CARRERA TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES

TEMA:

"IMPLEMENTACIÓN DE UN SERVICIO VPN PARA ACCESO REMOTO A EQUIPOS ACTIVOS DEL LABORATORIO CISCO EN EL CAMPUS RAMÍREZ DÁVALOS DEL ITI"

Proyecto Integrador de grado previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones.

AUTOR: Jimmy Jossué Díaz Oña

DIRECTOR: Cristian David Muñoz Tenempaguay

D.M. Quito, mayo 2023

DEDICATORIA

Este proyecto está dedicado a mi familia quien siempre estuvo ahí desde el primer día que incursione en la carrera, especialmente a mi madre quien me motivo a seguir adelante y no dejarme dar por vencido a pesar de las dificultades, el insistirme y hacerme entender que el estudio será fundamental para mi vida y el legado más valioso que me han dejado. A mis maestros, por brindarme sus conocimientos que fueron fundamentales y a mi tutor asignado para el proyecto.

AGRADECIMIENTO

En primer lugar, agradezco a Dios por darme la oportunidad de poder cumplir un sueño junto al apoyo de mis padres quien son el pilar fundamental de mi vida y con quienes estoy muy agradecido por darme la oportunidad de estudiar, por inculcarme valores, por no dejarme dar por vencido y motivarme a seguir adelante haciéndome entender que el estudio es fundamental para forjar una vida, a mis maestros a quienes fui conociendo en el transcurso de la carrera y me supieron brindaron sus preciados conocimientos, a mi tutor que me guio, apoyo en el desarrollo del presente proyecto.

AUTORIA

Yo, Jimmy Jossué Díaz Oña, autor del presente informe, me responsabilizo por los conceptos, opiniones y propuestas contenidos en el mismo. El patrimonio intelectual de la misma pertenece al INSTITUTO TECNOLOGICO INTERNACIONAL UNIVERSITARIO ITI.

Atentamente

Jimmy Jossué Díaz Oña

D.M. Quito, 30 de mayo del 2023

Cristian David Muñoz Tenempaguay

DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICA

Haber revisado el presente informe de investigación, que se ajusta a las normas institucionales y académicas establecidas por el Instituto Tecnológico Superior Internacional ITI, de Quito, por tanto, se autoriza su presentación final para los fines legales pertinentes.

Cristian David Muñoz Tenempaguay

D.M. Quito, 30 mayo del 2023

DECLARACIÓN DE CESIÓN DE DERECHOS DE TRABAJO FIN DE CARRERA

Yo, Jimmy Jossué Díaz Oña, declaro ser autor del Trabajo de Investigación con el nombre "IMPLEMENTACION DE UN SERVICIO VPN PARA ACCESO REMOTO A EQUIPOS ACTIVOS DEL LABORATORIO CISCO EN EL CAMPUS RAMIREZ DAVALOS DEL ITI" como requisito para optar al grado de Tecnólogo Superior en Redes y Telecomunicaciones y autorizo al Sistema de Bibliotecas del Instituto Tecnológico Internacional Universitario ITI para que con fines netamente académicos divulgue esta obra a través del Repositorio Digital Institucional.

Los usuarios de la biblioteca podrán consultar el contenido de este trabajo en las redes de información del país y del exterior, con las cuales el Instituto tenga convenios. El Instituto Tecnológico Internacional Universitario ITI no se hace responsable por el plagio o copia del contenido parcial o total de este trabajo.

Del mismo modo, acepto que los Derechos de Autor, Morales y Patrimoniales, sobre esta obra, serán compartidos entre mi persona y el Instituto Tecnológico Internacional Universitario ITI, y que no tramitaré la publicación de esta obra en ningún otro medio, sin autorización expresa de la misma. En caso de que exista el potencial de generación de beneficios económicos o patentes, producto de este trabajo, acepto que se deberán firmar convenios específicos adicionales, donde se acuerden los términos de adjudicación de dichos beneficios.

Para constancia de esta autorización, en la ciudad de Quito, a los 30 días del mes de mayo del 2023, firmo conforme: Conste por el presente documento la cesión de los derechos en trabajo fin de carrera, de conformidad con las siguientes clausulas:

PRIMERA: El Ing. Cristian David Muñoz Tenempaguay y por sus propios derechos en calidad de Director del trabajo fin de carrera; y el Sr. Jimmy Jossué Díaz Oña por sus propios derechos, en calidad de autor del trabajo fin de carrera.

SEGUNDA:

UNO. -El Sr. Jimmy Jossué Díaz Oña realizó el trabajo fin de carrera titulado: IMPLEMENTACION DE UN SERVICIO VPN PARA ACCESO REMOTO A EQUIPOS ACTIVOS DEL LABORATORIO CISCO EN EL CAMPUS RAMIREZ DAVALOS DEL ITI, para optar por el título de, Tecnólogo Superior en Redes y Telecomunicaciones en el Instituto Tecnológico Superior Internacional ITI, bajo la dirección del Ing. Cristian David Muñoz Tenempaguay.

DOS. -Es política del Instituto Tecnológico Superior Internacional ITI, que los trabajos fin de carrera se aplique, se materialicen y difundan en beneficio de la comunidad.

TERCERA: Los comparecientes, Ing. Cristian David Muñoz Tenempaguay, en calidad de director del trabajo fin de carrera y el Sr. Jimmy Jossué Díaz Oña como autor del mismo, por medio del presente instrumento, tienen a bien ceder en forma gratuita sus derechos en el trabajo fin de Carrera titulado IMPLEMENTACION DE UN SERVICIO VPN PARA ACCESO REMOTO A EQUIPOS ACTIVOS DEL LABORATORIO CISCO EN EL CAMPUS RAMIREZ DAVALOS DEL ITI, y conceden autorización para que el ITI pueda utilizar este trabajo en su beneficio y/o de la comunidad, sin reserva alguna.

CUARTA: aceptación: las partes declaradas que aceptan expresamente todo lo estipulado en la presente cesión de derecho.

CRISTIAN DAVID MUÑOZ TENEMPAGUAY

JIMMY JOSSUÉ DÍAZ OÑA

D.M. Quito, 30 de mayo del 2023

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Este proyecto tiene como meta proporcionar a los estudiantes de la carrera de Redes y Telecomunicaciones del Instituto Tecnológico Internacional Universitario ITI, modalidad en línea, mediante la creación de un servicio VPN, acceso a los equipos LAN ubicados en el laboratorio Cisco del campus Ramírez Dávalos. El objetivo principal es reforzar el conocimiento teórico y práctico de los estudiantes sobre el uso remoto de estos dispositivos, lo que les permitirá desempeñarse mejor en un entorno laboral y ampliar sus conocimientos sobre redes.

Los estudiantes contarán con una guía detallada del proceso de creación del servidor VPN, así como de cómo acceder a él, lo que garantizará su correcto uso y funcionamiento. Con este proyecto, los estudiantes podrán mejorar sus habilidades en el uso de dispositivos de redes y aprenderán a crear un servicio VPN, lo que les dará una ventaja competitiva en el mercado laboral.

Palabras claves: OpenVPN, SSH, Mikrotik, Puertos de Red, Certificados VPN.

INTRODUCCIÓN

Nombre del proyecto

"IMPLEMENTACION DE UN SERVICIO VPN PARA ACCESO REMOTO A EQUIPOS ACTIVOS DEL LABORATORIO CISCO EN EL CAMPUS RAMIREZ DAVALOS DEL ITI"

Antecedentes

El Instituto Tecnológico Universitario ITI, en sus veinte y nueve años de vida institucional cuenta con una sede en el centro norte de la ciudad de Quito, el Campus Ramírez Dávalos que entró en funcionamiento en el año 2020. La carrera Redes y Telecomunicaciones cuenta con un laboratorio Cisco, el cual es aprovechado por los estudiantes de la carrera presencial, sin embargo, los estudiantes de la carrera Instalación y Mantenimiento de Redes en la modalidad en línea no pueden utilizar el laboratorio, tampoco tienen acceso remoto que permita el ingreso a los estudiantes a los equipos LAN del laboratorio en el Campus Ramírez Dávalos del ITI.

Este trabajo propone una solución en base a una VPN (Red Privada Virtual) que permitirá una conexión remota para la interacción con los equipos LAN del laboratorio de Redes y Telecomunicaciones.

En el proyecto propuesto por (Reyes, 2015) se llevó a cabo una red privada virtual (VPN) para un sistema de telemedicina entre el hospital provincial general docente de Ambato y sus centros de salud, permitiendo de manera segura y fácil la obtención de historiales médicos de pacientes, mejor atención hacia los usuarios, los servicios que ofrece cada centro e información del personal.

En el trabajo realizado por (Ñacato, 2007), se plantea un diseño e implementación de una red privada virtual (VPN) para la empresa HATO Telecomunicaciones, llevando a cabo la interconexión de varios usuarios de manera remota con las oficinas y a su vez estas con la oficina matriz. Dichas oficinas se encuentran aisladas de comunicaciones de la oficina principal.

Marco contextual

Una VPN es un servicio que permite el acceso remoto a la red interna de la organización y a los recursos corporativos. Este acceso a través de internet de forma segura, permite la movilidad del trabajador o incluso interconectar sedes separadas geográficamente, en lo establecido por (INCIBE, 2015). Una VPN permite la conectividad de forma segura con las instalaciones, en este caso con el laboratorio de Cisco de Redes y Telecomunicaciones en el Campus Ramírez Dávalos, con lo cual podrán manipular desde cualquier punto donde los estudiantes se encuentren, al ser aplicado en el laboratorio, brindara facilidad a los estudiantes para poder conectarse a los equipos LAN para así hacer uso de ellos desde un lugar remoto.

Las redes VPN son una tecnología que permite la extensión segura de la red local (LAN) sobre una red pública, mediante la encapsulación y encriptación, permitiendo una conexión desde diferentes puntos de manera remota, por ello en el campus Ramírez Dávalos del ITI se aplicará este sistema para ayudar a los estudiantes a interactuar con equipos reales, ya que en los años pasados muchos de ellos se limitaron a sólo utilizar simuladores debido a la pandemia ocasionada por el COVID 19. (INCIBE, 2015)

Problema de investigación

El poco uso de los equipos del laboratorio de Redes y Telecomunicaciones del campus Ramírez Dávalos ha generado consecuencias negativas en los estudiantes de modalidad virtual o en línea, tales como poca experiencia en el ámbito laboral, dificultad para reconocer los usos de cada equipo y poco conocimiento en general. Las causas principales de este problema son la falta de uso adecuado del laboratorio, la falta de tiempo para realizar prácticas en clase y la ausencia de los equipos en casa para practicar. Durante el confinamiento el 90% de los estudiantes de carreras técnicas no realizaron prácticas presenciales y muchos de ellos han optado por mantenerse en la virtualidad en la actualidad.

Formulación del problema

¿En que influye la falta de interacción presencial por parte de los estudiantes con los equipos (LAN) del laboratorio de Redes y Telecomunicaciones del Campus Ramírez Dávalos?

Definición del problema

Ante la falta del uso de los equipos (LAN) del laboratorio de Redes y Telecomunicaciones en el nuevo Campus Ramírez Dávalos del ITI, dado por el confinamiento en la pandemia mundial y la modalidad de estudio en línea, los estudiantes que retornaron a la prespecialidad presentaron falencias con los procedimientos para interactuar físicamente con los equipos y conocer funciones específicas que posee cada uno, antes sólo fueron instruidos con simuladores.

Idea a defender

Implementar una conexión remota a través de una VPN para los estudiantes del campus Ramírez Dávalos del ITI proporcionara beneficios significativos en términos de aprendizaje y desarrollo laboral a futuro.

Justificación

Un servicio de conexión remota a los equipos Cisco por medio de una VPN permite el ingreso de cualquier persona de manera digital, con previa autorización y la debida seguridad desde cualquier sitio donde esta se encuentre, pudiendo realizar las mismas actividades que las llevaría a cabo presencialmente en su lugar de trabajo o estudio. El ITI se vería beneficiado al fomentar la práctica y desarrollo de conocimiento dentro del campo digital, potenciando mayor interés en los estudiantes sobre cómo se configurar un equipo y experimentando su funcionamiento en el mundo real.

Objetivo General

Implementar un servicio VPN de conexión remota hacia los equipos LAN para el laboratorio CISCO que se encuentra en el campus Ramírez Dávalos del Instituto Tecnológico Internacional ITI.

Objetivos Específicos

- Identificar la necesidad de la implementación del servicio VPN de conexión remota en el Campus Ramírez Dávalos.
- Crear un servicio que facilite al uso de equipos LAN de manera remota.
- Realizar pruebas del correcto funcionamiento del sistema.

Síntesis de la introducción

Se propone la implementación de una VPN para permitir una conexión remota y mejorar la interacción de los estudiantes con los equipos del laboratorio CISCO. La implementación de redes VPN es una tecnología que permite la conexión segura de redes locales sobre una red pública, lo que permitiría a los estudiantes interactuar con los equipos reales desde cualquier lugar. Se identifica que la falta de acceso a los equipos del laboratorio ha generado consecuencias negativas en los estudiantes, como la falta de conocimiento práctico y poco manejo en el ámbito laboral. Una conexión remota a los equipos LAN por medio de una VPN ayudaría a los estudiantes a practicar y adquirir conocimientos técnicos desde cualquier lugar, lo que reduciría la brecha de conocimiento y mejoraría su formación académica.

CAPÍTULO I: FUNDAMENTACIÓN TEÓRICA

Ubicación

El presente proyecto se llevará a cabo en el 4to piso en el laboratorio de Cisco de la carrera de Redes y Telecomunicaciones ubicado en el campus Ramírez Dávalos del Instituto Tecnológico Universitario ITI, en la siguiente imagen se muestra la ubicación exacta del establecimiento educativo donde se realizará el proyecto:

Figura 1.

Ubicación Campus Ramírez Dávalos ITI.

Nota: La imagen corresponde a la ubicación del campus Ramírez Dávalos - ITI. (Google, 2022)

Fundamentación Conceptual

Una red privada virtual (VPN) es una red privada que utiliza la infraestructura de las redes públicas para transferir información. (Gonzalez , 2006)

La tecnología VPN comenzó en 1996 cuando los empleados de Microsoft desarrollaron PPTP. Este protocolo crea una conexión privada más segura entre el dispositivo de un usuario e Internet. Unos años más tarde, en 1999, se publicó la

especificación. Las VPN comenzaron a crecer a medida que crecía la necesidad de conexiones a Internet más seguras. (Gillis , 2021).

A principios de la década de los 2000, las empresas asociaban y utilizaban principalmente las VPN. Esta tecnología aún no ha sido utilizada por el usuario promedio en línea. En aquel entonces, las empresas usaban VPN para acceder a redes corporativas privadas. En este caso de uso, las organizaciones pueden acceder a los datos corporativos desde cualquier lugar mientras parece estar en la oficina. El intercambio seguro de archivos entre diferentes oficinas se ha vuelto posible. (Gillis , 2021).

El acceso remoto significa que alguien externo está intentando crear un flujo de paquetes cifrados dentro de su organización. Este túnel puede provenir de Internet, pero también puede provenir de una línea telefónica. (Brown, 2001)

Fundamentación Legal

En la constitución de la república del Ecuador, Redes y Prestación de servicios de Telecomunicaciones, Capítulo Primero – establecimiento y explotación de redes, Art. 10 (Constitución del Ecuador, 2015). Las Redes que dependen de la prestación de servicios públicos de telecomunicaciones o a su vez utilizan para servicios de soporte de terceros, se considera una red pública y lo requiere en los términos de esta Ley, su aplicación general y su reglamento emitido por el Reglamento de Telecomunicaciones. Puede ser accedida por los proveedores de servicios de telecomunicaciones.

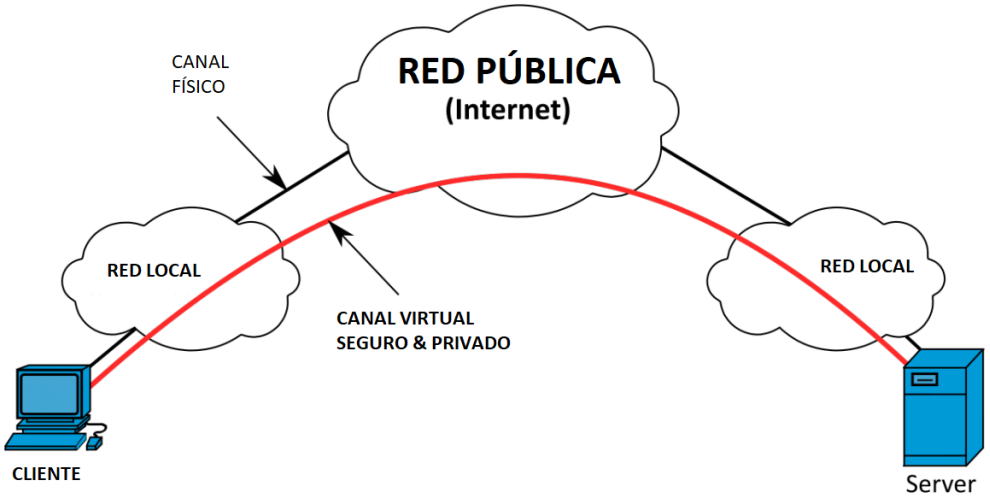
MARCO TEORICO

Red Privada Virtual

Una red privada virtual es en realidad una red creada sobre una red pública, para así poder simular una red privada, Generalmente las VPN pertenecen a una compañía que le permite acceder de forma remota y segura a diferentes sedes interconectadas con un proveedor de servicio, en este caso un proveedor de internet (Zapata, 2016).

Es por ello que la VPN es una red pública funcionando en un entorno seguro y confidencial permitiendo que el usuario o usuarios ingresen desde un sitio distante a una sede y realicen labores como si estuvieran de manera presencial dentro de una red local. (Zapata, 2016)

Figura 2.
Mapa de una red VPN.



***Nota*:** El gráfico representa el mapa de funcionamiento de una red privada virtual.

Tecnologías de acceso remoto.

Según (Quishpe, 2021), la conexión desde un punto distante o acceso remoto ha sido primordial en los últimos años, muchas empresas se han inclinado a este tipo de red,

ofrecen la disponibilidad de trabajar desde la comodidad de sus hogares dando accesibilidad a datos de la empresa de manera segura, surgiendo así las redes virtuales privadas o más conocidas como VPN.

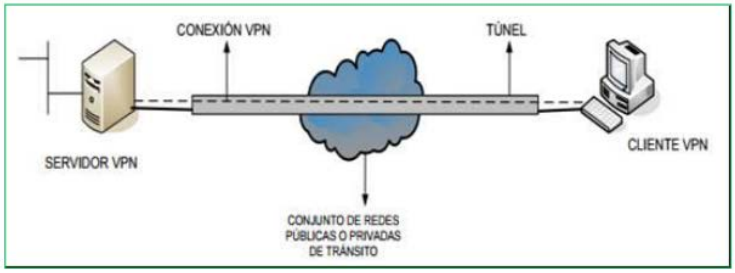
Las empresas mucho antes que existan las redes VPN realizaban el acceso remoto de manera rustica por medio de módems, se conectaban a la empresa de igual forma que las redes VPN pero con la diferencia que eran físicas y ocupaban espacio, instalando pilas de módems para dar acceso a grupos determinados y siendo muy costoso por lo cual muchas empresas no optaron por realizar el teletrabajo, en la actualidad esto ha cambiado totalmente, los módems se han perdido y ya solo hace falta de un servidor VPN para que las personas puedan ingresar a los archivos de la empresa de forma segura. (Fonseca, Castañeda, & Arevalo, 2018)

Componentes de una red VPN

Las redes VPN se conforman por los siguientes componentes para su funcionamiento (Muñoz, 2007).

Figura 3.

Componentes de una red VPN



Nota: Estructura base para el funcionamiento de una red VPN.

- Cliente VPN: Estos pueden ser un enrutador que inicie la conexión VPN o también conocido como enrutador de llamada.

- Servidor VPN: Es el enrutador que acepta las conexiones desde el cliente VPN, también conocido como enrutador de respuesta.
    - Protocolos de túnel: son protocolos utilizados para administrar los túneles y encapsular los datos privados, los mismos que deben estar cifrados para establecer una conexión VPN.
    - Datos del túnel: son los datos que normalmente se envían a través de un vínculo punto a punto privado.
- Conexión VPN: Parte donde los datos se cifran y encapsulan en la misma conexión, generando una red VPN.
- Red pública de tránsito: Es la red pública o privada que atraviesa los datos encapsulados.

Tipos de VPN

Los tipos de VPN son los siguientes:

- Sistemas basados en Hardware.
- Sistemas basados en Firewall.
- Sistemas Basados en Software.

Sistemas basados en Hardware. Son aquellos routers con hardware dedicado que se encriptan de manera segura para el cruce de información, su instalación es rápida y fácil. (Trujillo, 2006).

Principales Ventajas:

- Capacidad de asegurar el flujo de paquetes entre dos redes, a través de una red pública.

- Capacidad de autorizar y autenticar a los usuarios el acceso sobre la red privada.

Sistemas basados en firewall. Sistemas implementados con software de cortafuegos o firewall teniendo como ventajas. (Trujillo, 2006)

- Posee mecanismos de seguridad con acceso restringido a la red interna.
- Realizan un NAT traduciendo direcciones para validar los requerimientos de autentificación fuerte.

Sistemas basados en Software. Implementados cuando 2 puntos de conexión no se encuentran controlados por la empresa o cuando los firewalls no están implementados en la misma empresa. Este sistema permite que el manejo del tráfico sea más flexible, este mismo puede ser enviado a través de un túnel en función de las direcciones o protocolos. (Trujillo, 2006).

Arquitecturas de la VPN

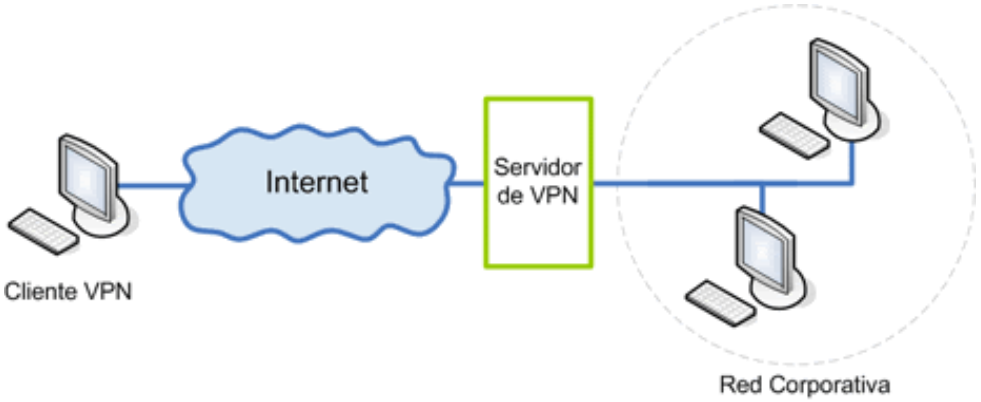
Los tipos más comunes de redes privadas virtuales:

- VPN de Acceso Remoto.
- VPN Sitio a Sitio.
- VPN Interna.

VPN de Acceso Remoto. Es probablemente el método más utilizado, los usuarios acceden a la empresa desde sitios remotos por medio de un servicio de internet, permite un nivel de acceso similar al que se encuentra en las redes corporativas locales (Humans, 2013)

Figura 4.

VPN Acceso Remoto

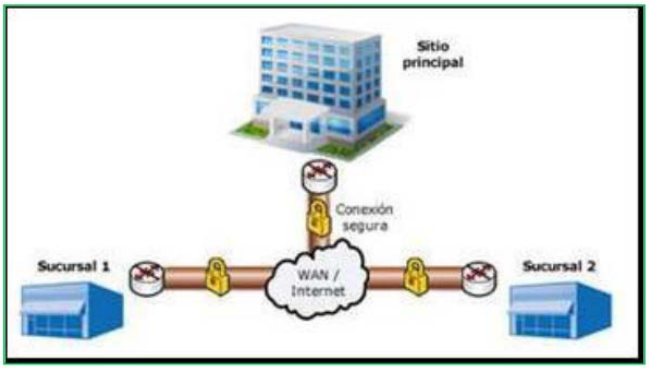


Nota: Topología de una red de acceso remoto.

VPN Sitio a Sitio. Utilizado para conectar oficinas remotas a la sede principal de la organización, usa como medio el servicio de internet persistente (Humans, 2013).

Figura 5.

VPN Sitio a Sitio



Nota: Diagrama de una conexión VPN sitio a sitio.

Existen dos tipos de configuración:

Tipo Intranet.

Una empresa tiene una o más sucursales remotas y desea combinarlas en una red privada, puede hacerlo creando una VPN y conectando ambas redes locales. (Humans, 2013)

Tipo Extranet

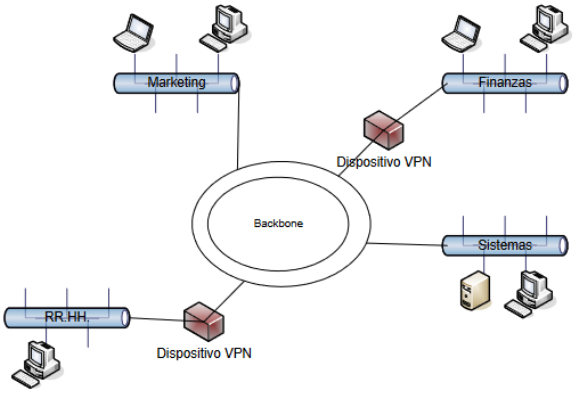
Una empresa tiene una relación cercana con otra empresa (como una empresa asociada, proveedor o cliente), desarrolla una VPN que conecte ambas redes, lo que permitirá que las empresas trabajen en un entorno compartido. Las arquitecturas VPN de extranet requieren que cada empresa controle cuidadosamente el acceso a sus propios recursos de red y a los datos que intercambia con los socios comerciales. (Humans, 2013).

VPN Interna.

Variante del acceso remoto con la diferencia de en vez de usar internet como medio de conectividad, utiliza la red de área local (LAN) de la misma empresa para crear redes privadas virtuales dentro de la misma, aumenta la seguridad en la red inalámbrica (Humans, 2013).

Figura 6.

VPN Interna



Nota: Topología de una red VPN Interna.

Protocolos de Red

PPTP.

“Point-to-Point Tunneling Protocol, este protocolo fue desarrollado por un grupo de ingenieros de Ascend Communcations:U.S. Robotics,3Com Corporation, Microsoft y ECI Telematics” (Zapata, 2016), permite el intercambio seguro de datos, cliente -

servidor formando una Red Privada Virtual (VPN) basado en un protocolo de transmisión (TCP/IP) que permite conexión e intercambio entre dos anfitriones (Zapata, 2016).

IPSec

"Protocolo de seguridad de internet que permite varios servicios de seguridad para el protocolo de internet (IP) tanto para IPv4 como para IPv6, este protocolo fue diseñado para soportar dos modos de cifrado" (Zapata, 2016). Los dos modos de cifrado son el modo de transporte que protege cada paquete y el modo de túnel que es el más seguro, protege la identidad del remitente y del receptor, oculta varios campos de IP permitiendo que funcione IPSec, todos los dispositivos comparten una clave en común. (Menéndez, 2012).

L2TP

"Llamado también Layer 2 Tunneling Protocol, es un protocolo de estándar aprobado por el IETF, creado para corregir la deficiencia del protocolo de tuberización Punto a Punto" (Zapata, 2016), Usa PPP para tener acceso telefónico que es dirigido a través de un túnel por internet hasta un punto determinado, L2TP, es variante de un protocolo de encapsulamiento IP, incluye mecanismos de autentificación PPP, PAP Y CHAP (Zapata, 2016)

SSH

El protocolo SSH (Zapata, 2016), se utiliza para conectarse de forma segura a dispositivos y sistemas a través de redes de computadoras. La principal función del protocolo SSH es proporcionar una conexión segura y cifrada entre dos dispositivos, lo que permite a los usuarios acceder y administrar de forma remota sistemas y

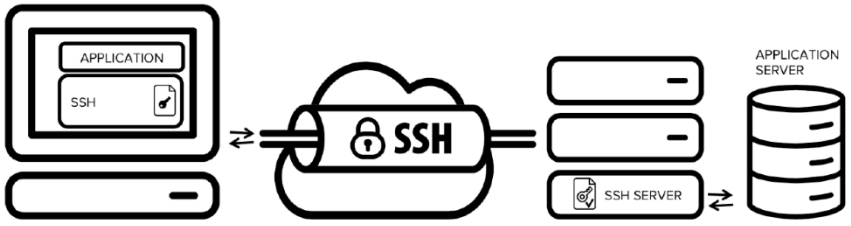
dispositivos, sin tener que estar físicamente presentes en el lugar donde se encuentran estos equipos.

Algunos de los usos más comunes del protocolo SSH incluyen:

- Acceso remoto a servidores y dispositivos de red: Los administradores de sistemas utilizan SSH para acceder a servidores y dispositivos de red de forma remota para realizar tareas de configuración y mantenimiento.
- Transferencia segura de archivos: Los usuarios pueden transferir archivos de forma segura entre dos dispositivos utilizando el protocolo SCP o SFTP, que son extensiones de SSH.
- Conexiones seguras entre sistemas: Los usuarios pueden establecer conexiones seguras y cifradas entre dos sistemas, lo que permite a los usuarios compartir información sensible sin correr el riesgo de que la información sea interceptada por terceros

Figura 7.

Topografía del protocolo SSH



Nota: Representación del funcionamiento del protocoló SSH.

Puertos de red

(WALTON, 2002) Los puertos de red son números de identificación de 16 bits que se utilizan para distinguir los diferentes tipos de tráfico que se transmiten a través de

una red. Cada puerto está asociado a un protocolo de red específico, que permite a los dispositivos en la red comunicarse entre sí de manera efectiva.

Existen dos tipos principales de puertos de red: TCP (Transmission Control Protocol) y UDP (User Datagram Protocol). Los puertos TCP se utilizan para conexiones de red confiables y orientadas a la conexión, como el correo electrónico y la navegación web. Los puertos UDP, por otro lado, se utilizan para conexiones de red no confiables y sin conexión, como las transmisiones de video y voz en tiempo real.

Los puertos de red también se utilizan para administrar la red y los dispositivos conectados a ella. Por ejemplo, el puerto 80 se utiliza para la comunicación de navegación web, mientras que el puerto 22 se utiliza para la comunicación SSH (Secure Shell) y el puerto 21 se utiliza para la comunicación FTP (File Transfer Protocol).

Es importante tener en cuenta que los puertos de red pueden estar abiertos o cerrados en función de la configuración de la red y los dispositivos conectados a ella. Los puertos abiertos pueden representar un riesgo de seguridad si no se gestionan adecuadamente, ya que los hackers pueden aprovecharlos para acceder a la red y a los datos de los dispositivos conectados a ella.

Puertos Conocidos

La tabla que representa los puertos conocidos se encuentra en el apartado de anexos.

Puertos Registrados

La tabla que representa los puertos registrados se encuentra en el apartado de anexos.

MICROTIK

MikroTik se destaca por sus soluciones de enrutamiento avanzadas que se ejecutan en el sistema operativo RouterOS, el cual es altamente personalizable y proporciona una amplia gama de características de enrutamiento y seguridad. Sus soluciones de red también ofrecen capacidades de gestión y monitoreo avanzadas, lo que permite a los administradores de red configurar y monitorear sus redes de manera eficiente. (MIkrotik, 2016)

MikroTik RouterBoard 951Ui-2HnD

El MikroTik RouterBoard 951Ui-2HnD es un enrutador inalámbrico de alta velocidad y alto rendimiento fabricado por MikroTik, una empresa letona que produce soluciones de redes de alta calidad. (MIkrotik, 2016)

El dispositivo cuenta con una antena incorporada, cinco puertos Ethernet Gigabit, una interfaz inalámbrica de doble banda de 2,4 GHz y 5 GHz, y una fuente de alimentación PoE (Power over Ethernet) pasiva.

RouterBoard 951Ui-2HnD se ejecuta en el sistema operativo RouterOS de MikroTik, que es altamente personalizable y proporciona una amplia gama de características de enrutamiento y seguridad.

Este dispositivo es especialmente adecuado para su uso en pequeñas empresas y hogares, ya que proporciona una conectividad confiable y de alta velocidad para múltiples dispositivos, así como funciones avanzadas de seguridad y gestión de red.

OPENVPN

(Castillo, 2020) indica que OpenVPN es un software de código abierto que proporciona una solución de red privada virtual (VPN) segura y escalable, utiliza un túnel virtual para crear una conexión segura y privada a través de Internet. El túnel se establece entre el cliente OpenVPN y el servidor VPN utilizando protocolos de encriptación y autenticación para proteger la información transmitida a través del túnel.

El software de OpenVPN es compatible con diferentes protocolos de red, incluyendo TCP y UDP.

Aunque OpenVPN es una solución VPN muy sólida, hay algunas limitaciones que se deben tener en cuenta:

1. Velocidad: El cifrado de los datos a través de OpenVPN puede afectar la velocidad de la conexión a Internet.
2. Configuración: La configuración de OpenVPN puede ser un poco complicada para usuarios inexpertos.
3. Costo: Aunque OpenVPN es de código abierto, algunas empresas cobran por su servicio de VPN basado en OpenVPN.

CAPÍTULO II: DIAGNÓSTICO

En el presente proyecto se utilizan métodos cualitativo y deductivo verificando así que la información detallada sea aplicada en la práctica y obtener resultados de cuan beneficioso llega este a ser. Este proyecto se centra en resolver problemas relacionados con la comprensión del desarrollo de la formación a través de prácticas desarrolladas en trabajos de investigación, la práctica se entiende junto con la teoría implementada en este documento, quedando igualmente claro lo que se puede hacer.

Tipos de investigación

Bibliográfico documental. - La aplicación de esta técnica brinda la información necesaria para el desarrollo de la investigación y permite ampliar los criterios y teorías de los diversos autores de las fuentes presentadas en este documento.

Descriptiva. – Este método ha sido útil para comprender las características y la forma en que se llevará a cabo el proyecto, basándose en el uso de los equipos de manera remota.

Métodos de investigación

Método cualitativo. – en el presente proyecto de investigación se aplicó este método para comprender el alcance de la calidad del servicio que se pretende brindar enfocado al desarrollo de los estudiantes basándonos e os conceptos básicos para el desarrollo dentro de una red segura privada.

Método deductivo. – en el presente proyecto de investigación se aplicó este método para entender por medio de la información aplicada a la práctica de cómo este en beneficioso entendiendo todas las partes que lo componen uno solo.

Técnicas e instrumentos de investigación

En el proyecto se enfoca en un sondeo de opinión por medio de una encuesta dirigida a los estudiantes de la Carrera de Redes y Telecomunicaciones modalidad en línea acerca de si conocen sobre las redes VPN y si están de acuerdo en implementarlas en el Campus Ramírez Dávalos del ITI.

Población y muestra

Para calcular la muestra se toma como referencia a la población de 16 estudiantes que conforman la modalidad en línea de la carrera de Redes y Telecomunicaciones Del ITI.

$$\mathbf{X=}\frac{N*P\times Q}{(N-1)\left(\frac{E}{K}\right)^2+P*Q}$$

$$\mathbf{X=}\frac{16*0.5\times 0.5}{(16-1)\left(\frac{0.05}{2}\right)^2+0.5*0.5}$$

$$\mathbf{X=}\frac{4}{(15)\left(\frac{1}{1600}\right)+0.25}$$

$$\mathbf{X=}\frac{4}{0.26}$$

X= 15

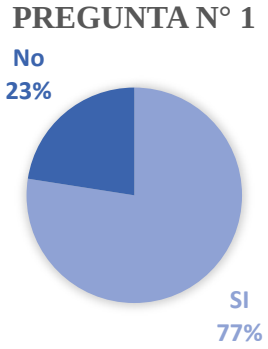
15 es el número de encuestas que se realizarán para el presente proyecto.

Presentación gráfica, análisis e interpretación de resultados obtenidos

Tabla 1.

¿Conoce acerca sobre los accesos remotos?

Opciones	Valor Numérico	Valor Porcentaje
Si	11	77%
No	4	23%



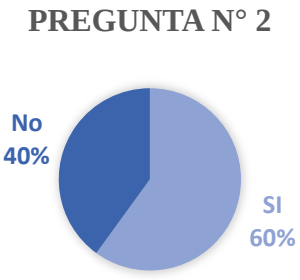
Interpretación:

La mayor parte de los encuestados tiene un conocimiento sobre los accesos remotos, mientras que un porcentaje mínimo no sabe con detalle sobre los accesos remotos.

Tabla 2.

¿Sabe Ud. que son y cómo se utilizan las redes VPN?

Opciones	**Valor Numérico**	**Valor Porcentaje**
Si	9	60%
No	6	40%



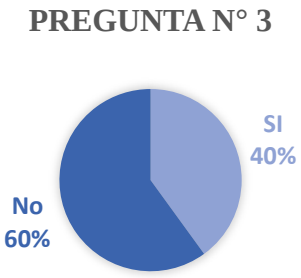
Interpretación:

Entre los encuestados se encuentra que la mayor parte sabe que es y cómo se usan las redes VPN, lo cual es un punto a favor al proyecto, restaría impartir información sobre el tema.

Tabla 3.

¿Alguna vez Ud. ha creado un servidor VPN?

Opciones	Valor Numérico	Valor Porcentaje
Si	6	40%
No	9	60%



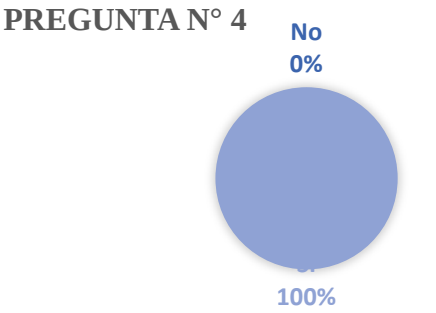
Interpretación:

La mayor parte de la población nunca ha empleado un servidor VPN, mientras que un pequeño grupo si sabe cómo realizarlo.

Tabla 4.

¿Le gustaría saber cómo se usa una red VPN?

Opciones	Valor Numérico	Valor Porcentaje
Si	15	100%
No	0	0%



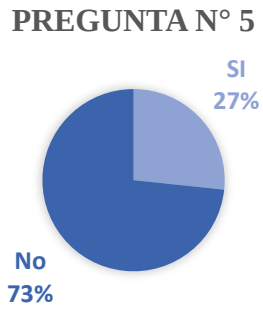
Interpretación:

La totalidad de los encuestados, respondió de manera positiva dando a conocer que si les gustaría saber cómo se usa una red VPN.

Tabla 5.

¿Ha utilizado algún programa para generar una rede VPN?

Opciones	Valor Numérico	Valor Porcentaje
Si	4	27%
No	11	73%



Interpretación:

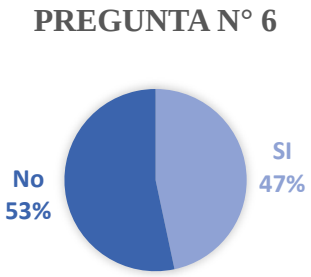
Los encuestados afirman haber usado un programa para crear una red VPN representando solo el 21%, mientras que el 73% no ha hecho uso de ningún programa.

Tabla 6.

¿Conoce el programa OPENVPN?

Valor Numérico	Valor Numérico	Valor Porcentaje

7	7	47%
8	8	53%



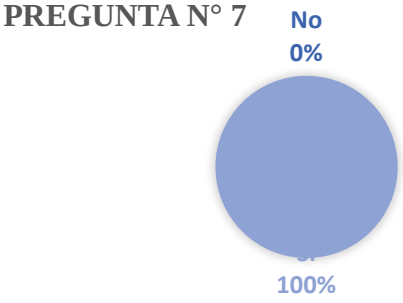
Interpretación:

La mitad de personas encuestadas conocen el programa OpenVPN, con la restante mitad se podrá dar a conocer este programa mediante el presente proyecto.

Tabla 7.

¿Considera importante el poder acceder de forma remota a los equipos Cisco del laboratorio de la Carrera Redes y Telecomunicaciones para desarrollar prácticas reales?

Opciones	Valor Numérico	Valor Porcentaje
Si	15	100%
No	0	0%



Interpretación:

La totalidad de los encuestados está de acuerdo con implementar un servicio VPN para el acceso remoto a los equipos activos del laboratorio Cisco de Redes y Telecomunicaciones del campus Ramírez Dávalos del ITI.

Análisis e interpretación de resultados

El análisis general de la encuesta realizada a los estudiantes de la carrera de Redes y Telecomunicaciones en modalidad en línea indica un apoyo óptimo para la creación de un servidor VPN a equipos activos del laboratorio Cisco. Las redes VPN dentro de la carrera de Redes y Telecomunicaciones son muy importantes, estas son empleadas por empresas para cuidar el envió de información puesto que esta tecnología hace que los datos sean seguros y cifrados. Los resultados revelan que la mayor parte de los estudiantes poseen interés acerca de lo que se va a emplear en el presente proyecto, lo que este conlleva desde sus conceptos básicos, el proceso de realización y la utilización del servidor VPN asi como como el ingreso hacia los equipos activos de Cisco lo que genera confianza en el desarrollo del mismo. En tanto a la parte de los encuestados que no poseen conocimiento alguno o leve de lo que se va emplear serán guiados por medio del presente documento.

Síntesis del capítulo

Como síntesis del capítulo se destaca la experiencia positiva de la utilización de la técnica de aplicar encuestas a los estudiantes, destacando la necesidad y la aceptación en la implementación del servidor VPN para la conexión con los equipos LAN del laboratorio de Cisco de la carrera de Redes y Telecomunicaciones en el Instituto Tecnológico Internacional Universitario ITI. Tomando en cuenta que, en la actualidad sólo pueden realizar prácticas mediante simuladores, que no es lo mismo que realizar con dispositivos reales, por lo que la implementación de este tipo de tecnología de manera remota tiene como fin ayudar en el conocimiento teórico-práctico de los estudiantes.

CAPÍTULO III: PROPUESTA

Descripción de la propuesta

Título de la propuesta – descripción

Implementación de un servicio VPN para acceso remoto a equipos activos del laboratorio cisco en el campus Ramírez Dávalos del ITI.

Beneficiarios

Los estudiantes de la carrera de Redes y Telecomunicaciones del Instituto Tecnológico Internacional Universitario ITI, serán los principales usuarios beneficiados del proyecto, ya que podrán hacer uso del servidor VPN para conectarse a los equipos LAN del laboratorio de CISCO.

Viabilidad

Después de revisar la propuesta del proyecto, se ha concluido que es factible, debido a que el instituto cuenta con los equipos necesarios para llevar a cabo la implementación sin incurrir en costos de inversión, sino sólo de mano de obra. Además, se realizó una encuesta entre los estudiantes de la modalidad virtual, y su aceptación ha demostrado que existe una alta probabilidad de éxito en la implementación de una Red Privada Virtual (VPN) que se conecte a los equipos de la red local (LAN) del laboratorio de Cisco en el Campus Ramírez Dávalos. Esta opinión positiva de los estudiantes es una de las razones principales de la viabilidad del proyecto.

Impacto

La implementación de este proyecto tendrá un efecto positivo en la carrera Redes y Telecomunicaciones, ya que los estudiantes de educación virtual podrán acceder a los

equipos de forma remota y realizar prácticas en lugar de sólo utilizar simuladores. Además, el proyecto proporcionará conocimientos sobre redes privadas virtuales y su funcionamiento.

Recursos

En la presente tabla se muestra los elementos usados en el proyecto, la cantidad y la característica que estos poseen.

Tabla 8.
Recurso para el proyecto.

Recurso	Cantidad	Característica
Laptop	1	Realizar configuraciones en los dispositivos usados para el proyecto y conectividad a los mismos.
Wifi	1	Conexión a internet, mediante ella nos permite conectar con los equipos Cisco del laboratorio.
Router	2	Cisco 1921: ofrece un alto rendimiento en la gestión de redes empresariales, gracias a su procesador de doble núcleo y su capacidad de integración de servicios.
Switch	3	Cisco Catalys 2960-s: capacidad de ofrecer conectividad de red confiable y segura para aplicaciones empresariales críticas.
Mikrotik	1	RouterBoard 951Ui 2HND: enrutador inalámbrico de alta velocidad que funciona con el sistema operativo RouterOS ideal para redes pequeñas y medianas.
Conector	12	Rj45, tiene ocho pines, lo que permite transmitir y recibir datos simultáneamente a través de cuatro pares de cables.
Cable de red	6	Cat5, Es un tipo de cable de cobre de alta calidad, que utiliza pares de hilos de cobre trenzados para reducir la interferencia electromagnética y mejorar la calidad de la señal.

Capuchones	12	Brinda una protección en la unión del cable de red y el conector, evitando desprendimiento.
Tester	1	Comprueba la conectividad entre ambos polos de un cable de red.
Ponchadora	1	Permite la unión entre el cable de red(Cat5) con el conector (Rj45).
Software	3	WinBoX: Administración de redes desarrollada por MikroTik para configuración y monitoreo de sus dispositivos. OpenVPN: Software libre para establecer conexiones VPN seguras y encriptadas a través de internet. PuTTY: Acceso a los equipos de Cisco por medio del protocolo SSh
Datacenter	1	Se encuentra el servidor de red VPN para una conexión segura.
Lab. Cisco	1	Alberga los equipos de cisco.

Nota: Se muestra los materiales requeridos para el proyecto.

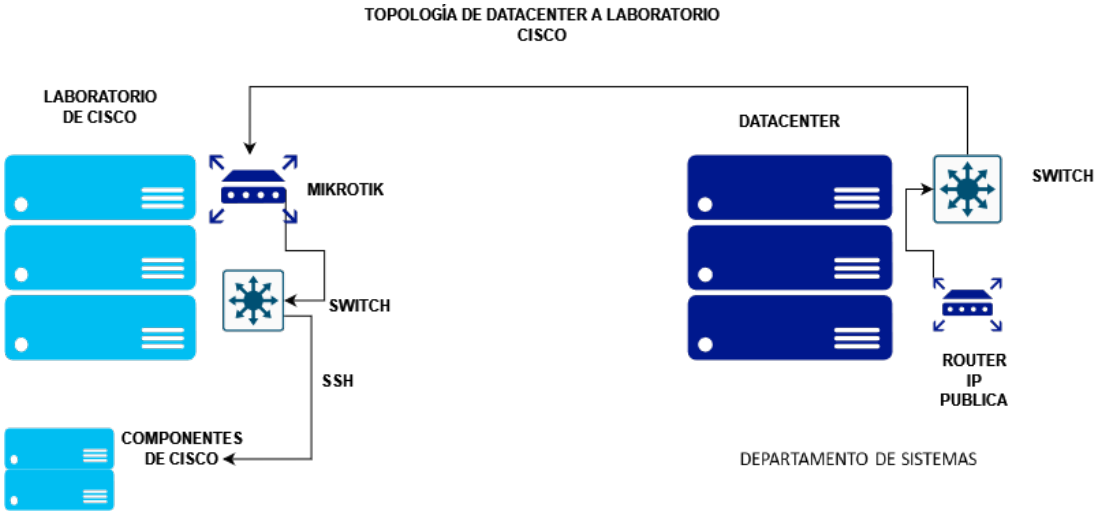
Desarrollo de la propuesta

Diseño del proyecto.

La imagen exhibe el funcionamiento interno del proyecto que se lleva a cabo en el cuarto piso del campus Ramírez Dávalos del ITI. En dicho lugar, se encuentra el Datacenter que incluye el router con la dirección IP pública y el switch, el cual se conecta mediante un cable CAT 5 al laboratorio de Cisco ubicado en la misma planta. Una vez allí, el Mikrotik se conecta al switch y, a través del protocolo SSH, se establece la conexión con los componentes de Cisco mediante OpenVPN.

Figura 8.

Topología Interna DataCenter-Laboratorio de Cisco.

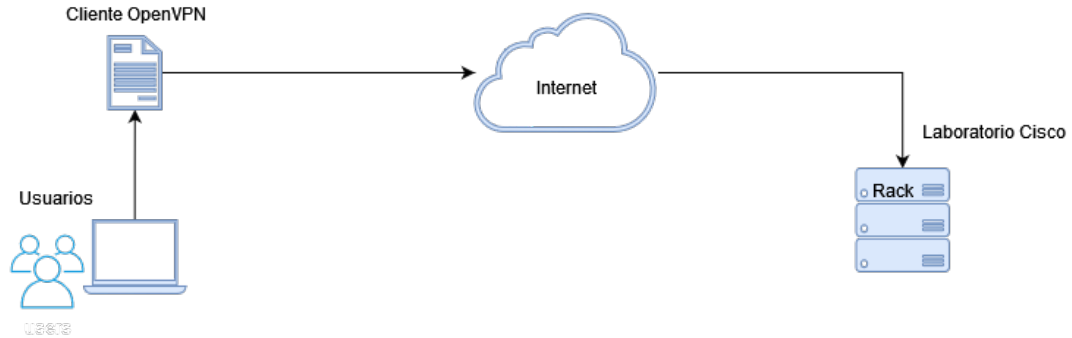


Nota: Se detalla el funcionamiento del servidor VPN dentro del plantel educativo.

La imagen muestra el diagrama del funcionamiento externo del proyecto. Los usuarios acceden a través de OpenVPN y un certificado de cliente el cual se envía a través de Internet y atraviesa la topología anteriormente mencionada. De este modo, los usuarios llegan al laboratorio de Cisco, al rack principal, y pueden hacer uso de los componentes de Cisco.

Figura 9.

Topología Externa Usuario-Laboratorio Cisco.



Nota: Se detalla como el certificado cliente OpenVPN viaja desde el usuario al laboratorio para el acceso del mismo.

Configuraciones en el Mikrotik RouterBoard 951Ui 2HnD por medio de su plataforma WinBox.

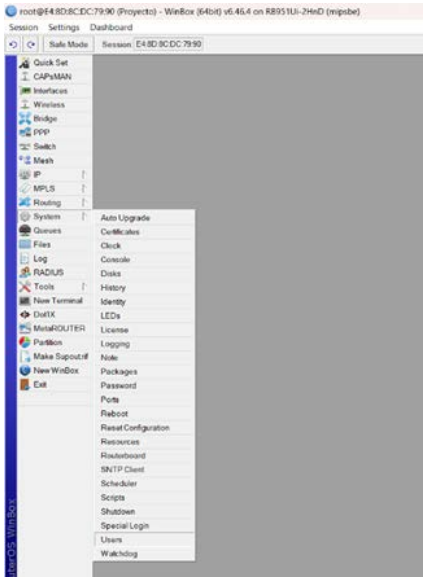
Creación de un usuario Full

Pasos:

- Ingresar al menú izquierdo lateral opción “System” en “Users”.

Figura 10.

Creación de un usuario full.

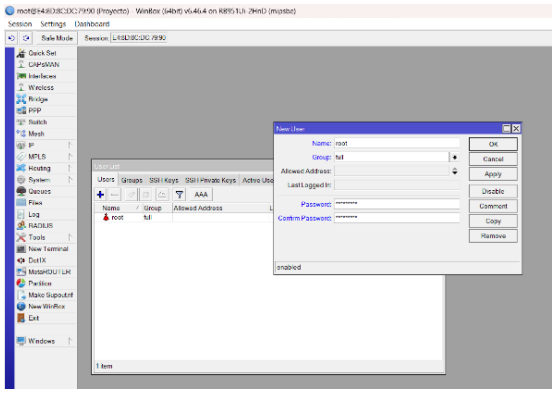


Nota: primer paso para la creación del usuario en WinBox.

- Se comenzará por aprender cómo agregar una contraseña al usuario admin. Para ello, dar clic doble sobre dicho usuario y, en la ventana emergente, seleccionar la opción "Password". Luego, en la nueva ventana que aparecerá, ingresaremos el password deseado dos veces.

Figura 11.

Creación de un usuario full.



Nota: Creación del usuario en WinBox de manera precisa.

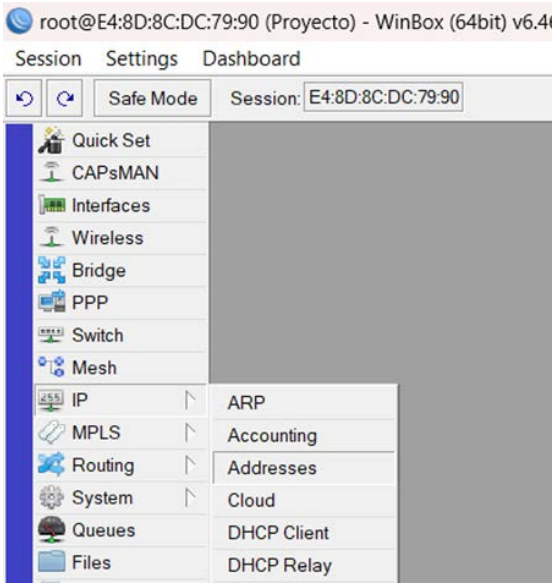
Configuración de un puerto para WAN.

Paso 1. Asignación de la dirección IP a una interface.

- Para asignar una dirección IP a una interfaz, se debe acceder a la sección de "Direcciones" ubicada en la sección "IP" en el Winbox.

Figura 12.

Asignación de la dirección IP a una interface.

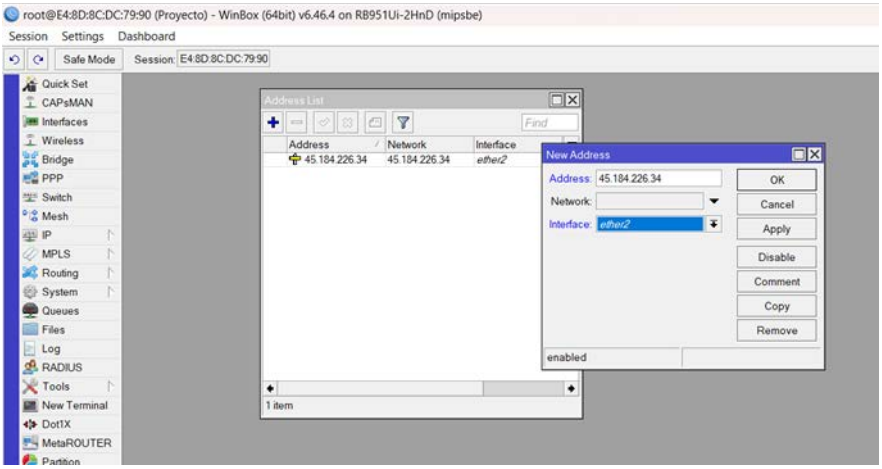


Nota: La asignación de una IP es fundamental para realizar el puerto WAN.

- En la ventana de "Lista de direcciones", se pueden añadir las direcciones IP que corresponden a cada una de las interfaces del Router. Para agregar una nueva IP a una interfaz específica, basta con hacer clic en el botón "Agregar" (+).
- Una vez abierta la ventana de "Nueva dirección", se debe especificar la dirección IP y la máscara de subred en notación simplificada. Luego, se selecciona la interfaz correspondiente, en este caso "ether2", donde se aplicará la configuración. Finalmente, al hacer clic en el botón "Aceptar", se visualizará la dirección IP asignada a la interfaz en la lista correspondiente.

Figura 13.

Asignación de la dirección IP a una interface.



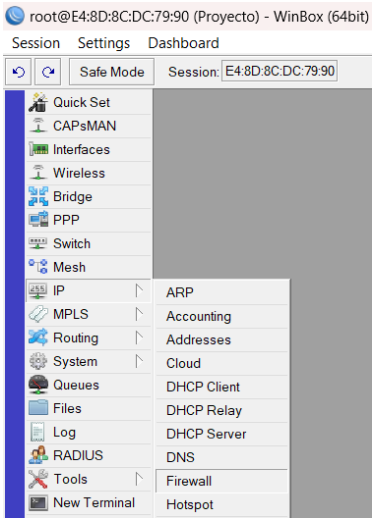
Nota: Es importante tener en claro que dirección IP se va usar.

Paso 2. Configuración del enmascaramiento

- El enmascaramiento se utiliza para que el tráfico de la red LAN aparezca con la dirección IP del puerto WAN al salir de la red. Para configurar el Network Address Translation (NAT), es necesario acceder a la sección "Firewall" en el Winbox, ubicada en la pestaña "IP".

Figura 14.

Configuración del enmascaramiento.

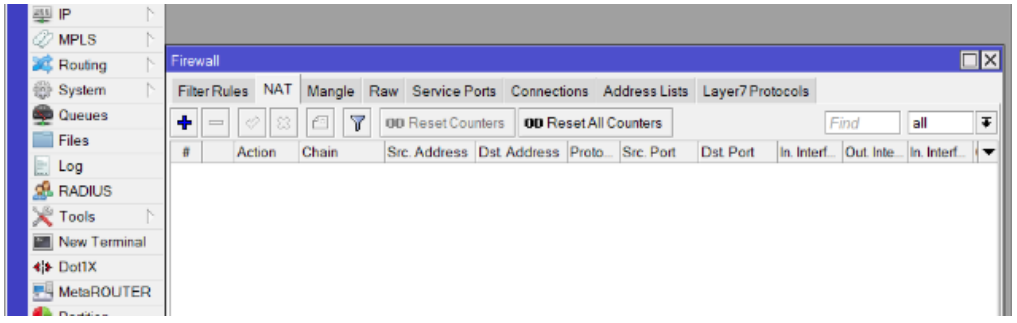


Nota: Tener en cuenta el firewall para configurar el NAT.

- En la sección de Firewall, se debe cambiar a la pestaña NAT para agregar una regla de NAT a una interfaz. Para ello, solo es necesario hacer clic en el botón "Agregar" (+).

Figura 15.

Configuración del enmascaramiento.

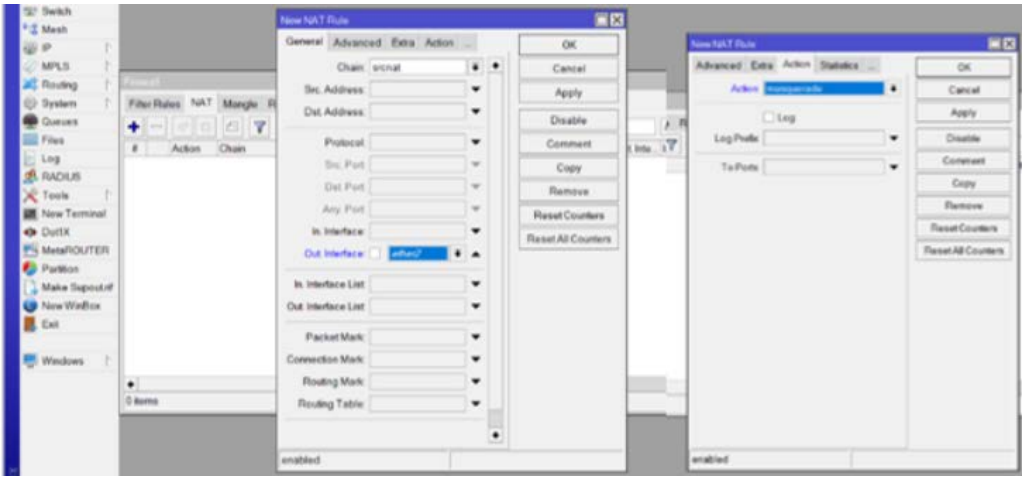


Nota: Establecer una regla en el NAT.

- En la ventana de "Nueva Regla NAT", se debe especificar el "Chain" como "srcnat" y la "Interfaz de Salida" como "ether2" o la interfaz correspondiente al Gateway. Luego, se cambia a la pestaña "Acción", donde se configura la acción como "masquerade".

Figura 16.

Configuración del enmascaramiento.

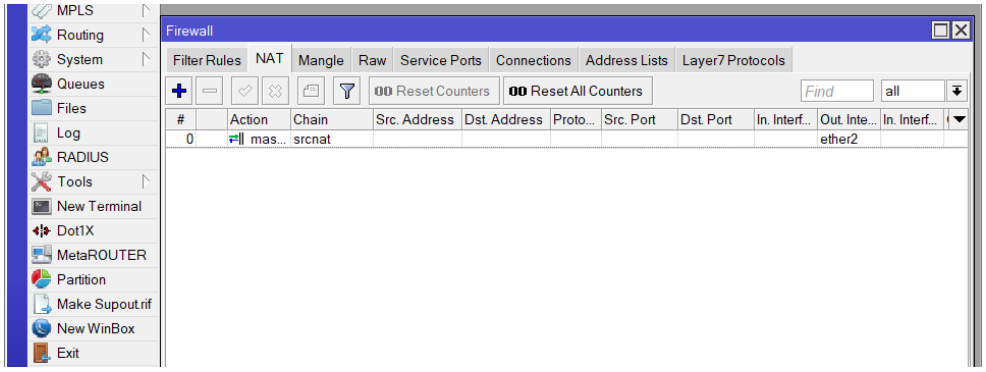


Nota: Importante poner los parámetros tal cual se explica.

- Nos deberá quedar un registro como el de la siguiente imagen:

Figura 17.

Configuración del enmascaramiento.



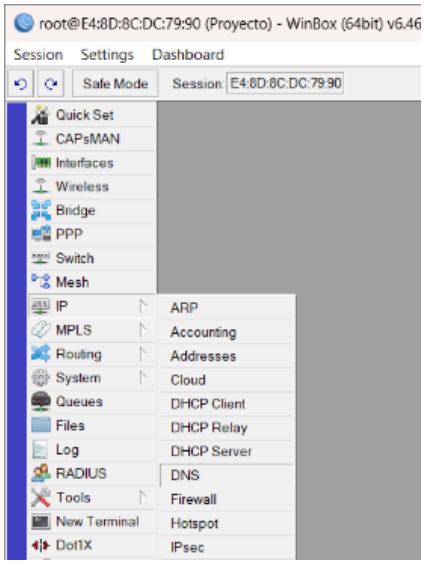
Nota*:* verificar que se encuentre como la imagen.

Paso3. Configuración del DNS.

- El enrutador necesitará del servicio DNS para resolver los nombres de dominio. Para asignar la dirección IP del servidor correspondiente, se debe acceder a la sección de "DNS" ubicada en la sección "IP" en el Winbox.

Figura 18.

Configuración del DNS.

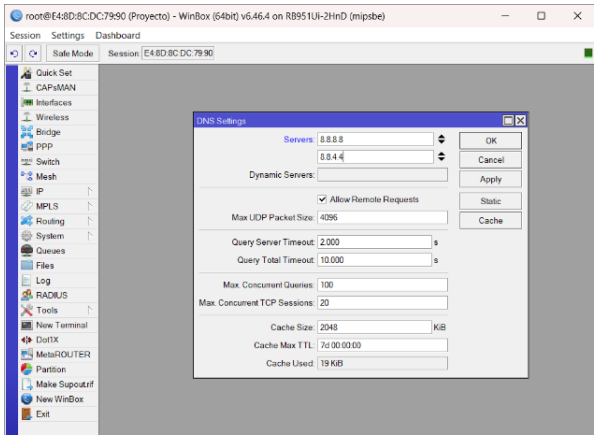


Nota: El DNS designara una IP al usuario.

- En la ventana de "Configuración de DNS", se deben ingresar las direcciones IP de los servidores DNS que el enrutador consultará. Además, se debe habilitar la opción "Permitir solicitudes remotas".

Figura 19.

Configuración del DNS.



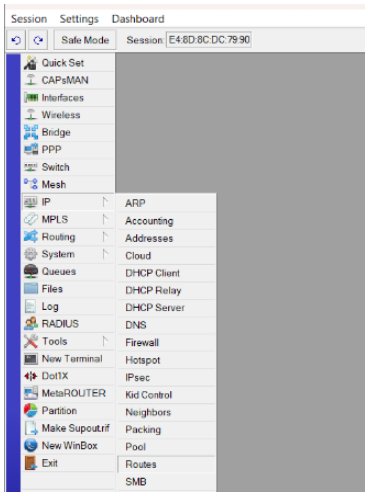
Nota: Colocar como servidor la IP que sea designada.

Paso 4. Configuración en el Gateway.

- La configuración del Gateway es necesaria para enviar el tráfico de red desde el router hacia el equipo que brinda el servicio a través del puerto WAN. Para asignar el Gateway en el Winbox, es necesario acceder a la sección de "Rutas" ubicada en la sección "IP".

Figura 20.

Configuración en el Gateway.

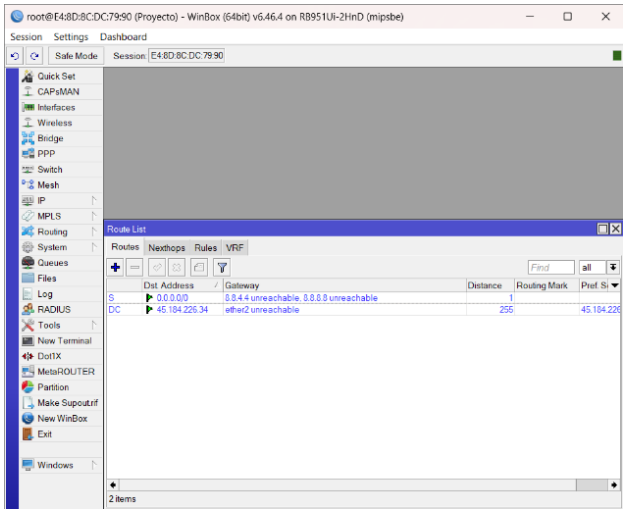


Nota: Con esto se brindará el servicio al puerto WAN.

- En la ventana de la lista de rutas, se pueden ingresar las direcciones de destino junto con la dirección del gateway correspondiente para llegar a esa dirección. Para agregar un nuevo gateway, solo se debe hacer clic en el botón "Agregar" (+). De esta manera, el gateway quedará registrado y se mostrará en la lista como se observa en la imagen siguiente:

Figura 21.

Configuración en el Gateway.

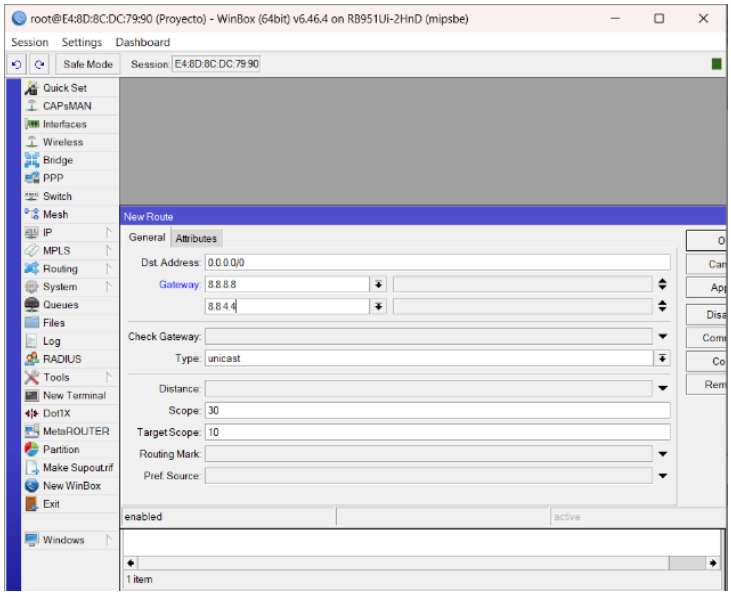


Nota: se agrega el parámetro de Gateway.

- En la ventana "Nueva Ruta", se indica la dirección de destino general "Dst. Address " y la dirección IP del enrutador que se está utilizando como puerta de enlace predeterminada, "Gateway", por último, dar en "OK".

Figura 22.

Configuración en el Gateway.



Nota: Se establece el Gateway.

- Deberá quedar como la siguiente imagen el Gateway.

Figura 23.

Configuración en el Gateway.

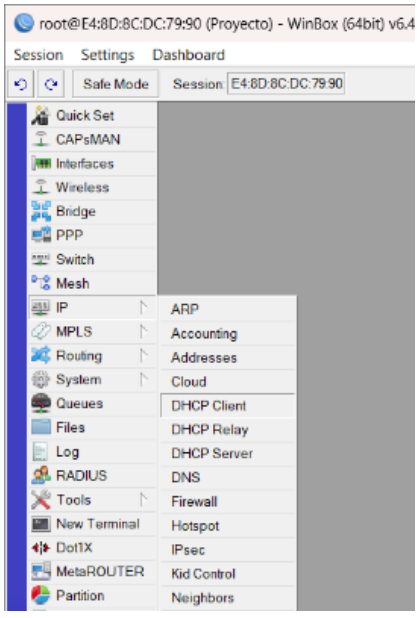
Nota: se estableció con eficacia los demás pasos.

Paso5. Configuración del DHCP.

- Acceder a la sección de "Cliente DHCP" en el Winbox es necesario para realizar la configuración del cliente DHCP.

Figura 24.

Configuración del DHCP.



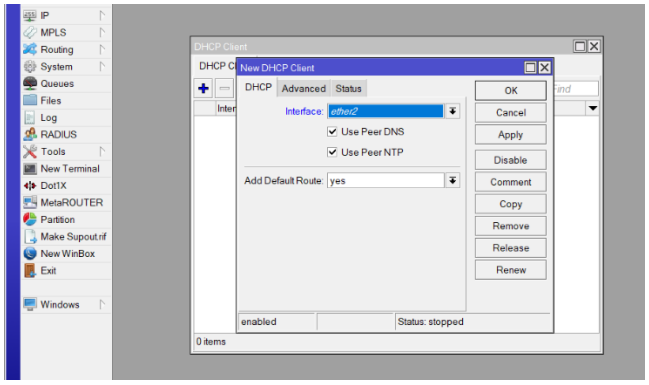
Nota: Se muestra el apartado principal para crear el DHCP.

- En la ventana de "DHCP Client", se puede configurar que el router busque y

acepte la configuración a través de Broadcast por medio del puerto "ether1". Para agregar un nuevo "DHCP Client", solo es necesario hacer clic en el botón "Agregar" (+). En la ventana emergente de "Nuevo DHCP Client", se debe especificar el parámetro "Interfaz: ether1", que es la interfaz por la cual se recibirá el servicio. Finalmente, basta con hacer clic en el botón "Aceptar" para guardar los cambios realizados.

Figura 25.

Configuración del DHCP.

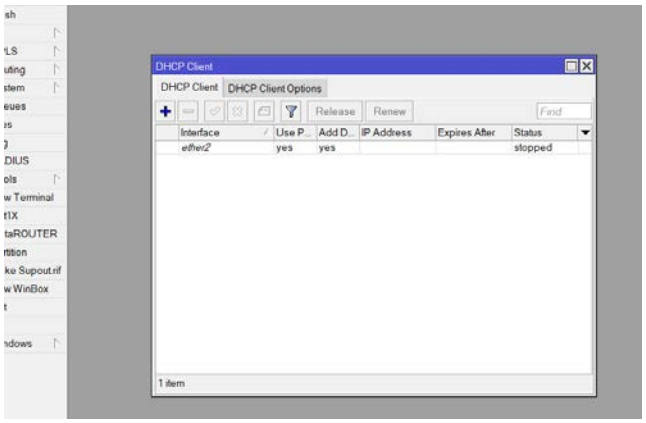


Nota: Se estable las interfaces según lo usado en el Mikrotik físicamente.

- Asi se tendrá la configuración automática, se verá como en la siguiente imagen.

Figura 26.

Configuración del DHCP.



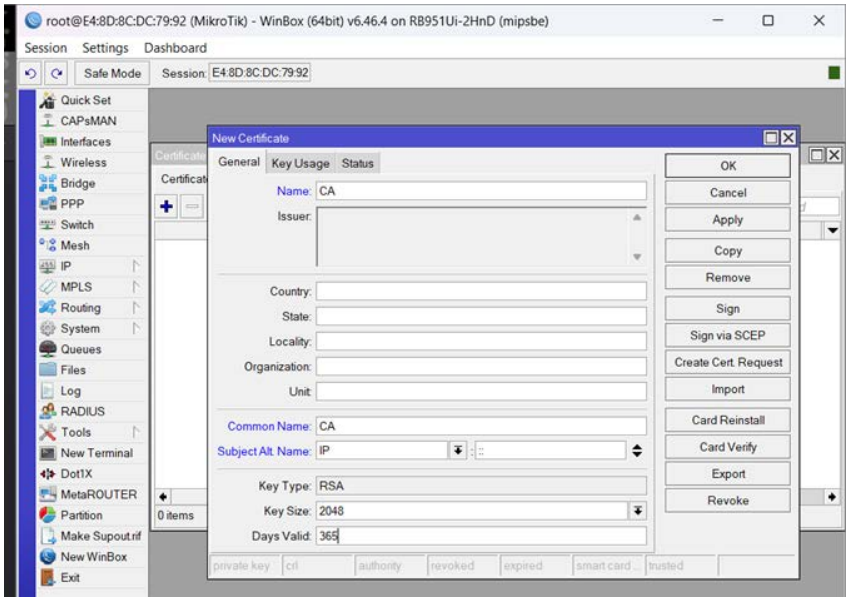
Nota: Se con éxito El DHCP.

CREACIÓN DE CERTIFICADOS OVPN.

Paso 1. Ingresar al MikroTik, dirigirse al apartado System y hacer clic en certificados. A continuación, debe hacer clic en el botón "+", para crear el primer certificado que será la Autoridad certificadora (CA). En la sección "Name" se debe ingresar el nombre correspondiente y en "Common Name" se debe repetir el nombre nuevamente. Además, en la sección "Key Size" se debe seleccionar el nivel de encriptación del certificado a crear.

Figura 27.

Creación de certificados OVPN.

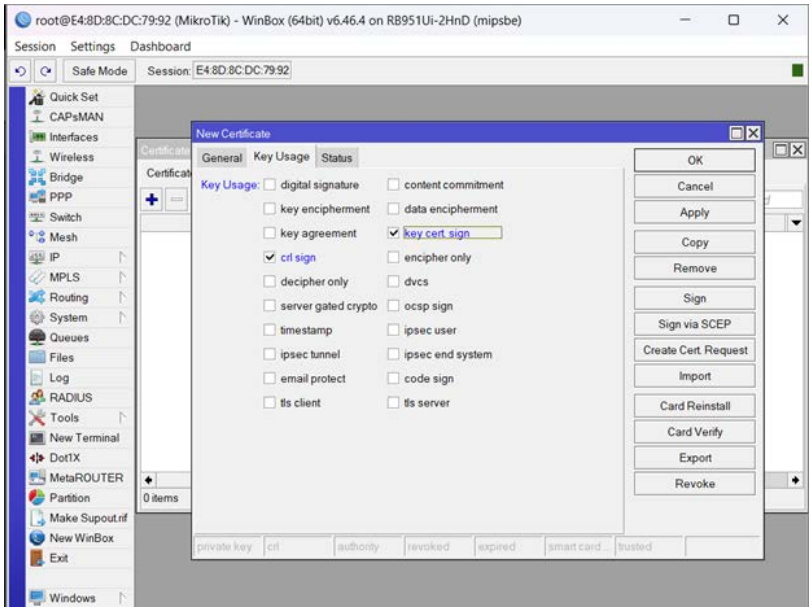


Nota: Apartado para la creacion de certificados.

Paso 2. Para definir los parámetros del certificado, se debe seleccionar CRL Sing y KEY Cert. Sing, y luego hacer clic en "Aplicar".

Figura 28.

Creación de certificados OVPN.

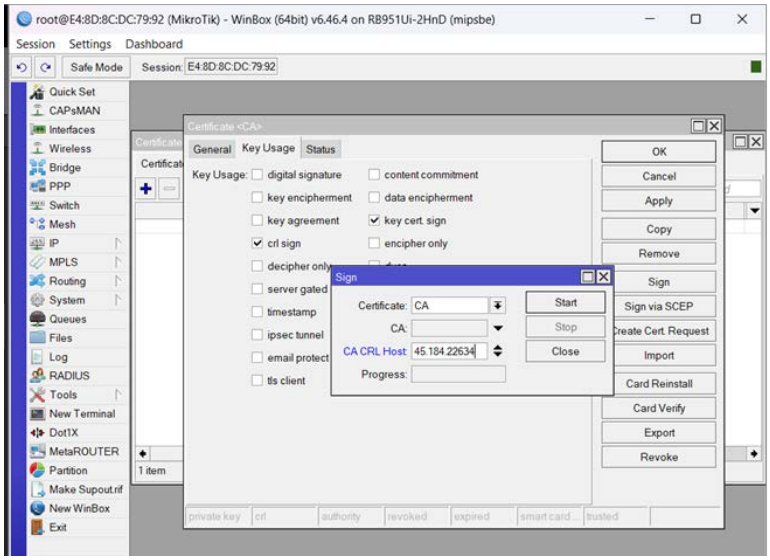


Nota: Se muestra los parámetros requeridos para el certificado.

Paso 3: Después hacer clic en "Sing" para asignar el host o el DDNS a su certificado en CA CRL Host, y luego hacer clic en "Start".

Figura 29.

Creación de certificados OVPN.

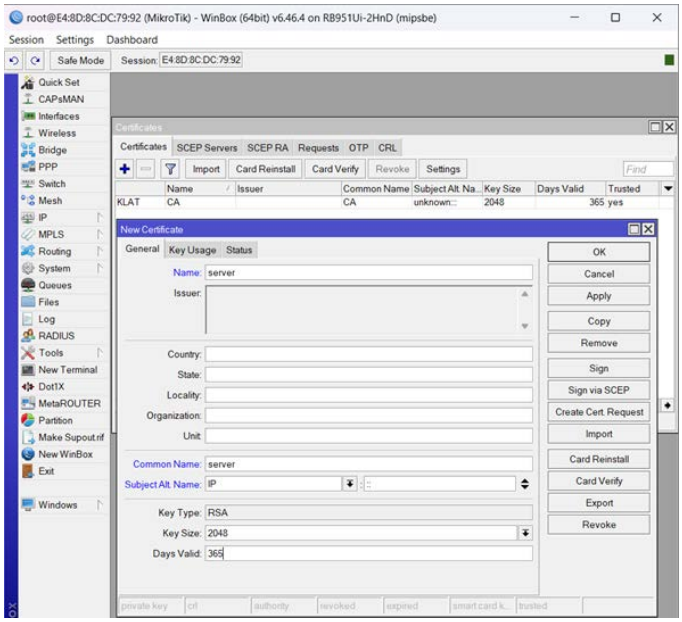


Nota: Se muestra los parámetros requeridos para el certificado.

Paso 4: El siguiente paso es la creación del certificado servidor. Se debe tener en cuenta que el parámetro "Key Size" será el mismos que del certificado anterior.

Figura 30.

Creación de certificados OVPN.

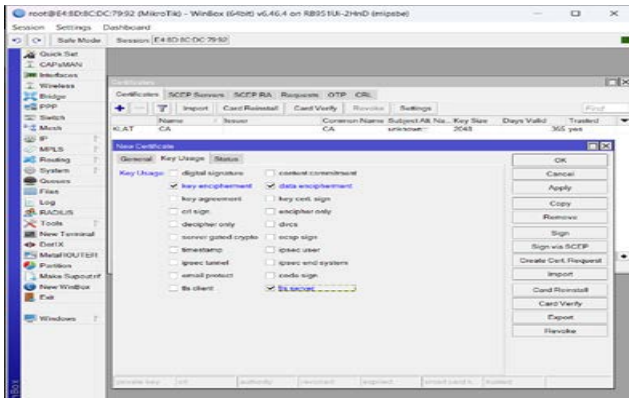


Nota: Apartado para la creacion de certificados server.

Paso 5: En este caso se debe seleccionar "Key Encipherment" y "Data Encipherment", y después hacer clic en "Aplicar" y luego en "Sing".

Figura 31.

Creación de certificados OVPN.

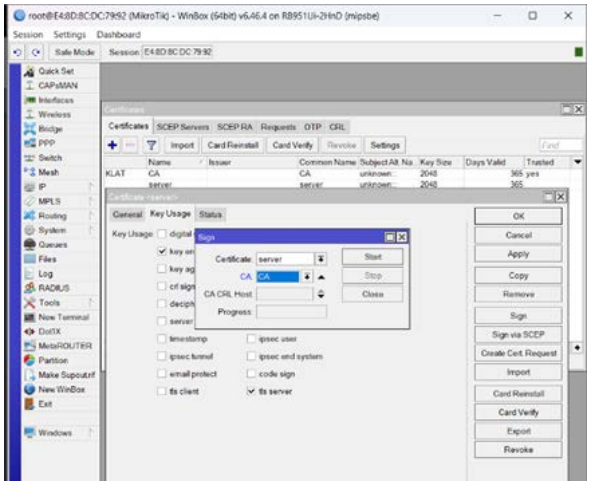


Nota: Se muestra los parámetros requeridos para el certificado.

Paso 6: Sincronizar el certificado del servidor con la Autoridad Certificadora (CA) correspondiente y, posteriormente, hacer clic en "Start".

Figura 32.

Creación de certificados OVPN.

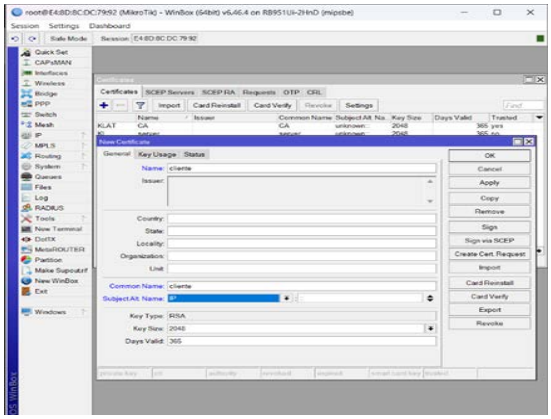


Nota: Se muestra los parámetros requeridos para el certificado.

Paso 7: Para crear el certificado cliente, se debe seguir los mismos pasos del certificado anterior, excepto en la sección "Key Usage" donde solo se debe seleccionar "TLS Client".

Figura 33.

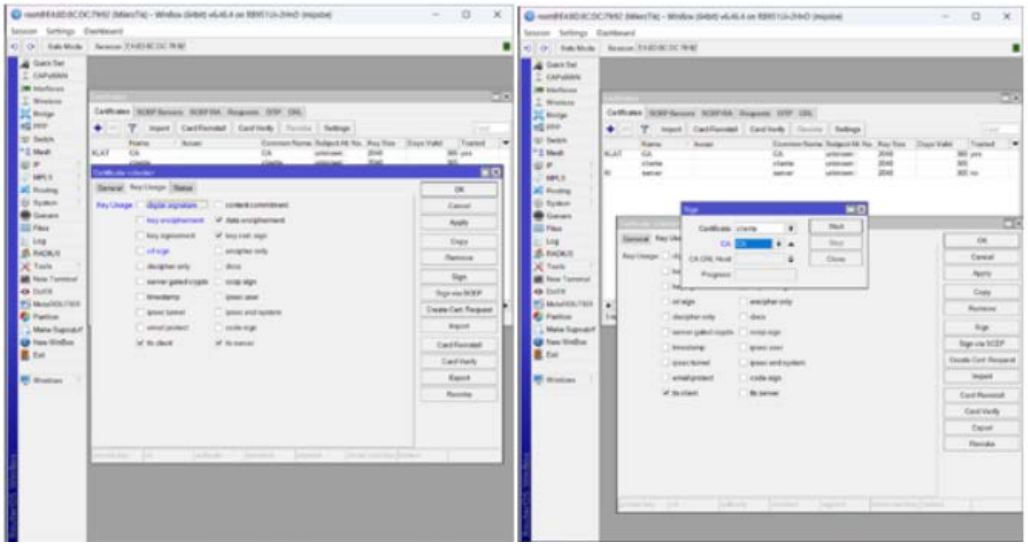
Creación de certificados OVPN.



Nota: Apartado para la creacion de certificados cliente.

Figura 34.

Creación de certificados OVPN.

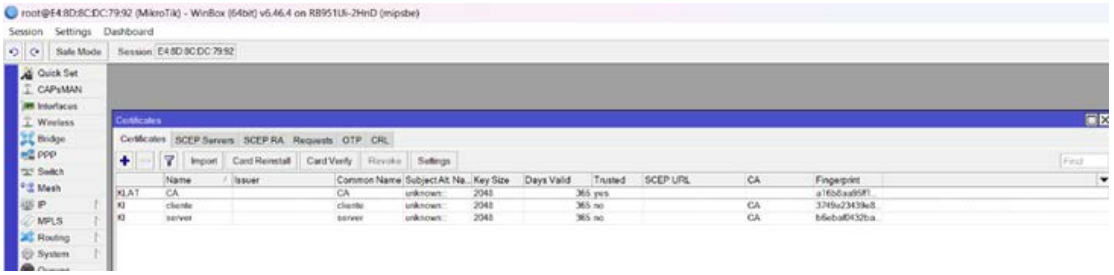


Nota: Se muestra los parámetros requeridos para el certificado.

Paso 8: Para verificar los certificados creados, debe asegurarse de que todo se haya realizado correctamente. Si es así, los certificados deberían aparecer como se muestra en la siguiente imagen.

Figura 35.

Creación de certificados OVPN.



Nota: Se presentan con éxito los certificados creados.

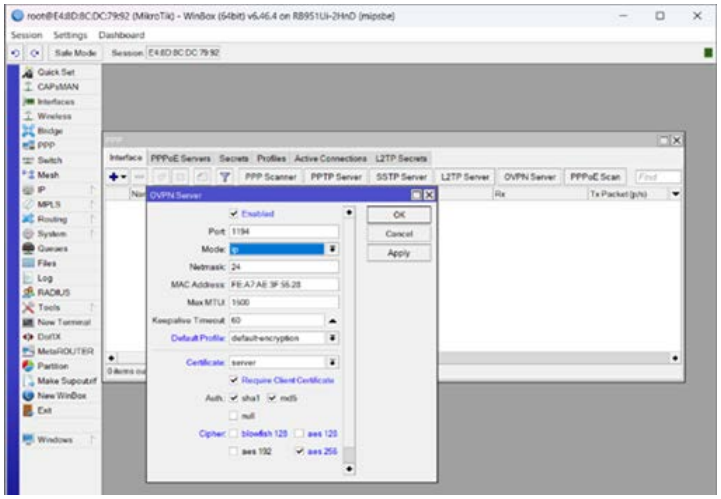
Configuración OVPN server Mikrotik - Client Mikrotik.

Paso 1: Después de haber generado los certificados en el dispositivo Mikrotik, el usuario deberá dirigirse a la sección de configuración y seleccionar la opción "Servidor

OVPN". A continuación, se habilitará el servidor y se mantendrá el puerto predeterminado (1194).

Figura 36.

Configuración OVPN server Mikrotik - Client Mikrotik.

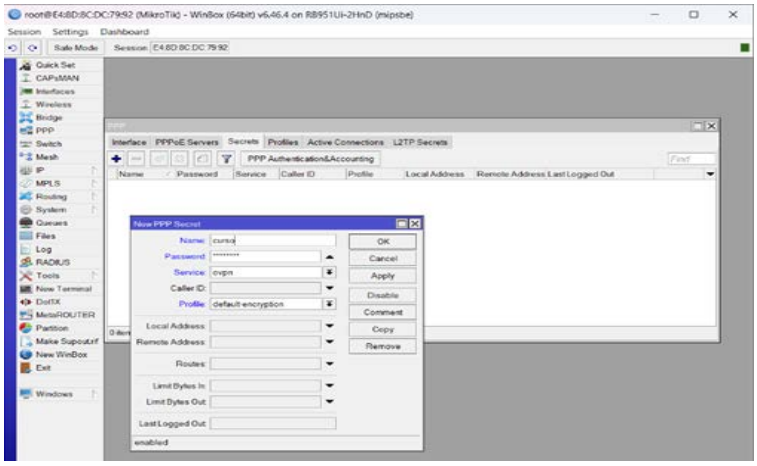


Nota: Se muestra los parámetros requeridos para el certificado.

Paso 2: Crear el usuario correspondiente en la pestaña "Secrets". Es importante asegurarse de seleccionar "ovpn" en el campo "Servicio" y elegir el perfil previamente asignado a la conexión.

Figura 37.

Configuración OVPN server Mikrotik - Client Mikrotik.

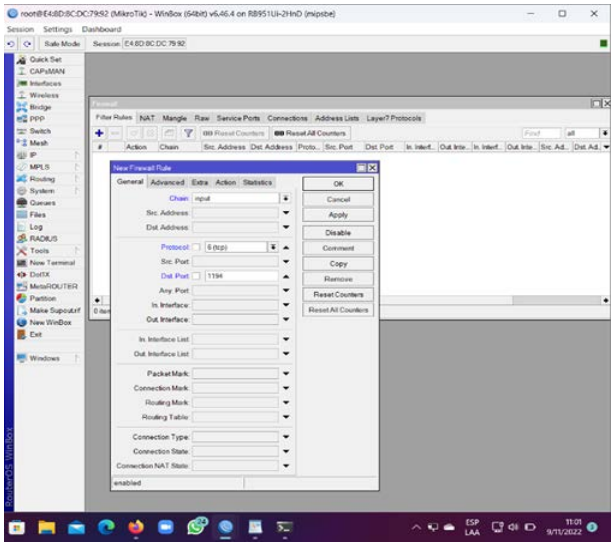


Nota: Se muestra el campo para crear el usuario para OpenVPN.

Paso 3: En este paso, es necesario verificar la regla de entrada en el firewall para abrir el puerto 1194.

Figura 38.

Configuración OVPN server Mikrotik - Client Mikrotik.

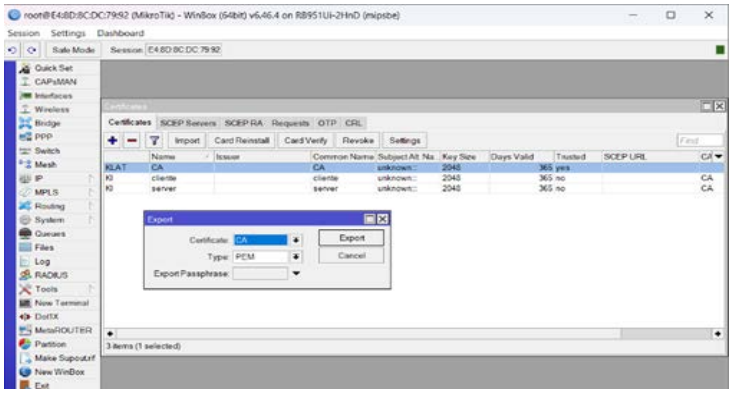


Nota: Se muestra los parámetros requeridos para el usuario.

Paso 4: El paso siguiente consiste en iniciar la descarga de los certificados para comenzar con la configuración del cliente. El primer certificado que se descargará es el certificado CA.

Figura 39.

Certificados Descargados.

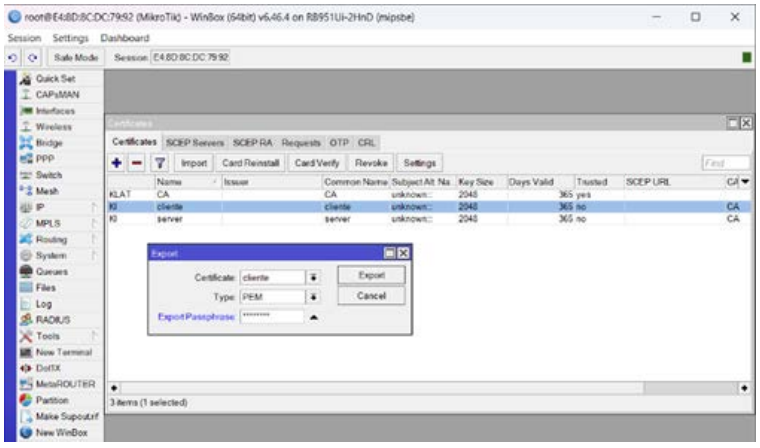


Nota: Se muestra los parámetros requeridos para descargar los certificados.

Paso 5: Se exportará el certificado del cliente, que contendrá su clave correspondiente. Para realizar esta acción, se utilizará una contraseña específica, en este caso "Curso.123!".

Figura 40.

Certificados Descargados.

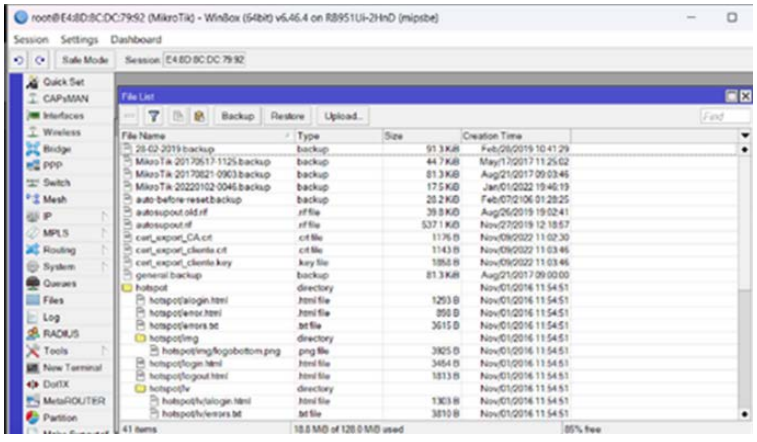


Nota: Se muestra los parámetros requeridos para descargar los certificados.

Paso 6: Una vez completado el paso anterior, la persona debe dirigirse a la opción "File". En dicha sección, se mostrarán los certificados que han sido exportados y están listos para su descarga.

Figura 41.

Certificados Descargados.



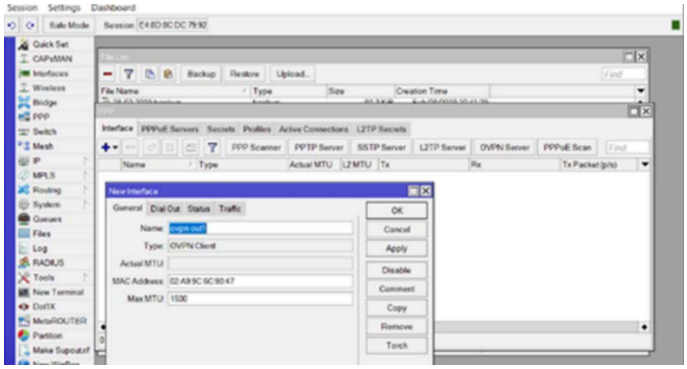
Nota: Se muestra los certificados listos para descargar.

Cliente Mikrotik

Paso 1: Exportamos nuestros certificados al Mikrotik cliente.

Figura 42.

Cliente Mikrotik.

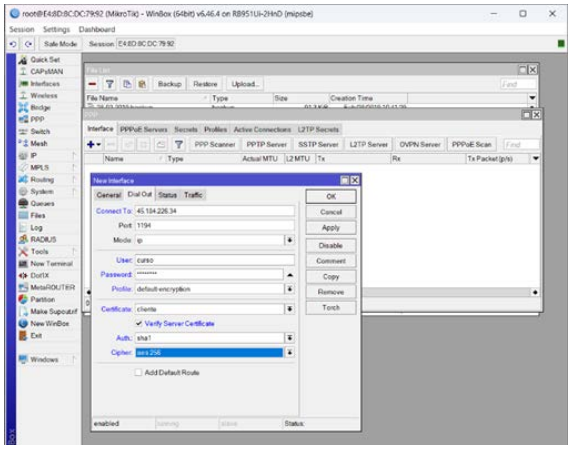


Nota: Se muestra los parámetros requeridos para el certificado Cliente.

Paso 2: Dirigirse a la sección de PPP-Interface y seleccionar el ícono de suma (+) para añadir una interfaz de cliente OpenVPN. Luego, se deberán ajustar los parámetros que se presentan en la imagen correspondiente. Es importante considerar la ubicación de los certificados y verificar que los valores de "Auth" y "Cipher" sean idénticos a los del servidor.

Figura 43.

Cliente Mikrotik.



Nota: Se muestra los parámetros requeridos para el certificado.

Conexión en OpenVPN – MikroTik

- Exportar los certificados de WinBox al escritorio de nuestro ordenador.

Figura 44.

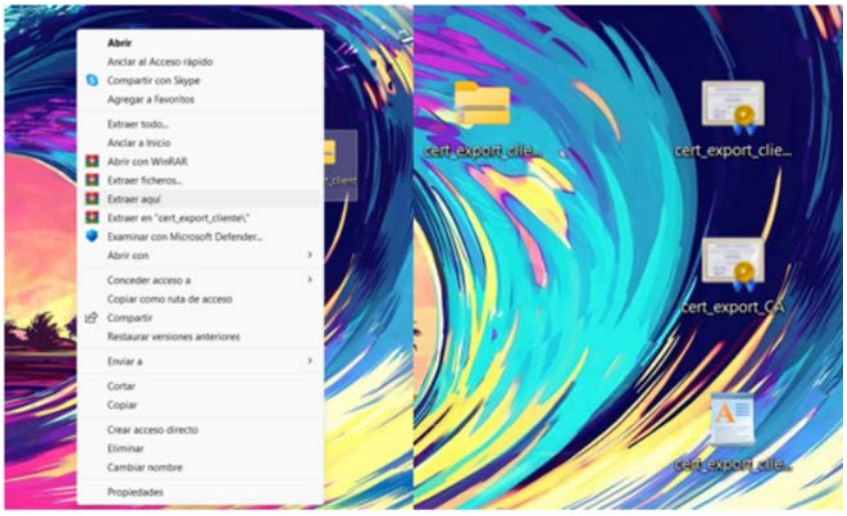
Conexión en OpenVPN – MikroTik

Nota: Se visualizan los archivos ya descargados ene le escritorio.

- Extraer los archivos ZIP en el escritorio.

Figura 45.

Conexión en OpenVPN – MikroTik



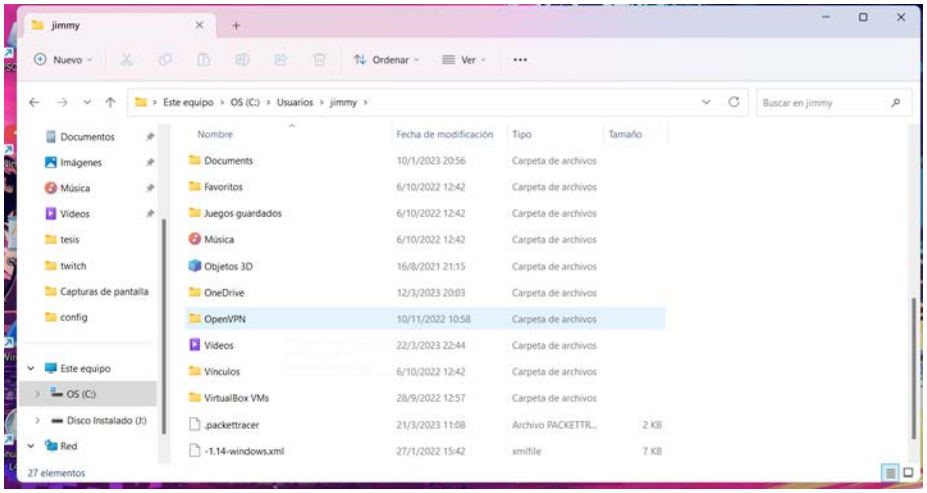
Nota: Se muestra los certificados ya extraídos.

- Seleccionar los archivos extraídos y cortarlos, dirigirse a documentos, disco local, clic en el nuestro usuario y buscamos la carpeta.

OpenVPN.

Figura 46.

Conexión en OpenVPN – MikroTik

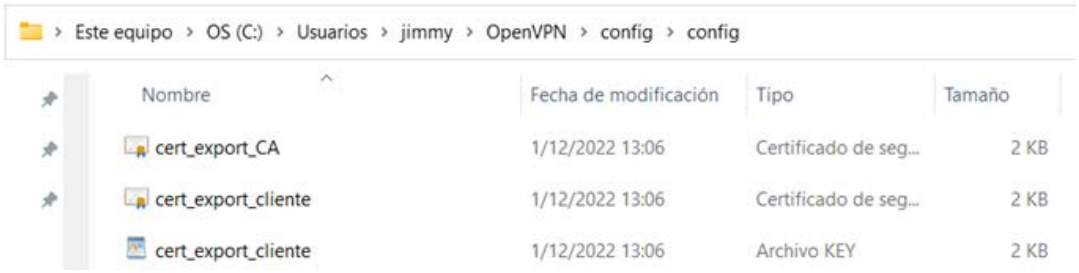


Nota: Se muestra la ubicación de la carpeta madre de OpenVPN.

- Ingresar a la carpeta OpenVPN, luego a la carpeta “config” dos veces y pegar los certificados en la carpeta.

Figura 47.

Conexión en OpenVPN – MikroTik

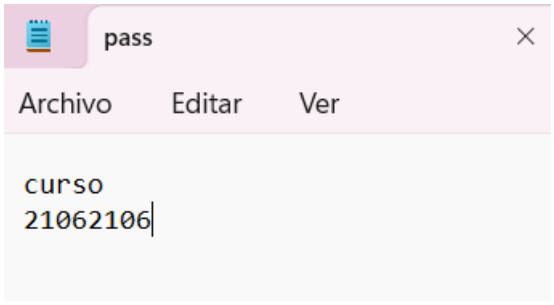


Nota: Colocación de los certificados en la carpeta principal.

- Lo siguiente es crear un Documento de Texto dentro de la carpeta config donde pegamos los certificados, para poner el usuario y la contraseña, guardándolo con el nombre “pass”.

Figura 48.

Conexión en OpenVPN – MikroTik

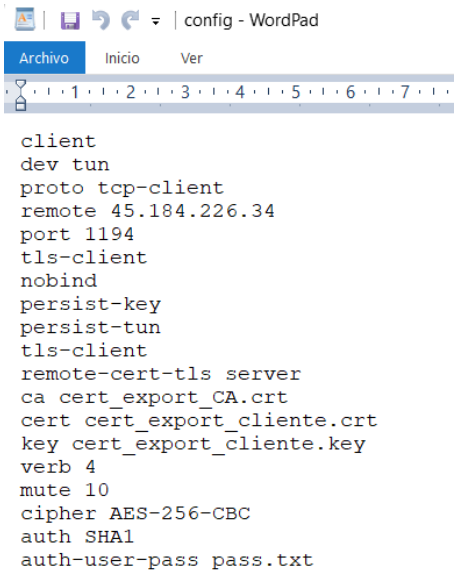


Nota: Se muestra la contraseña y usuario.

- Seguido a eso crear un blog de notas con las siguientes características.

Figura 49.

Conexión en OpenVPN – MikroTik

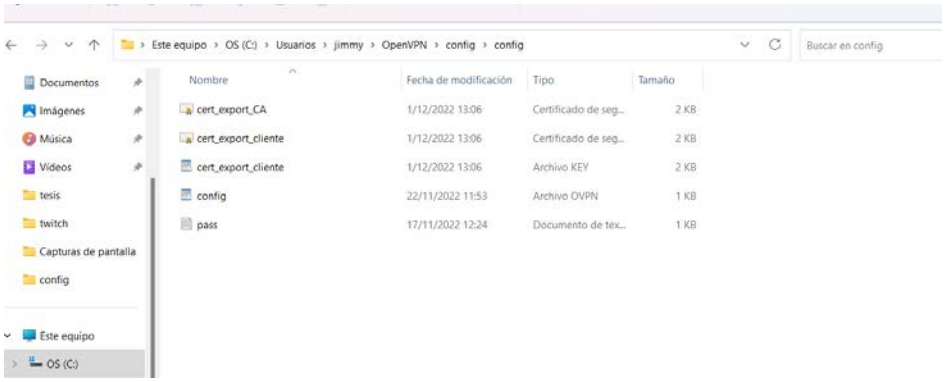


Nota: Se presenta los parámetros del archivo config para el uso de OpenVPN.

- Debe quedar todo lo establecido de la siguiente forma:

Figura 50.

Conexión en OpenVPN – MikroTik



Nota: Se visualiza todos los requisitos “archivos” para el uso de OpenVPN.

- Por último, prender OpenVPN, así se estaría conectado al datacenter del Campus Ramírez Dávalos del ITI.

Figura 51.

Conexión en OpenVPN – MikroTik

Nota: Se evidencia que está funcionando correctamente.

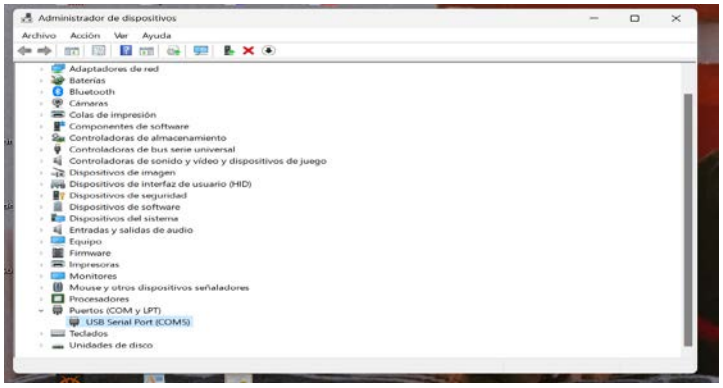
Configuración del protocolo SSH en Switch y Router Cisco.

Con el fin de configurar correctamente los equipos, fue necesario obtener acceso a ellos y establecer ciertos parámetros específicos para asegurar su correcto funcionamiento para ello se debió seguir los siguientes pasos.

- Conectar el cable de consola en el equipo de cisco y luego a nuestro computador.
- Ingresar al administrador de dispositivos, dirigirse al apartado de puertos y detectar que número de USB Serial Port es, en este caso es el (COM5).

Figura 52.

Administrador de dispositivos(Puerto-COM).

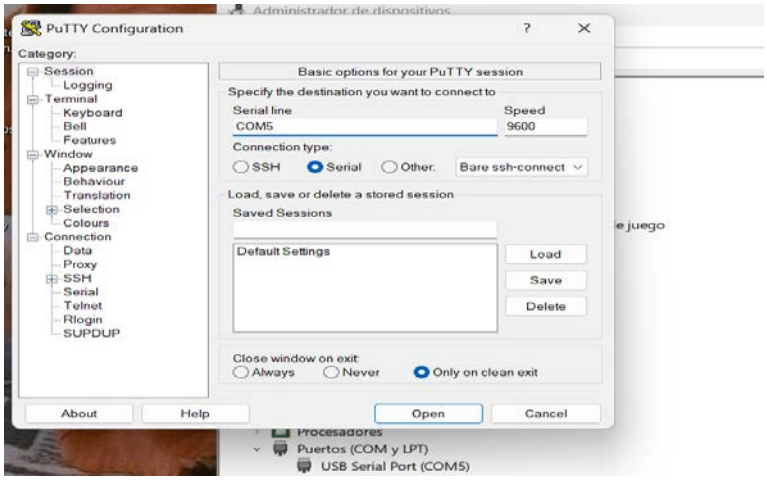


Nota: el puerto serial varía dependiendo al cable de consola.

- Ingresar a la aplicación PuTTY, colocar la línea serial anterior mente vista, tipo de conexión “serial” por medio de Bare ssh-connect, por último, poner Open.

Figura 53.

Ventana de Configuración de PuTTY.



Nota: Se muestra la ventana de PuTTY para el ingreso a los equipos de cisco.

Habilitación del protocolo SSh en Switch cisco.

Una vez ingresados al equipo por medio de PuTTY se podrá ingresar las siguientes líneas de comando necesarias para las configuraciones:

- Direcciones IP establecidas.

IP address: 10.1.0.10

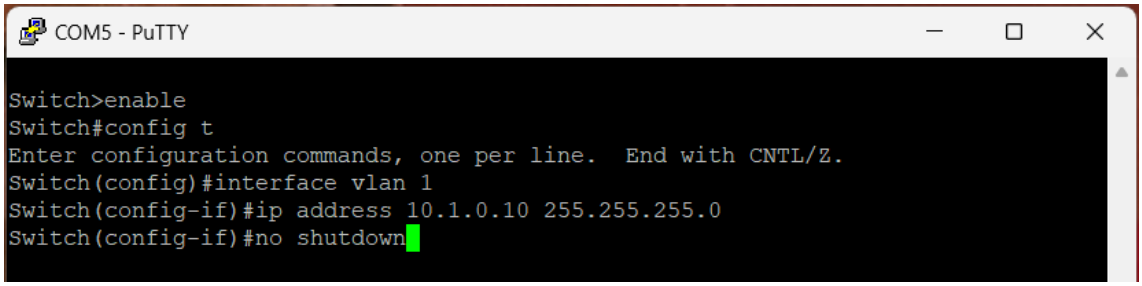
Mascara: 255.255.255.0

Default Gateway: 10.1.0.15

- Configuración de IP de administración:

Figura 54.

Habilitación del protocolo SSh en Switch cisco.

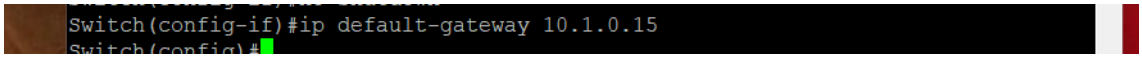


Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

- Configuración de default Gateway hacia el router

Figura 55.

Habilitación del protocolo SSh en Switch cisco.

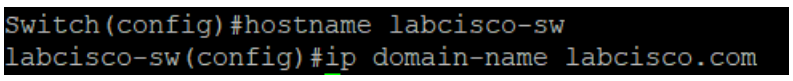


Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

- Configuración del hostname u nombre de dominio.

Figura 56.

Habilitación del protocolo SSh en Switch Cisco.



Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

- Generación de llaves RSA.

Figura 57.

Habilitación del protocolo SSh en Switch cisco.

```
labcisco-sw(config)#crypto key generate rsa
The name for the keys will be: labcisco-sw.labcisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 22 seconds)
```

Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

- Configuración a SSH versión 2

Figura 58.

Habilitación del protocolo SSh en Switch cisco.

```
labcisco-sw(config)#ip ssh version 2
```

Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

- Configuración de Line VTY.

Figura 59.

Habilitación del protocolo SSh en Switch cisco.

```
labcisco-sw(config)#line vty 0 15
labcisco-sw(config-line)#transport input ssh
labcisco-sw(config-line)#login local
labcisco-sw(config-line)#exit
```

Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

- Establecer Nombre de usuario y password.

Figura 60.

Habilitación del protocolo SSh en Switch cisco.

```
labcisco-sw(config)#username labcisco privilege 15 secret cisco 123
```

Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

- Habilitación del enable secret.

Figura 61.

Habilitación del protocolo SSh en Switch cisco.

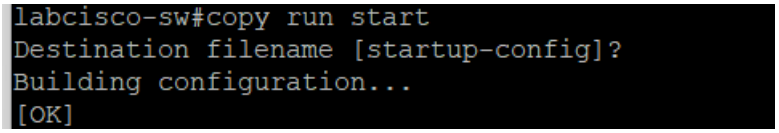
```
labcisco-sw(config)#enable secret cisco123
```

Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

- Guardar cambios.

Figura 62.

Habilitación del protocolo SSh en Switch cisco.



Nota: Se evidencia las configuraciones dentro del switch cisco por medio de un cable de consola.

Habilitación del protocolo SSh en el router Cisco

Se realizan los mismos pasos que el apartado anterior, con ciertos parámetros variados los cuales son:

- Habilitación de una interface g.
- Designación del Gateway como IP Address

Figura 63.

Habilitación del protocolo SSh en el router cisco.

```
Router#enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname labcisco-router
labcisco-router(config)#interface g0/0
labcisco-router(config-if)#ip address 10.1.0.15 255.255.255.0
labcisco-router(config-if)#no shutdown
labcisco-router(config-if)#
*Apr 13 16:30:27.831: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed stat
e to downe
*Apr 13 16:30:31.343: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed stat
e to up
*Apr 13 16:30:32.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet0/0, changed state to up
% Ambiguous command:  "e"
labcisco-router(config-if)#exit
labcisco-router(config)#ip domain-name labcisco.com
labcisco-router(config)#username labcisco privilege 15 secret cisco123
labcisco-router(config)#crypto key generate rsa
The name for the keys will be: labcisco-router.labcisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 13 seconds)

labcisco-router(config)#
*Apr 13 16:32:19.595: %SSH-5-ENABLED: SSH 1.99 has been enabled
labcisco-router(config)#ip ssh version 2
labcisco-router(config)#enable secret cisco123
labcisco-router(config)#line vty 0 15
labcisco-router(config-line)#transport input ssh
labcisco-router(config-line)#login local
```

Nota: Se evidencia las configuraciones dentro del router cisco por medio de un cable de consola.

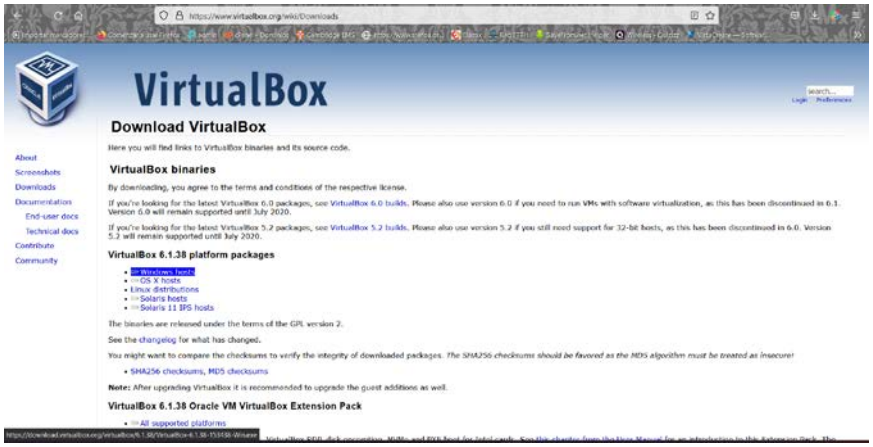
PRÁCTICA CON MÁQUINAS VIRTUALES.

Virtual Box.

- Descargar el instalador de VirtualBox desde el sitio web oficial de Oracle: https://www.virtualbox.org/wiki/Downloads

Figura 64.

VIRTUAL BOX.



Nota: Pestaña de descarga del Virtual Box.

- Ejecutar el archivo de instalación descargado y sigue las instrucciones en pantalla.

Figura 65.

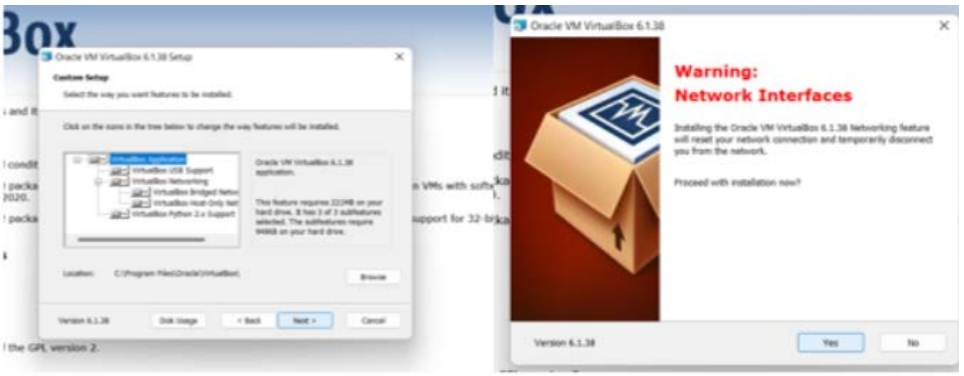
VIRTUAL BOX.

Nota: Pestaña de ejecución del Virtual Box.

- Seleccionar la ubicación en la que deseas instalar VirtualBox.
- Configurar las opciones de red según tus preferencias

Figura 66.

VIRTUAL BOX.



Nota: Se evidencia los parámetros para el uso de virtual box.

- Haz clic en "Instalar" para comenzar la instalación.

Figura 67.

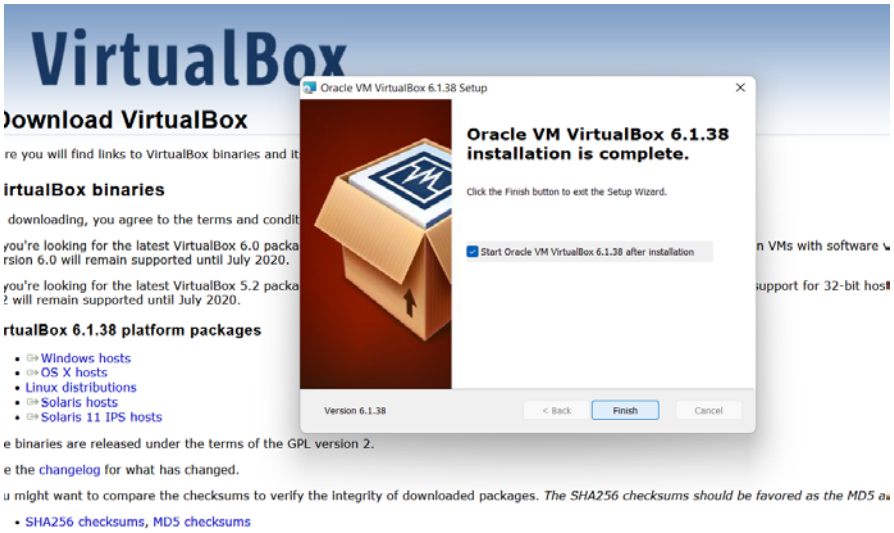
VIRTUAL BOX.

Nota: Se refleja la correcta instalación del programa.

- Una vez completa la instalación,clic en "Finalizar" para salir del instalador.

Figura 68.

VIRTUAL BOX.



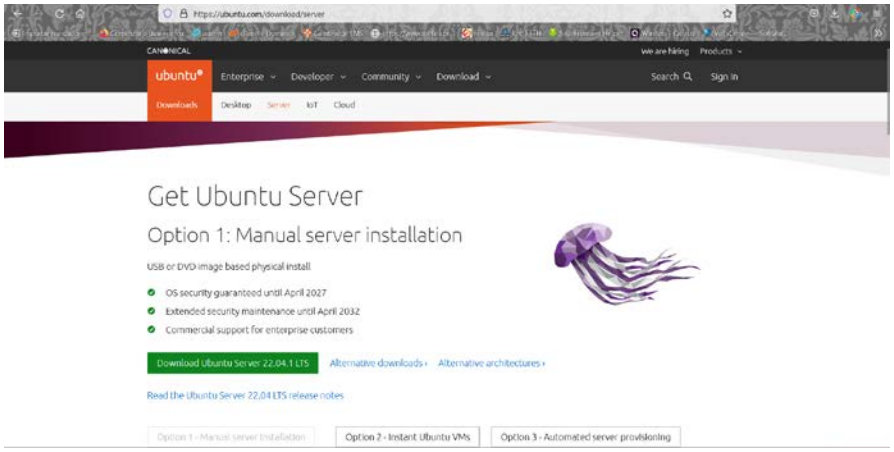
Nota: Finalización de la instalación del programa.

Ubuntu Server

- Acceder al sitio web oficial de Ubuntu: https://ubuntu.com/download/server
- Seleccionar la versión de Ubuntu Server que deseas descargar
- Seleccionar la arquitectura de tu sistema
- Hacer clic en "Descargar" para descargar el archivo ISO de Ubuntu Server.

Figura 69.

UBUNTU SERVER

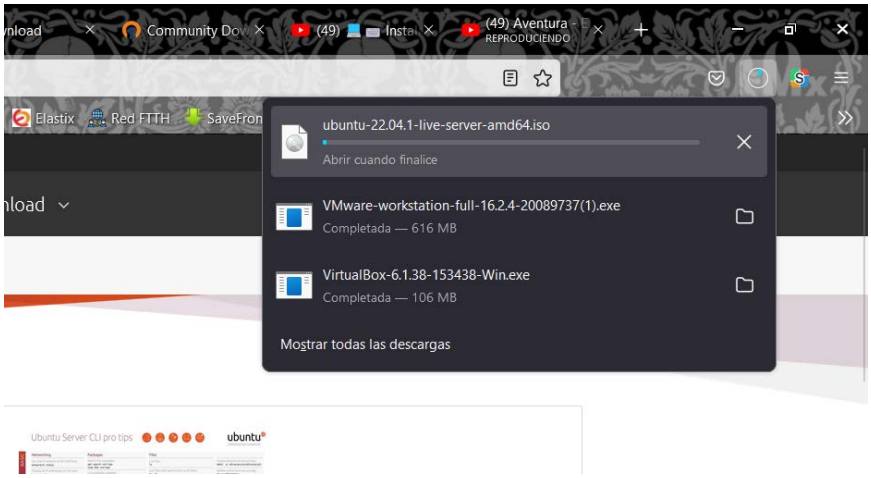


Nota: Se muestra la página de descarga de Ubuntu SERVER.

- Esperar a que se complete la descarga. Esto puede tardar varios minutos, dependiendo de la velocidad de tu conexión a Internet.

Figura 70.

UBUNTU SERVER



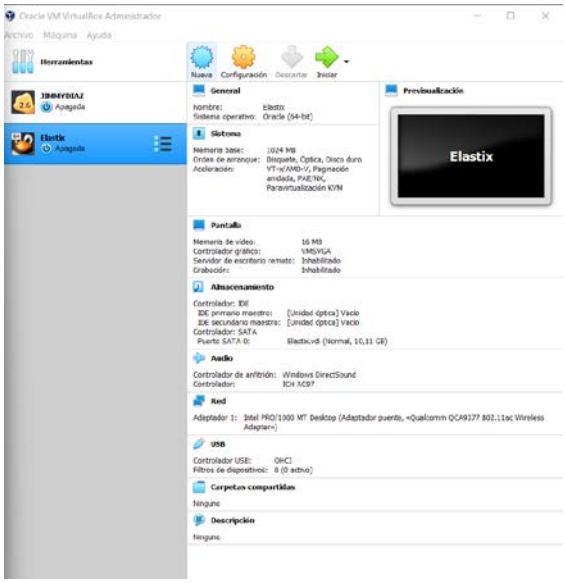
Nota: se muestra la descarga del programa.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server

- Abrir Virtual Box y haz clic en "Nuevo" en la barra de herramientas.

Figura 71.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.

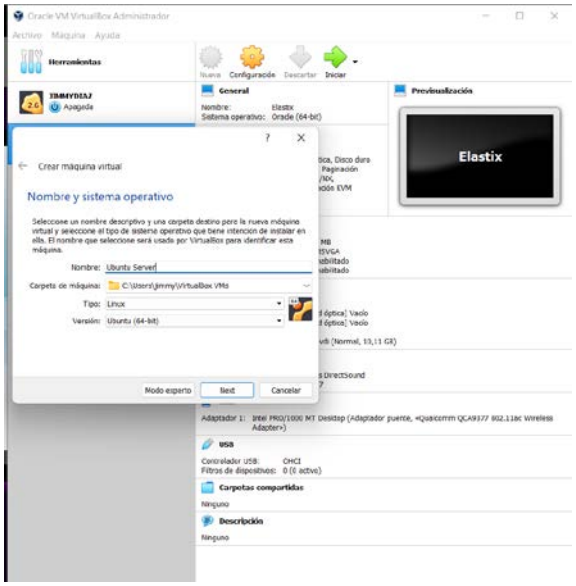


Nota: Interfaz de VirtualBox donde se ejecutará la máquina virtual.

- Asignar un nombre a la máquina virtual y seleccionar "Linux" como el tipo de sistema operativo y "Ubuntu" como la versión.

Figura 72.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.

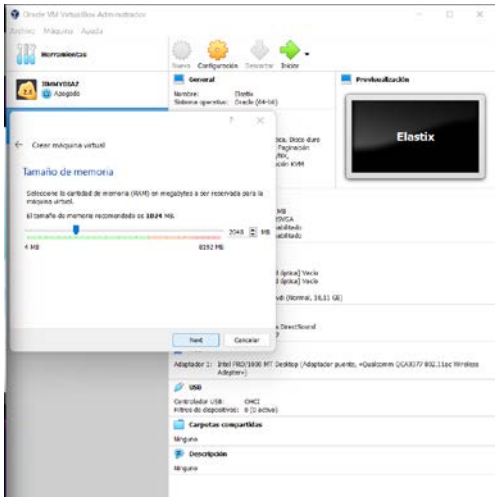


Nota: Se visualiza la asignación de los parámetros de la máquina virtual.

- Asignar la cantidad de memoria RAM deseada que tenga la máquina virtual. Se recomienda al menos 1 GB de RAM para Ubuntu Server.

Figura 73.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.

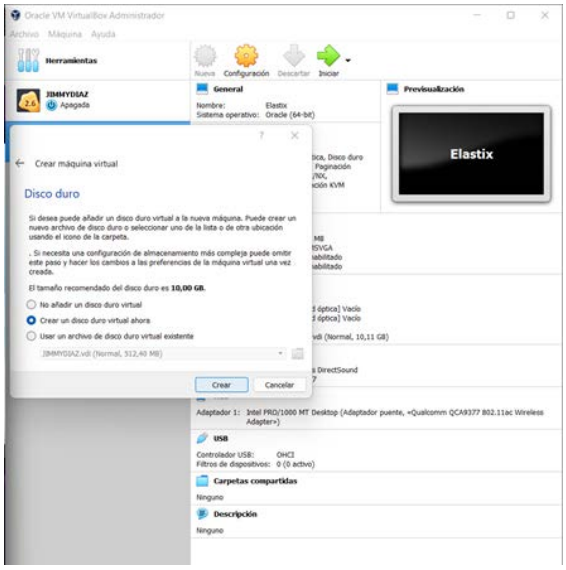


Nota: La cantidad de memoria puede ser usada según su conveniencia.

- Crear el disco duro de manera virtual.

Figura 74.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.

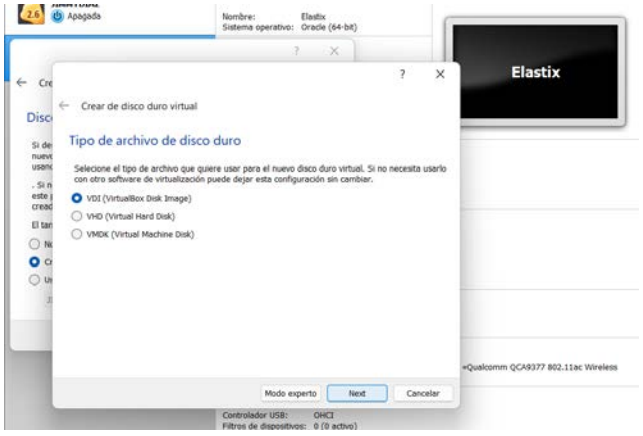


Nota: Se establece que tipo de disco duro será “virtual”.

- Seleccionar el tipo de disco duro (se recomienda "VDI") y hacer clic en "Siguiente".

Figura 75.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.



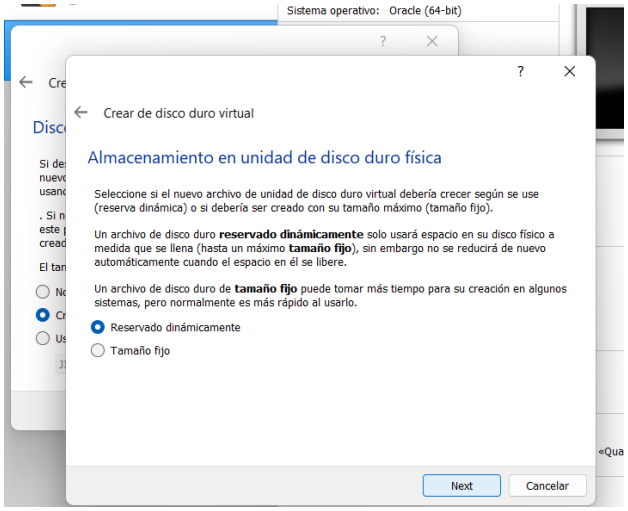
Nota: Se muestra el tipo de archivo del disco duro.

- Seleccionar si deseas que el disco duro sea dinámico o fijo. La opción

"dinámico" permite que el disco duro se expanda automáticamente a medida que se necesite más espacio. La opción "fijo" asigna todo el espacio de una vez y no permite expandirlo más adelante.

Figura 76.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.

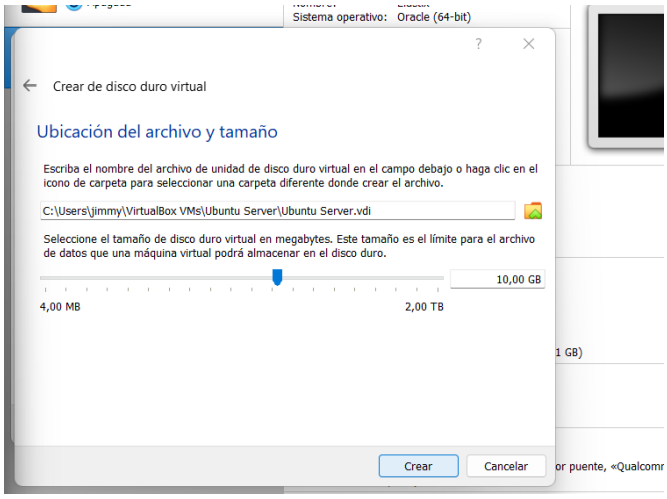


Nota: importante poner un almacenamiento dinámico al disco duro.

- Asignar el tamaño del disco duro.
- Haz clic en "Crear" para crear el disco duro virtual.

Figura 77.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.

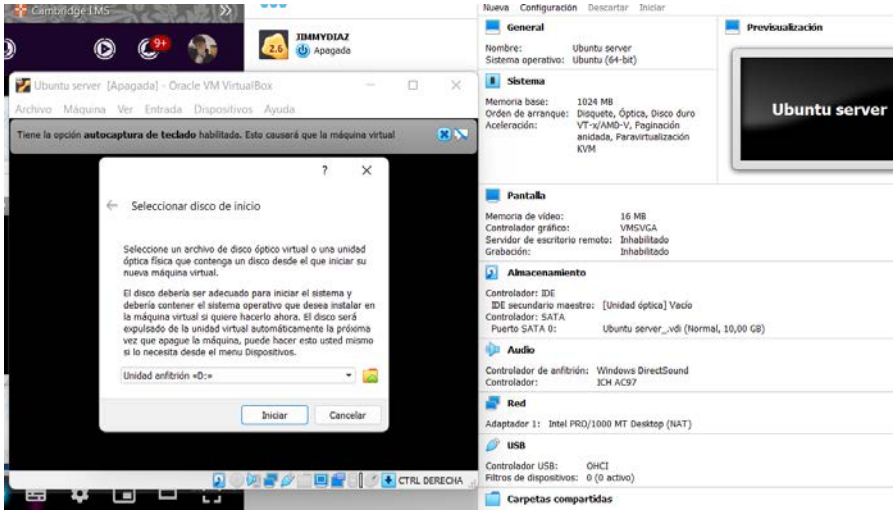


Nota: Se recomienda al menos 20 GB para Ubuntu Server.

- Selecciona el archivo ISO de Ubuntu Server que descargaste previamente y haz clic en "Iniciar"

Figura 78.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.



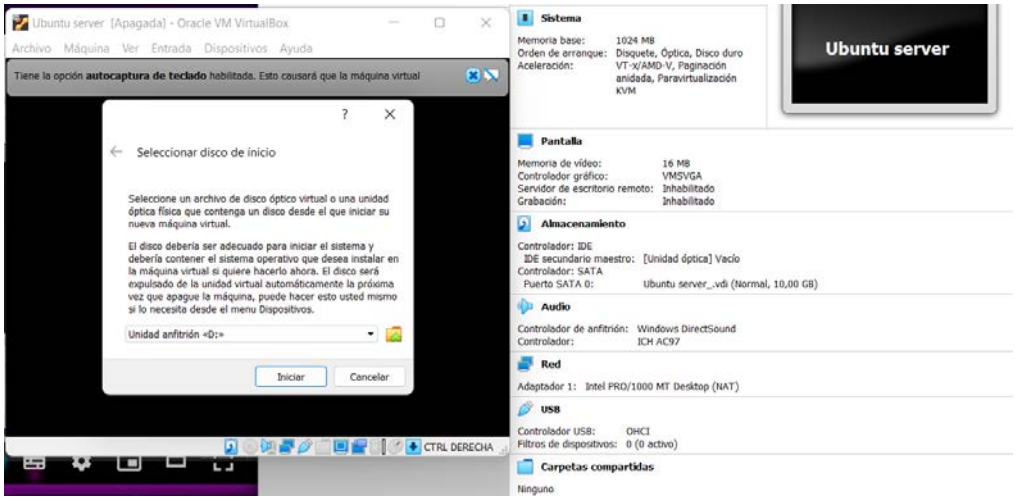
Nota: Se debe seleccionar el archivo ISO según su fuente de ubicación.

- Una vez que hayas creado la máquina virtual, sigue los siguientes pasos para instalar Ubuntu Server:

- Haz clic en la máquina virtual recién creada y haz clic en "Iniciar".

Figura 79.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.

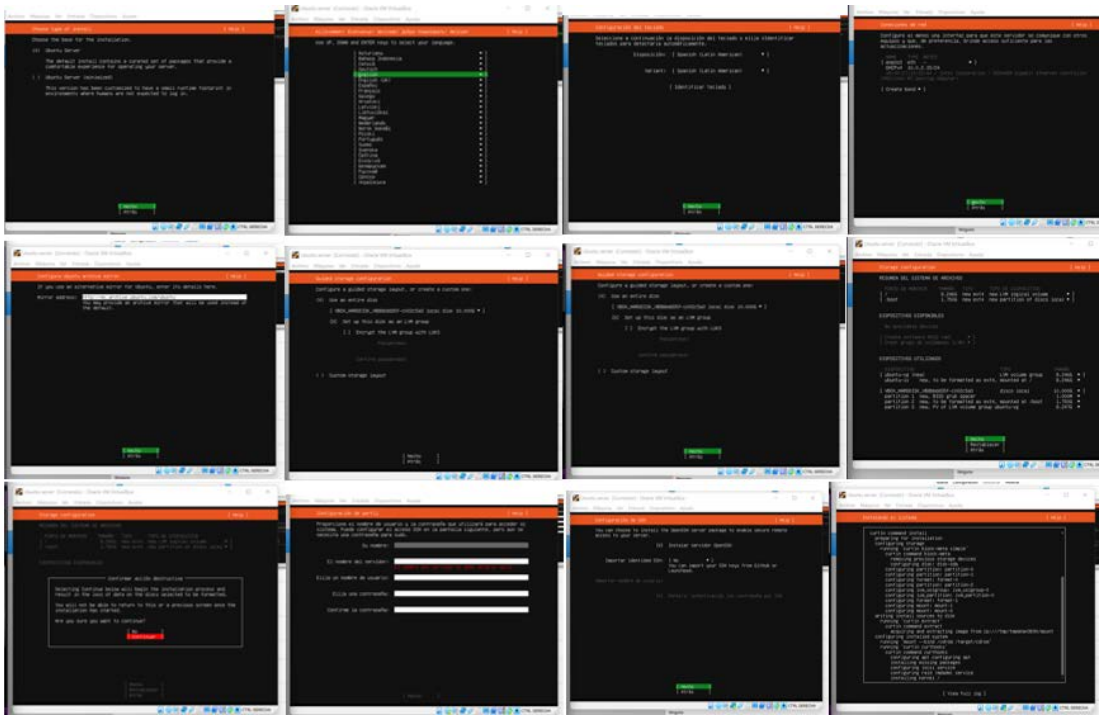


Nota: Se muestra la iniciación de la instalación de Ubuntu SERVER.

- Sigue las instrucciones en pantalla para instalar Ubuntu Server. Esto incluye seleccionar el idioma, configurar la red, crear un usuario y contraseña, y seleccionar el software adicional que deseas instalar.

Figura 80.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.

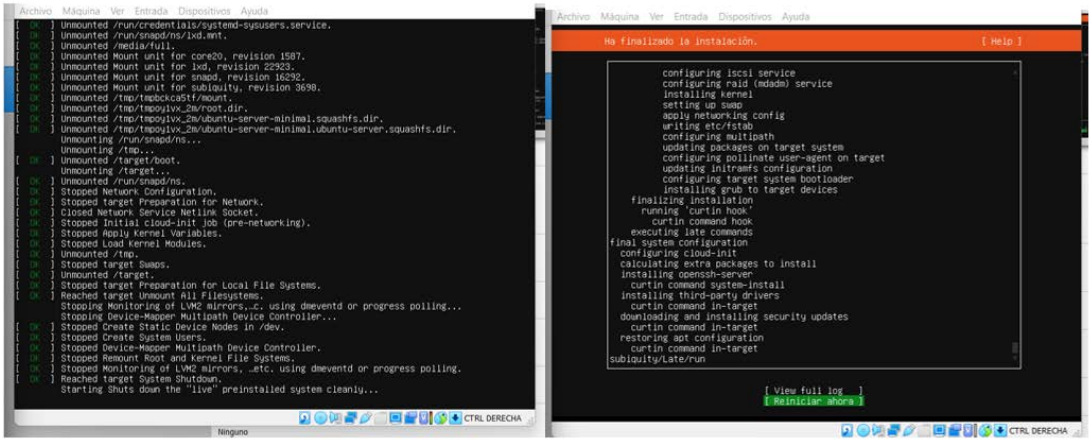


Nota: se muestra todos parámetros básicos que Ubuntu SERVER establece.

- Una vez que se complete la instalación, reinicia la máquina virtual y accede a Ubuntu Server ingresando tu nombre de usuario y contraseña.

Figura 81.

Creación de una Máquina Virtual con Virtual Box y Ubuntu Server.



Nota: Se visualiza con éxito la instalación de Ubuntu Server.

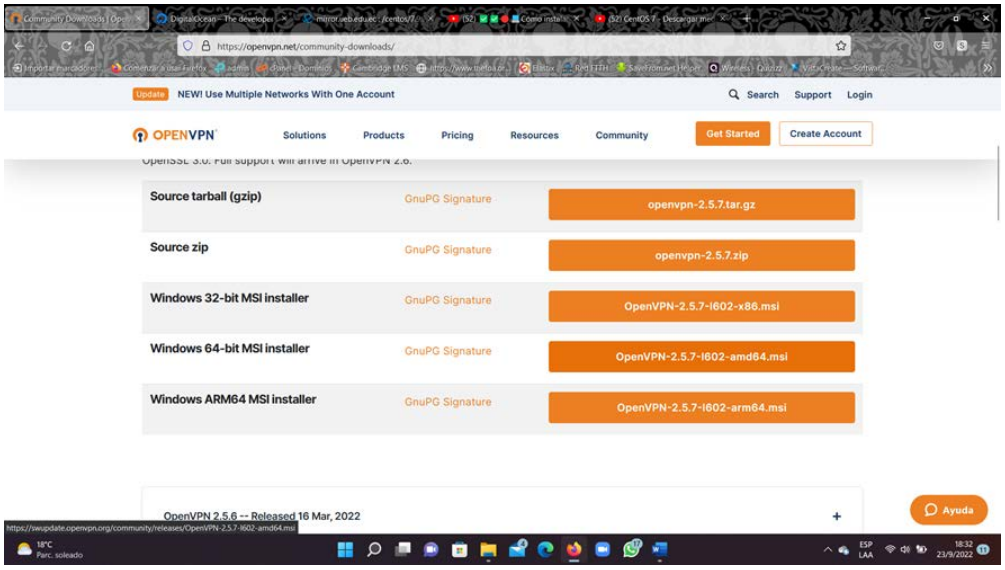
OPEN VPN

- Descarga el instalador de OpenVPN desde el sitio web oficial:

  https://openvpn.net/community-downloads/

Figura 82.

OPEN VPN

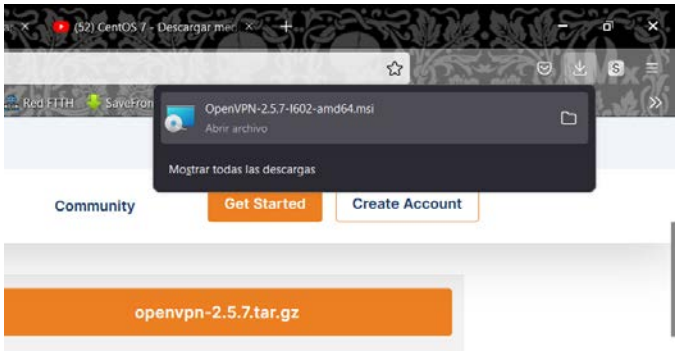


Nota: Se presenta la página oficial de Open VPN.

- Descargar el archivo según los parámetros que posea tu computador.

Figura 83.

OPEN VPN

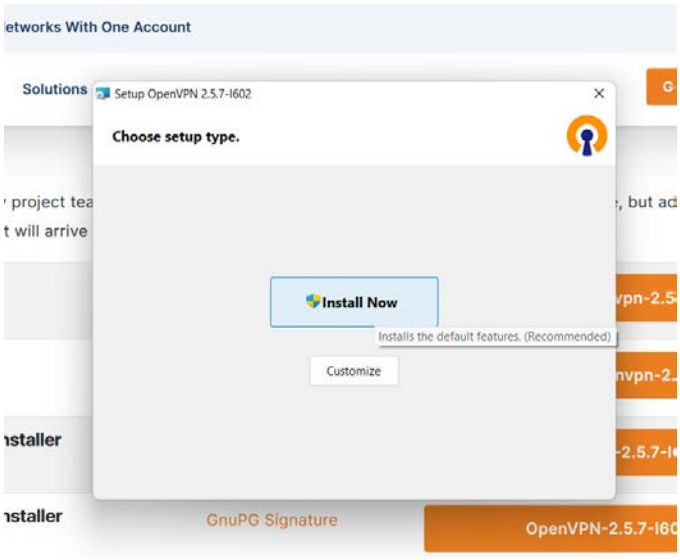


Nota: Se visualiza la descarga del programa.

- Haz clic en "Instalar" para comenzar la instalación. Espera a que se complete la instalación.

Figura 84.

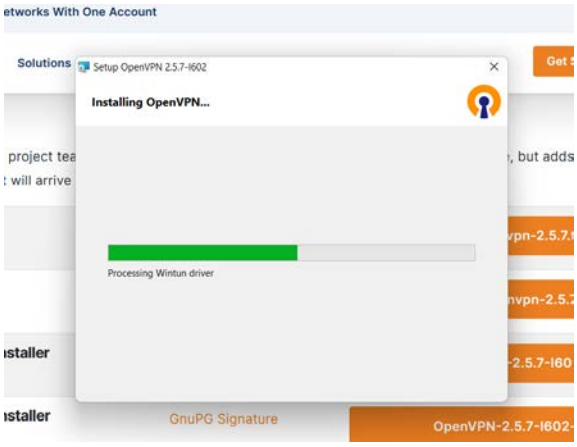
OPEN VPN



Nota: Se comienza con la instalación del programa.

Figura 85.

OPEN VPN



Nota: Se comienza con la instalación del programa.

PuTTY

- Ingresar a la pagina official de Putty en el siguiente link https://www.putty.org/ luego al apartado de Download PuTTY y escoger el packete files dependiendo a las características del ordenador.

Figura 86.

PuTTY

Package files

You probably want one of these. They include versions of all the PuTTY utilities (except the ne

Bug: this installer was built differently to other versions, in a way that causes trouble for upgrad versions, we recommend completely uninstalling the existing version first. You can avoid the ne

```
msiexec.exe /i path\to\putty-64bit-0.78-installer.msi ALLUSERS=1
```

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge do

MSI ('Windows Installer')

64-bit x86:	putty-64bit-0.78-installer.msi	(signature)
64-bit Arm:	putty-arm64-0.78-installer.msi	(signature)
32-bit x86:	putty-0.78-installer.msi	(signature)

Unix source archive

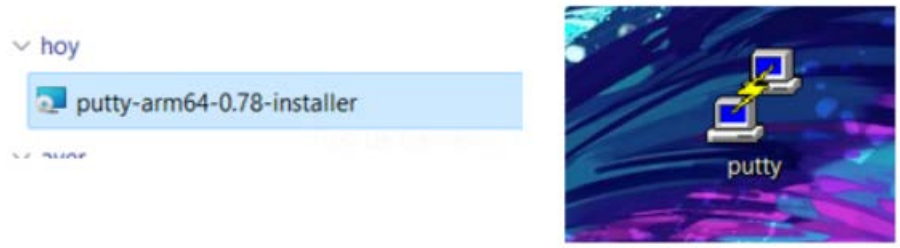
.tar.gz:	putty-0.78.tar.gz	(signature)

Nota: Página oficial de PuTTY.

- Una vez descargado ejecutar el archivo y dar los permisos necesarios para su ejecución una vez finalizado se tendra el programa instalado.

Figura 87.

PuTTY

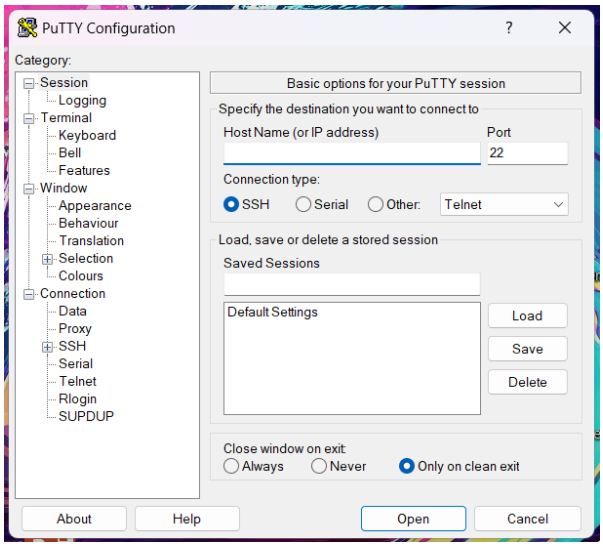


Nota: Se muestra el archivo y luego el programa ya instalado.

- Abrir el programa y en el apartado de host name poner la IP que asignada en la máquina virtual al igual que su puerto, en tipo de conexión seleccionar por medio de SSH.

Figura 88.

PuTTY

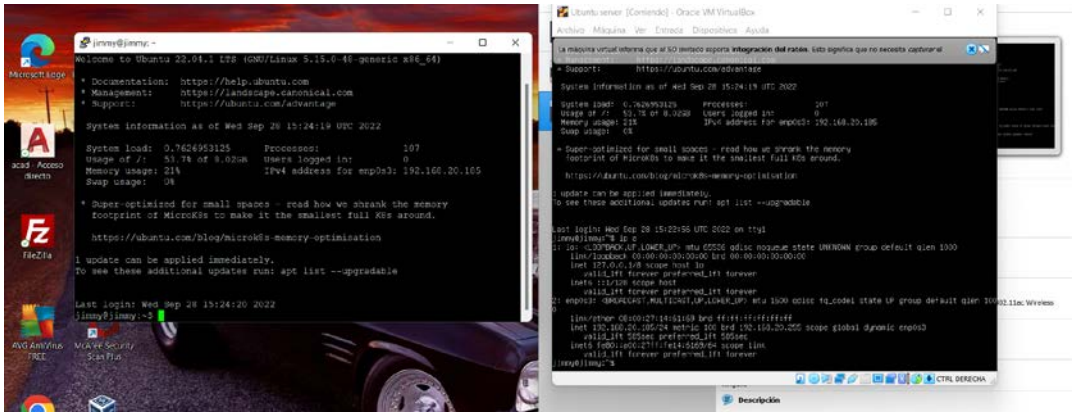


Nota: Se muestra la interfas principal de PuTTY.

- Una vez completados todos los pasos se estara conectado por medio de una VPN a la máquina virtual.

Figura 89.

Conexión Con el servidor VPN.



Nota: Se visualiza con éxito la práctica.

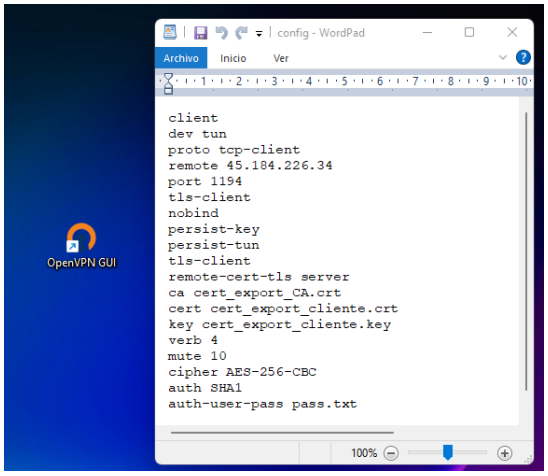
RESULTADOS

En las presentes capturas se muestra evidencia del proyecto desarrollado dando pautas de los pasos para su conexión.

- Verificacion de la config con la direccion ip publica y el puerto.

Figura 90.

Resultados del proyecto.

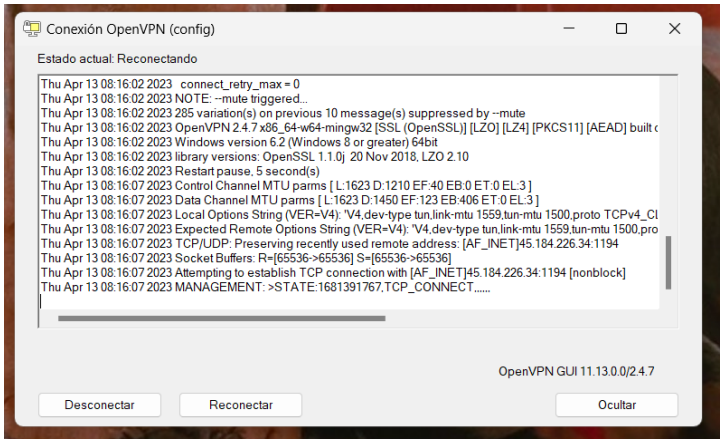


Nota: Se muestra la config. de ingreso al servidor vpn.

- Una vez establecida la conexión con el servidor mediante OpenVPN.

Figura 91.

Resultados del proyecto.



Nota: Se muestra la conexión con el servidor VPN exitoso.

Figura 92.

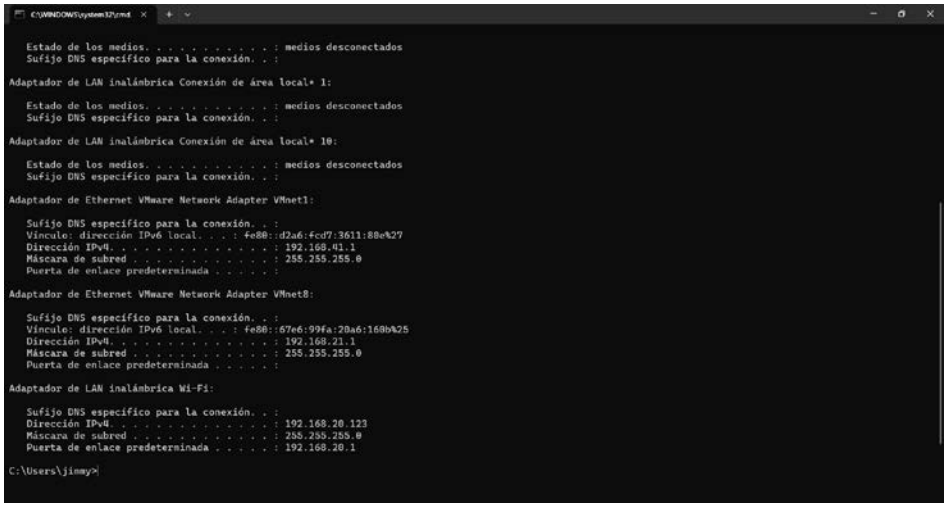
Resultados del proyecto.

Nota: Se muestra la conexión con el servidor VPN exitoso.

- Verificar el acceso a la VPN.

Figura 93.

Resultados del proyecto.

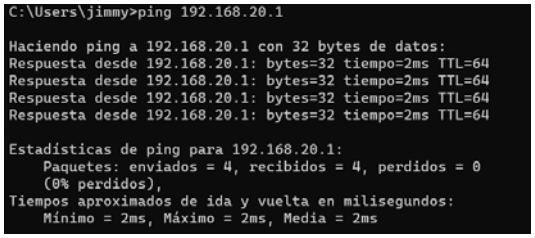


Nota: Se evidencia la conexión con el servidor VPN.

- Ping de conexión exitosa con el servidor.

Figura 94.

Resultados del proyecto.

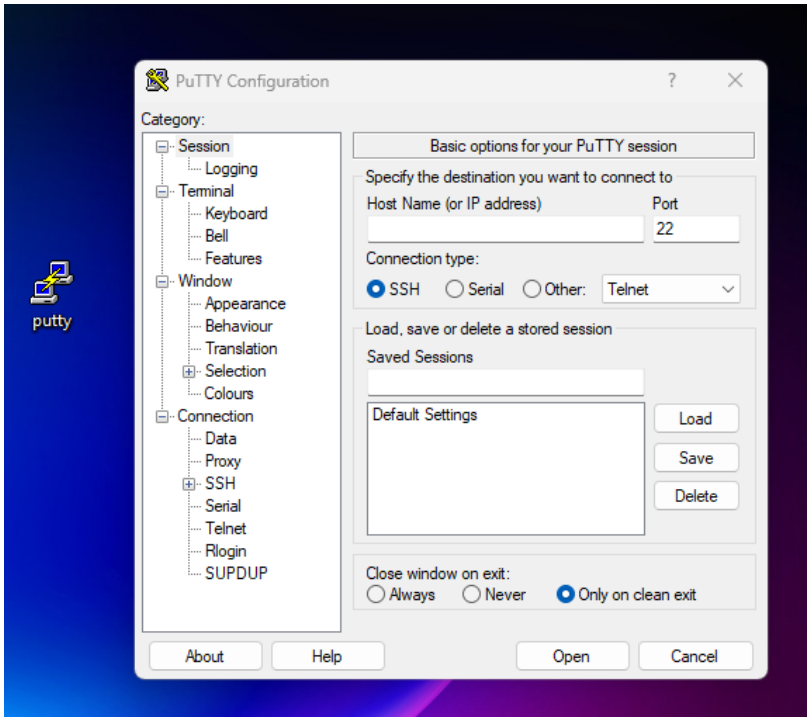


Nota: Se realiza un ping para verificar la conectividad.

- Usar el programa PuTTY para acceder a los equipos del laboratorio de cisco con el código del rack (LAB cisco-KIT-1).

Figura 95.

Resultados del proyecto.

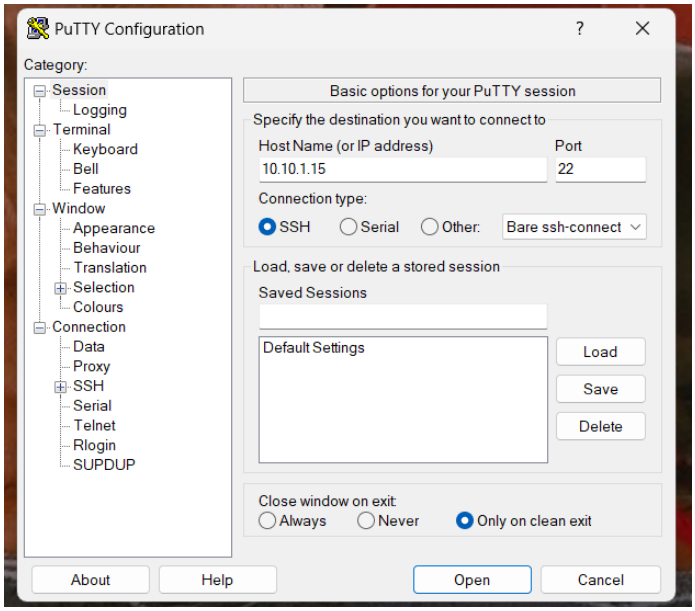


Nota: Se muestra la página principal de PuTTy donde se ingresa a los equipos por medio del protocolo SSh.

- Ingreso al Router del laboratorio por medio del protocolo SSh, mediante una dirección IP, puerto 22, conexión “Bare ssh-connect”

Figura 96.

Resultados del proyecto-Router.

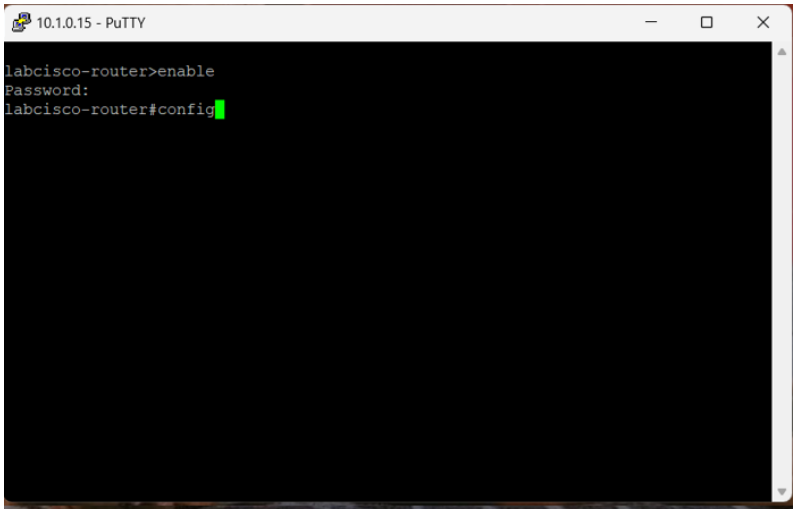


Nota: Ingreso al equipo de cisco por medio del protocolo SSh.

- Ingreso exitoso al equipo (Router) ubicado en el laboratorio de cisco.

Figura 97.

Resultados del proyecto-Router.

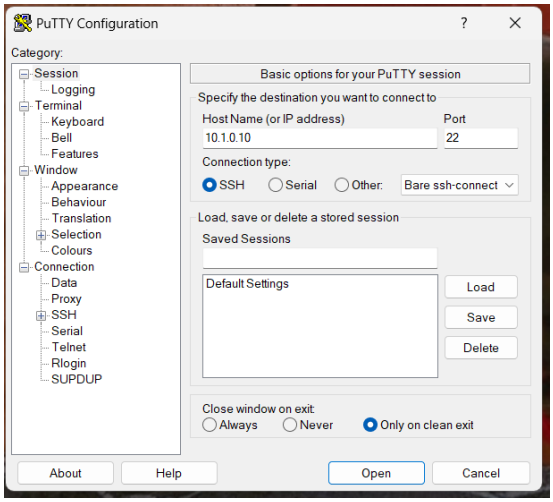


Nota: En anexos se muestra más evidencia del ingreso a los equipos cisco.

- Ingreso al Switch del laboratorio por medio del protocolo SSh, mediante una dirección IP, puerto 22, conexión “Bare ssh-connect”

Figura 98.

Resultados del proyecto-Switch.

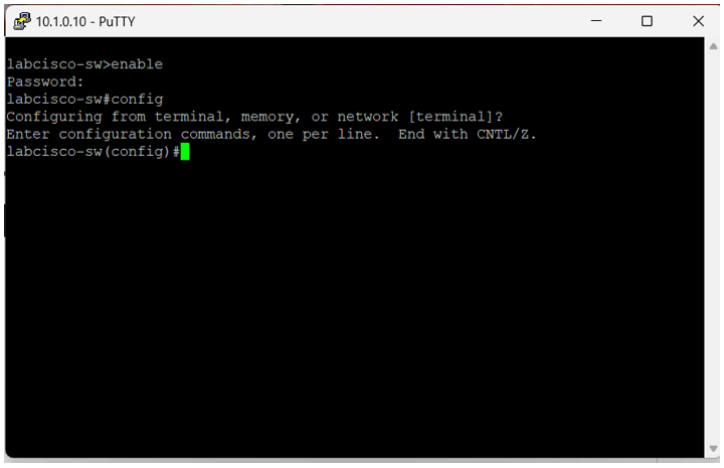


Nota: Ingreso al equipo de cisco por medio del protocolo SSh.

- Ingreso exitoso al equipo (Switch) ubicado en el laboratorio de cisco.

Figura 99.

Resultados del proyecto-Switch.



Nota: En anexos se muestra más evidencia del ingreso a los equipos cisco.

Se adjunta video como muestra de un resultado positivo mediante el siguiente enlace:

https://youtu.be/LFc28-a_28M

CONCLUSIONES

- Luego de completar el proyecto actual, se ha llegado a la conclusión de que el ámbito de estudio de la tecnología de redes VPN es amplio. Estas redes son seguras y confiables, dado que empresas e instituciones de renombre las utilizan para la transferencia de datos e ingreso a las mismas de manera remota, logrando cumplir la necesidad del uso de los equipos Cisco por parte de los estudiantes de modalidad en línea.
- Se logró crear el servidor VPN y la conexión a equipos Cisco del laboratorio de Redes y Telecomunicaciones.
- Se evidencia el resultado esperado desde el día uno que se puso en desarrollo el proyecto, este está demostrado a través de un video e imágenes.

RECOMENDACIONES

- Seguir los pasos establecidos previamente en este documento para así garantizar un buen uso y conexión con los equipos.
- Usar de manera adecuada los equipos de Cisco ya que un fallo dentro de estos podría hacer perder la conexión con los mismos.
- Mantener los equipos conectados para al momento de querer usarlos.

REFERENCIAS BIBLIOGRÁFICAS

Ánonimo.(2021).*ComparaSofware*. Obtenido de https://www.comparasoftware.com/nuestra-empresa

Brown, S. (2001). *Implementacion de Redes Privadas Virtuales.* McGraw-Hill interamericana.

Castillo, J. (5 de abril de 2020). *Qué es OpenVPN y qué características nos da en las Redes Privadas Virtuales.* Obtenido de https://www.profesionalreview.com/2020/04/05/openvpn-que-es/

Fonseca, Castañeda, & Arevalo. (2018). DISEÑO DE UNA RED PRIVADA VIRTUAL (VPN) CON SEGURIDAD L2PT PARA LA EMPRESA LABORATORIOS EXPOFARMA S.A. Bogotá, Colombia. Obtenido de https://repository.ucc.edu.co/handle/20.500.12494/6193

Gillis , A. (Agosto de 2021). *TechTarget*. Obtenido de https://www.computerweekly.com/es/definicion/Red-privada-virtual-o-VPN

Gonzalez , A. (2006). Redes Privadas Virtuales. Hidalgo.

Humans. (2013). *Net.* . Obtenido de Humans: https://www.nethumans.com/solutions/itSecurity/VPN.aspx

INCIBE. (23 de 03 de 2015). *INCIBE*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/acceso-remoto-oficina-posible-vpn

IONOS, D. G. (08 de 07 de 2020). *Digital Guide IONOS*. Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/puertos-tcp-puertos-udp/

Menéndez, R. (Agosto de 2012). *Estudio del desempeño e implementación de una solución MPLS-VPN sobre múliples sistemas aútonomos.* Lima, Perú. Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1500/MENENDEZ_AVILA_RICARDO_SOLUCION_MPLS_VPN.pdf?sequence=1

MIkrotik. (2016). Mikrotik Routerboards Modelos. *Mikrotik Routerboards Modelos*. Obtenido de https://mikrotik.com/

Muñoz, S. F. (Febrero de 2007). Diseño de un canal Privado de comunicaciones entre dos puntos utilizando la infraestructura de Internet y Análisis del Canal VPN de la Universidad Politécnica Salesiana. Cuenca, Azuay, Ecuador. Obtenido de http://www.dspace.ups.edu.ec/bitstream/123456789/754/12/Tesis.pdf

Ñacato, M. (enero de 2007). DISEÑO E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL. *DISEÑO E IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL*. quito, pichincha.

Oliverio, G. (2006). *Universidad y Tecnologica de Colombia*. Obtenido de https://repositorio.uptc.edu.co/bitstream/001/1297/1/RED-70.pdf

Quishpe. (03 de 2021). *TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE MASTER EN TECNOLOGIAS DE LA INFORMACION MENCION REDES DE COMUNICACIONES.* Obtenido de TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE MASTER EN TECNOLOGIAS DE LA INFORMACION MENCION REDES DE COMUNICACIONES: http://repositorio.puce.edu.ec/bitstream/handle/22000/18899/MTI%20TESIS_

Quishpe%20Iza%20Luis%20Marcelo_2021-03-29.pdf?sequence=1&isAllowed=y

Reyes, E. (ambato de Enero de 2015). RED PRIVADA VIRTUAL (VPN) PARA UN SISTEMA DE TELEMEDICINA. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/8597/1/Tesis_t955ec.pdf

Trujillo. (Marzo de 2006). DIseño e implementacion de una VPN en una empresa comercializadora utilizado IPSEC. Quito, Pichincha, Ecuador. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/214/1/CD-0210.pdf

Trujillo, E. M. (Marzo de 2006). DISEÑO E IMPLEMENTACION DE UNA VPN EN UNA EMPRESA COMERCIALIZADORA UTILIZANDO IPSEC. Quito, Pichincha, Ecuador. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/214/1/CD-0210.pdf

WALTON, A. (111 de 6 de 2002). *CCNADESDECERO*. Obtenido de CCNADESDECERO: https://ccnadesdecero.es/numeros-de-puerto-tcp-udp/

Zapata. (Marzo de 2016). *EVALUACIÓN DE PARÁMETROS DE CALIDAD DE SERVICIO*. Obtenido de http://repositorio.puce.edu.ec/handle/22000/12327

ANEXOS

Tabla 9.
Fundamentación del problema.

CAUSAS →	**DEFINICION DEL PROBLEMA**	**CONSECUENCIAS** ←
• no dar el uso adecuado al laboratorio. • poco tiempo para realizar prácticas en clase. • no tener los equipos en casa para poder practicar en ellos.	La falta de acceso a los equipos (LAN) del laboratorio de redes y telecomunicaciones del campus Ramírez Dávalos por parte de los estudiantes de virtual.	• Poco manejo en el ámbito laboral. • Dificultar para reconocer los usos de cada equipo. • Poco conocimiento.

INDICADORES ↑
- Durante el confinamiento el 90% de estudiantes de carreras técnicas, no realizaron practicas presenciales. - En la actualidad muchos de los estudiantes han optado por mantenerse en la virtualidad.

ANEXO 2: Encuesta

En la presente encuesta se necesita saber su opinión sobre la Implementación de un servicio de VPN para acceso remoto a equipos LAN en el Campus Ramírez Dávalos del ITI.

Instrucciones:

- Marque con una "X" en el cuadrado la respuesta que más de adapte a su criterio.

1. **¿Conoce acerca sobre los accesos remotos?**

   SI ☐ NO ☐

2. **¿Sabe Ud. que son y cómo se utilizan las redes VPN?**

   SI ☐ NO ☐

3. **¿Alguna vez Ud. ha creado un servidor VPN?**

   SI ☐ NO ☐

4. **¿Le gustaría saber cómo se usa una red VPN?**

   SI ☐ NO ☐

5. **¿A utilizado algún programa para generar una red VPN?**

   SI ☐ NO ☐

6. **¿Conoce el programa OPENVPN?**

   SI ☐ NO ☐

7. **¿Considera importante el poder acceder de forma remota a los equipos Cisco del laboratorio de la Carrera Redes y Telecomunicaciones para desarrollar prácticas reales?**

   SI ☐ NO ☐

ANEXO 3: Puertos de Red más comunes

Puerto	TCP	UDP	Nombre	Descripción
1	✓	✓	tcpmux	Multiplexor TCP
5	✓	✓	rje	Entrada de tarea remota (remote job entry)
7	✓	✓	echo	Protocolo Echo
9	✓	✓	discard	Protocolo Discard (evaluación de conexiones)
11	✓	✓	systat	Información del sistema (enumera los puertos conectados)
13	✓	✓	daytime	Protocolo Daytime: indica fecha y hora
17	✓	✓	qotd	Envía la cita del día (quote of the day)
18	✓	✓	msp	Protocolo de envío de mensajes
19	✓	✓	chargen	Protocolo Chargen: envía una cadena infinita de caracteres
20	✓		ftp-data	Transmisión de datos FTP
21	✓	✓	ftp	Conexión FTP
22	✓	✓	ssh	Servicio Secure Shell
23	✓		telnet	Servicio Telnet
25	✓		smtp	Simple Mail Transfer Protocol
37	✓	✓	time	Protocolo de tiempo legible de forma mecanizada
39	✓	✓	rlp	Protocolo de envío de recursos (Resource Location Protocol)
42	✓	✓	nameserver	Servicio de nombres
43	✓		nicname	Servicio de directorio WHOIS

49	✓	✓	tacacs	Terminal Access Controller Access Control System
50	✓	✓	re-mail-ck	Protocolo de verificación de correo remoto (Remote Mail Checking)
53	✓	✓	domain	Resolución de nombres por DNS
67		✓	bootps	Protocolo Bootstrap (servidor)
68		✓	bootpc	Protocolo Bootstrap (cliente)
69		✓	tftp	Protocolo Trivial de Transferencia de Ficheros (Trivial File Transfer Protocol)
70	✓		gopher	Búsqueda de documentos
71	✓		genius	Protocolo Genius
79	✓		finger	Proporciona información de contacto de usuarios
80	✓		http	Protocolo de Transferencia de HiperTexto (Hypertext Transfer Protocol)
81	✓			Torpark: Onion-Routing (no oficial)
82		✓		Torpark: Control (no oficial)
88	✓	✓	kerberos	Sistema de autenticación de red
101	✓		hostname	Servicios de nombres de host (NIC Host Name)
102	✓		Iso-tsap	Protocolo ISO-TSAP
105	✓	✓	csnet-ns	Servidor de correo
107	✓		rtelnet	Telnet remoto
109	✓		pop2	Post Office Protocol v2 para comunicación de correo electrónico
110	✓		pop3	Post Office Protocol v3 para comunicación de correo electrónico

111	✓	✓	sunrpc	Protocolo RPC para NFS
113		✓	auth	(Antiguo) servicio de autenticación
115	✓		sftp	Protocolo de transferencia de archivos seguros o Simple File Transfer Protocol (versión simplificada de FTP)
117	✓		uucp-path	Transmisión de datos entre sistemas Unix
119	✓		nntp	Transmisión se noticias en Newsgroups
123		✓	ntp	Protocolo de sincronización de tiempo
137	✓	✓	netbios-ns	NETBIOS Servicio de nombres
138	✓	✓	netbios-dgm	NETBIOS Servicio de envío de datagramas
139	✓	✓	netbios-ssn	NETBIOS Servicio de sesiones
143	✓	✓	imap	Internet Message Access Protocol para comunicación de correo electrónico
161		✓	snmp	Simple Network Management Protocol
162	✓	✓	snmptrap	Simple Network Management Protocol Trap
177	✓	✓	xdmcp	X Display Manager
179	✓		bgp	Border Gateway Protocol
194	✓	✓	irc	Internet Relay Chat
199	✓	✓	smux	SNMP UNIX Multiplexer
201	✓	✓	at-rtmp	Enrutamiento AppleTalk
209	✓	✓	qmtp	Quick Mail Transfer Protocol
210	✓	✓	z39.50	Sistema de información bibliográfico
213	✓	✓	ipx	Internetwork Packet Exchange
220	✓	✓	imap3	IMAP v3 para comunicación de correo electrónico

369	✓	✓	rpc2portmap	Coda Filesystem Portmapper
370	✓	✓	codaauth2	Servicio Coda Filesystem Authentication
389	✓	✓	ldap	Lightweight Directory Access Protocol
427	✓	✓	svrloc	Service Location Protocol
443	✓		https	HTTPS (HTTP a través de SSL/TLS)
444	✓	✓	snpp	Simple Network Paging Protocol
445	✓		microsoft-ds	SMB a través de TCP/IP
464	✓	✓	kpasswd	Modificación de contraseña para Kerberos
500		✓	isakmp	Protocolo de seguridad
512	✓		exec	Remote Process Execution
512		✓	comsat/biff	Mail Client y Mail Server
513	✓		login	Inicio de sesión en ordenador remoto
513		✓	who	Whod User Logging Daemon
514	✓		shell	Remote Shell
514		✓	syslog	Servicio Unix System Logging
515	✓		printer	Servicios de impresión Line Printer Daemon
517		✓	talk	Talk Remote Calling
518		✓	ntalk	Network Talk
520	✓		efs	Extended Filename Server
520		✓	router	Routing Information Protocol
521		✓	ripng	Routing Information Protocol para IPv6
525		✓	timed	Servidor de tiempo
530	✓	✓	courier	Courier Remote Procedure Call
531	✓	✓	conference	Chat a través de AIM y IRC
532	✓		netnews	Servicio Netnews Newsgroup

533		✓	netwall	Broadcast de emergencia
540	✓		uucp	Unix-to-Unix Copy Protocol
543	✓		klogin	Kerberos v5 Remote Login
544	✓		kshell	Kerberos v5 Remote Shell
546	✓	✓	dhcpv6-client	DHCP v6 Client
547	✓	✓	dhcpv6-server	DHCP v6 Server
548	✓		afpovertcp	Apple Filing Protocol a través de TCP
554	✓	✓	rtsp	Control de streams
556	✓		remotefs	Remote Filesystem
563	✓	✓	nntps	NNTP a través de SSL/TLS
587	✓		submission	Message Submission Agent
631	✓	✓	ipp	Internet Printing Protocol
631	✓	✓		Common Unix Printing System (no oficial)
636	✓	✓	ldaps	LDAP a través de SSL/TLS
674	✓		acap	Application Configuration Access Protocol
694	✓	✓	ha-cluster	Servicio Heartbeat
749	✓	✓	kerberos-adm	Kerberos v5 Administration
750		✓	kerberos-iv	Servicios Kerberos v4
873	✓		rsync	Servicios de transmisión de datos rsync
992	✓	✓	telnets	Telnet a través de SSL/TLS
993	✓		imaps	IMAP a través de SSL/TLS
995	✓		pop3s	POP3 a través de SSL/TLS

ANEXO 4. Tabla de puertos de red registrados.

Puerto	TCP	UDP	Nombre	Descripción
1080	✓		socks	SOCKS Proxy
1433	✓		ms-sql-s	Microsoft SQL Server
1434	✓	✓	ms-sql-m	Microsoft SQL Monitor
1494	✓		ica	Citrix ICA Client
1512	✓	✓	wins	Windows Internet Name Service
1524	✓	✓	ingreslock	Ingres DBMS
1701		✓	l2tp	Layer 2 Tunneling Protocol/Layer 2 Forwarding
1719		✓	h323gatestat	H.323
1720	✓		h323hostcall	H.323
1812	✓	✓	radius	Autenticación RADIUS
1813	✓	✓	radius-acct	Acceso RADIUS
1985		✓	hsrp	Cisco HSRP
2008	✓			Teamspeak 3 Accounting (no oficial)
2010		✓		Teamspeak 3 Weblist (no oficial)
2049	✓	✓	nfs	Network File System
2102	✓	✓	zephyr-srv	Zephyr Server
2103	✓	✓	zephyr-clt	Zephyr Client
2104	✓	✓	zephyr-hm	Zephyr Host Manager
2401	✓		cvspserver	Concurrent Versions System
2809	✓	✓	corbaloc	Common Object Request Broker Architecture
3306	✓	✓	mysql	Servicio de bases de datos MySQL (también para MariaDB)

4321	✓		rwhois	Remote Whois Service
5999	✓		cvsup	CVSup
6000	✓		X11	Servicios X Windows System
11371	✓		pgpkeyserver	Keyserver público para PGP
13720	✓	✓	bprd	Symantec/Veritas NetBackup
13721	✓	✓	bpdbm	Symantec/Veritas Database Manager
13724	✓	✓	vnetd	Symantec/Veritas Network Utility
13782	✓	✓	bpcd	Symantec/Veritas NetBackup
13783	✓	✓	vopied	Symantec/Veritas VOPIE
22273	✓	✓	wnn6	Conversión Kana/Kanji
23399				Skype (no oficial)
25565	✓			Minecraft
26000	✓	✓	quake	Quake y otros juegos multijugador
27017				MongoDB
33434	✓	✓	traceroute	Seguimiento de red

ANEXO 5: Elaboración y testeo de cables de red.

ANEXO 6: Instalación en los equipos y configuración.


ATENCION

ANEXO 7: Resultados de funcionamiento.