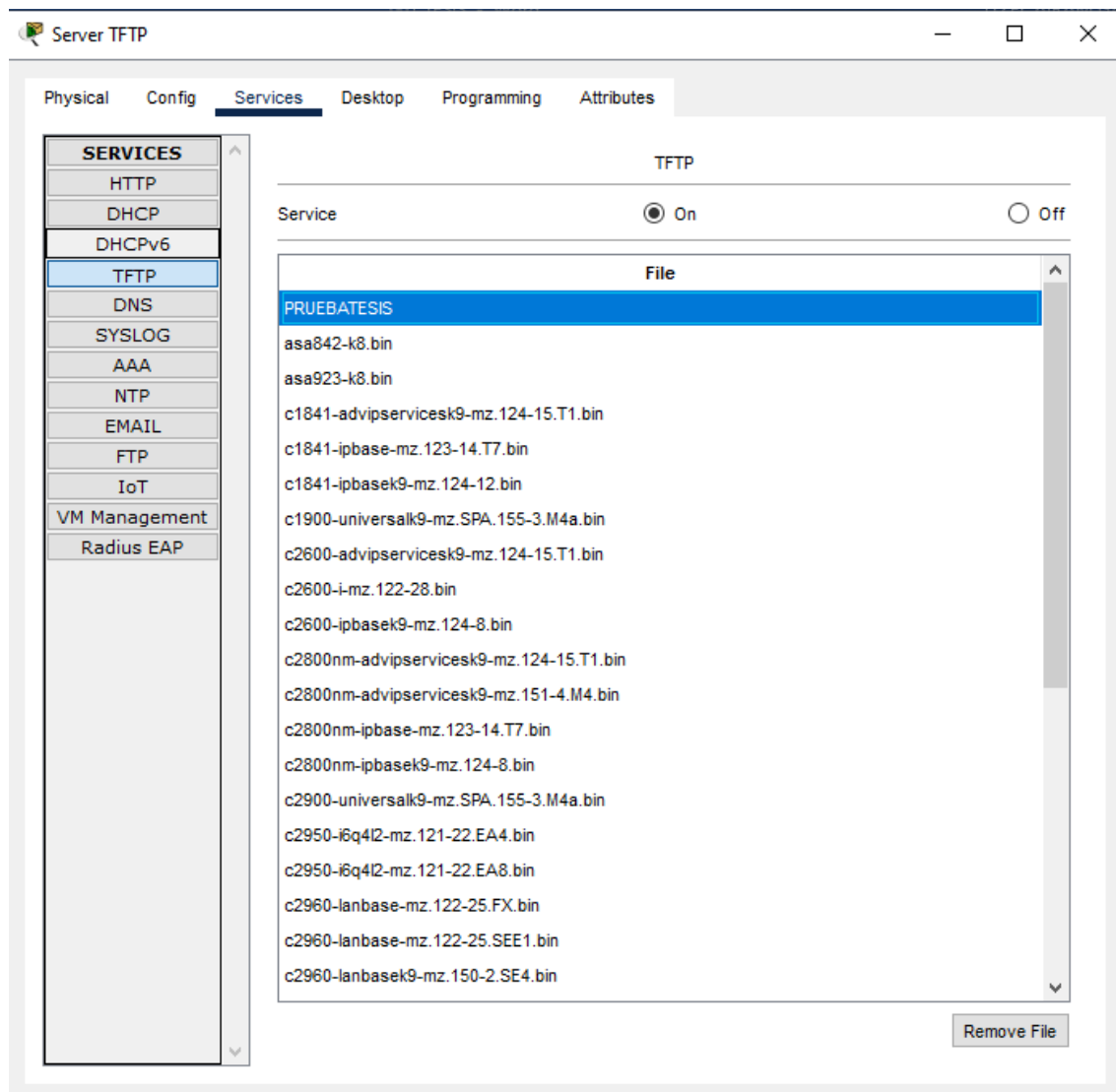


Ilustración 53. Archivo Transferido correctamente.

Fuente: Propia.

7.6 Representación de forma Física

A continuación, las pruebas realizadas para comprobar el funcionamiento del protocolo TFTP de interés en este trabajo fueron haciendo la implementación con equipos de cómputo personales, esto para no atrasar el trabajo escrito y llevando a cabo una demostración dentro de instalaciones administrativas para que el personal viera la funcionalidad del protocolo.

Hasta el momento me encuentro en espera de una respuesta donde me autoricen realizar la implementación fija dentro de la institución educativa, ya que hay un proceso de seguimiento y de cambio de direcciones por el cual debo esperar y llevar a cabo las indicaciones recibidas para así poder implementarlo en la institución finalmente.

Para realizar la demostración física del protocolo TFTP, es necesario descargar el software tftp32 e instalarlo en los ordenadores a utilizar. Esto para hacer la transferencia de los archivos que sean.



Ilustración 54. Software tftp32 Download.

Fuente: https://download.cnet.com/es/tftpd32/3000-2085_4-10114225.html

Para poder tener una descarga exitosa es necesario desactivar el Firewall porque si no la descarga se cancelará directamente. Este es uno de los factores por el cual no se considera seguro y confiable el uso del protocolo.

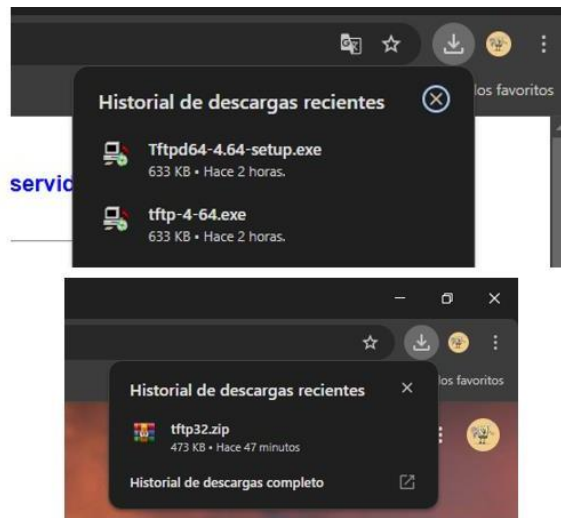


Ilustración 55. Historia de Descargas.

Fuente: Propia.

Después se ejecuta la aplicación de tftp32 para poder abrir la ventana inicial de software como se ve en la siguiente Ilustración 56. Y así poder comenzar la transferencia real de un archivo.

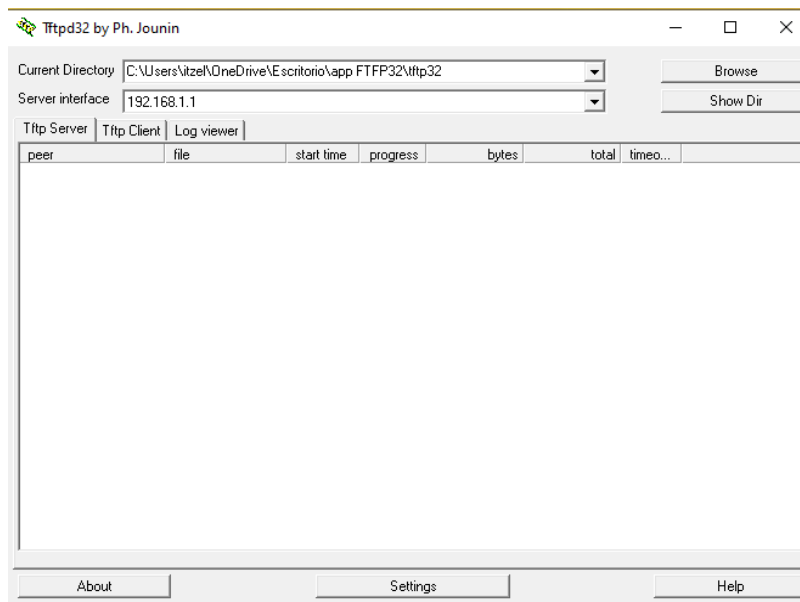


Ilustración 56. Interfaz de software tftp32.

Fuente: Propia.

7.6.1 Implementación y Verificación del funcionamiento del protocolo TFTP con software tftp32

Recordando la información de este protocolo, las computadoras deben estar conectadas a la red LAN para que el funcionamiento de la aplicación ejecute correctamente el protocolo.

Para saber si ambas computadoras se encuentran en la misma red, se realiza lo siguiente:

Entramos con las teclas WIN+R y escribiendo en el cuadro de ejecución CMD, se abrirá una ventana como la de la Ilustración 57 de abajo.

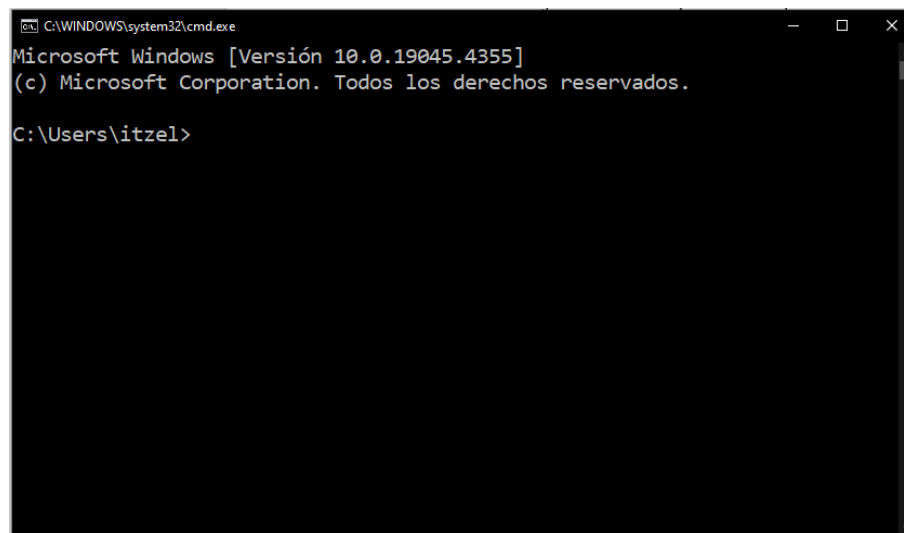


Ilustración 57. Ventana del CMD.

Fuente: Propia.

Si se encuentran conectadas por medio de WiFi la dirección IP debe verse en la sección de "Adaptador de LAN Inalámbrica WI-FI", si están conectadas por medio de cable Ethernet en la sección "Adaptador de Ethernet".

Siguiendo con el procedimiento realizado, dentro de esa ventana del cmd se escribe en ambos ordenadores ipconfig, esto para conocer las direcciones IP de cada una de las computadoras, así como se mira la Ilustración 58, enseña la máquina principal que enviará el archivo que tiene una dirección IP “192.168.43.20”.

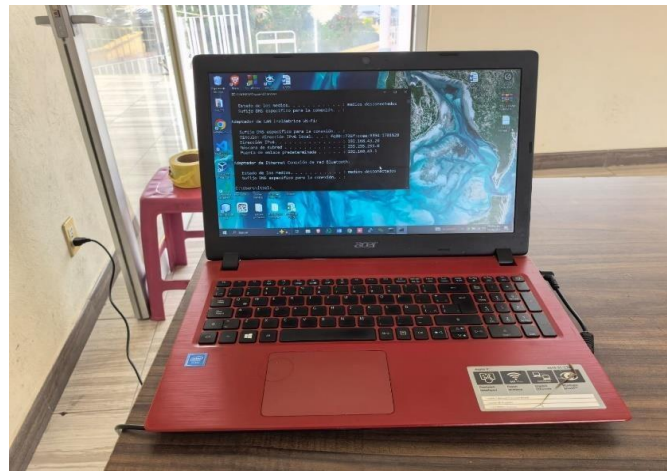


Ilustración 58. Dirección IP de pc Servidor.

Fuente: Propia.

Y en la computadora cliente, la que recibirá la transferencia tiene la dirección IP “192.168.43.62”.



Ilustración 59. Dirección IP de pc Cliente. Fuente: Propia.

Una vez que se corroboraron que las computadoras están conectadas dentro de la misma red, para corroborar que hay una conexión entre ellas se escribe el siguiente comando: ping + dirección IP de la máquina destino, ejemplo (ping 192.168.43.62).

Si se mandaron los paquetes como se muestra en la siguiente Ilustración 60 es porque si hay comunicación entre ambos ordenadores y obviamente están ubicadas dentro de la misma red.

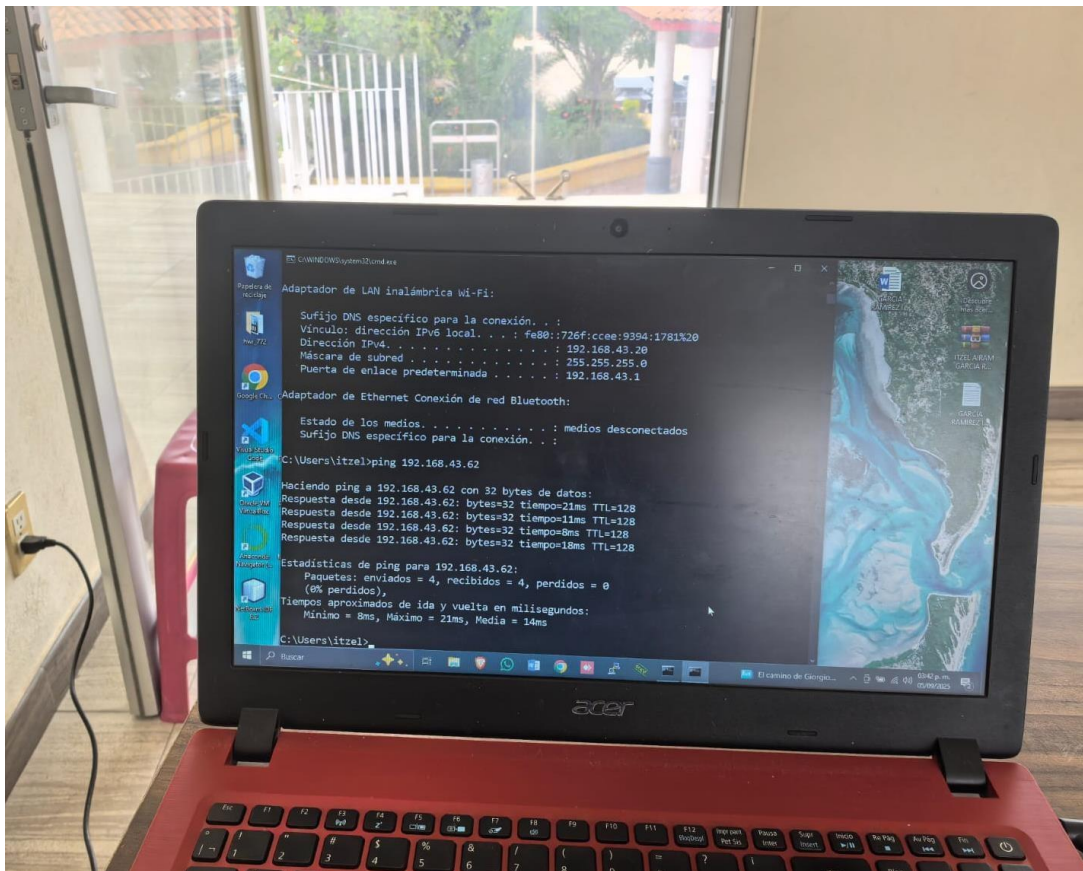


Ilustración 60. Muestra de paquetes enviados de servidor a cliente.

Fuente: Propia.



Ilustración 61. Muestra de paquetes enviados de cliente a servidor.

Fuente: Propia.

Una vez corroboradas las redes de los ordenadores, se empieza a llevar a cabo la implementación del protocolo TFTP dentro del software tftp32.

Selecciona en el apartado de "tftp client" para ambas computadoras involucradas de las cuales se hará el procedimiento de transferencia de archivo.

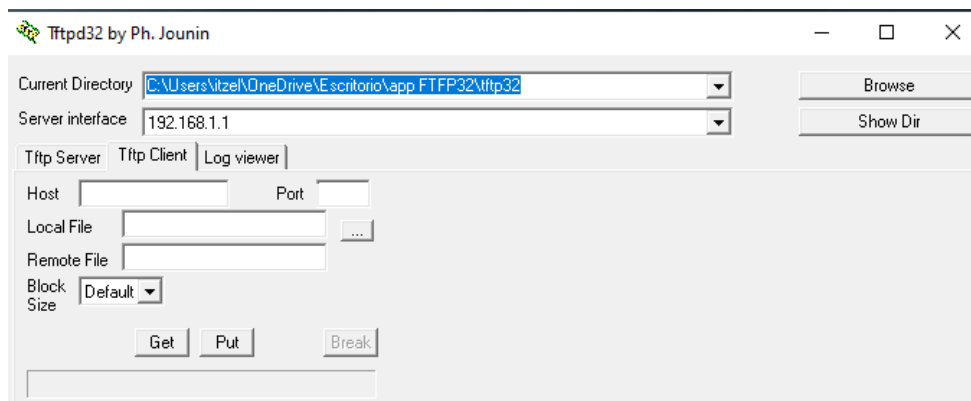


Ilustración 62. Sección de "tftp client". Fuente: Propia.

En el apartado de Host se coloca la IP de la computadora cliente y el puerto como ya se sabe es el 69, puerto definido por las normas. En local file se selecciona el archivo a transferir, para observar los campos a llenar se muestra en la Ilustración 63 de abajo.

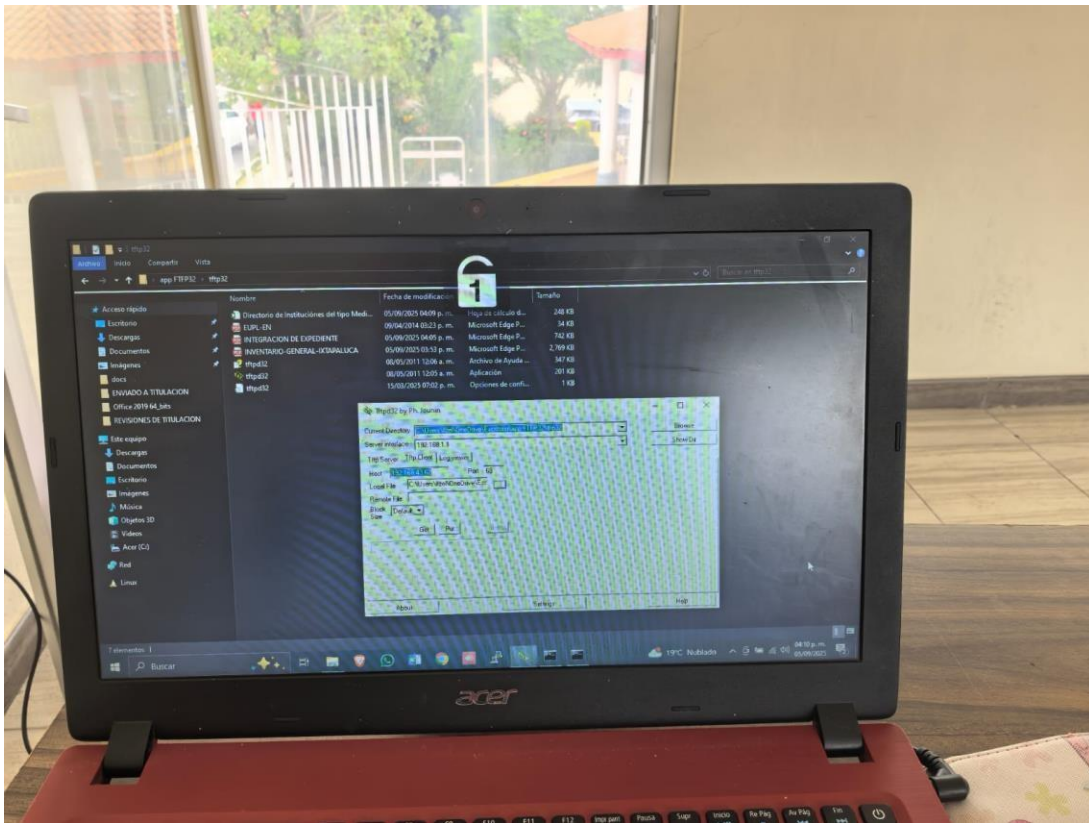


Ilustración 63. Campos a llenar.

Fuente: Propia.

Para comprobar que el puerto está en el 69, en el apartado de Settings se elige TFTP y se visualiza como en la Ilustración 64.

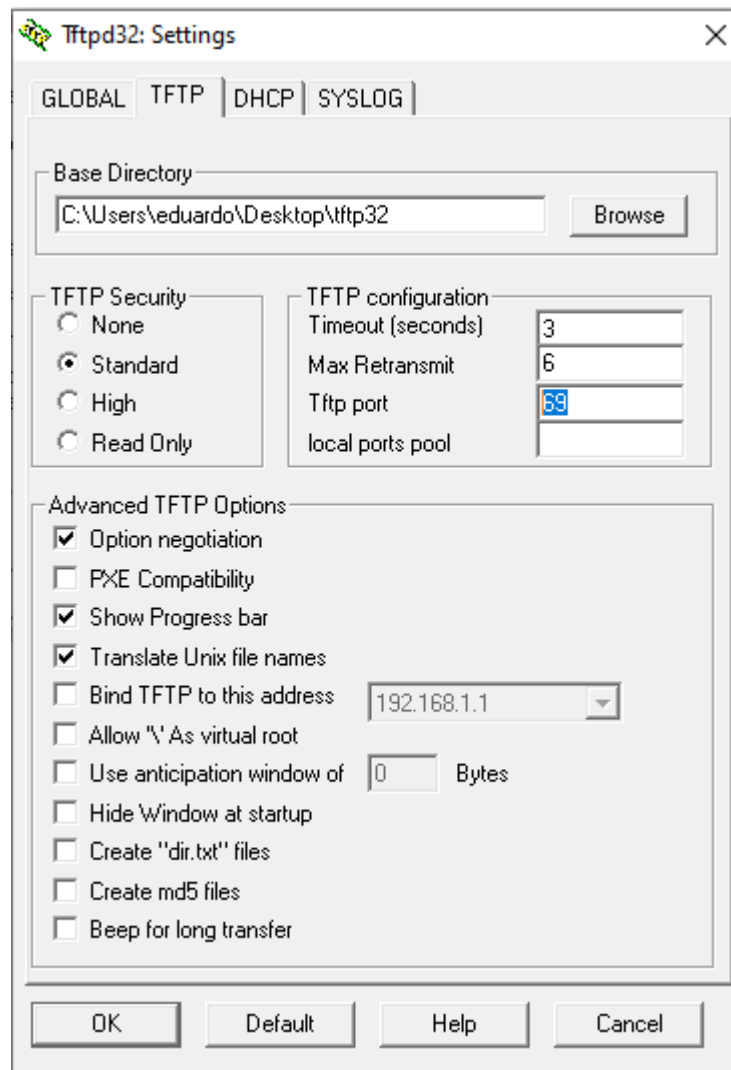


Ilustración 64. Puerto 69 de TFTP.

Fuente: Propia.

Se observa el archivo que se va a transferir está en formato PDF nombrado “INVENTARIO-GENERAL-IXTAPALUCA” ubicado dentro de la carpeta del software tftp en el escritorio de la computadora principal.

Para comprobar que la computadora cliente no cuenta con ese archivo se muestra lo que tiene guardado en la carpeta ubicada dentro del escritorio de la computadora cliente.

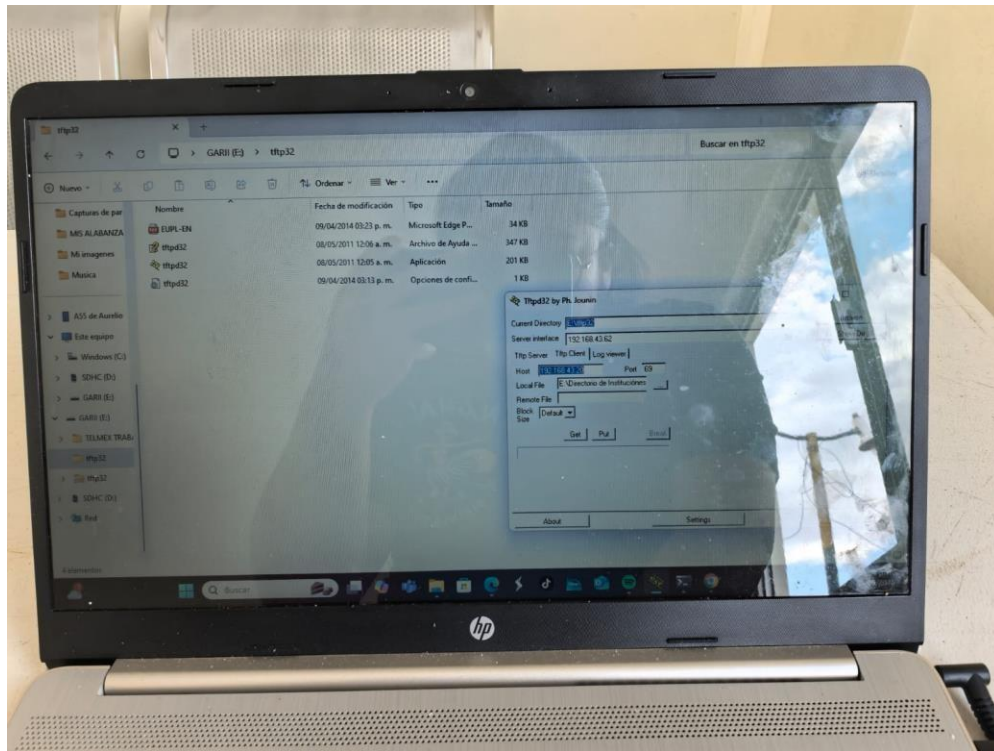


Ilustración 65. Carpeta con solo archivos determinados del software tftp32.

Fuente: Propia.

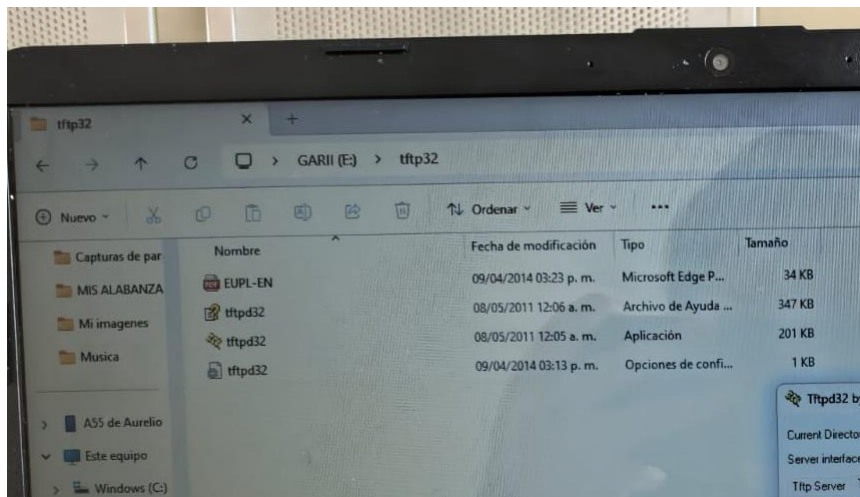


Ilustración 66. Demostración del equipo sin archivo recibido aún.

Fuente: Propia.

Ya que se tienen los campos y el archivo listos se da clic en el botón de Put y empezará a cargar una barra indicando que la transferencia comenzó. La

Ilustración 67 muestra el tiempo transcurrido que se hizo la transferencia hacia la computadora destino (el tiempo dependerá de la estabilidad de la red o el peso del archivo).

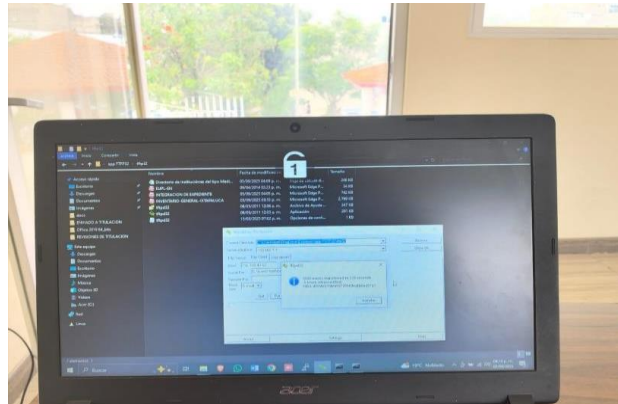


Ilustración 67. Transferencia del archivo.

Fuente: Propia.

Mientras se hace la transferencia de la computadora servidor a la computadora cliente, se observa un cuadro con una línea de carga indicando que la transferencia está en **curso**, como se muestra en la Ilustración 68.

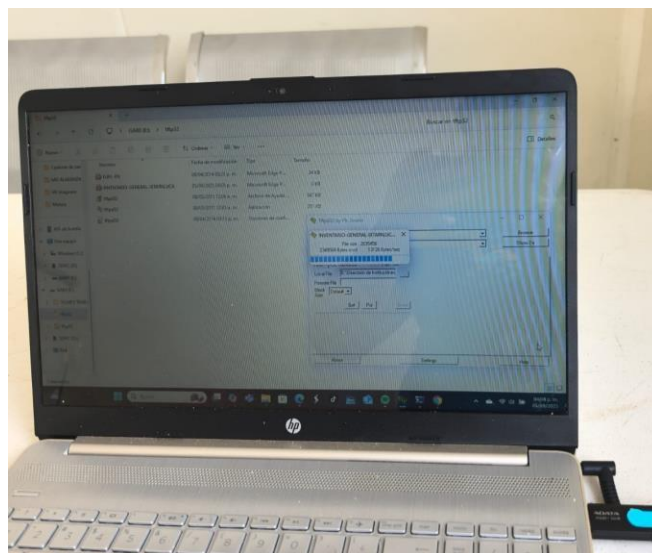


Ilustración 68. Transferencia en curso en pc cliente.

Fuente: Propia.

Una vez que termina la transferencia del archivo el cuadro de carga se cierra y directamente el archivo que se envió se localiza dentro de la carpeta donde se tiene ubicado el software tftp32, así como se ve en la Ilustración 69.

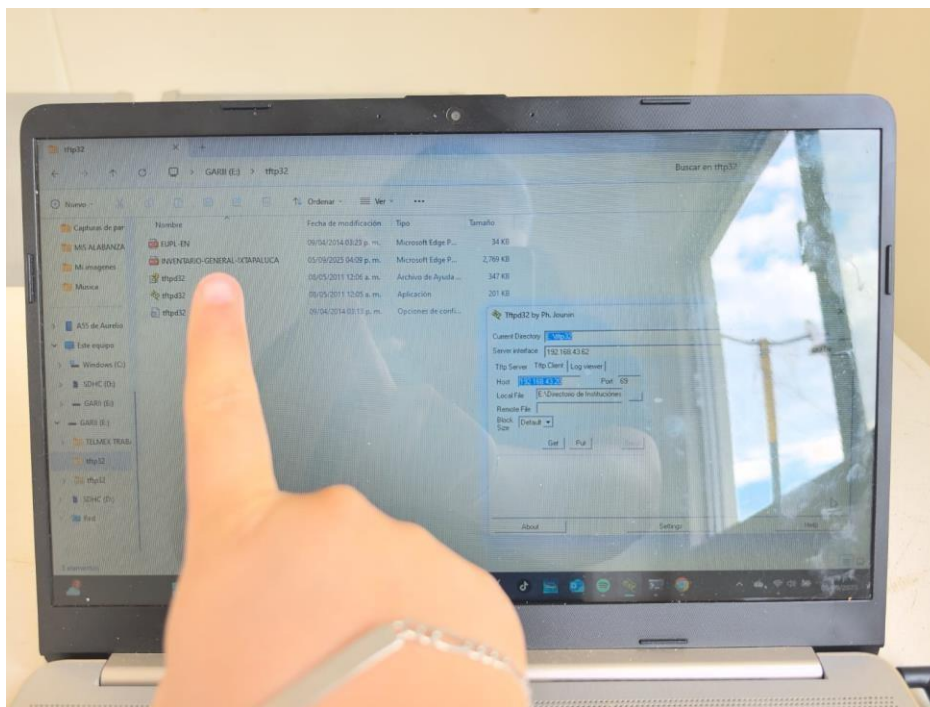


Ilustración 69. Archivo transferido al cliente exitosamente.

Fuente: Propia.

Hacemos la verificación dentro del cliente mostrando que el archivo recibido abre correctamente como si el documento hubiera existido desde un inicio ahí.

La Ilustración 70, enseña que el PDF nombrado “INVENTARIO-GENERAL-XTAPALUCA” abre con normalidad y sin afectación al documento por la transferencia con el uso del software tftp32.

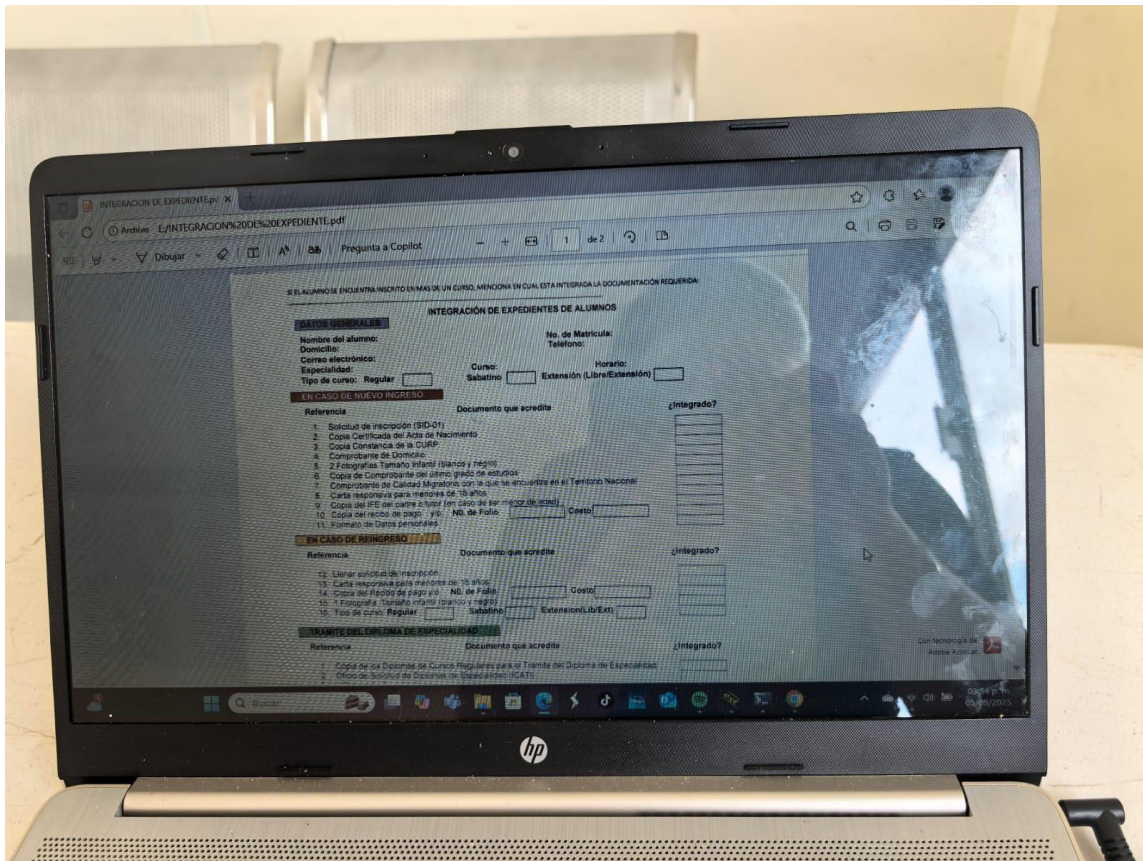


Ilustración 70. Archivo funcionando en Pc cliente después de la transferencia.

Fuente: Propia.

Si es verdad, que para el uso del software tftp32 debe seguir desactivado el Firewall de ambos ordenadores desde que se va a realizar la descarga de este software.

Se puede notar que sin problemas se le puede dar una oportunidad al protocolo TFTP y en un futuro este ya sea utilizado a lo mejor como el FTP.

Así como se hizo la transferencia del Servidor al cliente, se puede hacer de una forma viceversa de Cliente a servidor y funciona igual.

Escenarios Finales Virtual y Real

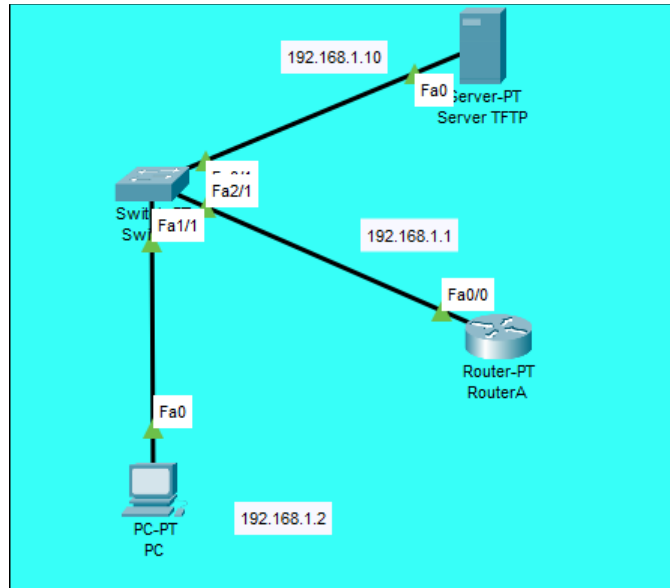


Ilustración 71. Escenario Virtual Final.

Fuente: Propia.



Ilustración 72. Escenario Físico Final Servidor-Cliente.

Fuente: Propia.

VIII. CONCLUSIONES Y SUGERENCIAS

8.1 Conclusiones

- Se concluyó que el uso de las herramientas tecnológicas como en el caso del uso de software para poder hacer las demostraciones de transferencia de archivos en una manera adecuada y sin colocar en riesgo la integridad de cada documento, ayudan a dar solución rápida a algún problema de error humano, de catástrofe o simplemente en alguna situación fuera de nuestros alcances.
- El uso del software tanto de Cisco Packet Tracer como el de tftp32 facilitan acciones que saquen en el momento dudas, situaciones o incluso necesidades que se requieran de momento, tftp32 hace la transferencia de los archivos sin necesidad de tener la clave para su transferencia, ya que si su transferencia es por medio del uso del protocolo tftp aunque es muy poco segura de ese método, este software si puede sacar con facilidad la urgencia sin afectar el archivo, por supuesto dependiendo circunstancias.
- El uso del protocolo TFTP facilita tareas de las personas dentro de algún institución educativa, laboral o incluso personal, ya que sin necesidad de una clave o algún permiso de autenticación se pueda transferir el archivo y así estar evitando de ir de un punto a otro a solicitar dicho archivo.

8.2 Sugerencias

- Si bien no es necesario el uso de software tftp32 actualizado o de cables para su manipulación y realización de su transferencia.
- Como trabajo futuro se podría implementar ya un servidor TFTP específico para el área responsable

IX. REFERENCIAS

- AWS. (2024). Obtenido de <https://aws.amazon.com/es/what-is/api/>
- Beal, V. (28 de Abril de 2024). Obtenido de <https://www.techopedia.com/definition/5107/wireless-local-area-network-wlan>
- Bush, G. (2024). *The white house*. Obtenido de <https://georgewbush-whitehouse.archives.gov/government/cerf-kahn-bio.html>
- Castelán, J. (9 de Junio de 2022). *Talently*. Obtenido de <https://talently.tech/blog/que-es-una-mascara-de-subred/>
- CCNA. (2025). Obtenido de https://ccnadesdecero.es/capa-transporte-definicion-y-funciones/#google_vignette
- Cisco. (9 de Mayo de 2025). Obtenido de <https://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/48700-tftp-server.html>
- Cisco. (2025). Obtenido de <https://www.cisco.com/site/us/en/learn/topics/networking/what-is-routing.html>
- Cloudflare. (28 de Marzo de 2024). Obtenido de <https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/>
- Cloudflare. (2025). Obtenido de <https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-metropolitan-area-network/>
- Cohen, C. (20 de Octubre de 2023). Obtenido de <https://www.cbttuggets.com/common-ports/what-is-port-69>
- Corona, A. E. (2004). Protocolos TCP/IP de Internet. *Revista Digital Universitaria UNAM*, 4-7.
- Dávila, G. (2015). Obtenido de <https://bonga.unisimon.edu.co/items/cbb661ef-30e3-4263-b7b2-810e88237f5f>
- Estrada, J. (2025). *Universidad Autónoma Metropolitana*. Obtenido de <https://academicos.azc.uam.mx/jestrada/archivos/redes2/capa2/ICMP.pdf>

Fernández, E. C. (19 de Febrero de 2025). Obtenido de <https://www.tokioschool.com/noticias/tipos-redes-informaticas/>

Fernández, Y. (18 de Abril de 2024). *Xataka*. Obtenido de <https://www.xataka.com/basics/ftp-que-como-funciona>

Fortinet. (2025). Obtenido de <https://www.fortinet.com/lat/resources/cyberglossary/what-is-arp>

Garn, D. (19 de Enero de 2024). Obtenido de <https://www.techtarget.com/searchnetworking/tutorial/How-to-use-TFTP-to-transfer-files-across-the-network>

Gorman, B. (23 de Febrero de 2023). *Avast*. Obtenido de <https://www.avast.com/es-es/c-tcp-vs-udp-difference>

Hostinger. (9 de Febrero de 2025). Obtenido de https://www.hostinger.com/mx/tutoriales/protocolo-tcp#%C2%BFQue_es_el_Protocolo_TCP

Huawei. (2025). Obtenido de <https://support.huawei.com/enterprise/en/doc/DOC1000091883/b07acf1a/transferring-files-using-ftp-tftp>

IBM. (3 de Marzo de 2021). Obtenido de <https://www.ibm.com/docs/es/aix/7.1.0?topic=protocol-tcpip-protocols>

IBM. (27 de Agosto de 2024). Obtenido de <https://www.ibm.com/docs/es/aix/7.2.0?topic=protocols-internet-application-level>

IONOS. (8 de Junio de 2020). Obtenido de <https://www.ionos.mx/digitalguide/servidores/know-how/wan/>

IPData. (5 de Octubre de 2025). Obtenido de <https://ipdata.es/packet-tracer/>

Lenovo. (2025). Obtenido de https://www.lenovo.com/mx/es/glosario/que-es-un-bit/?orgRef=https%253A%252F%252Fwww.google.com%252F&srsIid=AfmBOopF13vcgjp5FQXc9ApM_hKNQ0474OgldCUjE7_FumBjKS8hDKE7

Luz, S. D. (7 de Abril de 2025). Obtenido de <https://www.redeszone.net/tutoriales/redes-cable/puerto-wan-que-es/>

Luz, S. D. (18 de Junio de 2025). Obtenido de <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/>

Meza, Q. (2018). *Platzi*. Obtenido de <https://platzi.com/cursos/redes/modelo-osi/>

Meza, Q. (2024). *Platzi*. Obtenido de <https://platzi.com/cursos/redes/modelo-tcpip/>

Microsoft. (2024). Obtenido de <https://www.microsoft.com/es-mx/security/business/security-101/what-is-authentication>

Microsoft. (14 de Julio de 2025). Obtenido de <https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>

Oracle. (2010). Obtenido de <https://docs.oracle.com/cd/E19957-01/820-2981/ipov-15/index.html>

Oracle. (2014). Obtenido de https://docs.oracle.com/cd/E55837_01/html/E54251/makehtml-id-38.html

PC Solución. (2025). Obtenido de <https://pc-solucion.es/diferencias-entre-ftp-y-tftp/>

Research, A. (14 de Mayo de 2024). Obtenido de <https://www.appinio.com/en/blog/market-research/experimental-research>

Sapalomera. (2025). Obtenido de <https://www.sapalomera.cat/moodlecf/RS/1/course/module6/6.1.2.1/6.1.2.1.html>

SDI Industrial. (2025). Obtenido de <https://sdindustrial.com.mx/blog/protocolos-de-comunicacion-que-son/>

Sollins. (2 de Julio de 1992). Obtenido de <https://datatracker.ietf.org/doc/html/rfc1350>

Spasojevic, A. (2 de Octubre de 2024). Obtenido de <https://phoenixnap.mx/glosario/transmisi%C3%B3n-de-datos>

Stepanets, A. (17 de Enero de 2024). *GanttPro*. Obtenido de <https://blog.ganttpro.com/es/metodologia-de-cascada/#:~:text=%C3%A1giles%20y%20cascada-,%C2%BFQu%C3%A9%20es%20el%20m%C3%A9todo%20de%20casc>

Universidad del Azuay. (2025). Obtenido de https://www.uazuay.edu.ec/sistemas/teleprocesos/capa_enlace

UsuarioDebian. (15 de Marzo de 2008). Obtenido de <https://usuariodebian.blogspot.com/2008/03/impresora-local-compartida.html>

Videgain, J. (16 de Mayo de 2019). *Academy*. Obtenido de <https://academy.bit2me.com/que-es-el-servidor-dns/>

Villanueva, J. C. (2 de Marzo de 2025). Obtenido de https://www-jscape-com.translate.goog/blog/what-is-tftp?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Villanueva, J. C. (2025). Obtenido de <https://www.jscape.com/blog/active-v-s-passive-ftp-simplified>

Wordpress. (2025). Obtenido de <https://redessegunsudistanciadetransmision.wordpress.com/red-lan/ventajas-y-desventajas-de-la-red-lan/>