UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

previo a la obtención del título de:

INGENIERO EN TELECOMUNICACIONES

"IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL CON PROTOCOLO WIREGUARD A TRAVÉS DE UNA INTERFAZ UNIFI."

AUTOR:

GONZALO JAVIER DEL PEZO ROCA

TUTOR:

ING. LUIS AMAYA FARIÑO, MGT

LA LIBERTAD – ECUADOR

2022-1

AGRADECIMIENTO

Para empezar, nada de lo que digo puede transmitir verdaderamente lo importante que son ustedes en mi vida. Así que quiero agradecerles a los dos por ser los padres más maravillosos de la historia. Gracias mamá y papá por todo.

A mi hermana, te agradezco por estar siempre ahí sin importar cuánto te moleste. Hay un rincón especial en mi corazón, que siempre te guardará gratitud. Gracias por cuidarme, hermana.

A mis amigos, honestamente estoy extremadamente feliz de decir que desde el primer año que nos unió a todos, mi experiencia universitaria sería menos memorable y mucho menos placentera sin ustedes. Gracias por las palabras de aliento y el apoyo mutuo durante nuestra trayectoria universitaria.

A los docentes de la Facultad de Sistemas y Telecomunicaciones, sobre todo a mi tutor de proyecto de titulación, su apoyo y orientación a lo largo del proceso de tesis fue extremadamente útil. Gracias.

A mi compañera ideal, mi novia, mis palabras nunca podrán expresar lo agradecido que estoy contigo, por todo el afecto, por la motivación, por el apoyo incondicional, por tu hermosa presencia a mi lado. Gracias.

Sin ustedes nada de esto hubiera sido posible.

Gonzalo Javier Del Pezo Roca

DEDICATORIA

Este trabajo de titulación está dedicado con mucho afecto y cariño a mis padres, Leonardo Del Pezo y Glenda Roca, sinónimos de amor, trabajo y sacrificio, gracias a ellos he logrado estar aquí y convertirme en lo que soy, por todo el apoyo brindado en cada momento a lo largo de esta etapa para llegar a ser un profesional. Por este motivo les dedico mi título profesional.

Gonzalo Javier Del Pezo Roca

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de titulación denominado: "**Implementación de una Red Privada Virtual con protocolo WireGuard a través de una interfaz UniFi**", elaborado por el estudiante **Gonzalo Javier Del Pezo Roca**, de la carrera de Telecomunicaciones de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.

La Libertad, 1 de septiembre del 2022

Ing. Luis Miguel Amaya Fariño, Mgt.

TRIBUNAL DE GRADO

Ing. Ronald Rovira Jurado, Ph. D.
DIRECTOR DE LA CARRERA DE TELECOMUNICACIONES

Ing. Vladimir García Santos, Mgt.
DOCENTE ESPECIALISTA

Ing. Luis Miguel Amaya Fariño, Mgt.
DOCENTE TUTOR UIC

Ing. Corina Gonzabay De La A, Mgt.
SECRETARIA

RESUMEN

A raíz de que surgió la crisis pandémica, llegó a afectar radicalmente la continuidad en la formación de los estudiantes en los diferentes niveles de educación; ante esto, las instituciones educativas aplicaron diferentes estrategias inmediatas como la educación a través de plataformas virtuales y la aplicación de muchos métodos innovadores para el proceso de enseñanza-aprendizaje. Sin embargo, a nivel nacional aún siguen existiendo inconsistencias de continuidad en la educación a nivel superior académico, donde las ciencias de ingenierías se ven afectadas por estos factores. Para la carrera de Ingeniería en Telecomunicaciones, mediante estos factores se presentan grandes vacíos o inconsistencias en la experimentación a través de las prácticas de laboratorio y que muchas veces sirve para comparar con la teoría y sumergirse en el área del campo laboral. El laboratorio de telecomunicaciones cuenta con equipos de redes de Telecomunicaciones, los cuales pueden ser utilizados de forma remota por los estudiantes; aunque, por temas de seguridad, la universidad la no puede otorgar la IP Pública al igual que los correspondientes permisos para el acceso a la intranet de la UPSE. Como solución se buscó un método seguro que redirija solo al acceso del laboratorio, implementado por nuevos equipos capaces de suplir esta demanda, teniendo grandes ventajas como el costo y una interfaz gráfica intuitiva. Con esto se fortalece la educación para los universitarios, teniendo la posibilidad de operar equipos de redes telecomunicaciones con la supervisión de un docente tutor, creciendo el interés del alumnado en adquirir los conocimientos necesarios para la carrera de Ingeniería en Telecomunicaciones.

ABSTRACT

As a result of the pandemic crisis, it came to radically affect the continuity in the training of students at the different levels of education; Given this, educational institutions applied different immediate strategies such as education through virtual platforms and the application of many innovative methods for the teaching-learning process. However, at the national level there are still inconsistencies of continuity in education at the academic higher level, where engineering sciences are affected by these factors. For the Telecommunications Engineering career, through these factors there are great gaps or inconsistencies in experimentation through laboratory practices and that often serves to compare with theory and immerse in the area of the labor field. The telecommunications laboratory has telecommunications network equipment, which can be used remotely by students; although, for security reasons, the university cannot grant the Public IP as well as the corresponding permissions for access to the UPSE intranet. As a solution, a safe method was sought that redirects only to the laboratory access, implemented by new equipment capable of meeting this demand, having great advantages such as cost and an intuitive graphic interface. With this, education for university students is strengthened, having the possibility of operating telecommunications network equipment with the supervision of a tutor teacher, increasing the interest of students in acquiring the necessary knowledge for the Telecommunications Engineering career.

DECLARACIÓN

El contenido del presente Trabajo de titulación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Gonzalo Javier Del Pezo Roca
CI. 092814692-7
AUTOR

INDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En la educación universitaria en el área de ingenierías, la teoría debe estar completamente entrelazada con la experimentación a través de la práctica, por lo que este factor representa ser indispensable en el proceso de enseñanza-aprendizaje y que se trabaje de forma dinámica en el laboratorio. Por lo tanto, es necesario que se aborde los componentes teóricos y prácticos para explicar su veracidad en la realidad y así plantear soluciones a los diversos problemas que pueden surgir en el campo laboral.

Debido a los problemas suscitados ante diversas adversidades de crisis nacional y mundial, se ha optado por la educación virtual; ante ello, para las carreras de ciencias de ingeniería representa una desventaja en conocimientos prácticos experimentales en los laboratorios. Ante estas razones, se crea un compromiso con esta propuesta de trabajo de titulación que consiste en diseñar e implementar un mecanismo de control de acceso remoto a los equipos de redes que se encuentran en el laboratorio de telecomunicaciones, atendiendo a las necesidades para complementar el proceso de enseñanza-aprendizaje de las materias afines a la carrera de Ingeniería en Telecomunicaciones. La respectiva propuesta se divide en tres capítulos donde se desglosan todos los procesos teóricos y prácticos para llevar a cabo esta implementación.

En el primer capítulo se detallan los antecedentes que a su misma vez sirve para describir el proyecto y justificando la solución; de la misma manera, se plantean los objetivos con sus respectivos resultados esperados ante la propuesta, haciendo el uso de metodologías como la investigación exploratoria y aplicada realizada en dos fases como la investigación e implementación.

En capitulo dos consta de tres partes como el marco contextual, en donde se analiza todo el contexto para el desarrollo de la propuesta; en el marco conceptual, se busca información a

través de fuentes bibliográficas enfocadas en las Redes Privadas Virtuales y sus componentes; y en el marco teórico, mediante la consulta de trabajos de grado e investigaciones, se realiza la relación a las variables relacionadas con la propuesta de trabajo.

En el tercer capítulo, se realiza la topología de diseño para dar paso a la implementación de la propuesta; se analiza la importancia del acceso remoto al laboratorio de telecomunicaciones y el tipo de tecnología a utilizar para la respectiva solución del mismo, se detalla el proceso de configuración y las correspondientes pruebas para su funcionamiento.

Por último, se presentan las conclusiones y recomendaciones surgidas al momento de la elaboración de esta propuesta de implementación con la interfaz UniFi y el aplicativo correspondiente para su operación.

Capítulo uno

Generalidades de la propuesta

1.1 Antecedentes

La Red Privada Virtual VPN data desde la decrepitud de la Internet desde el decenio de 1960 tanto como ARPANET, este último fue el primer método de redes desarrollada por la inteligencia militar de Estados Unidos. Desde el año 1982, cuando ARPANET puso en marcha el protocolo TCP/IP, el internet ha estado en constante evolución para garantizar la seguridad que anteriormente era muy vulnerable a través de diversos protocolos y que, en muchos casos, algunos no fueron seguros y tuvieron que ser reemplazados o mejorados.

En 1993, John Ioannidis en compañía de amigos de la Universidad de Columbia y AT&T Bell Labs crearon el Software IP Encryption Protocol, hoy en día conocido como Swipe, siendo esta la primera versión de VPN en la historia. Por su parte. Xu Wei acogió esta tecnología y la mejoró redoblando la seguridad a través del mejoramiento de los protocolos IP. A nivel global, muchas empresas usan VPN que dependen del tráfico de Internet Público, un transporte poco confiable que puede generar problemas ya que las conexiones se realizan desde diferentes partes del planeta, a su vez, esto se traduce en ralentizaciones y reducción de la calidad del servicio en general.

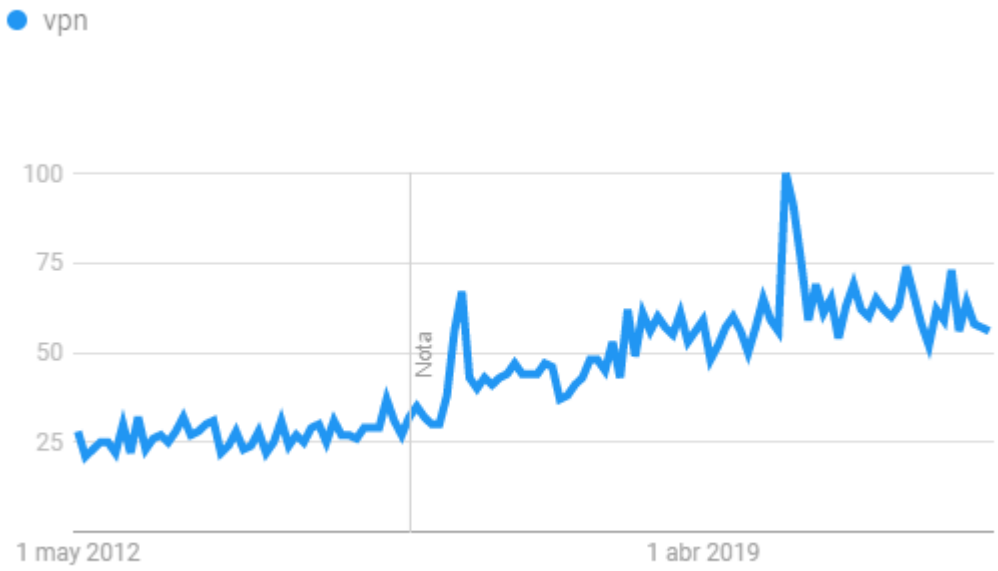
Hasta la fecha, hay casi 8 mil millones de personas en el mundo y más de 5 mil millones (65,6%) de ellos son usuarios de Internet. De estos, se estima que hay más de 1200 millones (31 % de todos los usuarios de Internet) de personas que usan VPN. Sin embargo, estos números son aproximados porque solo representan países donde la penetración del mercado de VPN es superior al 10%. La penetración de mercado mide cuánto se utiliza un servicio en comparación con el

mercado total estimado. Por lo tanto, es probable que el número total de usuarios de VPN sea mayor (Jauniškis , 2022).

Debido a los problemas generados por la pandemia, muchas organizaciones en el Ecuador han pasado de un entorno de oficina tradicional a optar por un plan para proporcionar acceso remoto seguro a sus instalaciones, esto con el fin de que se disminuyan casos de contagios y posibles efectos adversos en las operaciones diarias. Los datos muestran que las búsquedas en línea relacionadas con VPN comenzaron a aumentar a mediados de marzo en los días posteriores a la declaración de pandemia mundial por parte de la Organización Mundial de la Salud. La siguiente tendencia destaca la popularidad del término de búsqueda “VPN”, que ha ido en constante aumento durante los últimos 10 años. Como puede verse, el interés en el término de búsqueda alcanzó su nivel más alto en marzo de 2020, justo cuando comenzaron a entrar en vigor las disposiciones generales del gobierno ecuatoriano.

Figura 1

Búsquedas realizadas en internet con VPN



Nota. Tomado de la web (Google Trends, s.f.).

Este crecimiento en el uso de VPN se puede atribuir a un aumento en las personas que buscan información en línea mientras están en casa debido al estado de excepción. Se cerraron las escuelas, se prohibieron las reuniones públicas y los empleados trabajaban de forma remota. Esto dio como resultado que las personas pasaran mucho más tiempo en línea y muchos utilizaban servicios VPN para acceder a plataformas y contenidos de transmisión bloqueados geográficamente.

Dicho esto, la mayoría de todos los usuarios de VPN optan por servicios de VPN gratuitos. Y las VPN gratuitas no ofrecen seguridad en línea; en general, son muy inseguras y venden los datos de sus usuarios para mantener sus servicios. Esta información es muy poco conocida por los usuarios y para los expertos no es nada nuevo, lo que quiere decir es que la intención del usuario no es buscar seguridad en una red a través de una VPN gratuita, sino acceder a contenido geo restringido.

En el país se tiene registro de la implementación de una Red Privada Virtual para empresas comerciales, como es el caso de la cadena comercial Súper Éxitos de Guayaquil y la empresa American Jeans de la ciudad de Ambato a través de Acceso Remoto; asimismo, se ha optado por esta tecnología para en el área de la salud, específicamente desde la Telemedicina se realizó un estudio para mejorar la atención pública en las Unidades de Salud de la Provincia de Tungurahua entre el Hospital Provincial General Docente Ambato y sus Centros de Salud.

Desde el área educativo, se destaca en el Instructivo para la Implementación de Educación Abierta el uso de protocolos de seguridad en clases virtuales como el uso de VPN si la red de internet es proporcionada por la propia entidad educativa (Ministerio de Educación, 2020). Basado en este contexto se tiene en la Educación Superior el uso de VPN para el acceso a los repositorios

de la biblioteca virtual de algunas universidades en el país; de igual forma, el control de servicios de voz a través de la internet y video vigilancia en los Infocentros Comunitarios.

Las universidades y los colegios están experimentando un cambio importante hacia el aprendizaje a distancia en el aula. Con la pandemia de coronavirus, obligó a los estudiantes a alejarse de la cercanía social, las computadoras personales se convirtieron en el aula de los estudiantes. Ante esto, muchas universidades en el Ecuador cancelaron sus clases personales y trasladaron las aulas a la modalidad en línea; aunque el aprendizaje en línea ha existido desde que el uso de las computadoras evolucionó para incluir multimedia. A medida que crece el número de estudiantes que se conectan a la web, hay personas que se dedican a integrarse a estas redes públicas, por ende; la mayoría de los estudiantes son particularmente vulnerables mientras están en casa y tienden a navegar libremente por las redes sociales, dejando muchas huellas de perfil o datos que pueden provocar al robo de identidad, entre otras cosas.

En la provincia de Santa Elena, las búsquedas realizadas a través de internet sobre la implementación de VPN para el acceso remoto a las unidades educativas con fines educativos, reflejan muy poca información sobre el uso de esta implementación; por otra parte, no se tiene algún registro de proyectos de titulación en el repositorio de la Universidad Estatal de Santa Elena. Por ello, surge la necesidad de esta propuesta de titulación, para acceder a los servicios institucionales internos desde cualquier lugar remoto dirigido para docentes y estudiantes de la universidad.

1.2 Descripción del proyecto

FACSISTEL cuenta con un laboratorio para la carrera de telecomunicaciones, donde se realizan diferentes prácticas educativas tanto en el área de redes, comunicaciones ópticas y comunicaciones inalámbricas, en beneficio para el desarrollo profesional estudiantil. Sin embargo,

con los problemas generados por la pandemia del coronavirus, el acceso al laboratorio fue restringido para salvaguardar la salud de la familia educativa; en tal sentido, se generaron vacíos en el tema de prácticas de laboratorio para las materias afines de la carrera de ingeniería en Telecomunicaciones.

Actualmente, los estudiantes acceden a las clases en línea a través de computadoras portátiles, tablets y teléfonos inteligentes, los cuales son conectados de forma cableada a través de Ethernet para acceder al internet en el caso de una computadora, o de manera inalámbrica a través de WiFi o 4G LTE. El internet abre muchas puertas a la educación como el acceso a bibliotecas en línea y un sinfín de contenido multimedia, comunicación por video y acceso a los servicios del establecimiento educativo. Aunque, conectarse de forma inalámbrica resulta ser peligroso al estar conectado en una red pública, por lo tanto, no se puede estar seguro a través de un enrutador WiFi, y tiene sentido usar una VPN para mantener la conexión segura.

Las redes privadas virtuales son comúnmente utilizadas por organizaciones medianas y grandes para conectar sitios remotos mediante una red pública como Internet. En muchos casos, dentro de la Universidad Estatal Península de Santa Elena a los encargados del área de redes, se les otorga acceso VPN para entrar a la intranet de la universidad en situaciones en las que necesitan trabajar de forma remota, cuando viajan a una ciudad diferente o problemas de salud y no puedan dirigirse al establecimiento, etc., el uso de la VPN sirve como una gran herramienta para solucionar inconvenientes que surgen cada día en la intranet de la institución.

Si bien es cierto, la universidad cuenta con un gran número de reglas de firewall en sus servidores, esto con el fin de salvaguardar la seguridad de los datos almacenados en la institución. Por lo tanto, es de mucha responsabilidad entregar al estudiante direcciones IP Públicas y darle

acceso a la intranet mediante una VPN. Cabe aclarar que, el personal que tiene acceso remoto a través de una VPN debe estar autorizado por el departamento de TIC de la UPSE.

Al respecto, solo tienen acceso aquellas personas autorizadas para gestionar los equipos fuera de la institución. Por cuestiones de seguridad no se entrega acceso a los estudiantes por diferentes inconvenientes que se suscitan a diario en la intranet. Por ello, se busca una alternativa segura que permita el acceso al laboratorio de Telecomunicaciones, sin la necesidad de acceder a los equipos que gestionan la red universitaria. Esto puede ser factible utilizando VPN de nuevas generaciones donde no se necesite el acceso mediante una IP Pública y que se redireccione por equipos empresariales que manejen un entorno diferente creado por expertos desarrolladores en códigos abiertos gestionados desde la nube de internet.

En este contexto, a través de esta propuesta tecnológica, se pretende implementar una Red Privada Virtual que permita el acceso de estudiantes a quien el docente autorice, y que se realice el respectivo seguimiento mientras se ejecutan las labores de prácticas educativas en el laboratorio de Telecomunicaciones de forma remota. Esto quiere decir, que un dispositivo móvil electrónico situada en algún lugar de la provincia o del país, puede acceder a los recursos de redes como router y switch de forma remota del laboratorio de Telecomunicaciones.

Para llevar a cabo este trabajo, se pretende armar una estación de trabajo compuesto por enrutadores y controladores que permitan realizar cambios de configuración en sus interfaces, gestionar acciones para garantizar la calidad de servicio de estas redes e implementar diferentes mejoras como proceso de evaluación del desempeño de la red VPN. Para dar garantía a la seguridad se hace el uso del protocolo WireGuard en la red VPN a través de una interfaz UniFi de la marca Ubiquiti, lo cual nos permite vincular dos o más ubicaciones remotas a través de un medio que no es de confianza como Internet. Estos controladores son de nivel empresarial que ofrecen

una experiencia de red escalable y una plataforma integral para el uso de múltiples aplicaciones para la gestión centralizada de usuarios, donde los administradores puedan asignar y crear las credenciales necesarias para entrar a la red VPN para el acceso remoto al laboratorio de Telecomunicaciones.

1.3 Objetivos

1.3.1 Objetivo General

Implementar una Red Privada Virtual con protocolo WireGuard a través de una interfaz UniFi.

1.3.2 Objetivos Específicos

- Identificar la importancia del acceso remoto a los equipos de redes del laboratorio de Telecomunicaciones.
- Diseñar la topología para la Red privada Virtual de acceso remoto a implementar en el laboratorio de Telecomunicaciones utilizando equipos de la línea UniFi de Ubiquiti.
- Evaluar el desempeño de la red VPN en los dispositivos móviles y el acceso hacia los diferentes equipos que componen la estación de trabajo.

1.4 Resultados Esperados

- Instalación de los equipos con la respectiva configuración de seguridad de red aplicando VPN.
- Proporcionar las credenciales necesarias al personal administrativo para el uso de la red VPN.
- Los estudiantes utilizan una red VPN universitaria y realizan diversas prácticas en busca de mejorar el desempeño de seguridad de la red.

Se incentiva el uso de VPN para diferentes enfoques de la sociedad en la Provincia de Santa Elena para proyectos futuros de grado y postgrado.

1.5 Justificación

Hoy en día, se puede evidenciar que existe un problema con frecuencia en la enseñanza académica en lo que corresponde a experiencia como enriquecedora de conocimientos, ante esto, no hay una preocupación sobre las diversas metodologías pedagógicas en la educación superior.

A través de esta implementación, será posible lograr los objetivos de aprendizajes en donde se requiera el uso de equipos de redes de Telecomunicaciones, que serán supervisadas por los docentes de ingeniería y así poder lidiar con los vacíos que se pueden presentar al no poder asistir al laboratorio, ante una adversidad de índole problemático a nivel nacional o mundial, que obliga a restructurar la enseñanza en la ingeniería.

Por otra parte, los beneficiarios del desarrollo de este proyecto son los estudiantes y docentes ingenieros de la carrera de Ingeniería en Telecomunicaciones, siendo una herramienta fundamental para la enseñanza de prácticas de laboratorio; permitiendo a los estudiantes acceder de forma remota a través de internet y que logra la participación en la mejora de sus competencias preparándose para ser más eficientes al ingresar al futuro mercado laboral. De igual forma, este trabajo de titulación, sirve como fuente de guía para futuros trabajos de grado y post grado, en donde se requiera un acceso remoto al laboratorio de Telecomunicaciones para gestionar equipos de redes de Telecomunicaciones mediante una VPN.

Al implementar la VPN en el laboratorio de Telecomunicaciones, entra en las estrategias para mejorar el proceso de enseñanza, siendo un punto de referencia y de conocimientos sobre la mejor manera de brindar a los estudiantes un acceso equitativo a oportunidades de participación virtual de calidad. Garantiza que los estudiantes tengan un acceso justo a los recursos del

laboratorio, necesarios que verán en el mercado laboral y que se necesita aprender para afrontar los obstáculos que se les presentan. En definitiva, se considera una medida educativa importante en el proceso de enseñanza de la universidad en la carrera de Ingeniería en Telecomunicaciones.

1.6 Metodología

El presente proyecto tiene como propósito implementar una red privada virtual de acceso remoto que usa protocolo WireGuard y para el laboratorio de Telecomunicaciones UPSE. Este trabajo de grado se desarrolla en dos diferentes tipos de investigación:

1.6.1 Investigación Exploratoria.

Una de las características de la investigación exploratoria es que resulta ser económica, interactiva, sin restricciones y de naturaleza abierta. Mediante este proyecto se pretende que posteriormente al momento de su implementación, los equipos que se utilizarán para su ejecución, queden en el laboratorio para que sean manipulados por los estudiantes de la carrera de ingeniería en Telecomunicaciones, este este sentido, se basa en la recolección de datos para explicar su funcionamiento para lograr que sea de forma didáctica.

1.6.2 Investigación Aplicada

La investigación aplicada es un tipo de diseño de investigación que busca resolver un problema específico o brindar soluciones innovadoras a problemas que afectan a un individuo, grupo o sociedad. A menudo se lo denomina método científico de investigación o investigación contractual porque implica la aplicación práctica de métodos científicos a problemas cotidianos. Por ello la información recopilada servirá para llevar a cabo el proceso del desarrollo del proyecto; aunque, también se basa en la implementación, por lo cual es necesario establecer dos fases definidas:

- **Fase 1: Investigación**

En esta fase se recopila toda la información de fuentes bibliográficas en la cual se aprenderán los requisitos necesarios para diseñar una red VPN por medio de la teoría, para llevarlo a cabo en los dispositivos de la marca Ubiquiti. De igual forma, se hace el análisis bibliográfico sobre la importancia de la educación remota mediante la VPN, teniendo en cuenta las tecnologías requeridas en la red a implementarse en el laboratorio de Telecomunicaciones.

- **Fase 2: Implementación**

Esta fase consiste en crear la estación de trabajo, en la que se describe y se identifica cada elemento o dispositivo a utilizar, se deberá cumplir con lo establecido para crear la red VPN de control de acceso remoto con protocolo WireGuard con su respectivo enlace compartido para los usuarios.

Capítulo dos

Propuesta Tecnológica

2.1 Marco Contextual

Este proyecto se basa en el armado de un rack con nuevos dispositivos diferentes a las marcas de los equipos existentes en el laboratorio, siendo estos accesibles para diseñar redes enfocándose a la parte administrativa y mejorando su utilidad en trabajos posteriores. La implementación de los protocolos de seguridad a utilizar estará configurada en los enrutadores o controladores para ser distribuidas a diferentes destinos mediante los switches y estos a dispositivos finales.

Para el armado de la estación de trabajo, se utiliza los cables respectivamente para la instalación de equipos, todo aquello basándose en la normativa internacional ANSI/TIA/EIA-568-A-B. Con ello también se garantiza un trabajo de forma organizada, eficiente, y sirve como parte de conocimiento en el ámbito laboral cuando se necesite realizar cambios dentro de la red de una empresa.

Para el acceso remoto a través de una VPN se utilizarán dispositivos móviles, pueden ser de diferentes compañías, pero con sistemas operativos Android y iOS, por lo que se debe instalar una aplicación propia de la línea UniFi para su ejecución y evaluación respectiva sobre el uso de la VPN y la gestión que se puede realizar en los módulos controladores, enrutadores y conmutadores.

La supervisión de acceso por medio de la VPN debe estar dirigida por el tutor que hará uso de esta herramienta; de igual forma, será el encargado de gestionar los perfiles necesarios para distribuirlos a cada estudiante o grupo de trabajo que sea designado.

2.2 Marco Conceptual

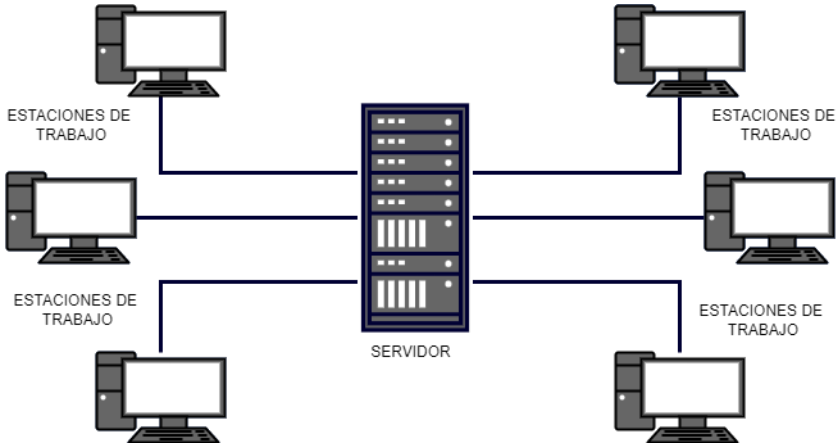
2.2.1 Redes LAN

Las redes en sus inicios se conformaban por una estación de trabajo. Las estaciones de trabajo normalmente tenían un usuario humano que interactúa con la red a través de ellas. Tradicionalmente estaba compuesto por una computadora de escritorio, teclado, pantalla y mouse, o una computadora portátil, con teclado, pantalla y panel táctil integrados. Con la llegada de la tablets y los dispositivos de pantalla táctil, nuestra definición de estación de trabajo está evolucionando rápidamente para incluir esos dispositivos, debido a su capacidad para interactuar con la red y utilizar servicios de red.

Para Ruiz y Reina (2002), definen a la Red de Área local como: "Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión; por ejemplo, una oficina o un centro educativo. Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información" (p. 6). En efecto, es una red que se limita a un área relativamente pequeña. Por lo general, a un área geográfica, como un laboratorio, una escuela o un edificio.

Figura 2

Red de Área Local



Nota. Elaborado por el autor

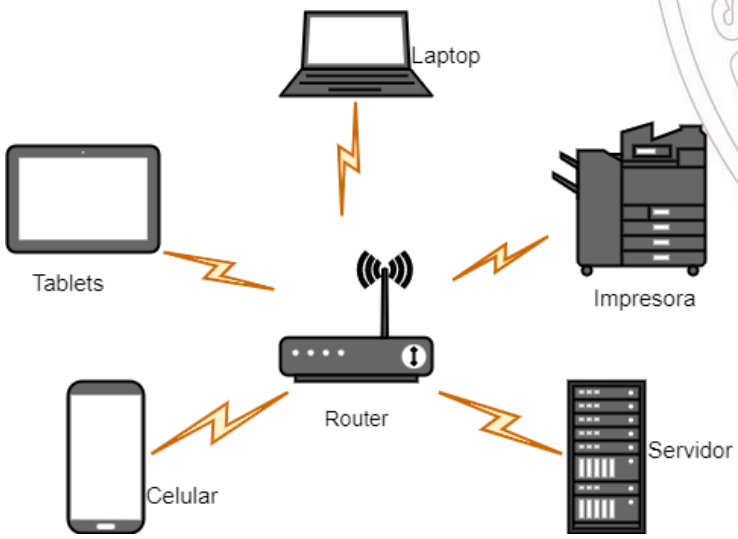
Las computadoras conectadas a una red se clasifican ampliamente como servidores o estaciones de trabajo. Los servidores generalmente no son utilizados directamente por humanos, sino que se ejecutan continuamente para proporcionar servicios a las otras computadoras en la red. Los servicios proporcionados pueden incluir impresión y envío de fax, alojamiento de software, almacenamiento y uso compartido de archivos, mensajería, almacenamiento y recuperación de datos, control de acceso completo de seguridad para los recursos de la red y muchos otros.

2.2.2 Redes WLAN

En algunos casos, las tecnologías inalámbricas se utilizan para ahorrar costos y evitar el tendido de cables, mientras que, en otros casos, es la única opción para brindar acceso público a Internet de alta velocidad. Sea cual sea el motivo, las soluciones inalámbricas están apareciendo por todas partes.

Figura 3

Red de Área Local Inalámbrica WLAN



Nota. Elaborado por el autor

La Red de Área Local Inalámbrica denominada por sus siglas WLAN, es solo un punto de acceso que permite que uno o más dispositivos accedan a Internet, pero los dispositivos no están conectados entre sí como en el caso de una Red de Área Local. Debe reconocerse que los

componentes de la WLAN se conocen como estaciones. En este sentido, es fundamental señalar que las estaciones se clasifican además en dos clases que son los clientes inalámbricos y los puntos de acceso.

> Están diseñadas para proporcionar acceso inalámbrico en zonas con un rango típico de hasta 100 metros, las WLAN se basan en el estándar 802.11 del IEEE. El IEEE 802.11 comprende toda una familia de diferentes estándares para redes inalámbricas de área local. El IEEE 802.11b fue el primer estándar aceptado, admitiendo hasta 11 Mbps en la banda frecuencial sin licencia de 2,4 GHz. Posteriormente, el estándar IEEE 802.11g fue diseñado como el sucesor del IEEE 802.11b con un mayor ancho de banda (Salazar, 2016, p. 13).

Al igual que 802.11b, los dispositivos 802.11g sufren interferencias de otros productos que operan en la banda de 2,4 GHz, por ejemplo, teclados inalámbricos. Un comité de la organización Instituto de Ingenieros Eléctricos y Electrónicos IEEE son los encargados de desarrollar los estándares para las comunicaciones inalámbricas, el nuevo comité comenzó a trabajar en 1990, las versiones nuevas y mejoradas del estándar aparecieron con bastante frecuencia en los años siguientes.

2.2.3 Red Privada Virtual

Los orígenes de las VPN se remontan a Microsoft en 1996, cuando los empleados crearon el protocolo de túnel punto a punto, también conocido como protocolo de túnel punto a punto o PPTN. Este protocolo era un método para crear una red segura entre usuarios mediante el cifrado de datos y la formación de un túnel a través de una conexión LAN o WAN. Este protocolo hizo que la transferencia de datos importantes fuera segura y protegida, incluso a través de redes públicas. Todo lo que se requiere para enviar datos a través de PPTN es un nombre de usuario, una

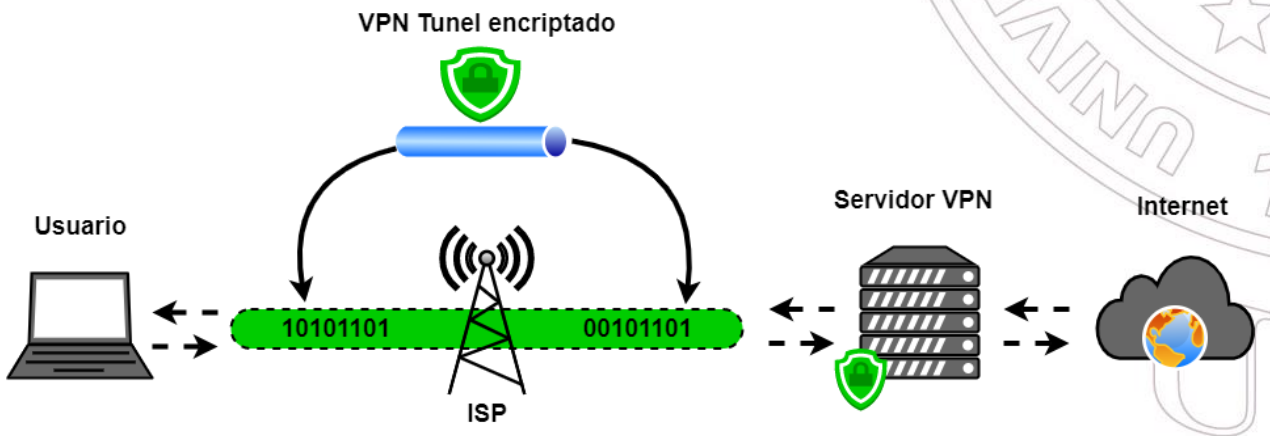
contraseña y una dirección de servidor. Debido a esto, sigue siendo una de las VPN más populares y fáciles de usar.

> Una VPN se trata de redes de comunicación entre dos puntos (cercanos o lejanos según podamos suponer), y que queremos que sean privados, o en la misma medida, que la información que se transmite sea privada entre emisor y receptor. El término virtual se aplica a la privacidad y no al término de red, porque en la mayoría de los casos lo que se quiere decir es transmisión por un canal público y abierto a través de una red privada y esta será virtual. (Hernández et al., 2006)

En términos simples, es un servicio que protege la privacidad y conexión a Internet, ayuda a evitar la censura y otras restricciones. Esto es posible mediante la creación de un túnel encriptado a través del cual envía los datos. En cierto sentido, una VPN actúa como intermediario entre el dispositivo y los servidores remotos, y transporta los datos a través de las redes existentes sin exponerlas a la Internet pública.

Figura 4

Internet VPN



Nota. Una VPN envía el tráfico de Internet a través de un túnel cifrado.

Cuando se haya establecido la conexión, ocurrirá lo siguiente con los datos:

- El software VPN en la computadora encripta el tráfico de datos y lo envía al servidor VPN a través de una conexión segura. Los datos también pasan por el Proveedor de Servicios de Internet ISP, pero con la diferencia que no permite el acceso al rastreo del cifrado.
- El servidor VPN descifra los datos cifrados de su computadora.
- El servidor VPN enviará sus datos a Internet y recibirá una respuesta que está destinada al usuario.
- Luego, el servidor VPN cifra nuevamente el tráfico y se lo devuelve.
- El software VPN en el dispositivo descifrará los datos para poder usarlos.

La VPN ofrece soluciones económicas al momento de diseñar e implementar una red a un sitio distante a través de internet, además de que permite la autenticación de usuarios o equipos mediante la encriptación, claves de acceso para identificación, integridad de los datos enviados desde el emisor hacia el receptor y confidencialidad; de esta manera, que el cifrado hace que los datos transmitidos no sean interceptados por nadie más a excepción del emisor y receptor. Sin embargo, Älvarez Delgado el al., (2014) para garantizar esta operación es necesario que cumpla los siguientes requisitos:

> Las redes privadas virtuales deben contar con ciertas bases antes de su implementación, tales son un set de políticas de seguridad para la codificación de datos, pues no deben ser visibles por clientes no autorizados en la red; administración de claves, para asegurar la codificación entre clientes y servidor; compartir datos, aplicaciones y recursos; un servidor de acceso y autenticación, para que en la red se tenga control de quiénes ingresan, verificar su identidad y tener registro estadístico sobre accesos; administración de direcciones, pues la VPN debe establecer una dirección para el cliente dentro de la red privada y debe

asegurar que estas direcciones privadas se mantengan así; y finalmente soporte para múltiples protocolos, pues debe manejar los protocolos comunes a la red Internet, como IP, por ejemplo (p. 3).

Sin una VPN, el ISP sabe todo lo que está haciendo en Internet. En países con estrictos controles de Internet, los datos del ISP a menudo están disponibles gratuitamente para las agencias gubernamentales. Ante esto, existe una serie de ventajas y desventajas que ofrece una VPN que se encuentran en la siguiente tabla.

Tabla 1

Principales ventajas y desventajas de una VPN

Ventajas	Desventajas
Precio de acceso económico	Dependencia doble de estabilidad de conexión
La tecnología VPN es una de las más seguras	Falta de conocimiento y negligencia por parte del usuario final
Disponibilidad de información	
Sencillez	Equipo cliente sin control de administrador

Nota. Elaborado por el autor

Dentro de esta tabla se destaca la estabilidad de conexión, es cierto que algunas VPN tienen este efecto; después de todo, una VPN redirige la conexión a través de un servidor remoto. Esto puede llevar más tiempo, por lo que podría ralentizar la conexión a Internet. Sin embargo, este no es siempre el caso. Hay muchas VPN que hacen todo lo posible para que la conexión a Internet sea lo más rápida posible y, a veces, incluso más rápido de lo que está acostumbrado. En este sentido, es importante contar con un servicio de VPN que tenga un porcentaje muy mínimo en establecer la conexión a internet.

2.2.4 Tipos de VPN de Acuerdo a su Aplicación o Arquitectura

Tanto el acceso remoto como las soluciones de VPN de sitio a sitio resuelven los mismos problemas utilizando métodos diferentes. El objetivo final sigue siendo el mismo, proteger los

recursos de las personas naturales, jurídicas, entidades educativas, gubernamentales, etc., del acceso no autorizado.

2.2.4.1 VPN de Acceso Remoto

Este tipo de VPN es actualmente el más utilizado por la gran mayoría de las empresas, y se dirige a los usuarios móviles, ya sean empleados o proveedores que acceden a la red de una organización desde una ubicación remota. Utiliza el acceso a Internet de alta velocidad como medio de comunicación y, una vez que los usuarios remotos se autentican, pueden trabajar como si estuvieran conectados localmente a la organización.

La VPN de acceso remoto es una conexión cifrada temporal entre el centro de datos de la empresa y el dispositivo del usuario. Se activa solo cuando el usuario lo habilita. De lo contrario, no tiene un enlace permanente. Las empresas utilizan principalmente este tipo para acceder de forma segura a las aplicaciones y los datos en un concentrador central a través de un túnel VPN. Puede considerarlo como una conexión VPN que crea una ruta segura desde su dispositivo para acceder a documentos confidenciales o materiales de la empresa en el otro extremo. El cliente de acceso remoto inicia una conexión VPN al servidor VPN corporativo a través de Internet. Una vez que se establece el enlace, los usuarios pueden acceder a los recursos de la intranet privada de la empresa.

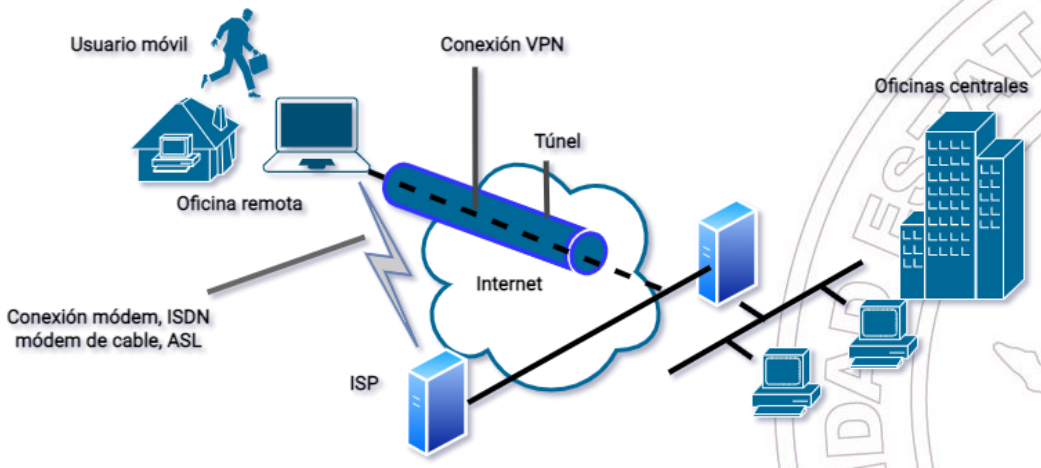
De acuerdo con la tecnología que se utilice, esta se divide en VPN dial-up y VPN directas.

VPN Dial-Up. La VPN de acceso telefónico permite a los usuarios conectarse a Internet mediante una conexión de acceso telefónico a través de líneas telefónicas convencionales o POTS (por sus siglas en inglés Plain Old Telephone Service) o conexiones mediante Red digital de Servicios Integrados ISDN. Los protocolos de red privada virtual se utilizan para proteger estas conexiones privadas.

VPN Directa. "Este tipo de VPN se utilizan las tecnologías de conexión a Internet de alta velocidad, como DSL y módem de cable las cuales ya ofreces muchos ISP, se ocupa principalmente entre los teletrabajadores, también se emplea para obtener conexiones desde el hogar" (Gómez, 2013, p. 10).

Figura 5

VPN de acceso remoto



Nota. Elaborado por el autor

Si bien las VPN de acceso remoto siguen siendo útiles, el almacenamiento en la nube es una alternativa popular si solo desea que las personas puedan acceder a los archivos de forma remota. El almacenamiento en la nube como, por ejemplo, las tecnologías que utiliza la marca Ubiquiti. utilizan una conexión de navegador encriptada para proteger sus datos y en su interfaz es mucho más fácil de configurar que una VPN.

2.2.4.2 VPN Sitio a Sitio

Para establecer una conexión con una organización, los usuarios remotos usan software instalado en sus terminales para crear un túnel virtual hacia la organización, ya sea un servidor, un enrutador o un firewall. La conexión está garantizada, pero no sin autenticación previa. La identidad del usuario que quiere conectarse a la red.

La configuración de VPN sitio a sitio se pueden configurar de dos tipos:

- Intranet
- Extranet

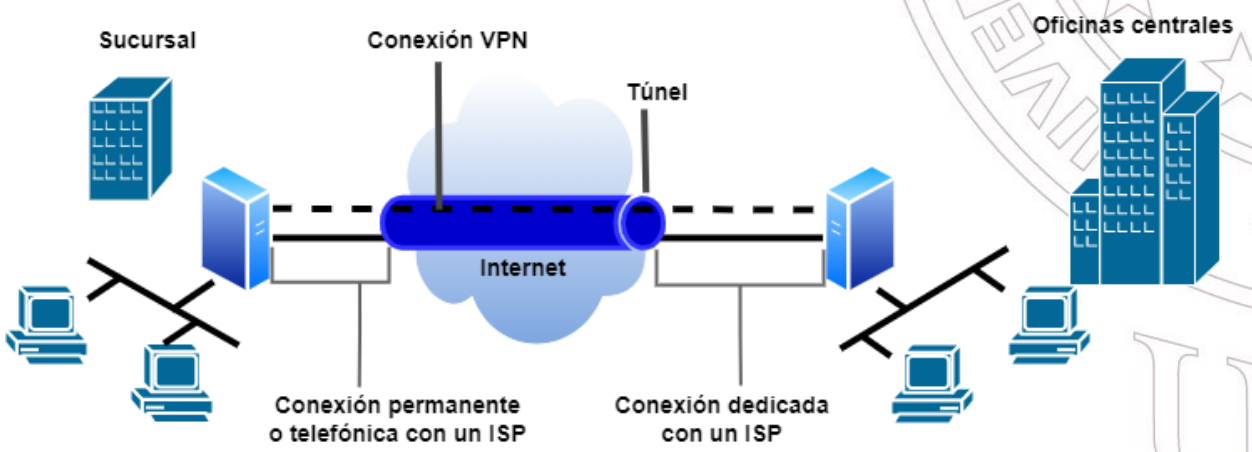
VPN Intranet. Conecta la sede corporativa, las oficinas remotas y las sucursales a través de una infraestructura compartida mediante conexiones dedicadas. Las empresas disfrutan de las mismas políticas que una red privada, incluida la seguridad, la calidad de servicio (QoS), la capacidad de administración y la confiabilidad.

Los beneficios de una VPN de intranet son los siguientes:

- Costos de ancho de banda WAN reducidos
- Conecta nuevos sitios fácilmente
- Aumento del tiempo de actividad de la red al habilitar la redundancia del enlace WAN entre los proveedores de servicios

Figura 6

Red VPN intranet



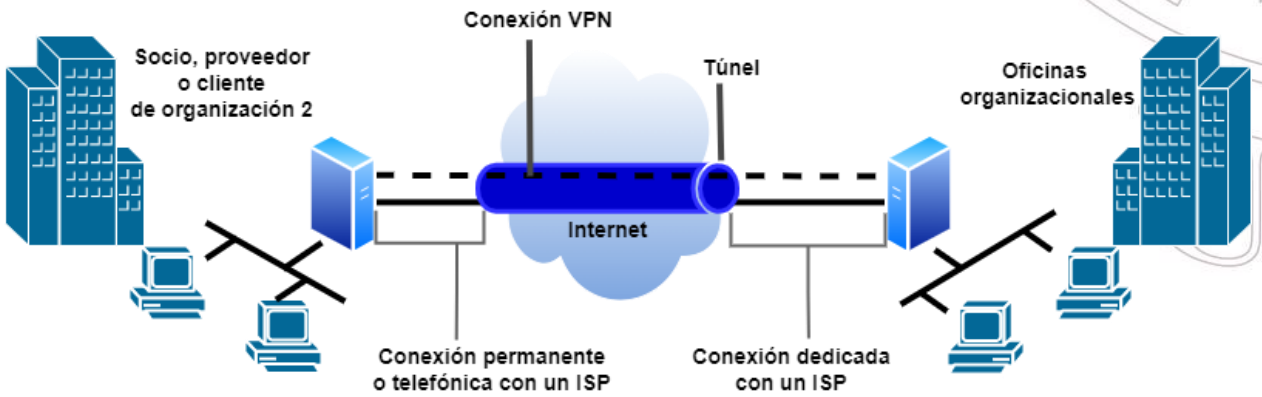
Nota. Un enrutador es el encargado de realizar una conexión VPN de dos puntos de una red privada.

Construir una VPN de intranet utilizando Internet es el medio más rentable de implementar la tecnología VPN. Sin embargo, los niveles de servicio generalmente no están garantizados en Internet. Al implementar una VPN de intranet, las corporaciones deben evaluar qué compensaciones están dispuestas a hacer entre los niveles de servicio garantizados, la ubicuidad de la red y el costo de transporte.

VPN Extranet. Surge cuando una organización tiene afiliados, proveedores o clientes que necesitan conectarse a su red para trabajar juntos, teniendo en cuenta restricciones de acceso a la red de la sede y niveles de seguridad discriminatorios. En este tipo de VPN se puede utilizar varios servidores, router o firewall, cuya función es crear una conexión VPN en la que ambos extremos de la comunicación deben utilizar los mismos algoritmos de cifrado y encapsulado. Una de las características más llamativas de este tipo de VPN es que los usuarios de ambos extremos no notan el proceso de encriptación o encapsulación, sino que ven la comunicación como si estuviera en la misma red local; por tanto, la seguridad en amenazas es muy mayor en comparación con la intranet; en este caso, debe ser diseñado cuidadosamente con pólizas de control de acceso y acuerdos de seguridad entre usuarios.

Figura 7

Red VPN extranet



Nota. Elaborado por el autor

Las VPN de acceso remoto se diferencian de las VPN de intranet y extranet principalmente por el método de conectividad a la red. Mientras que una VPN de acceso remoto se refiere a la conectividad de acceso telefónico (o de tiempo parcial), una VPN de intranet o extranet puede contener tanto enlaces de acceso telefónico como dedicados. La distinción entre las VPN de intranet y extranet radica esencialmente en los usuarios que se conectarán a la red y las restricciones de seguridad a las que cada uno estará sujeto.

2.2.5 Tipo de VPN de Acuerdo a su Implementación

Existen muchas maneras de implementar una VPN en una organización, donde cada fabricante brinda diversas soluciones de VPN. De aquí radica la importancia de decidir cual conviene utilizar, estos tipos de VPN se detallan en la siguiente tabla.

Tabla 2

Tipos de VPN según su implementación

Tipos de VPN	Descripción
Firewall	Establece normas de control de acceso entre dos o más redes, en función de lo que sean permiten o deniega su paso.
Router y de concentradores	Empresas como Cisco ofrecen servicios VPN integrados dentro de un router, por lo que se trata de la solución VPN más rápida.
Sistema operativo	Sistemas operativos como Windows o Linux ofrecen servicios de VPN ya integrados, estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización.
Aplicación	Es un programa que añade posibilidades VPN a un sistema operativo. Sin embargo, este programa no queda integrado con el sistema operativo.
Proveedor de servicios	El proveedor de servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a sus clientes.

Nota. Breve descripción de los tipos de VPN según la implementación. Fuente: Ramos Dillón, (2016, p. 51, 52, 53)

Tabla 3

Ventajas y desventajas de los tipos de VPN

Tipos de VPN	Ventajas	Desventajas
Firewall	Arquitectura de red simplificada, al establecer un único punto de control de seguridad.	La configuración del equipo firewall se convierte en más compleja.
Router y de concentradores	Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo.	Soporte de VPN por proveedores de enrutadores.
Sistema operativo	Es una solución muy económica. En un mismo sistema operativo se pueden contar con una gran diversidad de servicios y mejora los métodos de autenticación y la seguridad del sistema operativo	Es vulnerable a los problemas de seguridad del propio sistema operativo. Estas VPN se utilizan más para el acceso remoto
Aplicación	La aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo.	No soportan una gran cantidad de usuarios. Son mucho más lentas que una VPN basada en hardware.
Proveedor de servicios	Seguridad rentable. Puede evitar la limitación del ancho de banda. Mejoran los juegos en línea	Puede disminuir su velocidad Conexiones caídas. No es legal en todos los países. El servicio VPN podría monitorear su actividad y usar sus datos

Nota. Breve descripción de las ventajas y desventajas de los tipos de VPN según la implementación. Fuente: Ramos Dillón, (2016, p. 51, 52, 53)

En definitiva, Un enrutador VPN es una de las mejores soluciones para que todos los dispositivos dentro de una organización usen una conexión VPN, siempre y cuando si el proveedor

de producto impone límites de dispositivos. El uso de un enrutador habilitado para VPN garantiza que todos los dispositivos conectados a la red (computadoras, tablets, teléfonos inteligentes, etc.) puedan conectarse simultáneamente a los servidores de la VPN implementada. Es importante destacar que no todos los enrutadores son compatibles con el software VPN y no todos los servicios VPN pueden ejecutarse en un enrutador.

2.2.6 Topologías de VPN

La topología de VPN requerida por una organización debe estar dictada por los inconvenientes que la empresa está tratando de resolver. Sin embargo, varias topologías bien conocidas aparecen con tanta frecuencia como las que se presentan a continuación.

Para las VPN de sitio a sitio:

- Topología radial
- Topología de malla completa o parcial
- Topología híbrida

Para las VPN de acceso remoto:

- Topología de acceso remoto

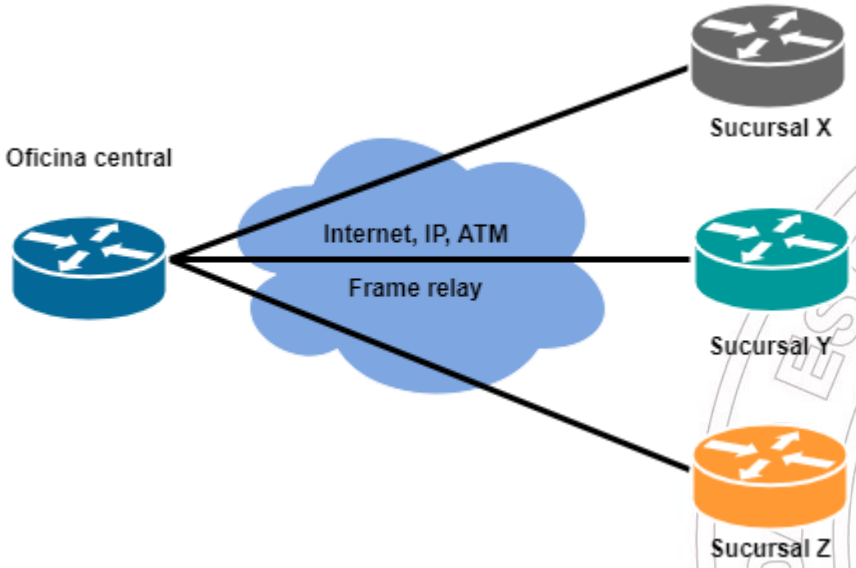
2.2.6.1 Topología Radial

La topología que se encuentra con más frecuencia es una topología radial, donde varias oficinas remotas están conectadas a un sitio central “HUB”. Delgado (2020) define “Un HUB, también llamado concentrador, es un aparato que hace de puente al que podemos conectar varios dispositivos, el HUB posee varias entradas y una salida o en algunos casos varias salidas y una entrada” (párr. 1). Las oficinas remotas normalmente pueden intercambiar datos, no existen restricciones de seguridad explícitas sobre el tráfico entre oficinas, pero la cantidad de datos intercambiados entre ellas es insignificante. La topología radial se usa normalmente en

organizaciones con estructuras jerárquicas estrictas, por ejemplo, bancos, gobiernos, tiendas minoristas, organizaciones internacionales con pequeñas oficinas en el país, etc.

Figura 8

Topología radial



Nota. Elaborado por el autor

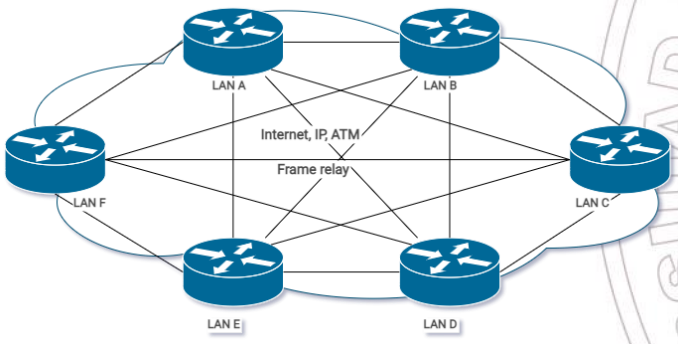
Cuando se implementan VPN basadas en tecnologías de Capa 2, como Frame Relay o ATM, la topología de VPN radial es más común de lo que cabría esperar. Esto se basa únicamente en las necesidades comerciales debido a los costos más altos o la mayor complejidad de enrutamiento asociada con otras topologías que usan este tipo de tecnologías. Frame Relay es un tipo de tecnología de Telecomunicaciones que se puede utilizar para conectar redes de área local (LAN) y para transmitir datos entre puntos finales en redes de área amplia (WAN); mientras que, ATM significa Modo de Transferencia Asíncrono , es una tecnología de comunicación de datos de transmisión de banda ancha y alta velocidad basada en la conmutación de paquetes , que utilizan las empresas de Telecomunicaciones, los operadores de larga distancia y las redes troncales para transportar información integrada de datos, voz y video.

2.2.6.2 Topología de Malla Completa o Parcial

Las topologías VPN en malla se pueden implementar en una configuración en malla completa o parcial. Las configuraciones completamente en malla tienen una gran cantidad de rutas alternativas a cualquier destino dado. Además, las configuraciones totalmente en malla tienen una redundancia excepcional porque cada dispositivo VPN proporciona conexiones a todos los demás dispositivos VPN. Un compromiso más simple es la topología de malla parcial, en la que todos los enlaces están conectados de una manera más limitada a otros enlaces.

Figura 9

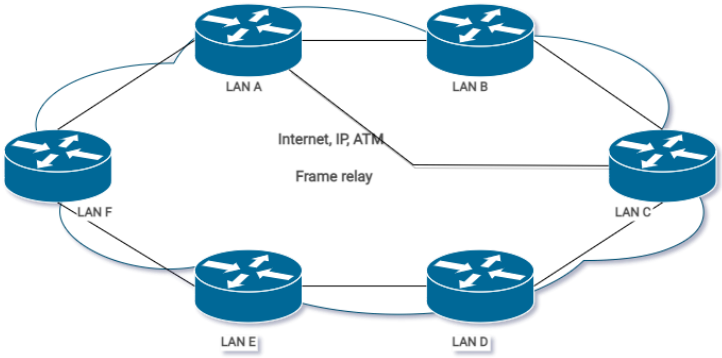
Topología malla completa



Nota. Elaborado por el autor

Figura 10

Topología malla parcial



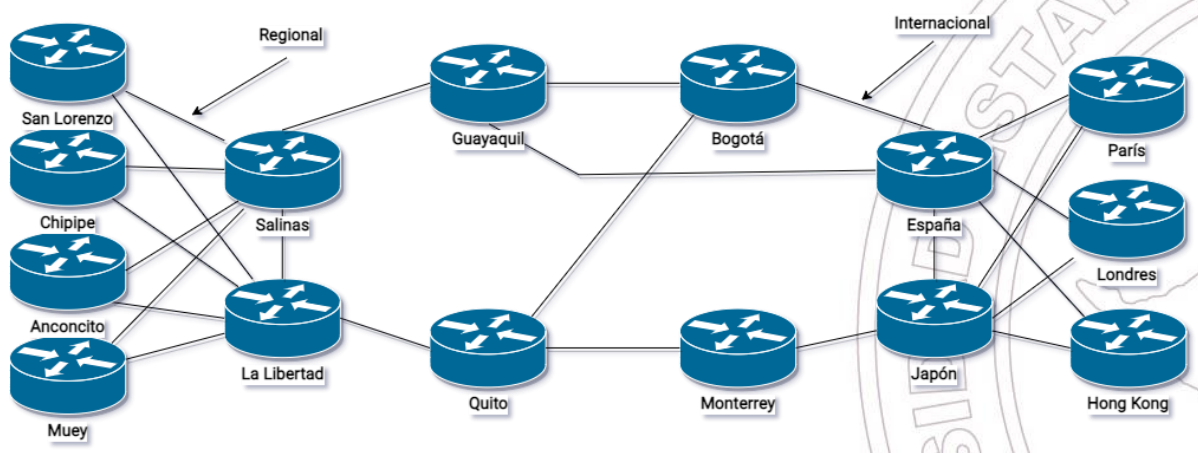
Nota. Elaborado por el autor

2.2.6.3 Topología Hibrida

Las grandes redes VPN creadas con un modelo de VPN superpuesto tienden a combinar la topología radial con la topología de malla parcial. Por ejemplo, una gran organización multinacional podría tener redes de acceso en cada país implementadas con una topología radial, mientras que la red central internacional se implementaría con una topología de malla parcial.

Figura 11

Topología híbrida



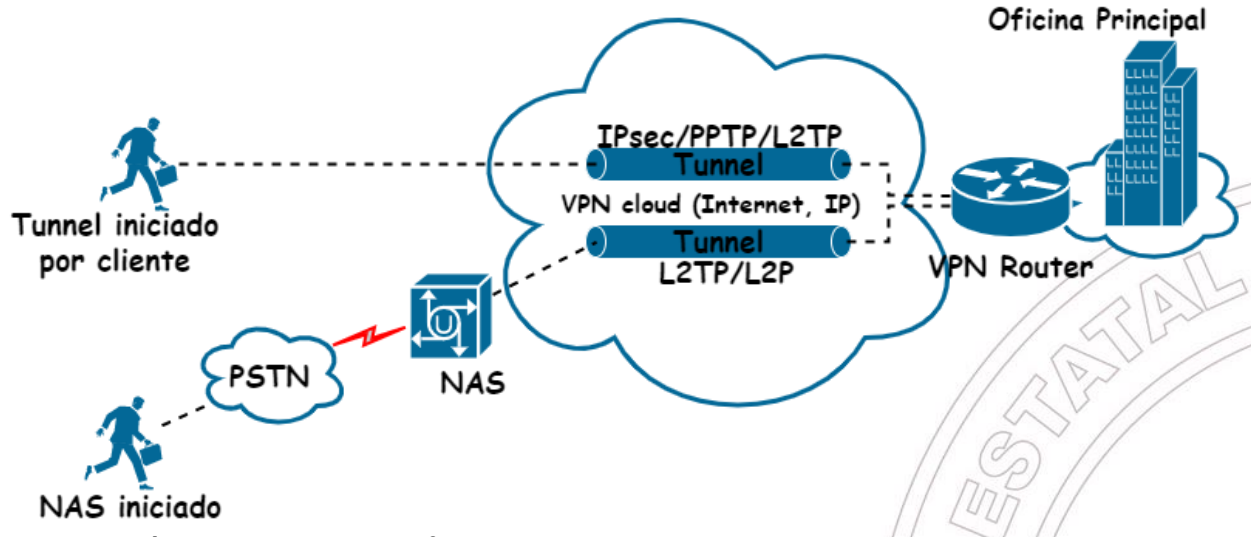
Nota. Elaborado por el autor

2.2.6.4 Topología de Acceso Remoto

Se utiliza una VPN de acceso remoto para permitir el acceso remoto desde una ubicación externa a una red física de capa 2. Usando este tipo de VPN es posible conectarse a una red LAN de la empresa desde fuera de la oficina (por ejemplo, desde la casa de un empleado o desde un hotel en un viaje de negocios) como si estuviesen conectados por un cable ethernet extremadamente largo.

Figura 12

Topología VPN acceso remoto



Nota. Los túneles se crean con diferentes protocolos: L2TP, Ipsec, PPTP, etc.

Un dispositivo NAS es un dispositivo que se conecta directamente a la red a través de un cable Ethernet (RJ45) o mediante WiFi, creando así una LAN en lugar de una WAN. Se le asigna una dirección IP y transferencia de datos entre usuarios, servidores y un NAS a través de TCP/IP. NAS funciona con un sistema de archivos tradicional, ya sea un sistema de archivos de nueva tecnología (NTFS) o NFS para servicios de archivos remotos y uso compartido de datos. Se accede a todo el almacenamiento en el dispositivo a nivel de archivo a través de un recurso compartido de registros.

Con el implemento de esta VPN en una organización, significa que los empleados remotos pueden iniciar sesión en la red de su oficina desde cualquier lugar (casa, viaje, en tránsito) que tenga acceso a Internet. Luego tienen acceso a todos los recursos de la empresa y, de alguna manera, sus datos están seguros, incluso si están usando WiFi público. (Quezada Lozano, 2016). Trabajar a través de un túnel de cifrado es importante porque reduce la posibilidad de que los espionajes informáticos roben los datos. En la era del trabajo independiente de la ubicación, el uso

de una VPN para el acceso remoto es una práctica recomendada que garantiza que los empleados puedan navegar en paz sin preocuparse de que los atacantes oportunistas secuestren información confidencial.

2.2.7 Tunneling

Tunneling es un protocolo para transferir datos de forma segura de una red a otra. Usando un método conocido como encapsulación, Tunneling permite que las comunicaciones de la red privada se envíen a través de una red pública, como Internet. La encapsulación permite que los paquetes de datos parezcan generales para una red pública cuando son paquetes de datos privados, lo que les permite pasar desapercibidos.

En síntesis, este proceso de Tunneling este compuesto por tres gases, estas son:

- Encapsulación
- Transmisión
- Desencapsulación

Cuando los datos se tunelizan, se dividen en partes más pequeñas llamadas paquetes a medida que viajan a través del túnel. Los paquetes se cifran a través del túnel y se lleva a cabo otro proceso conocido como encapsulación. Para la transmisión, los datos de la red privada y los detalles del protocolo se encierran en unidades de transmisión de la red pública. Las unidades tienen la apariencia de datos públicos, lo que permite su envío a través de Internet. La encapsulación permite que los paquetes lleguen a su destino previsto. El desencapsulado y el descifrado tienen lugar en el destino final.

El tunneling implica el uso de protocolos de tunelización para encapsular la carga útil de un paquete dentro de otro encabezado. Este encabezado contiene información de enrutamiento que se utiliza para transmitir el paquete de datos a través de un túnel. La ventaja de usar protocolos de

tunelización es que los paquetes de datos de diferentes protocolos se pueden transmitir a través de Internet. Por ejemplo, no puede transmitir Intercambio de paquetes entre redes (IPX) o un paquete de datos NetBEUI a través de Internet. Puede usar un protocolo de tunelización para encapsular estos paquetes de datos dentro del protocolo de red compatible con la red de tránsito. Un paquete NetBEUI encapsulado dentro de un encabezado IP se puede enviar a través de un túnel creado a través de Internet.

La creación de un túnel requiere lo siguiente:

Protocolo de portador: se refiere al protocolo de transporte de red compatible con la interconexión de redes de tránsito. Por ejemplo, PPP se utiliza como protocolo de operador en redes de tránsito basadas en IP.

Protocolo de encapsulación: se refiere al protocolo utilizado para encapsular la carga útil de un paquete de datos. La encapsulación de enrutamiento genérico (GRE), PPTP, L2F y L2TP son ejemplos de protocolos de encapsulación.

Protocolo de pasajeros: Se refiere al protocolo utilizado por las redes que están conectadas por el túnel. Lo utiliza el paquete de datos, que se encapsula mediante un protocolo de encapsulación. IP, IPX y NetBEUI son ejemplos de protocolos de pasajeros.

Figura 13

Estructura general de un paquete de tunneling

Nota. Elaborado por el autor

2.2.7.1 Tunneling en una VPN

El término tunelización VPN describe un proceso mediante el cual los datos se transportan de forma segura desde un dispositivo o red a otro a través de un entorno no seguro como Internet sin comprometer la privacidad. La tunelización implica proteger los datos al volver a empaquetarlos en una forma diferente.

En realidad, los datos tienen que viajar a través de los mismos cables que cualquier otro dato que pase por la red pública. Más bien, la tunelización VPN emplea los conceptos conocidos como encapsulación y encriptación de datos para transportar de forma segura el tráfico de datos a través del entorno no seguro. La encapsulación aísla el paquete de datos de otros datos que viajan por la misma red, mientras que el cifrado hace que los datos sean "invisibles" (ilegibles), es como si los datos viajaran dentro de un túnel.

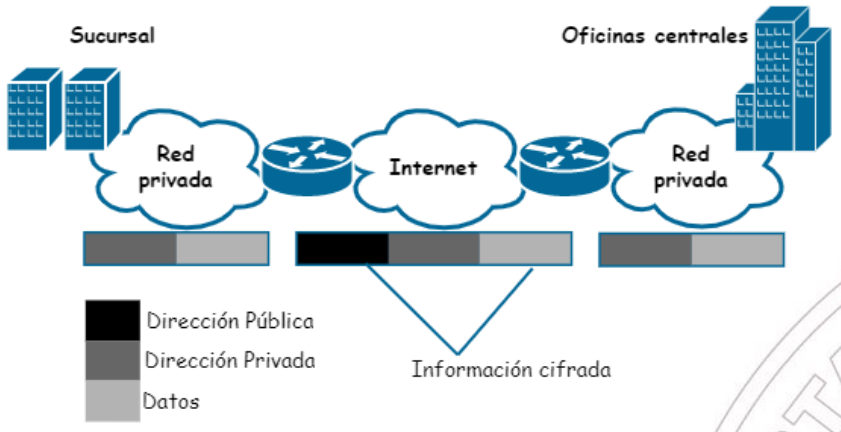
La tunelización es posible gracias a una variedad de procedimientos, que incluyen:

- Protocolo de tunelización punto a punto (PPTP)
- Protocolo de tunelización de capa dos (L2TP)
- Protocolo de Seguridad IP

En las VPN de acceso remoto se enfocan principalmente en la utilización de los protocolos PPTP y L2TP, mientras que Ipsec está mayoritariamente en las aplicaciones de VPN sitio a sitio. La siguiente figura demuestra como es el proceso de Tunneling en una VPN.

Figura 14

Tunneling en una VPN



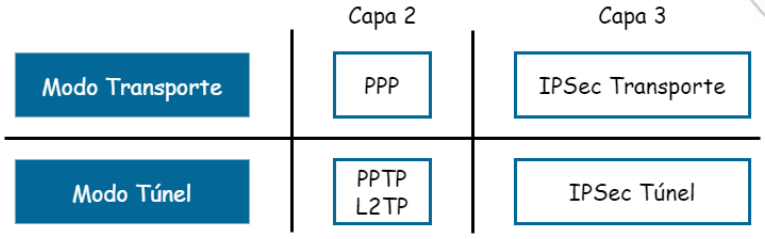
Nota. Elaborado por el autor

2.2.8 Protocolos de Tunelización

Los métodos de tunelización se diferencian según el tipo de protocolo de tunelización utilizado para encapsular los datos. Los túneles de capa 2 y capa 3 implican el uso de protocolos de túnel que corresponden a la capa de enlace de datos y la capa de red en el modelo de interconexión de sistemas abiertos (OSI).

Figura 15

Estructuración de modos VPN



Nota. Elaborado por el autor

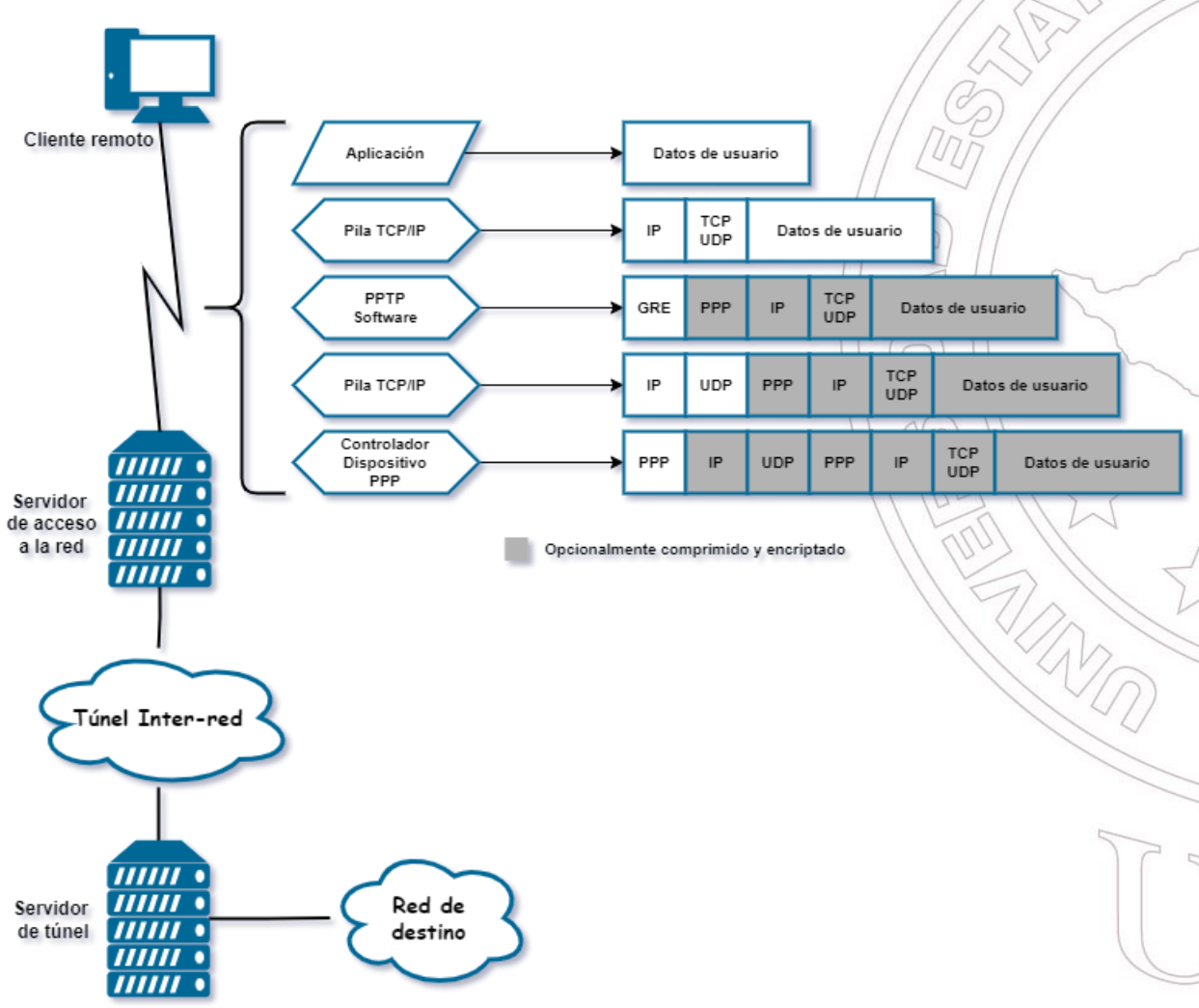
2.2.8.1 Protocolo PPTP

Desarrollado como una extensión del Protocolo punto a punto (PPP), PPTP agrega un nuevo nivel de seguridad mejorada y comunicaciones multiprotocolo a través de Internet. Al usar el nuevo Protocolo de autenticación extensible (EAP) con métodos de autenticación sólidos, como

certificados, la transferencia de datos a través de una conexión VPN habilitada para PPTP es tan segura como dentro de una sola LAN en un sitio corporativo (Microsoft, 2009). En general, este protocolo fue ampliamente utilizado por las empresas para permitir que los clientes o empleados accedieran a los servidores de su empresa desde sus hogares a través de Internet. Hoy en día todavía lo utilizan a menudo las empresas, pero también las personas que buscan una solución VPN rápida.

Figura 16

Construcción de un paquete PPTP



Nota. Elaborado por el autor

PPTP funciona en la segunda capa (datos) del modelo OSI. La conexión entre los dos dispositivos pasa por el puerto TCP 1723, que utiliza el protocolo de control de transmisión (TCP).

Este protocolo fue construido junto con y para el Protocolo de Internet (IP). TCP ofrece la entrega de paquetes de información de manera ordenada para que la información sea registrada. Posteriormente, los paquetes de datos se realizan mediante el proceso GRE (General Routing Encapsulation). GRE permite encapsular una gran variedad de protocolos de capa de red dentro de enlaces virtuales de puerto a puerto, esto se hace usando una red IP. El túnel está formado básicamente por los paquetes de datos que viajan hacia y desde el dispositivo cliente y el servidor VPN. La Figura 16 es el modelo del proceso en que se ensambla el paquete PPTP en el momento antes de realizar la transmisión. En el controlador de dispositivo PPP se representa el diseño final de la trama de la encapsulación.

2.2.8.2 Protocolo L2TP

El Protocolo de tunelización de capa dos (L2TP) es una combinación de PPTP y Reenvío de capa 2 (L2F). En lugar de tener dos protocolos de tunelización incompatibles que compitan en el mercado y causen confusión a los clientes, el IETF ordenó que las dos tecnologías se combinan en un solo protocolo de tunelización que representa las mejores características de PPTP y L2F. L2TP está documentado en RFC 2661

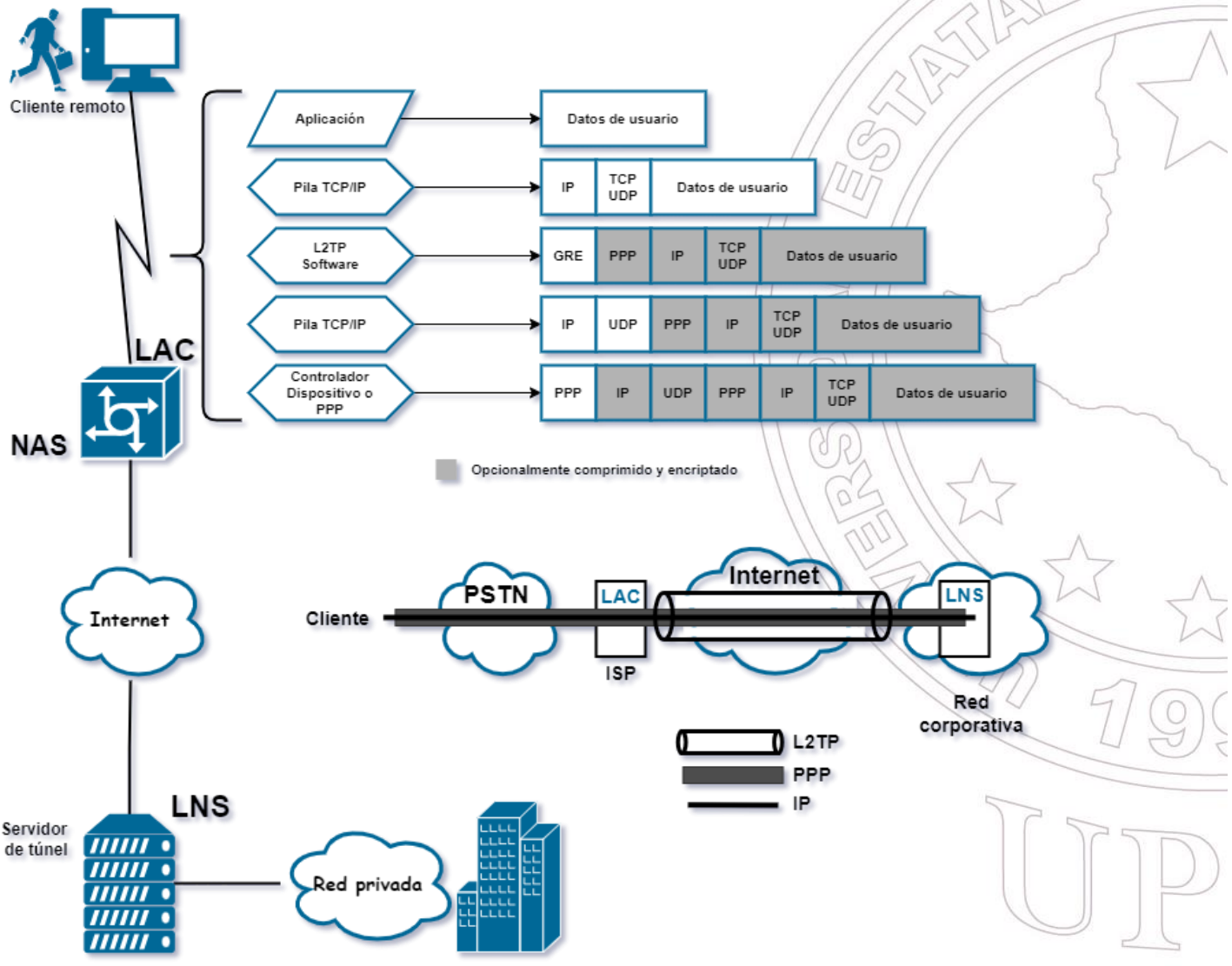
El autor Martel Víctor (2019), menciona que en el diseño de comunicación VPN sobre internet el protocolo L2TP es:

> Un protocolo que crea un túnel entre un cliente y servidor (ambos L2TP) donde encapsula las tramas PPP para su envió a través de redes como IP, X.25, Frame Relay o ATM. Una vez establecido el túnel se configura un mecanismo de autenticación de usuario con el fin de establecer su identidad. A través de las redes internas IP, L2TP utiliza el Protocolo de Datagrama de Usuario (UDP) y una serie de mensajes L2TP con el fin de crear, mantener y optimizar los túneles por donde se transmiten los datos. (p. 21)

En resumen, L2TP establece túneles punto a punto a través de una red pública (por ejemplo, Internet) y transmite tramas PPP encapsuladas (paquetes L2TP) a través de los túneles. Con L2TP, los usuarios remotos pueden acceder a las redes privadas a través de túneles L2TP después de conectarse a una red pública mediante PPP.

Figura 17

Construcción de un paquete L2TP



Nota. Elaborado por el autor

Como se muestra en la Figura, una red L2TP típica tiene los siguientes componentes:

Sistema remoto**:** un sistema remoto suele ser el host de un usuario remoto o el dispositivo de una sucursal remota que necesita acceder a la red privada.

LAC: un concentrador de acceso L2TP (LAC) es compatible con PPP y L2TP. Por lo general, es un servidor de acceso a la red (NAS) ubicado en un ISP local, que brinda servicios de acceso principalmente para usuarios de PPP. Un LAC es un punto final de un túnel L2TP y se encuentra entre un LNS y un sistema remoto.

LNS: un servidor de red L2TP (LNS) es compatible con PPP y L2TP. Por lo general, es un dispositivo de borde en una red empresarial. Un LNS es el otro extremo de un túnel L2TP. Es el punto de terminación lógico de una sesión PPP canalizada por el LAC. L2TP extiende el punto de terminación de una sesión PPP desde un NAS a un LNS mediante el establecimiento de un túnel.

Tabla 4

Ventajas y desventajas de L2TP

Ventajas	Desventajas
• Crea una excelente seguridad en línea cuando se combina con el protocolo IPSec. • Viene integrado en Windows y macOS. También funciona bien en otros dispositivos y sistemas operativos. • Fácil de configurar. El emparejamiento L2TP/IPSec también es fácil de configurar.	• L2TP, como independiente, es débil ya que no tiene cifrado propio. • Hay informes de Snowden de que la NSA ha descifrado el protocolo. Si bien es posible que no haya pruebas para respaldar esto, es mejor prevenir. • La característica de doble encapsulación hace que el L2TP consuma más recursos y sea un poco lento. • Puede ser interceptado por cortafuegos NAT si no está configurado manualmente para eludirlos.

Nota. L2TP presenta más desventajas que ventajas

Por otro lado, L2TP por sí solo no proporciona seguridad para las conexiones. Sin embargo, tiene todas las funciones de seguridad de PPP y permite la autenticación de PPP. L2TP por sí

mismo no utiliza métodos de encriptación o autenticación a pesar de ser un paso evolutivo desde PPTP. El objetivo principal de L2TP es establecer un túnel VPN. Para el cifrado, debe combinarse con otras tecnologías como IPSec, en siguiente tabla se muestran los pro y contras de L2TP.

Combinación L2TP/IPSec Para Mayor Seguridad. IPSec es un protocolo de seguridad fuerte que emplea un cifrado de cifrado AES robusto. Este protocolo también se basa en la doble encapsulación como método adicional de protección de datos. En cuanto al nivel de seguridad de IPSec, las filtraciones de Snowden han revelado que la NSA (Agencia de Seguridad Nacional, es una agencia de inteligencia a nivel nacional del Departamento de Defensa de los Estados Unidos) estaba tratando de descifrar o debilitar este protocolo como parte de su programa Bullrun. Si bien ninguna de estas acusaciones ha demostrado ser precisa, es algo que todo usuario de VPN debe tener en cuenta al pensar en la seguridad de sus datos y elegir su protocolo VPN.

La conexión VPN L2TP/IPSec comienza con la negociación de la Asociación de Seguridad (SA) IPSec que generalmente pasa por el Intercambio de Claves de Internet (IKE) y el puerto UDP 500. Esta conexión necesita una contraseña compartida, un certificado de Telecomunicaciones internacional X.509 o una clave pública.

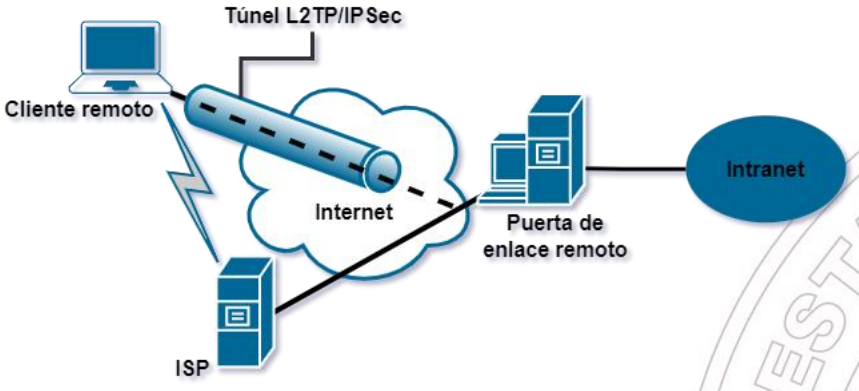
Posteriormente, este protocolo crea una carga útil de seguridad encapsulada (ESP o AH, o ambos) que permite que los dispositivos de ambos lados determinen de dónde provienen los datos. Luego, L2TP crea un túnel entre los extremos de la conexión y los datos se empaquetan dos veces: originalmente por L2TP y luego por el protocolo IPSec. Para mejorar la seguridad, la mayoría de las VPN ofrecen L2TP junto con IPSec.

VPN de Acceso Remoto con L2TP/IPSec. La implementación de acceso remoto permite que los empleados de la red empresarial trabajen en sus propios dispositivos de forma productiva cuando se encuentran fuera de la oficina. También significa que las empresas pueden contratar

empleados de todo el mundo y no solo donde tengan sedes o sucursales. Los trabajadores tendrán todas las herramientas digitales a su disposición, tal como si estuvieran en una oficina física.

Figura 18

VPN de acceso remoto con L2TP/IPSec



Nota. Elaborado por el autor

En la figura anterior, la puerta de enlace remota representa a un servidor que es el encargado de proporcionar una máxima seguridad para la intranet empresarial. El cliente remoto es un cliente o usuario que va de un lugar a otro sin permanecer en lugar fijo y que necesita tener un acceso constante a los recursos o la información de la red. En la ilustración el cliente utiliza un Proveedor de Servicios de Internet (ISP) para acceder a internet. La combinación de L2TP junto con IPSec proporcionan un modelo simple y eficaz para construir el túnel VPN y proteger la seguridad de la información a través de IP.

VPN sitio a sitio con L2TP/IPSec. En las grandes empresas comúnmente dispondrán de varios sitios, lugares o sucursales y que precisan estar en comunicación, por ejemplo, una oficina empresarial en Quito y una oficina de marketing en Guayaquil. En este escenario, L2TP junto con IPSec se juntan para establecer una conexión VPN y así, dar garantía a la protección de información este estos sitios establecidos en diferentes partes del país.

Figura 19

VPN de sitio a sitio con L2TP/IPSec

Nota. Elaborado por el autor

En la Figura 19, los enrutadores VPN son los encargados de la seguridad exterior. También es probable que estos enrutadores usen una línea alquilada, acceso a través de línea telefónica u otro tipo de acceso a internet. Entre los enrutadores se establecen la Asociación de Seguridad (SA) de IPSec y el túnel L2TP, la combinación de estos permite una comunicación segura a través de internet.

A modo de conclusión, L2TP es relativamente seguro de usar, siempre que esté emparejado con otro protocolo. No puede ser una excelente opción independiente y no es seguro usarlo solo. La forma de aprovechar al máximo el protocolo es a través del emparejamiento y está disponible en la mayoría de las plataformas, es fácil de configurar y usar, también puede resultar muy rápido en las circunstancias adecuadas. Con todo, el protocolo L2TP es una excelente opción si se usa correctamente.

2.2.8.3 Seguridad IP (IPSec)

IPsec se codificó por primera vez en la década de 1990, impulsado por la incipiente comprensión de que el tráfico de Internet debía protegerse: la Internet inicial conectaba principalmente edificios gubernamentales, universidades; y el protocolo de Internet (IP) que definiría cómo funcionaban las comunicaciones en línea, enviaba sin seguridad y sin cifrar. IPsec se diseñó para crear un estándar universal para la seguridad en Internet y permitió algunas de las

primeras conexiones a Internet realmente seguras. IPsec no es el protocolo de seguridad de Internet más común que se usa hoy en día; pero aún, tiene un papel vital que desempeñar en la seguridad de las comunicaciones de Internet. El término IPSec significa Internet Protocol Security, forma parte de un estándar creada a través de la IETF denominada Internet Engineering Task Force mediante el RFC 2401.

Dentro de la definición de IPSec el autor Víctor Limari (2004) en el contexto de tunelización menciona lo siguiente:

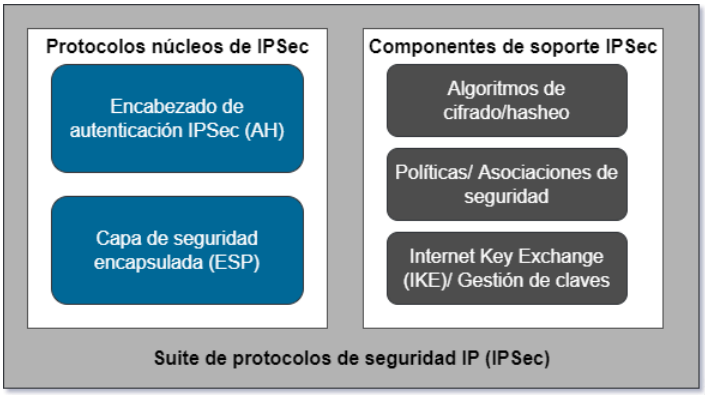
> Este protocolo es en realidad un conjunto de estándares lo cual asigna al sistema donde se implementa servicios criptográficos de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa 3 de red de OSI, de tal forma que su funcionamiento es bastante transparente al momento de llegar al nivel de aplicación, es decir se puede trabajar con HTTP, FTP, Telnet, SMTP, etc. IPSec es poderoso en comparación a las otras alternativas de túneles de seguridad. (p. 30)

A este respecto, garantiza la confidencialidad de los datos (los paquetes se cifran antes de su transmisión a través de una red) y la integridad de los datos (verificando si los paquetes no cambiaron durante la transmisión) en la capa IP. IPSec tiene una función denominada anti reproducción que identifica y rechaza los paquetes reproducidos, también vale la pena mencionar es que puede proteger más de un flujo de datos.

IPSec cuenta con un núcleo de protocolos que se adjuntan en los encabezados de los datagramas IP y componentes de soporte se detallan en la siguiente figura:

Figura 20

Suite de protocolos de seguridad IP



Nota. Descripción general de los protocolos y componentes de IPsec

IPsec consta de dos protocolos principales, AH y ESP, y tres componentes de apoyo.

Protocolos básicos de seguridad IP. El objetivo principal de los protocolos básicos es garantizar la seguridad al codificar la información. En IPSec, hay dos para mencionar: los protocolos AH y ESP.

- ***Encabezado o Cabecera de Autenticación (AH).*** AH se utiliza para autenticar la fuente de datos y verificar la integridad de los paquetes IP. Es decir, AH garantiza que se confíe en la fuente de los paquetes IP y que los datos no se alteren. AH, sin embargo, no proporciona la función de cifrado. Se agrega un encabezado AH al encabezado IP estándar en cada paquete de datos. AH comprueba la integridad de todo el paquete IP.
- ***Carga de Seguridad de Encapsulación (ESP).*** ESP puede cifrar datos además de autenticar la fuente de datos y verificar la integridad de los paquetes IP. Se agrega un encabezado ESP al encabezado IP estándar en cada paquete de datos, y los campos de datos ESP Trailer y ESP Auth se agregan a cada paquete de datos. ESP

en modo de transporte no verifica la integridad de los encabezados de IP. Por lo tanto, ESP no puede garantizar que los encabezados de IP no sean manipulados.

AH y ESP se pueden utilizar de forma independiente o conjunta. Cuando AH y ESP se usan juntos, la encapsulación ESP se realiza antes que la encapsulación AH y la desencapsulación AH se realiza antes que la desencapsulación ESP.

Componentes de soporte IPSec. De igual forma, presenta diversos algoritmos de cifrado y políticas de seguridad descritos a continuación:

- ***Algoritmos de cifrado.*** El cifrado es un proceso de conversión de datos de texto sin formato en datos de texto cifrado mediante un algoritmo. El receptor puede descifrar datos de texto cifrado solo cuando tiene la clave correcta. El mecanismo de encriptación garantiza la confidencialidad de los datos y evita que los datos sean espiados durante la transmisión. IPSec implica el cifrado de datos y el cifrado de mensajes de protocolo.
- ***Políticas de Seguridad.*** Una política de seguridad es una regla que está programada en la implementación de IPsec. Le dice a la implementación cómo procesar diferentes datagramas recibidos por el dispositivo. Por ejemplo, las políticas de seguridad deciden si IPsec debe procesar un paquete en particular o no. AH y ESP evitan por completo aquellos que no necesitan procesamiento.
- ***Asociación de seguridad.*** Una asociación de seguridad (SA) es un conjunto de información de seguridad que describe un tipo particular de conexión segura entre un dispositivo y otro. Especifica los mecanismos de seguridad particulares que se utilizan para las comunicaciones seguras entre los dos. Se pueden realizar dos configuraciones:

- Manualmente

  A veces denominado “manual keying”

  Se Configura en cada nodo:

  - Nodos participantes (es decir, selectores de tráfico)
  - AH y/o ESP [túnel o transporte]
  - Algoritmo criptográfico y clave

- Automáticamente

  Uso de IKE (intercambio de claves de Internet)

- ***IKE. Intercambio de claves de Internet (IKE)*** es un protocolo de capa de aplicación basado en el Protocolo de datagramas de usuario (UDP) creado en el marco del Protocolo de administración de claves y asociación de seguridad de Internet (ISAKMP). Implementa la negociación automática de claves y la configuración de IPSec SA para simplificar el uso y la administración de IPSec y facilitar la configuración y el mantenimiento de IPSec.

2.2.8.3.1 Modos de Operación IPSec

IPSec proporciona dos modos diferentes para intercambiar datos protegidos entre los diferentes tipos de VPN:

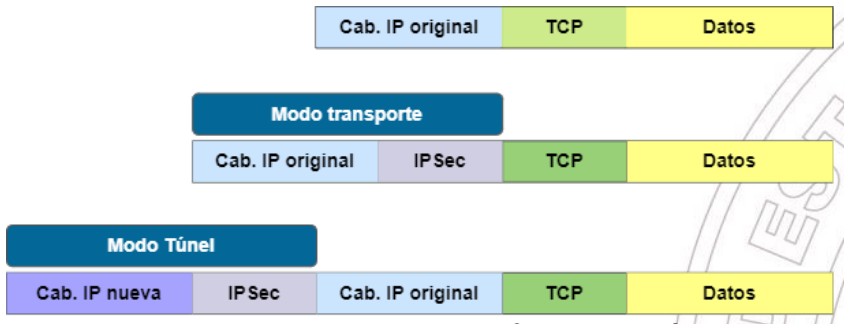
Modo de transporte: este modo solo se aplica a la seguridad de host a host. Aquí la protección se extiende a la carga útil de los datos IP. Las direcciones IP de los hosts deben ser direcciones IP públicas.

Modo de túnel: este modo se utiliza para proporcionar seguridad de datos entre dos redes. Proporciona protección para todos los paquetes IP y se envía agregando un encabezado IP externo correspondiente a los dos extremos del túnel. Los paquetes desprotegidos generados por anfitriones

viajan a través del túnel protegido creado por los Gateway en ambos extremos, el encabezado IP externo corresponde a estas pasarelas. Las VPN tanto intranet como extranet se habilitan a través de este modo, ya que en el modo túnel se esconde la cabecera IP original, facilitando la seguridad de las redes con espacio de direcciones IP privadas.

Figura 21

Modos de operación IPSec



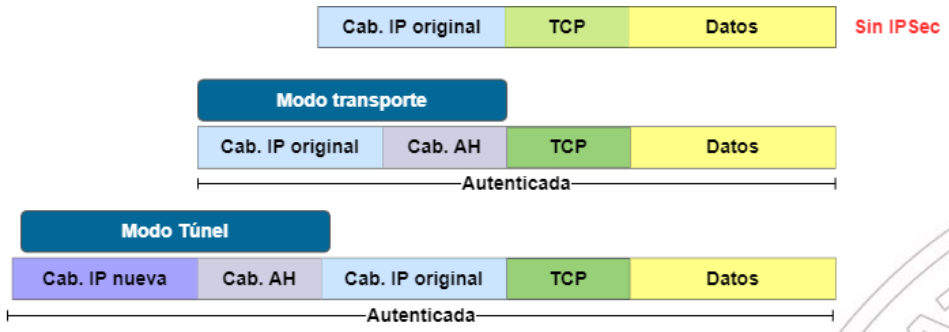
Nota. En el modo transporte el paquete original es modificado añadiéndole campos AH o ESP. En el modo túnel el paquete original se encapsula dentro de un nuevo paquete IP con los campos AH o ESP.

2.2.8.3.2. Encabezado o Cabecera de Autenticación (AH)

Authentication Header (AH) proporciona integridad de datos y protección de reproducción para todo el datagrama de IP y es una medida eficaz contra los ataques de suplantación de identidad y rastreo de sesiones. AH, como ESP, utiliza un algoritmo hash seguro para calcular el Valor de Verificación de Integridad (ICV) sobre el encabezado IP más la carga útil. El ICV se incluye como parte del encabezado AH. El protocolo AH especifica un conjunto de campos de encabezado de IP mutables (TOS, Fragment offset y flags, TTL, Checksum) que deben excluirse del cálculo de ICV. La Figura 22 ilustra el modo transporte y túnel de AH.

Figura 22

AH en modo transporte y túnel



Nota. En modo túnel, AH crea un nuevo encabezado IP para cada paquete; en modo transporte, AH no crea un nuevo encabezado IP. En las arquitecturas IPSec que utilizan una puerta de enlace, la verdadera dirección IP de origen o de destino de los paquetes debe modificarse para que sea la dirección IP de la puerta de enlace.

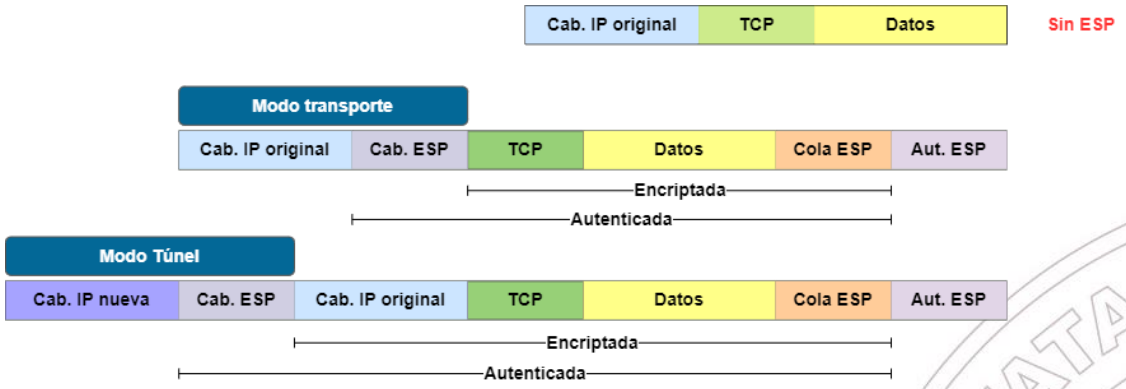
Debido a que el modo de transporte no puede alterar el encabezado IP original ni crear un nuevo encabezado IP, el modo de transporte generalmente se usa en arquitecturas de host a host. Como se muestra en la Figuras, AH brinda protección de integridad para todo el paquete, independientemente del modo que se utilice.

2.2.8.3.3. Carga de Seguridad de Encapsulación (ESP)

El protocolo Encapsulating Security Payload (ESP) proporciona todas las funciones del encabezado de autenticación (autenticación, integridad de datos y protección contra reproducción). La diferencia aquí es que la carga útil de seguridad encapsulada (ESP) proporciona la función de seguridad más crítica, la confidencialidad de los datos. La Figura 23 muestra la alteración del paquete a través del uso del protocolo ESP en modo transporte y túnel.

Figura 23

ESP en modo transporte y túnel



Nota. Los modos difieren en la aplicación de la política

En modo transporte, al igual que con AH, el modo de transporte encapsula solo la carga útil del datagrama y está diseñado estrictamente para comunicaciones de host a host. El encabezado de IP original se deja en su lugar (excepto por el campo Protocolo mezclado), lo que significa que, entre otras cosas, las direcciones IP de origen y destino no se modifican.

En modo túnel, se inserta un encabezado IPSec ESP entre el encabezado IP y el protocolo de la capa superior. Entre AH y ESP, ESP se usa más comúnmente en la configuración del túnel VPN IPSec.

2.2.9 VPN Basados en Código Abierto

Las VPN de código abierto no son bastante común en la actualidad. Sin embargo, su transparencia los convierte en un aliado para muchos usuarios. Estas son algunas de las mejores VPN de código abierto que existen:

2.2.9.1 Open VPN

Creado en 2001, el protocolo OpenVPN ahora lo utilizan casi todos los proveedores de VPN. Esto se debe en gran parte a su naturaleza de código abierto, que permite a los usuarios

verificar el código por sí mismos. La transparencia ha dado lugar a muchas pruebas, lo que demuestra que el protocolo es fiable y seguro.

Figura 24

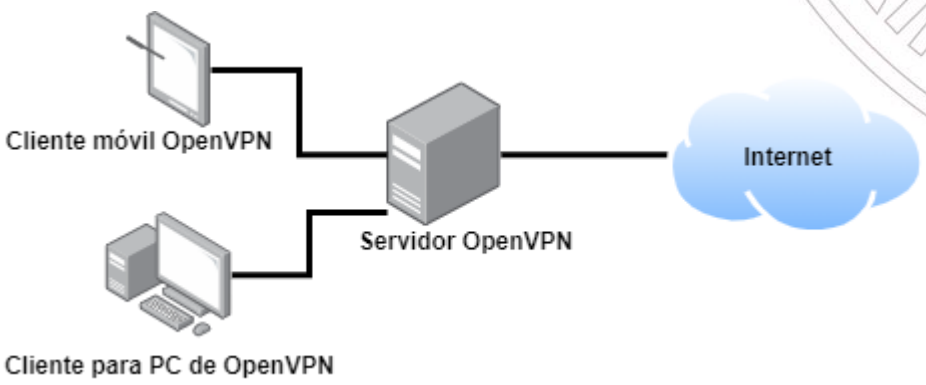
OpenVPN

Nota. Tomado de https://openvpn.net/

Es posible usar OpenVPN libremente ya que es de código abierto, lo que significa que puede usarlo libremente si sigue las condiciones del acuerdo de licencia del software. Pero si bien el código es gratuito, vale la pena señalar que requiere una gran cantidad de configuración manual (es decir, requiere algunos conocimientos técnicos).

Figura 25

Funcionamiento de OpenVPN



Nota. Elaborado por el autor

Para el funcionamiento de OpenVPN, se involucra dos partes, el cliente y un servidor. Este último tiene acceso a través de internet mientras que el cliente debe establecer una conexión a este

servidor mediante internet. Por lo tanto, el cliente asume la misma ubicación geográfica junto al servidor con su respectiva IP, lo que mantiene al cliente de forma anónima.

OpenVPN se divide en dos protocolos: OpenVPN UDP y OpenVPN TCP.

OpenVPN UDP significa Protocolo de datagramas de usuario e incluye reglas que permiten una conexión más rápida. La mayoría de las veces, esta será su conexión predeterminada simplemente porque le dará velocidades de Internet más rápidas.

OpenVPN TCP significa Protocolo de control de transmisión que, como su nombre indica, mantiene un mayor control sobre la transmisión de datos. Esto da como resultado velocidades más lentas, pero generalmente es una conexión más confiable.

2.2.9.1.1 Ventajas de usar OpenVPN

Hay tres cosas que hacen que OpenVPN se destaque como una herramienta muy útil y popular para VPN:

Los niveles de seguridad son los más altos: hay varias capas de seguridad que lo protegen mientras usa OpenVPN, como claves pre compartidas, autenticación de pares y muchos otros tipos de protección. Además, debido al uso de OpenSSL Library junto con algo llamado autenticación de paquetes HMAC, la seguridad de su red será máxima y no tendrá que preocuparse por las personas malintencionadas en línea.

Confiable para sus usuarios: se dice que OpenVPN es muy confiable debido al hecho de que las personas que lo mejoran y mantienen son las personas responsables y quienes se aseguran de que sus datos estén siempre encriptados y nunca se pierdan. Todo esto puede suceder si OpenVPN se desconecta por alguna razón: toda la red se detiene y todos sus datos aún están seguros.

El apoyo de la comunidad en todo el mundo: OpenVPN tiene una gran cantidad de fanáticos y una gran comunidad mundial que puede ayudar a todos a usar este tipo de red VPN. Todo esto es posible gracias al hecho de que OpenVPN es un software de código abierto que se puede modificar.

2.2.9.1.2 Desventajas de usar OpenVPN

Veamos ahora cuáles son las desventajas de usar este software.

Hay ciertos servidores proxy que no son compatibles y no admiten OpenVPN. Eso es todo: hay pocos servidores como este en el mundo y tienes que tener bastante mala suerte para estar en el lugar correcto y en el momento adecuado para conectarte a través de uno de estos. Sin embargo, hay soluciones; como un proxy de apoyo al que un usuario puede cambiar.

A veces, la latencia puede ser alta. El espacio del usuario juega un papel importante en OpenVPN y básicamente todas las etapas de encriptación ocurren en este espacio. Esto quiere decir que la seguridad está al máximo pero que en ocasiones puede afectar a la velocidad de la red y aumentar la latencia. Este problema puede ocurrir si su dispositivo no es lo suficientemente fuerte como para admitir todos los procesos en curso, pero si tiene una máquina fuerte, no debe preocuparse por eso.

No es realmente fácil de usar. OpenVPN tiene numerosas opciones y puede ser muy confuso para alguien que comenzó a usarlo. Afortunadamente, hay muchos foros y soporte profesional de proveedores de VPN que pueden ayudarlo a comprender los conceptos básicos y continuar experimentando por su cuenta.

2.2.9.1.3 OpenVPN frente a IPsec VPN

IPsec se considera una especie de estándar predeterminado en el mundo de las VPN. Sin embargo, hay pruebas que señalan que OpenVPN es muy superior a IPsec. Por ejemplo, la

desventaja de IPsec se ve en su complejidad. Utiliza una tecnología muy compleja y es muy difícil configurarlo. Por otro lado, OpenVPN tiene instrucciones claras en lo que respecta a la configuración y la tecnología detrás es bastante simple y está estructurada de tal manera que sea comprensible para todos.

OpenVPN utiliza la capa 2 y 3 del modelo OSI con los protocolos SSL / TLS, lo cual permite tener métodos flexibles de cifrado, autenticación de usuarios a través de certificados y políticas de control de clientes configuradas respectivamente en las reglas del firewall.

2.2.9.2 WireGuard

WireGuard es un tipo de implementación de VPN que pretende generar cambios en la industria de las VPN. De hecho, se puede considerar como el futuro de la tecnología VPN. Sin embargo, WireGuard aún está en desarrollo, tratando de convertirse en un estándar en la industria de las VPN.

Figura 26

Protocolo WireGuard

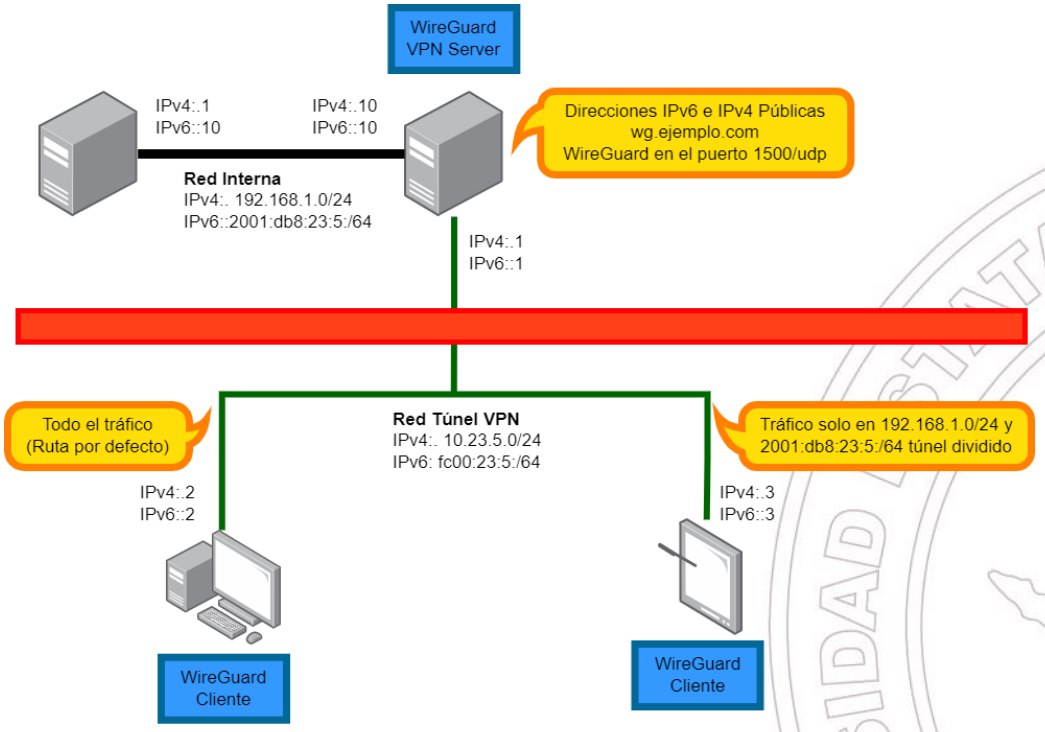
Nota. Tomado de https://www.wireguard.com/

WireGuard es un procedimiento VPN de código abierto de primera mano que tiene como objetivo ofrecer una práctica en línea más rápida, fácil y segura para los usuarios de Internet. Se apela al procedimiento para sugerir un mejor rendimiento que OpenVPN, y para ser comúnmente más valioso y mejor diseñado que IPSec. (Donenfeld, 2017)

WireGuard fue creado por Jason Donenfeld, el hombre que abrió Edge Security. A pesar de lo "joven" que es el procedimiento WireGuard formalmente surgió en 2018, pero estaba en

crecimiento antes de esa fecha, ha sido reconocido rápidamente por los usuarios en línea, en la Figura 27 que describe el WireGuard.

Figura 27



Funcionamiento WireGuard

Nota. Si el cliente móvil establece una conexión VPN con el teléfono móvil y usa el teléfono móvil como un punto de acceso WiFi para otro dispositivo (como una computadora portátil), el tráfico del punto de acceso WiFi no se enruta a través de la VPN.

Características de esta configuración:

- Se puede acceder a la infraestructura interna de IPv4 e IPv6 desde cualquier lugar a través de IPv4 e IPv6.
- El cliente VPN WireGuard se puede instalar y usar en Linux y teléfonos móviles como Android.

- Todo el tráfico (ruta predeterminada) o solo el tráfico deseado para la red interna se puede enrutar a través de la VPN (túnel dividido). Esto se puede configurar en el cliente.
- Si un guerrero de la carretera no tiene una conexión IPv6, esta se puede proporcionar a través del túnel VPN.
- El servidor VPN también puede estar detrás de un enrutador NAT, porque WireGuard funciona sobre UDP.

2.2.9.2.1 Ventajas y Desventajas de WireGuard

En sus etapas iniciales, se lanzó solo para dispositivos Linux, pero a partir de ahora es compatible con todos los sistemas operativos. Además, WireGuard tiende a ser más rápido y está bien diseñado en comparación con un protocolo IPSec. Es muy preferido por los usuarios debido a su velocidad y rendimiento. Aunque WireGuard posee beneficios potenciales, existen ciertos inconvenientes que se ignoran. Antes de usar WireGuard VPN, es necesario examinar sus ventajas y desventajas.

Tabla 5

Ventajas y desventajas de WireGuard

Ventajas	Desventajas
Código abierto	Todavía en desarrollo
Cuenta con una base de código muy liviana	Puede ser potencialmente bloqueado por los administradores de la red
Mucho más fácil de auditar	
Utiliza criptografía de última generación	
Extremadamente seguro	
Ofrece altas velocidades	

Nota. Tomado de VPN Unlimited (2022)

La velocidad es la primera gran ventaja de WireGuard. Tiene un toque ligero cuando consume los recursos de la CPU de su dispositivo y es un protocolo más eficiente en general, lo que generalmente significa una mayor duración de la batería y menos demoras cuando abre y usa otras aplicaciones en su dispositivo. Este aumento de velocidad también incluye velocidades de conexión y reconexión. Entonces, si está usando una VPN en su teléfono celular, por ejemplo, y cambia de datos móviles a WiFi, WireGuard debería ser lo suficientemente rápido en la mayoría de los casos para que no note una interrupción significativa en su conexión.

WireGuard al ser un protocolo nuevo conlleva a que, si bien su compatibilidad con las plataformas se está expandiendo, no todas las VPN lo admiten actualmente. Eso podría deberse a que ofrecer WireGuard mientras se protege la privacidad del usuario requiere un trabajo adicional por parte de una VPN.

PPTP frente a OpenVPN o WireGuard

PPTP es un protocolo VPN obsoleto cuyas debilidades de seguridad lo hacen inadecuado para su propósito. No creemos que ningún servicio VPN moderno y responsable deba ofrecer PPTP como opción a sus usuarios.

L2TP/IPSec frente a OpenVPN o WireGuard

L2TP/IPsec sigue siendo ampliamente utilizado y todavía se considera seguro en términos generales, a pesar de la evidencia de que ha sido descifrado por la NSA y que se debilitó deliberadamente durante su fase de diseño. La práctica común entre algunos servicios VPN comerciales de usar claves previamente compartidas también es motivo de preocupación.

La conclusión, sin embargo, es que L2TP/IPsec no ofrece ninguna ventaja sobre los protocolos VPN más modernos, como IKEv2 y WireGuard, tampoco ofrece las capacidades probadas de seguridad y anti censura de OpenVPN.

En promedio, WireGuard es aproximadamente un 50 % más rápido que OpenVPN. El rendimiento de la velocidad del protocolo sobre OpenVPN aumenta cuando se conecta a ubicaciones de servidor cercanas (baja latencia) y se reduce ligeramente en servidores lejanos (alta latencia).

2.2 Marco Teórico

En este apartado, se muestran las investigaciones de las cuales se han tomado información concerniente a trabajos Elaborados con VPN en nivel de la educación superior, ya que aportan con información relevante para llevar a cabo esta propuesta de implementación.

En Colombia, en la ciudad de Cartagena a través de un trabajo de titulación definido: **Implementación de una Red Virtual para teleoperación a través de internet**, presenta una solución para el acceso remoto a través de varios dispositivos para el control de equipos de laboratorio de circuitos digitales mediante Internet, resaltando la importancia de una VPN como herramienta para optimizar el proceso de enseñanza-aprendizaje poniendo en práctica los conocimientos se adquirieron en el aula. (Choto et al., 2007)

En Perú, se realizó un proyecto cuyo tema es: **Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo**, con motivo de agilizar el control de aplicaciones dentro de la intranet de la misma universidad, justificando el hecho de que por ser una institución de estado se encuentra vulnerable en problemas de gestión administrativa al realizar trámites de documentación, el sistema que usaron fue Softether VPN. (De La Cruz Bernilla y Vera Cruz, 2019)

Redirigiéndonos a nuestros país, en Santo Domingo, para la comunicación a través de VoIP se realizó un estudio y diseño denominado: **Desarrollo de un prototipo de una red VoIP segura mediante VPN utilizando Software libre, para la comunicación de la Pontificia Universidad Católica del Ecuador, Sede Santo Domingo PUCE SD,** la cual consistió en una VPN para la comunicación segura entre la Pontificia Universidad Católica del Ecuador y su sede Santo Domingo PUCE SD, este proyecto consistió en la elaboración de un prototipo de VPN logrado unificar la voz y datos en una infraestructura de red; de igual forma, permitió realizar comunicaciones seguras dentro del establecimiento universitario hacia el exterior usando esta herramienta virtual. Se hizo uso del acceso remoto con el fin de reducir costos y el tiempo que tardaría en dirigirse a la universidad para realizar diferentes operaciones y mantenimiento. (Calazacón Aguavil, 2015)

En la ciudad de Guayaquil, se realizó trabajo de titulación definido: **Estudio y diseño de una IP VPN en un entorno MPLS con tunelización para enlazar de manera segura y proveer conectividad al cuerpo docente hacia la red de la Facultad de Administración a través de un emulador**. El cual consistió en diseñar una VPN para establecer comunicación en un entorno de MPLS, esto con el objetivo de dar conectividad entre el departamento de docentes y la facultad de administración de la Universidad de Guayaquil, el mismo que basó en un emulador que tuvo como finalidad el beneficio de compartir información entre docentes ingenieros y estudiantes brindando confiabilidad y agilidad. (Guerrero Panchana, 2017)

Un proyecto de investigación sobre la implementación de VPN realizada en la Universidad Técnica de Cotopaxi extensión “La Maná” titulado como: **Implementación de la Red Privada Virtual VPN en la Universidad Técnica de Cotopaxi - Extensión "La Maná"**, tuvo como finalidad agilizar la comunicación entre docentes, directivos, universitarios; y brindar una mejor

distribución de acceso a la información en cuanto a los datos basándose en el uso de herramientas de Open Source en CSS y HTML, logrando acceder a la intranet desde cualquier lugar remoto a través de dispositivos conectados fuera del establecimiento universitario (Iza Ninasunta y Vera Zambrano, 2020).

En la ciudad de Loja, en la Universidad de Loja, esta institución brinda acceso remoto a sus estudiantes a través de una VPN, así lo detalla un manual descrito: **Acceso web a recursos institucionales mediante VPN-SSL**, del cual se describe que se puede acceder de forma segura y encriptada entre el dispositivo final y los servidores de la propia universidad, logrando así navegar de forma confiable y usar cualquier tipo de recurso que se encuentre dentro de la intranet. (Riofrío Herrera, 2020). De igual forma, en Cañar, la Universidad Nacional de Educación brinda acceso a sus estudiantes para que accedan de forma remota a su repositorio bibliotecario virtual mediante una conexión VPN que utiliza un protocolo de código abierto como OpenVPN. (UNAE Ecuador, 2020)

Tomando como referencias los proyectos de titulación y la información obtenida de las instituciones de educación superior, se establecen unos resultados en que a medida que las redes de nueva generación toman el lugar de muchas aplicaciones que en su época fueron bastante concurridas, también evoluciona la necesidad de brindar cada día la seguridad, rapidez e integridad de nuestra información que viaja a través de internet. Por ello, los últimos trabajos recalcan la importancia de MPLS y Open Source, que son un conjunto de mecanismos utilizados actualmente para establecer una comunicación más fiable. En base a este último análisis, a través de una aplicación que usa Open Source, nace la propuesta de "**Implementación de una Red Privada Virtual con protocolo WireGuard a través de una interfaz UniFi.**"

Capítulo tres

Desarrollo de la propuesta

3.1 La Importancia del Acceso Remoto a los Equipos de Redes del Laboratorio de Telecomunicaciones.

Es posible que la enseñanza en línea no haya sido la norma para la mayoría de los docentes antes de la pandemia de COVID-19; aunque, en carreras donde no se exige mucho el aprendizaje experimental a través de los laboratorios, los docentes no tienen dificultades para trabajar en línea y a menudo, disfrutan de la libertad de trabajar desde casa, siendo una ventaja la de elegir su horario de trabajo y en varias instancias ser su propio jefe.

Esto nos lleva a plantear la siguiente pregunta, ¿en qué consiste exactamente la enseñanza en línea? Esencialmente, es el proceso de educar a otros a través de Internet, mediante sesiones de videollamadas individuales o grupales, seminarios web o plataformas de mensajería. Normalmente es una combinación de metodologías de enseñanza para mantener a los estudiantes interesados en el currículo del proceso de estudios de su carrera universitaria.

Lo mejor del aprendizaje en línea es que es accesible para muchas personas. Aunque en ciertos ambientes donde se requiere del aprendizaje experimental, la tecnología también puede ser una barrera para la educación; si bien es cierto, a medida que pasan los años, esta barrera afortunadamente se está desmoronando gracias a las diferentes aplicaciones que existen en el mundo tecnológico.

El Acceso Remoto

El acceso remoto está ayudando a los estudiantes en todo el mundo a aprender desde casa, los desarrolladores son los encargados de brindar y mejorar esta herramienta ante cualquier adversidad sobre los problemas que se pueden suscitar. Este mecanismo ayuda a que, sin la necesidad de viajar, hace que el plan de estudios sea más accesible para los alumnos que tienen

necesidades debidas a la movilidad o la distancia. Por lo general, el software que brinda el servicio de acceso remoto brinda ahorros significativos en costos y tiempo en los métodos que son aplicados en las instituciones educativas.

El uso del acceso remoto resulta cada vez más necesario a medida que surge la necesidad de encontrarse en un lugar distante para realizar las diversas practicas educativas. De igual manera, el acceso remoto debe también generar seguridad y confiabilidad de los datos; además de que deba ser fácil de configurar y administrar por los anfitriones o docentes del aula para su mayor gestión en el control de usuarios remotos.

En este sentido, al hablar del acceso remoto en el ámbito educativo, es referirse al espacio donde los docentes hacen uso de un programa que se utiliza como herramienta para acceder a aquellas cosas que se pueden manejar a través de Internet, con la finalidad de que los estudiantes puedan interactuar con los recursos que se encuentren dentro del aula utilizando dispositivos móviles celulares o desde la computadora.

Para Rivera (2021), "el acceso remoto en la educación, es el uso de software que logra que un usuario conectarse a una computadora desde otra ubicación, permitiendo observar el escritorio de ese equipo e interactuar con él como si fuera local". Estos programas resultan ser herramientas innovadoras y dinámicas para agilizar su uso, en muchos países se ha incrementado la demanda de estos en beneficio para la educación.

Acceso Remoto para el Laboratorio de Telecomunicaciones.

Desde el punto de vista de la educación a través de la experimentación, Heradio et al., (2016) manifiestan que se tienen dos tipos de criterios a tomar en cuenta como:

De acuerdo con el medio por el cual se accede al ambiente, remoto o local.

De acuerdo con la naturaleza física del laboratorio, simulado o montaje experimental real. (pp. 14, 38)

A este respecto, Triana el al., (2020) señalan que a partir de estos criterios surgen los tipos de experimentación de manera real como simulada, donde se tiene:

1) Laboratorio físico real con acceso local: es el tipo de laboratorios tradicional donde el estudiante está al frente del montaje experimental.
2) Laboratorio simulado con acceso local: el ambiente es simulado no existe un entorno real y se accede localmente.
3) Acceso remoto a montaje físico real (laboratorio remoto): existe un ambiente real, al cual el estudiante accede a través de internet.
4) Acceso remoto ambiente virtual (laboratorio virtual): el ambiente es simulado, y el estudiante accede a través de internet. (p. 3)

Al analizar estos parámetros, nos encontramos que nuestro enfoque se basa en el tercero; es decir, crear un ambiente de acceso remoto para acceder a un montaje físico situado en el laboratorio de telecomunicaciones comprendido con equipos de redes como router y conmutadores totalmente administrables, de los cuales se tienen beneficios como:

- Se disminuyen costos para trasladarse a la universidad y realizar configuraciones.
- Repetir una y otra vez los eventos que se realizan como prácticas de laboratorio.
- Disponibilidad de tiempo para entender mejor su funcionamiento realizando un análisis de cada parámetro de los equipos administrables.
- El desarrollo de técnicas y habilidades que se realizan como método de adquirir más conocimientos en el uso de los equipos.

De igual forma, Monge y Méndez (2007) señalan que los beneficios del acceso remoto a través del internet dentro de un laboratorio representan en mucho la disminución de costos por diversos factores de movilidad; asimismo, el proceso de realizar diversas pruebas en los equipos y la disponibilidad en cualquier momento para desarrollar y adquirir más habilidades en el uso de los equipos conectados remotamente.

El concepto de Red Virtual Privada, más conocida como VPN, surgió como alternativa financiera de comunicación segura a través de enlaces de comunicación públicos, como es el caso de Internet, y luego se convirtió en una tecnología ampliamente utilizada para acercar negocios con un principal foco en seguridad, que garantice la integridad, la confidencialidad y la autenticidad de la información.

En el laboratorio de telecomunicaciones se encuentran equipos Mikrotik que se utilizan para realizar diferentes configuraciones a nivel empresarial y muchas veces son utilizadas por los proveedores de internet en sus redes de telecomunicaciones. De igual forma, la marca Ubiquiti es una de las pioneras a nivel mundial para la gestión o control de sus usuarios, la gran diferencia entre ambas marcas es que Mikrotik es más completo en funcionalidades, sin embargo, Ubiquiti presenta opciones más vanguardistas con una interfaz intuitiva, teniendo alternativas muy generosas que ayudan en gran cantidad a la solución de problemas como es el caso de la propuesta de implementación de este proyecto.

Ubiquiti, a lo largo de muchos años de desarrollo, esta empresa ha creado enrutadores y conmutadores de alto rendimiento, permiten operaciones en interiores y exteriores, utilizados por empresas e ISP para construir infraestructura de red en todo el mundo. Por tal motivo, es una marca muy usada a nivel global, donde el aprendizaje de este recurso va a ser imprescindible.

El tener acceso remoto al laboratorio de telecomunicaciones resulta ser una herramienta potencial para realizar las actividades que en muchas ocasiones la teoría no ayuda para el proceso de adquisición de experiencias. Al encontrarnos en un ambiente donde se presentan muchos factores de crisis sanitarias que ponen en peligro la vida de nosotros, se logra minimizar estos riesgos al no tener que salir de los hogares; aunque, representa una desventaja si en dado caso se requiera tener que realizar una conexión física en el laboratorio.

En definitiva, el acceso remoto por VPN en el laboratorio de telecomunicaciones tiene un enfoque positivo para alcanzar los objetivos de aprendizaje en el aula por parte de la docencia a través de actividades experimentales. Estando en un aislamiento social, resulta ser una herramienta de gran apoyo a los tutores y estudiantes tanto para una educación presencial y virtual.

3.2 Componentes de la propuesta

El proyecto incluye una serie de dispositivos electrónicos que deben estudiarse para una instalación adecuada. La mayoría de los dispositivos vienen con especificaciones y ajustes preestablecidos al momento de elegir dónde instalarlos; además, los dispositivos utilizados en este proyecto son de la marca Ubiquiti de la línea UniFi, antes de entrar en detalles, hablemos de la marca.

La empresa estadounidense de redes Ubiquiti Networks, Inc. proporciona tecnología para crear redes inalámbricas siendo éste su enfoque principal, considerando que pueden ser utilizadas en largas o cortas distancias, también diseñan software para cada pieza de hardware que venden (Wikipedia, 2022).

Dentro de la marca Ubiquiti Networks, Inc. Tiene diferentes líneas de equipos conocidas, entre ellas:

Tabla 6

Línea de productos Ubiquiti

Línea	Descripción
EdgeMAX	Serie de enrutadores, de altas prestaciones.
airMAX	Serie de productos wifi de exterior, que implementan las tecnologías AirMAX, AirSync
AirFiber	Serie de productos inalámbricos, destinados a conexiones troncales o Backbone, con tecnologías propietarias, que permiten la realización de conexiones de hasta 20 km, con velocidades de hasta 1,4Gb/s
UniFi	Serie de productos WiFi de interior y exterior para edificios o pequeños espacios abiertos.
UniFi Video	Serie de cámaras de vídeo vigilancia IP.
UniFi VoIP	Línea de teléfonos con comunicación por IP.

Nota. Elaborado por el autor

Cada línea de productos ofrece diferentes propósitos y también proporciona software de configuración, algunos con aplicaciones móviles. El proyecto utilizará equipos de la línea EdgeMAX, UniFi y UniFi Video.

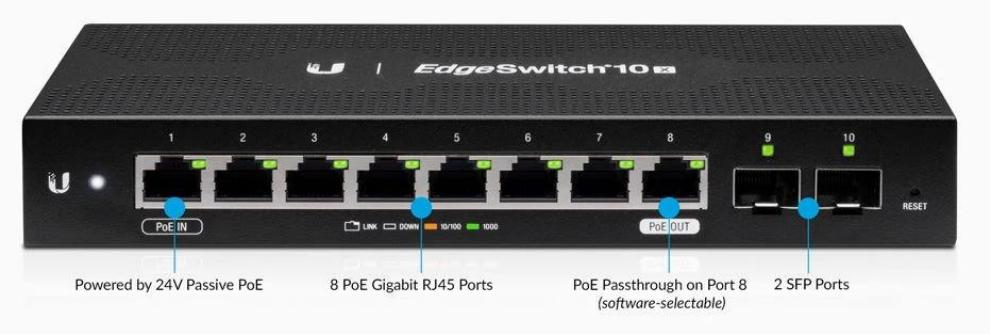
3.2.1 Ubiquiti ES-10X

Ocho puertos Gigabit RJ45 ofrecen una conectividad superior, con entrada PoE en el puerto 1 y salida PoE en el puerto 8. Dos puertos SFP garantizan la conectividad de fibra óptica.

Es nuestro caso, este conmutador estará conectado desde el EdgeRouter 4, para conectarlo al UDM-Pro. Las siguientes características se detallan en el Anexo 1.

Figura 28

Ubiquiti ES-10X



Nota. Tomado de (Ubiquiti, 2022)

EdgeSwitch 10X es compatible con un conjunto completo de funciones y protocolos de conmutación de nivel 2, se puede montar en una pared o en un bastidor; además, la nueva interfaz es fácil de aprender y nos permite monitorear y configurar funciones utilizando el panel de usuario gráfico intuitivo.

3.2.2 EdgeRouter 4

EdgeRouter 4 es parte de la próxima generación de enrutadores que se ejecutan bajo la plataforma EdgeMax. Combina confiabilidad de nivel de operación y funcionalidad de clase empresarial en un dispositivo compacto y económico. Basado en EdgeOS, una interfaz gráfica patentada e intuitiva, EdgeRouters se puede configurar fácilmente para las capacidades de enrutamiento, seguridad y administración necesarias para ejecutar la red de manera eficiente. Para los profesionales de redes avanzados, la CLI integrada está disponible para un acceso rápido y directo con comandos familiares.

Figura 29

EdgeRouter 4

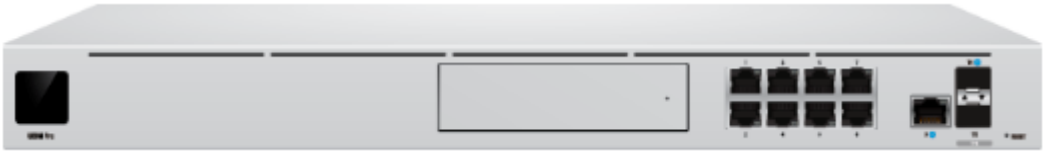
Nota. Tomado de (Ubiquiti, 2022)

3.1.3 UniFi Dream Machine Pro

UDM Pro incluye un controlador de red UniFi, el cual administrar puntos de acceso y conmutadores UniFi. También puede ejecutar el software UniFi Protect para facilitar la supervisión y la gestión general del sistema de vigilancia con cámara. Las grabaciones de video se almacenan en el NVR incorporado, aunque el disco duro no viene incluido, y se puede acceder a ellas fácilmente mediante la aplicación móvil UniFi Protect. El UDM Pro proporciona políticas de firewall avanzadas y gestión continua de amenazas al actuar como un sistema de prevención de intrusiones y un sistema de detección de intrusiones (Ubiquiti, 2022).

Figura 30

UniFi Dream Machine Pro



Nota. Tomado de (Ubiquiti, 2022)

En el Anexo 3 nos da las especificaciones generales del controlador UDM-Pro. Por defecto el controlador tiene una IP 192.168.1.1, con esa dirección entramos a la interfaz del equipo y luego nos registramos con nuestro nombre de usuario y contraseña.

3.1.4 UAP-AC-Pro y UAP-AC-Lite

Los puntos de acceso (AP) Ubiquiti UniFi son soluciones WiFi empresariales revolucionarias que combinan rendimiento de clase portadora, escalabilidad ilimitada, precios disruptivos y un controlador de gestión virtual.

Figura 31

UAP-AC-Pro

Nota. Tomado de (Ubiquiti, 2022)

Figura 32

UAP-AC-LITE

Nota. Tomado de (Ubiquiti, 2022)

Tanto como UAP-AC-PRO y UAP-AC-LITE, crean redes de área local (WLAN) inalámbricas y confiables en interiores y exteriores. Los tipos de puntos de acceso UniFi incluyen AC, In-Wall, HD, SHD, NanoHD, Mesh y XG, con constante evolución y mejora, los modelos de

la serie aseguran que existe una solución para cualquier escenario dado. Los puntos de acceso UniFi ofrecen potentes funciones para los mercados empresarial, y educativo.

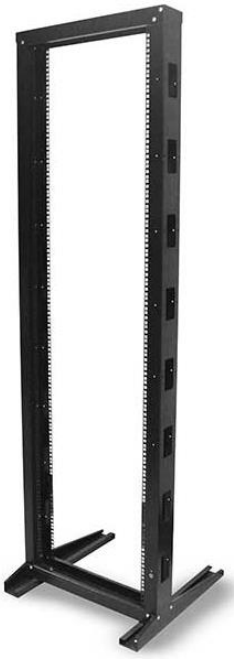
3.1.5 Rack

Los racks son una opción para el montaje de los servidores, redes y equipos de telecomunicaciones. Estos Rack son por lo general son de estructura de aluminio con orificios de montaje estándar EIA (redondos) u orificios de montaje universales (cuadrados). El espaciado de los orificios verticales en los racks está estandarizado para el montaje de equipos de telecomunicaciones o equipos informáticos de red. El uso de este rack cumple con las exigencias de nuestro proyecto porque tiene los siguientes beneficios:

- El rack de 19" estándar EIA se monta en la mayoría de los equipos de red
- Fácilmente Instalable
- Sin puertas ni paneles que obstaculicen el flujo de aire
- Tamaño de envío compacto
- Peso ligero
- Requiere menos espacio que un rack de 4 postes
- Amplia disponibilidad de accesorios para racks de relés: productos de gestión de cables, estantes en voladizo, regletas de enchufes, etc.

Figura 33

Rack



Nota. Tomado de la web

3.1.6 Patch panel

Un patch panel o panel de conexión es una pieza de hardware de red que se utiliza tanto en redes de cobre como de fibra y contiene una cantidad determinada de puertos para conectar y administrar los cables Ethernet entrantes y salientes. Permiten una red cableada más organizada y manejable. Hay diferentes tipos de paneles de conexión de fibra y cobre en el mercado. Los paneles de conexión de cobre están diseñados para cables de cobre blindados y no blindados como Cat5e, Cat6, Cat6a y Cat7. En nuestro ejercicio se hará uso del Patch Panel Cat 5e

Figura 34

Patch Panel Cat5e

Nota. Tomado de la web

Este Patch Panel de cobre se usa en una red de área local (LAN) como un conjunto de hardware montado que contiene puertos para conectar y administrar los cables Ethernet entrantes y salientes. Cumple con las especificaciones industriales TIA/EIA 568 y cuenta con configuraciones de cableado T-568A y T-568B. Estos paneles de conexión pueden maximizar el rendimiento de la red y mantenerse al día con los cambios crecientes en la red.

3.1.7 Regleta de Enchufe para Montaje en Rack

Una mejor regleta de enchufes para montaje en rack brinda comodidad a la configuración en el lugar determinado de implementación, al eliminar todos los cables colgantes del área circundante. Esto crea un espacio de trabajo mucho más limpio y organizado.

Funciona también como protector contra sobretensiones para proteger los equipos de telecomunicaciones contra cualquier sobretensión de energía imprevista.

Figura 35

Regletas de enchufe para montaje en rack

3.1.8 Bandeja para rack

La bandeja para rack presenta una característica de tipo voladiza, esta bandeja nos servirá para colocar los equipos EdgeRouter4 y EdgeSwitch 10X. Además, el estante se monta en múltiples orientaciones con una cresta en un lado para evitar que el equipo se deslice.

Figura 36

Bandeja para rack

Nota. Tomado de la web

3.1.9 Cable UTP

Par trenzado sin blindaje, también conocido como UTP, es actualmente el método más común y básico de construcción de cables, que consiste en pares de cables trenzados entre sí. No hay blindaje, sino que la torsión simétrica de los cables crea una línea de transmisión equilibrada, lo que ayuda a reducir el ruido eléctrico y la interferencia electromagnética. Además, las diferentes tasas de torsión de cada par se pueden usar para reducir la diafonía. En los cables de categoría superior, se puede encontrar un relleno de malla cruzada que separa los pares individuales para ayudar a reducir la diafonía externa de los cables adyacentes.

Actualmente los más usados en la industria de las telecomunicaciones son las que se presentan en la siguiente table, con su respectiva tasa de transferencia y ancho de banda soportado.

Tabla 7

Categorías de cables UTP

Categoría	Tasa de transferencia	Ancho de banda
Cat5	100 Mbit/s	100 MHz
Cat5e	1000 Mbit/s	100 MHz
Cat6	1000 Mbit/s	250 MHz
Cat6a	10000 Mbit/s	500 MHz
Cat7	10000 Mbit/s	1000 MHz
Cat7a	10000 Mbit/s	1200 MHz
Cat8	10000 Mbit/s	2000 MHz

Nota. Elaborado por el autor

En la implementación de la VPN, para conectar las redes entre los enrutadores, controladores y switch, el cable Cat5e cumple con los requerimientos, además de que no hay intenciones de requerir Ethernet más rápido que ocupe más allá de la tasa de transferencia y ancho de banda para los UAP-AC-PRO y LITE

Figura 37

Cable UTP Cat5e

Nota. Tomado de la web

3.1.10 Conector y Jack RJ45

El RJ45 es un tipo de conector comúnmente utilizado para redes Ethernet. Se parece a un enchufe de teléfono, pero es un poco más ancho. Dado que los cables Ethernet tienen un conector

RJ45 en cada extremo, los cables Ethernet a veces también se denominan cables RJ45. También existen jack RJ45 en el mercado como los que se muestran en la siguiente figura.

Figura 38

Conector y jack RJ45

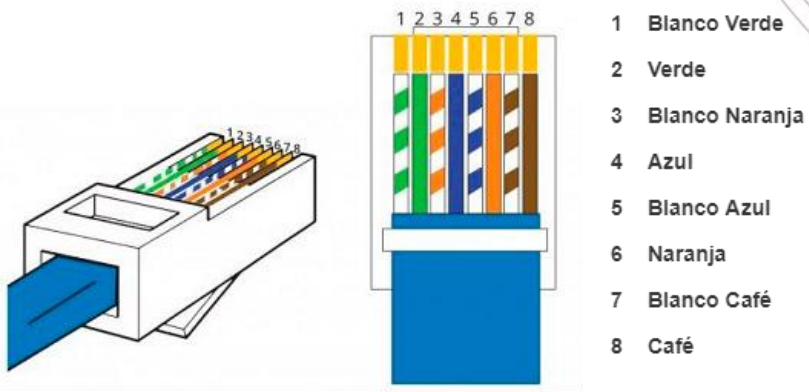
Nota. Tomado de la web

3.1.11 Norma EIA/TIA 568A y EIA/TIA 568B

La norma EIA/TIA 568A y EIA/TIA 568B se refieren a los dos principales estándares utilizados en las industrias de redes y telecomunicaciones. Estos estándares determinan el orden de los cables colocados en un conector RJ45. La única diferencia entre los dos estándares es la colocación de pares de cables en pines fijos, funcionalmente ambos estándares son iguales.

Figura 39

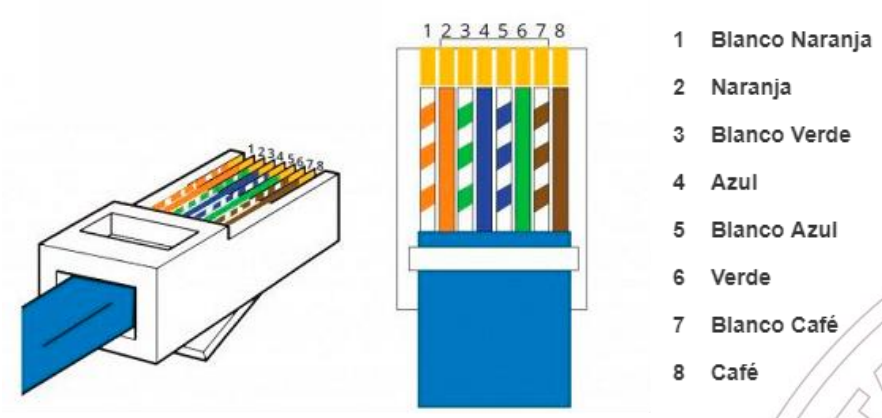
Norma EIA/TIA 568A



Nota. Elaborado por el autor

Figura 40

Norma EIA/TIA 568B



Nota. Elaborado por el autor

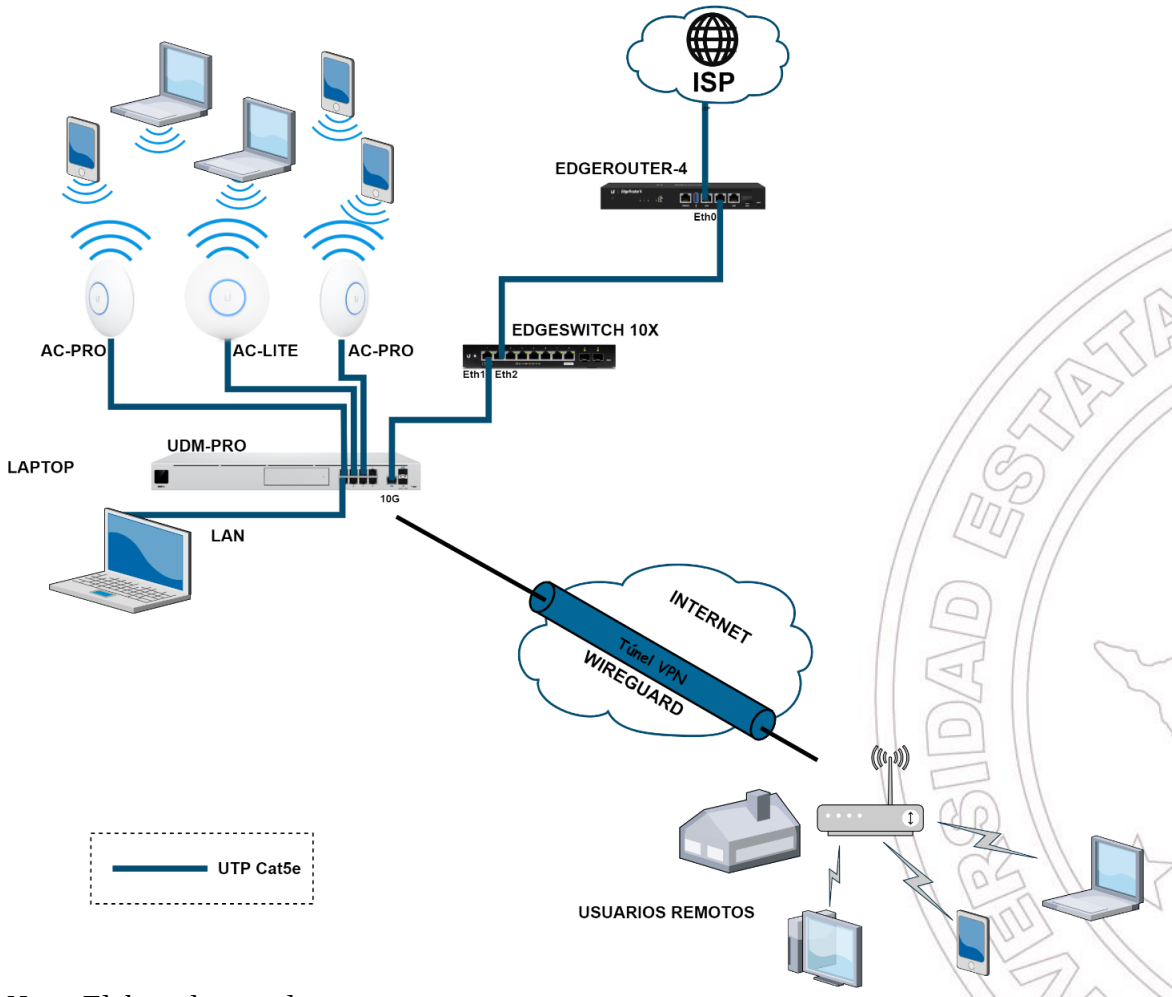
El esquema de cableado de la norma EIA/TIA 568B es, con mucho, el más común, aunque muchos dispositivos también admiten el esquema de cableado EIA/TIA 568A. Algunas aplicaciones de red requieren un cable Ethernet cruzado, que tiene un conector EIA/TIA 568A en un extremo y un conector EIA/TIA 568B en el otro. Este tipo de cable generalmente se usa para conexiones directas de computadora a computadora cuando no hay un enrutador, concentrador o conmutador disponible. La norma que se va a utilizar para la implementación del diseño de la red VPN es la EIA/TIA 568B.

3.2 Diseño VPN Acceso Remoto

La VPN de acceso remoto de la figura#, permite a los estudiantes establecer conexiones seguras con la red interna de la universidad de forma remota al laboratorio de telecomunicaciones. Los universitarios pueden acceder a los equipos de redes conectada a través del UDM-Pro o EdgeRouter-4 de forma segura como si estuvieran conectados directamente a los equipos Ubiquiti. Además, esta red contiene dispositivos terminales como como celulares conectados en las redes WiFi de sus hogares y conectamos a la red interna proporcionada por los Access Points.

Figura 41

Diseño VPN de acceso remoto para el laboratorio de telecomunicaciones



Nota. Elaborado por el autor

En la Figura 41, se muestra el diseño de la topología para el acceso remoto, donde el internet ISP entra al puerto Eth0 del EdgeRouter-4, se realiza un Bridge con un bloque de direcciones 192.168.1.0/24 y este se reparte a través del EdgeSwich-10X que le da acceso de Internet a través de la interfaz WAN1 del UDM-PRO. De igual manera, se crea un bloque de direcciones LAN que serán distribuidas en sus puertos Ethernet, dando direcciones a los dispositivos que se conecten de forma alámbrica o inalámbrica mediante los UAP-AC-PRO y UAP-AC-LITE.

Figura 42

Diagrama de flujo de configuración VPN acceso remoto

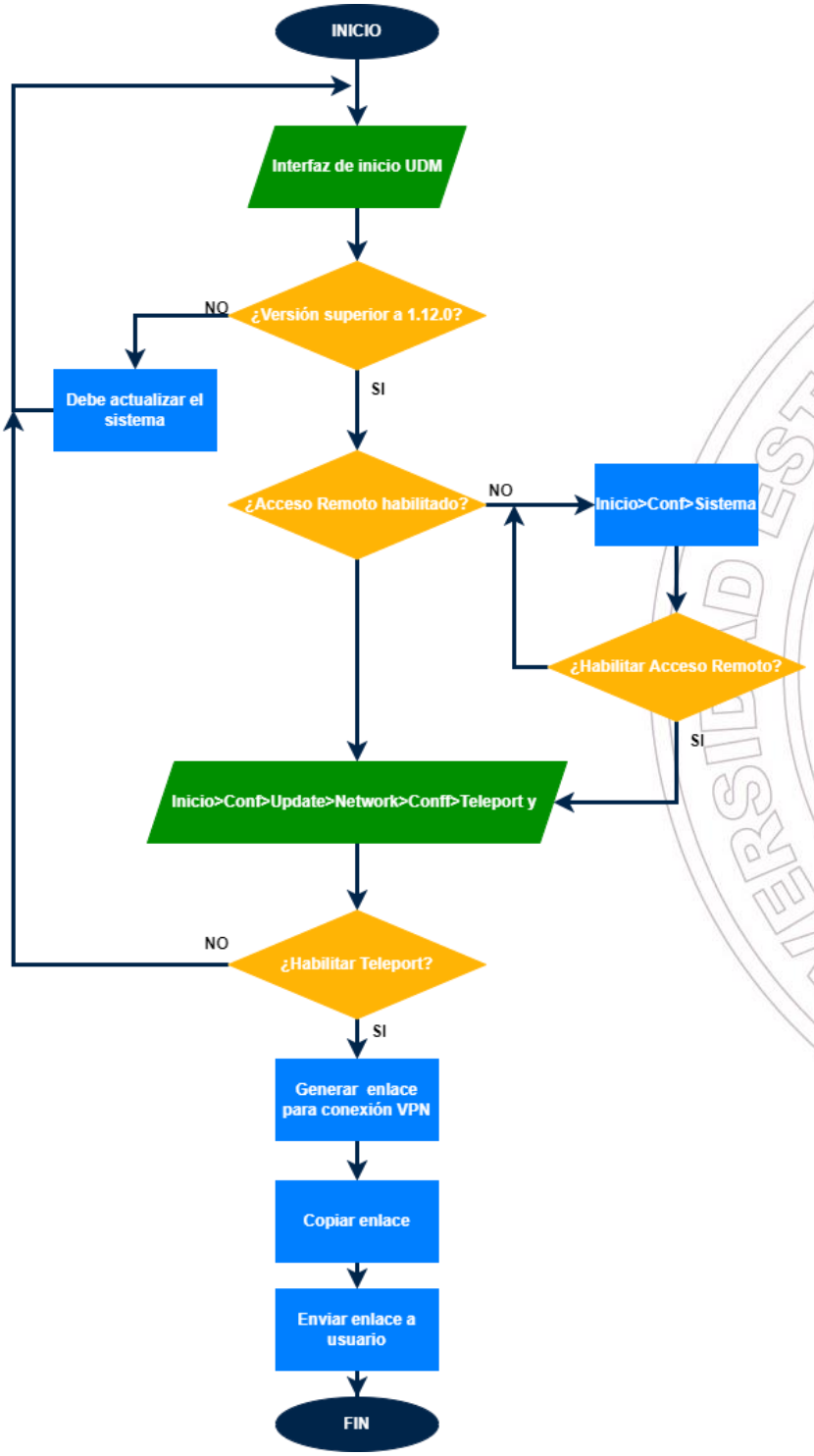
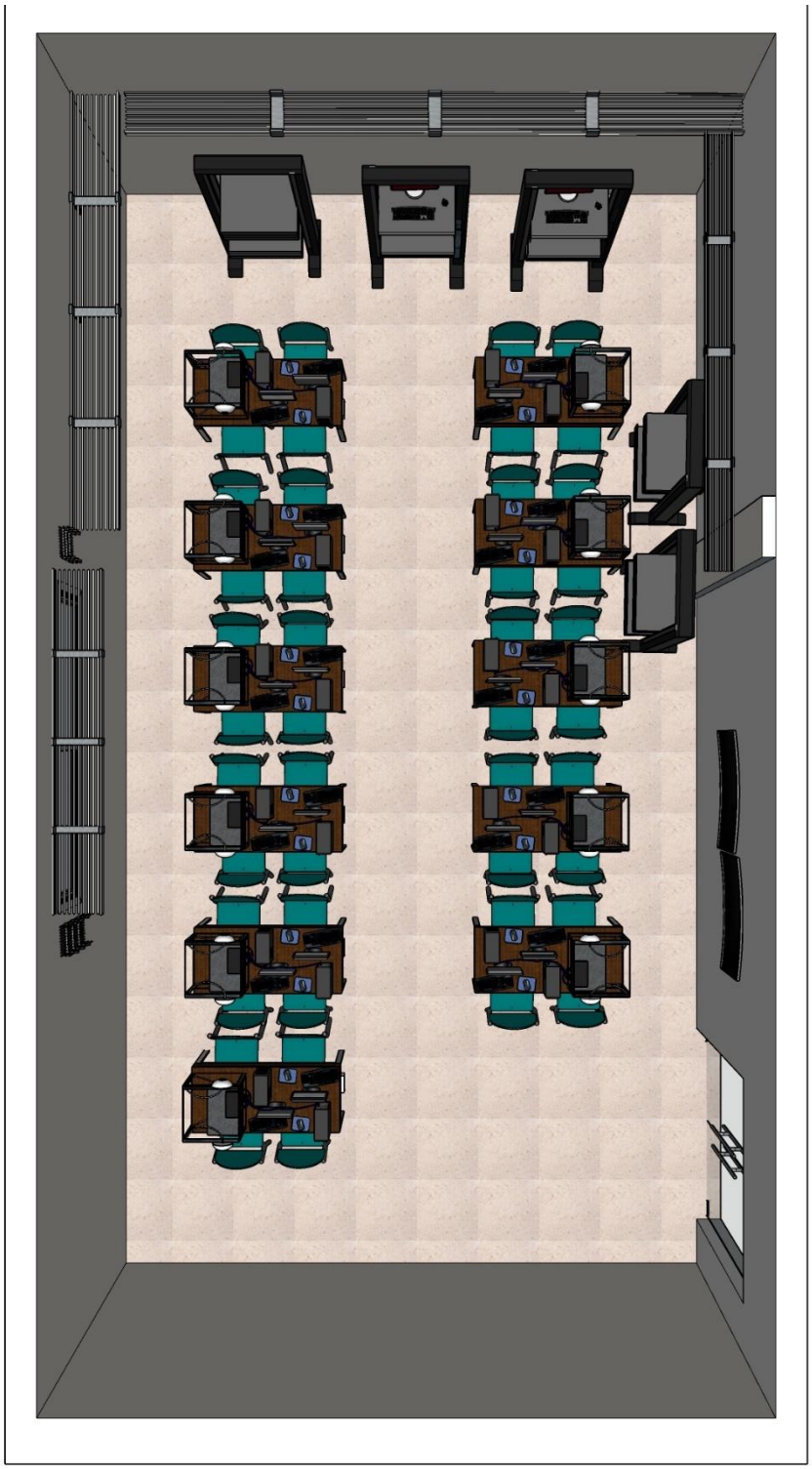


Figura 43

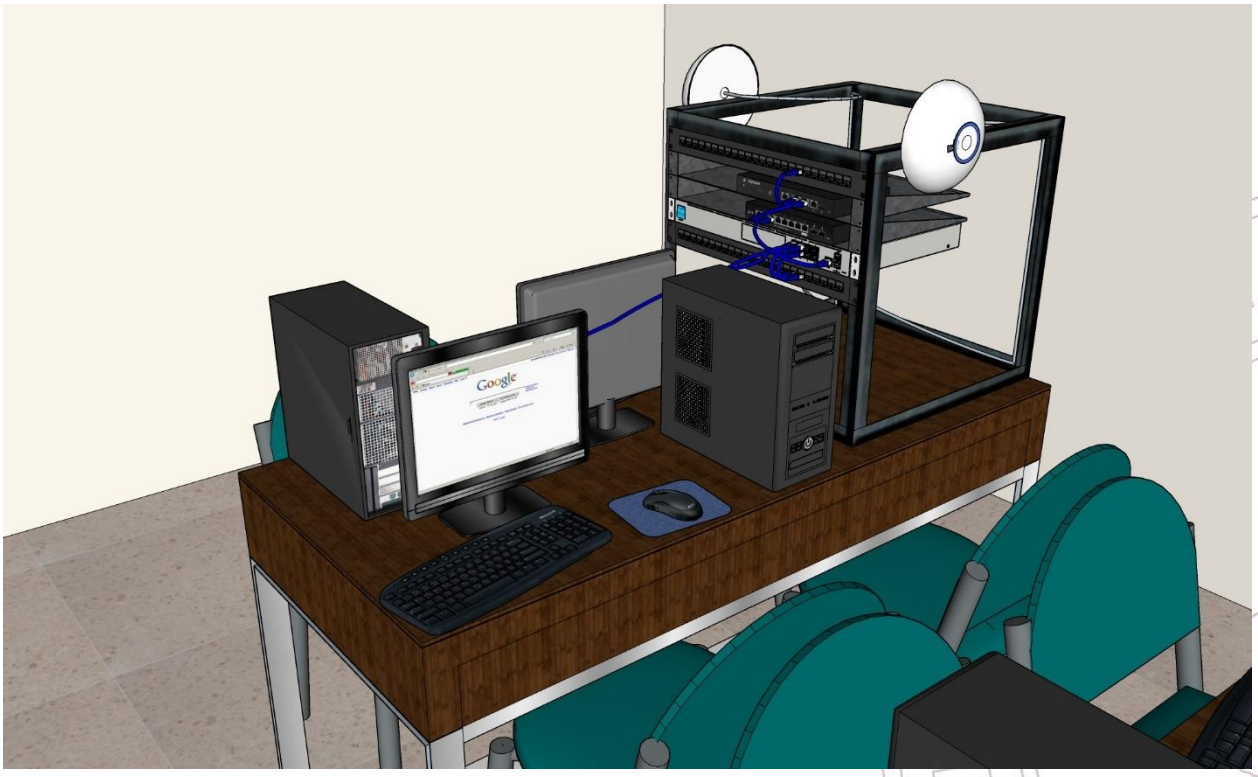
Diseño del laboratorio equipado con Ubiquiti en SketchUp



Nota. Elaborado por el autor

Figura 44

Diseño de la estación de trabajo en SketchUp



Nota. Elaborado por el autor

En la misma figura, en parte posterior se encuentra los usuarios remotos conectando a través del túnel VPN con protocolo WireGuard hacia el UDM-PRO, estos usuarios utilizan dispositivos móviles apoyados de una aplicación que es desarrollada por el mismo proveedor de equipos de la marca Ubiquiti, estos dispositivos tienen que tener sistema operativo Android, iOS o ser equipos Mac OS.

La Figura 42 representa el diagrama de flujos de la configuración para crear la VPN en el UDM-PRO, se detallan diferentes procesos necesarios que debe cumplir el controlador y la obligatoriedad para dar paso a la implementación; en dado caso, si no se cumple con la versión indicada, desde el principio no se puede realizar la configuración, lo recomendable es actualizar a la versión más reciente y que deba ser superior a la señalada.

La Figura 43 muestra cómo sería el escenario del laboratorio de Telecomunicaciones totalmente equipada con 11 estaciones de trabajo debajo de cada bloque donde se reparte el Internet, cada estación de trabajo está compuesto por:

- Un armario de redes pequeño
- Patch panel Cat5e
- Bandejas para rack
- EdgeRouter 4
- UDM-PRO
- EdgeSwitch 10X
- Access Points
- Dos computadores de escritorios

Estos equipos se pueden visualizar en la Figura 44, donde podemos apreciar de cerca la instalación de los equipos con su respectiva conexión con cables UTP Cat5e, cada computador está conectada al UDM-PRO como se quiere demostrar en la topología diseñada, cada Access Point también está conectada al UDM-Pro a través de los adaptadores PoE.

3.2.1 WireGuard en Teleport de la línea UniFi de la marca Ubiquiti

Teleport se lanzó originalmente en 2018 para la línea de productos AmpliFi de Ubiquiti. Pero ahora también está disponible para la consola de red UniFi. UniFi Teleport le permite crear una conexión VPN con un clic desde su dispositivo móvil a la red doméstica.

Como una VPN tradicional, se deberá configurar su red, abrir puertos, crear un nombre de usuario y contraseña, etc., antes de poder establecer una conexión VPN. Con UniFi Teleport, solo necesita crear un enlace de invención en su controlador.

UniFi Teleport permite realizar una conexión VPN a su red doméstica con un solo clic. Utiliza el protocolo WireGuard VPN, que suelen utilizar los grandes proveedores de VPN, como NordVPN o Surfshark.

La diferencia en comparación con estos proveedores de VPN es que con el teletransporte crea un túnel VPN a su red doméstica. Esto es ideal cuando se encuentra en una red inalámbrica pública y si se desea acceder de manera segura a su cuenta bancaria u otra información confidencial.

Con Teleport no solo se puede navegar de forma segura por Internet, sino que también se puede acceder a la red de la universidad. Una vez que haya realizado la conexión VPN, puede acceder a todos los dispositivos de la red del laboratorio estando conectado a la red inalámbrica en el hogar.

UniFi Teleport funciona con un enlace de invitación, este enlace debe generarse en el controlador de red UniFi y solo es válido durante 24 horas. El enlace solo puede ser utilizado por un dispositivo cliente. Por lo tanto, debe crear un enlace de invitación para cada dispositivo al que desee dar acceso.

El túnel VPN se almacena en sus dispositivos móviles después de aceptar el enlace, lo que le permite utilizar la conexión VPN en cualquier momento que desee a través de la aplicación WiFiman.

3.2.2 WiFiman

WiFiman es una aplicación móvil que nos permitirá monitorear el estado de nuestra red WiFi, probar la velocidad de la conexión a Internet y conocer los dispositivos de nuestra red local a los que podemos hacer una serie de pruebas.

Figura 45

WiFiman

Nota. tomado de la web

Es una aplicación del desarrollador y fabricante Ubiquiti que es gratuita y libre de publicidad. Gracias a WiFiman y sus herramientas podremos realizar las siguientes acciones:

- Descubre las redes WiFi disponibles y los dispositivos Bluetooth LE.
- Analiza una red inalámbrica, tiene soporte WiFi 6 y un medidor de intensidad de señal.
- Realiza la prueba de velocidad WiFi.
- Viene equipado con un escáner de red para el descubrimiento de dispositivos.
- Escanea las subredes de la red para obtener detalles adicionales sobre los dispositivos descubiertos.
- Dispone de un escáner de puertos que nos indicará cuáles tenemos abiertos.

Como podemos constatar, nos permitirá realizar una serie de pruebas con las que podremos diagnosticar si tenemos algún problema en nuestra red WiFi.

3.2.3 Requisitos para UniFi Teleport

Hay un par de requisitos en este momento antes de que pueda usar la función Teleport en la red UniFi en el laboratorio de telecomunicaciones. No todas las consolas UniFi OS son compatibles, solo los siguientes modelos pueden ejecutar Teleport:

- Dream Machine
- Dream Router
- Dream Machine Pro
- Dream Machine Pro SE

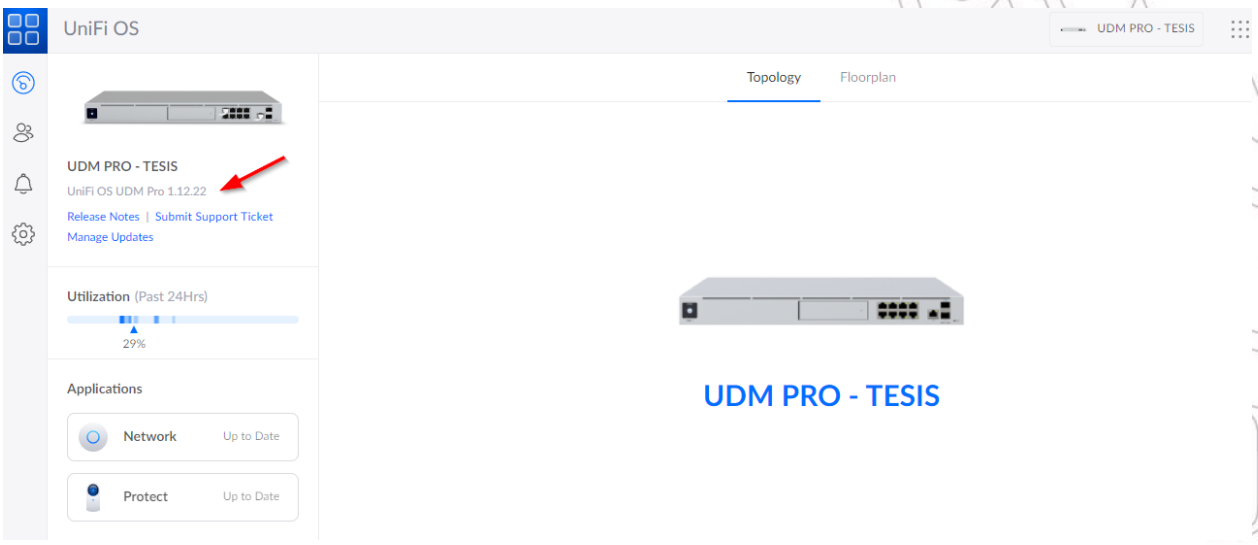
También deberá ejecutar el último firmware de UniFi OS Console, 1.12.0 (Figura), o posterior para Dream Machine y Dream Machine Pro. Y la versión 2.4.0 o posterior para Dream Router y Dream Machine Pro SE.

3.2.4 Configuración de la VPN WireGuard a través de Teleport

Para verificar la versión de su consola, simplemente puede abrir su Consola UniFi OS y encontrar la versión en el tablero debajo del nombre de su consola en la esquina superior izquierda.

Figura 46

Firmware de UniFi OS Console



Nota. Elaborado por el autor

Otros requisitos para Teleport son:

- Red UniFi 7.1 o posterior

- Acceso remoto habilitado en UniFi OS
- Aplicación móvil WiFiman (Android / iOS)

Para verificar si está ejecutando la última versión de la red UniFi, necesitaremos abrir la consola del sistema operativo UniFi y navegar a la configuración.

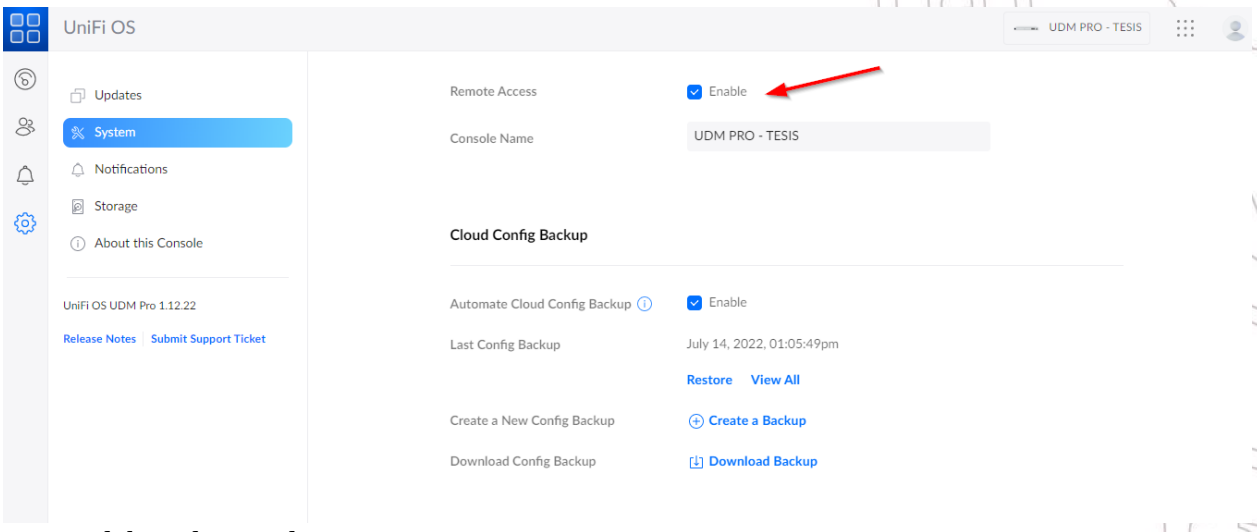
Aquí verá todas las aplicaciones UniFi que se ejecutan en su consola. Asegúrese de que la aplicación Red esté ejecutando la versión 7.1 o superior. Si está ejecutando una versión anterior, asegúrese de que esté actualizada.

3.2.4.1 Configuración de la VPN

El acceso remoto a la consola UniFi debe estar habilitado para usar Teleport. Puede habilitar el acceso remoto en UniFi OS en Configuración > Sistema.

Figura 47

Habilitar acceso remoto en UniFi OS



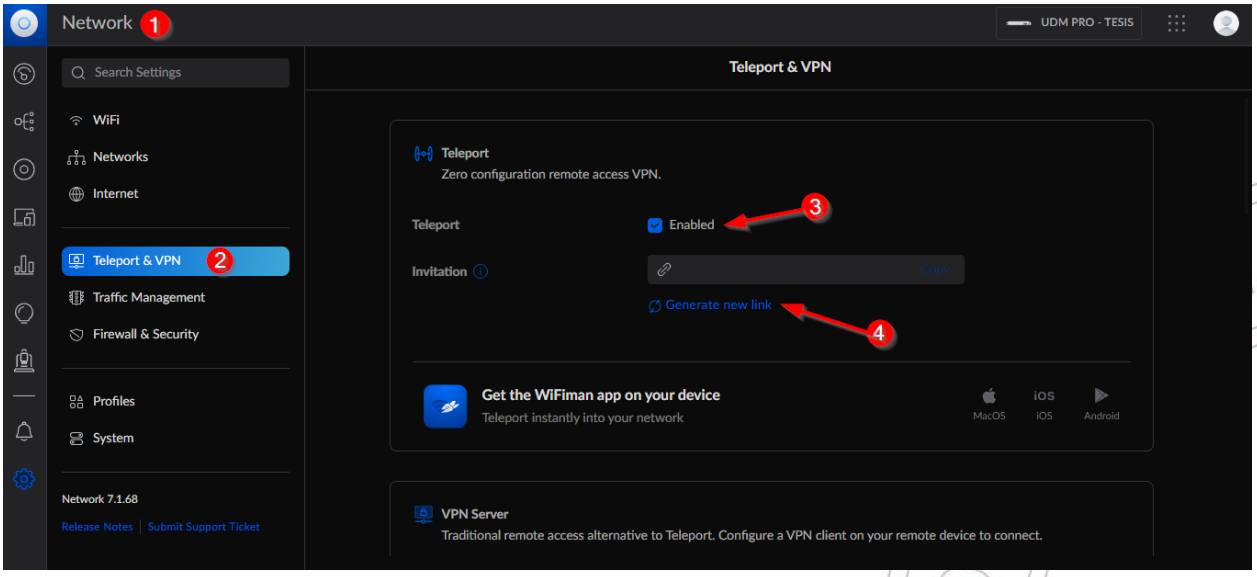
Nota. Elaborado por el autor

3.2.4.2 Habilitar Teleport UniFi

Habilitar Teleport es realmente fácil después de asegurarse de que todo esté actualizado. Todo lo que tenemos que hacer es habilitar la función en la aplicación UniFi Network.

Figura 48

Habilitación de Teleport



Nota. Elaborado por el autor

(1) Abra el controlador de red UniFi

(2) Ir a Configuración > Teletransporte y VPN

(3) Habilitar teletransporte

Solo necesita generar un nuevo enlace de invitación (4) después de haber habilitado Teleport. Tener en cuenta que el enlace caduco después de 24 horas. Copiar el enlace y enviar a su dispositivo móvil, por ejemplo.

3.2.4.3 Configuración Teleport UniFi

Para usar UniFi Teleport en su dispositivo móvil, por ejemplo, primero deberá obtener el enlace de invitación. Si abre el enlace, lo llevará a una pina de introducción donde puede descargar la aplicación WiFiman.

Figura 49

Configuración Teleport en Android

Nota. Elaborado por el autor

La aplicación se puede encontrar en la tienda Play Store para Android y App Store para iOS, la siguiente figura muestra la aplicación WiFiman desde Play Store donde se procederá a realizar la siguiente descarga.

Figura 50

WiFiman en Play Store

Nota. Elaborado por el autor

Figura 51

Mensaje de bienvenida WiFiman

Nota. Elaborado por el autor

La Figura 51 nos muestra un mensaje de bienvenida. WiFiman presenta unas opciones para obtener información del entorno de red en el lugar que estemos situados; es decir, brinda detalles

de puntos de red cercanos y dispositivos Bluetooth. Daremos en la opción solicitar permisos de ubicación.

Figura 52

Opción de test de velocidad de dispositivos

Nota. Elaborado por el autor

WiFiman también nos proporciona funcionalidades para realizar test de velocidades de forma gratuita, incluso entre dispositivos para conocer el upload y download entre ellos.

Al seleccionar “cerrar” al paso de la figura, nos muestra la interfaz de la Figura 53 que está compuesta por tres elementos: Internet, Puerta de enlace, Redmi Note 9 Pro (dispositivo utilizado para las pruebas)

El Internet es la dirección que observamos debajo de Internet, representa la IP Pública de la universidad. La puerta de enlace o Gateway, sirven como puntos de salida y entrada para los datos que viajan entre redes y se utilizan para conectar diferentes redes mediante protocolos de transmisión. La dirección del dispositivo móvil es la que le brinda la puerta de enlace.

Dirección: Campus matriz, La Libertad - prov. Santa Elena - Ecuador
Código Postal: 240204 - Teléfono: (04) 781732 ext 131
www.upse.edu.ec
upse_ec @upse_ec upse_ec UPSESantaElena

Figura 53

Direcciones visualizadas en WiFiman sin VPN

Nota. Elaborado por el autor

La siguiente acción consiste en seleccionar la opción Teleport, esta se encuentra situada en la parte inferior de la interfaz de WiFiman.

Figura 54

Ubicación de Teleport en la interfaz WiFiman

Nota. Elaborado por el autor

Figura 55

Acceso a la VPN por Teleport

Nota. Elaborado por el autor

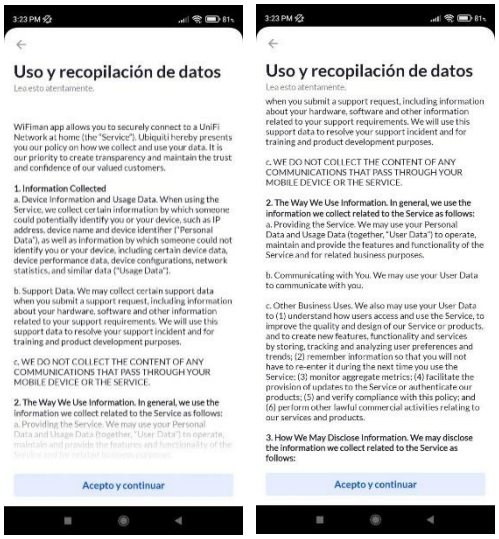
Al seleccionar “Conectar” nos muestra unos términos donde menciona que la aplicación WiFiman le permite conectarse de forma segura a una red UniFi en casa. Ubiquiti nos presenta la política sobre cómo recopila y usa nuestros datos. Haciendo hincapié a la prioridad de crear transparencia y mantener la confianza de sus valiosos clientes, donde:

1. Información recopilada. Al usar el Servicio, se recopila cierta información como su dispositivo, la dirección IP, el nombre del dispositivo y el identificador del dispositivo ("Datos personales"), así como información mediante la cual alguien no podría identificarlo a usted o a su dispositivo.

2. La forma en que usamos la información. En general, usa la información que se recopila relacionada con el Servicio.

Figura 56

Términos de uso y recopilación de datos



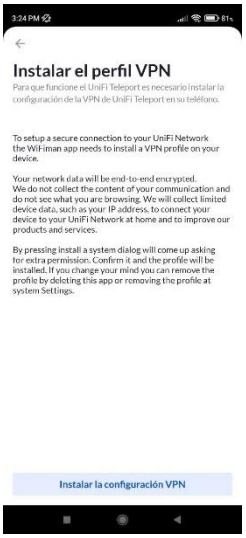
Nota. Elaborado por el autor

Luego de aceptar los términos y condiciones, se nos muestra una ventana para instalar el perfil VPN en el dispositivo, donde los datos de la red se cifrarán de extremo a extremo, se recopila los datos limitados del dispositivo, como la dirección IP.

Al presionar instalar, aparecerá un cuadro de diálogo del sistema solicitando un permiso adicional como se muestra en la figura. Confírmelo y se instalará el perfil.

Figura 57

Instalar el perfil VPN



Nota. Elaborado por el autor

Figura 58

Aceptación para la solicitud de conexión

Nota. Elaborado por el autor

Luego de aceptar la conexión, se estará estableciendo la conexión entre el WiFiman con el "UDM PRO – TESIS", este proceso tiende a durar unos segundos porque se está realizando el respectivo intercambio de claves de cifrado.

Figura 59

Estableciendo conexión de la VPN

Nota. Elaborado por el autor

Figura 60

Conexión VPN entre el móvil y el UDM

Nota. Elaborado por el autor

En la Figura 60, nos muestra el tiempo conectado a través de la VPN, de la misma forma se evidencia un cambio de direccionamientos IP, los cuales son mostrados en la siguiente tabla:

Tabla 8

Direcciones IP luego de establecer la conexión VPN

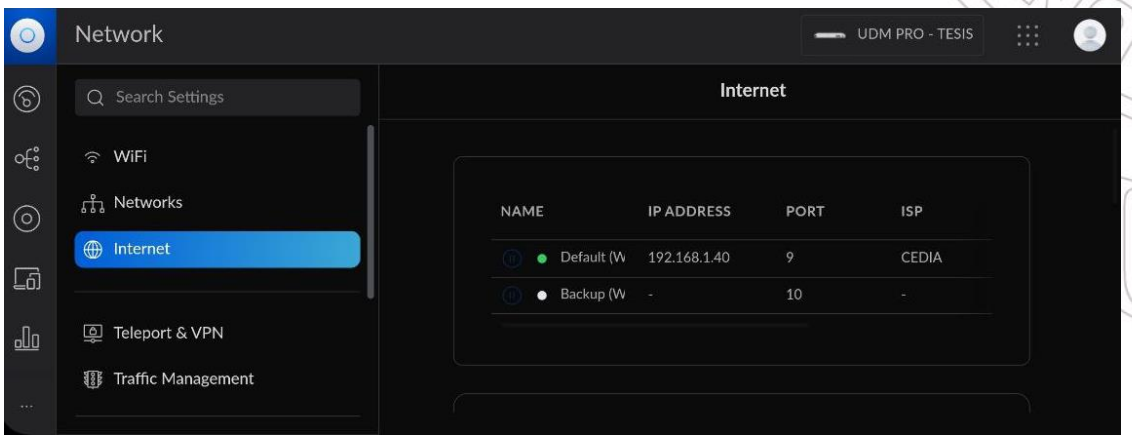
	Sin VPN	**Con VPN**
IP Pública	190.151.30.25	190.151.130.24
Gateway	192.31.0.1	192.168.1.40
IP dispositivo móvil	192.31.1.21	192.168.2.2

Nota. las direcciones proporcionadas fueron obtenidas en la universidad

Como se puede apreciar en la tabla, la dirección IP Pública no tiende a cambiar, ya que se está utilizando la red universitaria que tiene como proveedor a la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia. CEDIA. Al aplicarse la VPN a través de Teleport que usa el protocolo WireGuard, el Gateway toma la dirección que le proporciona en la WAN del UDM Pro como se muestra en la figura, que es asignado por el EdgeRouter 4, que maneja una segmentación DHCP en sus puertos LAN de 192.168.1.1/24 figura

Figura 61

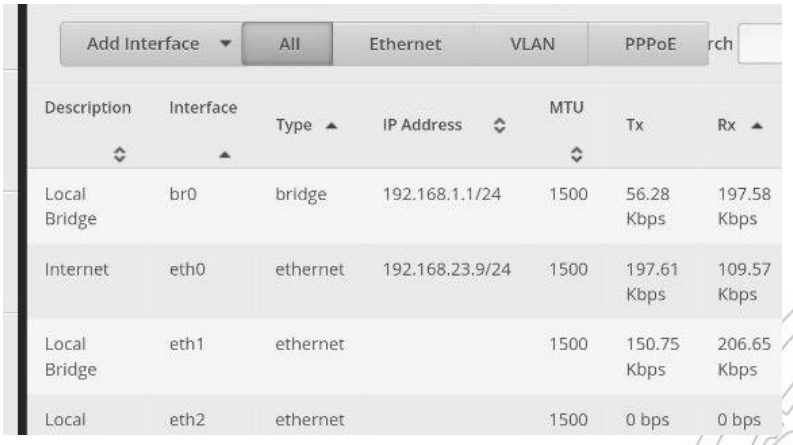
Dirección WAN en el puerto 9 del UDMPro



Nota. Elaborado por el autor

Figura 62

IP proporcionado a través del bridge en el EdgeRouter-4

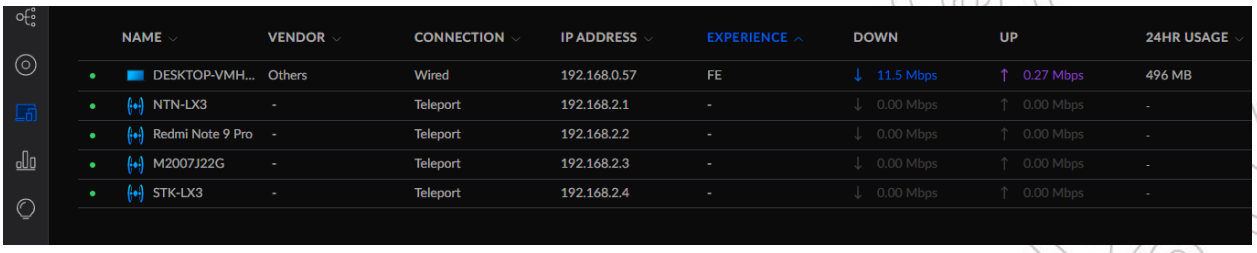


Nota. Elaborado por el autor

Del mismo modo, el controlador UDM Pro asigna direcciones IP a los equipos que se conectan a la VPN por medio del Teleport, estas direcciones comprenden la red 192.168.2.0

Figura 63

IP asignada a la VPN por medio de Teleport



Nota. Elaborado por el autor

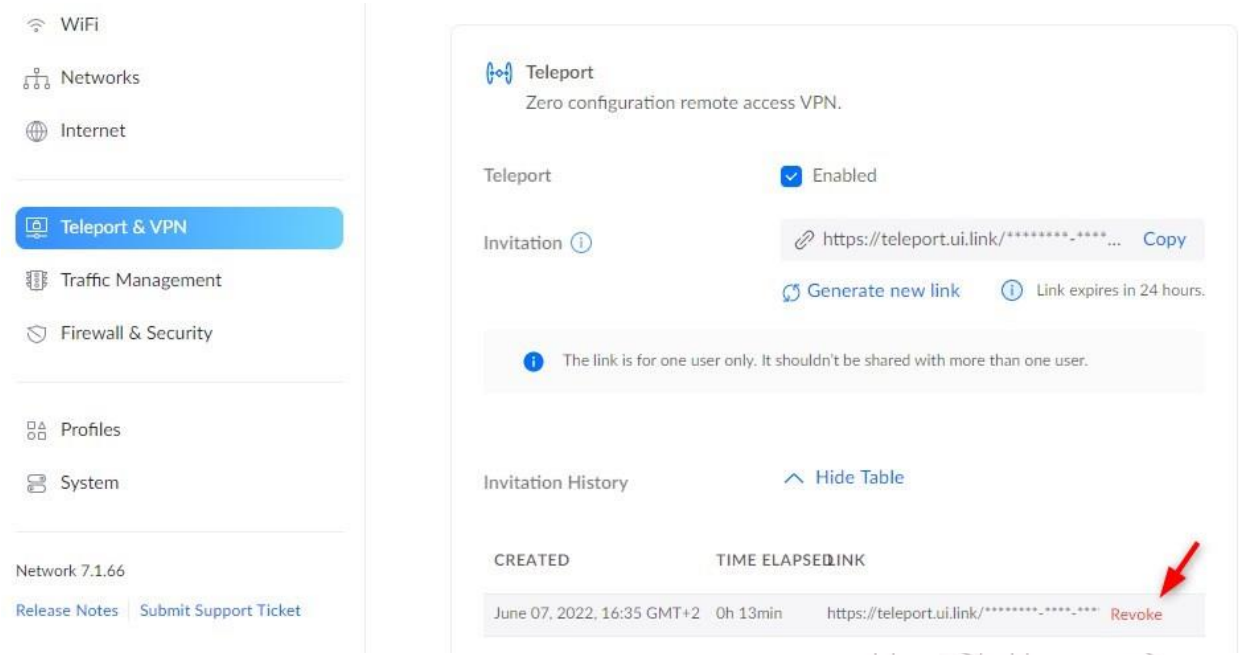
3.2.5 Revocación del acceso a Teleport

Hay dos formas de revocar el acceso a la aplicación de teletransporte. El método depende del estado de la invitación. Cuando ya se haya aceptado la invitación, deberá ir a Dispositivos cliente en la aplicación de red y revocar el acceso.

Si la invitación aún no se ha aceptado, puede revocar la invitación desde la pantalla de configuración de Teleport.

Figura 64

Revocación de acceso VPN



Nota. Elaborado por el autor

UniFi Teleport es una excelente manera de configurar y establecer fácilmente una conexión VPN a través de la red doméstica. Solo asegúrese de que su aplicación UniFi OS y Network estén actualizadas para usar esta función.

Culminado el proceso de configuración de la VPN en el UDM Pro como el acceso remoto a través del dispositivo telefónico, se deben realizar las pruebas realizando diversos tipos de configuraciones desde un sitio remoto fuera de la universidad.

3.3 Estudio de Factibilidad y Costos de la Propuesta

3.3.1 Factibilidad Técnica

La factibilidad técnica de esta propuesta de implementación dada las circunstancias que representa el proceso de enseñanza-aprendizaje para adquirir las experiencias adquiridas en las prácticas de laboratorio y que servirán para el campo laboral de las Telecomunicaciones, usando

un mecanismo de control de equipos a través de una VPN, salvaguardando la seguridad de la Intranet de la UPSE, se puede demostrar su viabilidad en aporte a la mejora de la educación. Se implementó una red compuesta por equipos de la línea Edge y UniFi de la marca Ubiquiti para llevar a cabo el diseño e implementación de la Red Privada Virtual que usa el protocolo WireGuard dentro de la interfaz Teleport que nos brinda el UDM-PRO.

Los equipos del laboratorio de telecomunicaciones como Mikrotik, TpLink, a pesar de que se encuentran en muy buenas condiciones, tienen años de uso y han sido manipulados por los estudiantes para obtener conocimiento; sin embargo, con el avance de la tecnología se requiere de innovación y al abrirse la carrera netamente para el área de las Telecomunicaciones, es necesario que se adquieran equipos de redes empresariales que son usados mayormente por los ISP a nivel mundial, con ello también se busca estar a la vanguardia de la tecnología y que sean manipulados de forma presencial o remotamente desde cualquier sitio del país.

En cuanto a la conexión de los equipos, para la comunicación física de los equipos de redes se utilizó el cable de categoría 5e, analizado anteriormente para dar una mejor tasa de transferencia en cuanto a ancho de banda, de igual manera el estándar 802.3af para los Access Points UniFi utilizados para brindar conexión inalámbrica a los usuarios finales; en definitiva, se utilizaron las respectivas normas y estándares a nivel mundial como la ANSI/TIA/EIA, los cuales han sido estudiados a lo largo de la carrera de Ingeniería en Telecomunicaciones.

La empresa Ubiquiti desarrolla avances tecnológicos, esto incluye actualizaciones de software e innovaciones en sus productos, por lo cual es uno de los pocas marcas del mercado que ofrece servicio de VPN de tipo Open Source ya instaladas, que a la misma vez, tienen a desarrolladores encargados de mejorar este servicio brindando la seguridad y confiabilidad que se requiere para este tipo de redes; de igual forma, al ser equipos altamente empresariales, se pueden

realizar diferentes configuraciones a través de una interfaz gráfica intuitiva y fácil de operar teniendo los conocimientos necesarios en redes de telecomunicaciones.

3.3.2 Costos de la Propuesta

La finalidad de realizar esta factibilidad económica al presente proyecto, conlleva a saber los valores que intervienen en el diseño de la VPN para su implementación y demostración de funcionamiento; del mismo modo, se detallan los herramientas y materiales que se utilizaron para el armado de la estación de rack en el laboratorio. La siguiente tabla muestra el costo de los equipos.

Tabla 9

Costo de equipos

Cantidad	Descripción	Marca	P. Unidad	P. Total
1	EdgeRouter 4	Ubiquiti	$130.00	$130.00
1	EdgeSwitch 10X	Ubiquiti	$110.00	$110.00
1	Dream Machine Pro	Ubiquiti	$360.00	$360.00
3	Acces Point UniFI	Ubiquiti	$100.00	$300.00
TOTAL				$900.00

Nota. Elaborado por el autor

De igual forma, se detalla en la siguiente tabla, los materiales que se utilizaron para la elaboración de la propuesta tecnológica.

Tabla 10

Costos de materiales

Cantidad	Descripción	P. Unidad	P. Total
1	Rack	$0.00	$0.00
1	Pach Panel Cat5e	$0.00	$0.00
1	Regleta de enchufe	$0.00	$0.00
2	Bandeja para rack	$0.00	$0.00

10m	Cable Cat5e	$0.00	$0.00
1	Jack RJ45 para Patch Panel	$0.00	$0.00
24	Conector RJ45	$0.15	$3.60
Total			$3.60

Nota. los precio de $0.00 representan a los materiales existentes en el laboratorio, por lo tanto, no se realizó un gasto por la compra.

Para la instalación de los equipos y el proceso de ponchar y pelar los cables se utilizaron los materiales presentados en la siguiente tabla:

Tabla 11

Lista de herramientas

Cantidad	Descripción
1	Destornillador
1	Alicate
1	Flexómetro
1	Ponchadora
1	Ponchadora de impacto

Nota. La lista contiene herramientas prestados y de disponibilidad propia

En la siguiente tabla se muestra el costo final; es decir, la suma de los costos de equipos y los costos por materiales. Teniendo ser un valor de referencia para la implementación de este proyecto.

Tabla 12

Costo final

Descripción de costos	Valor
Costos de equipos	$900.00
Costos de materiales	$3.60
Total de Costo Final	$903.60

Nota. Elaborado por el autor

3.4 Pruebas

En esta sección se realizarán pruebas de configuraciones como el acceso a través del navegador del dispositivo celular para entrar a la interfaz del UDM Pro y del EdgeRouter 4, de igual forma, se realiza una configuración de gestión de DPI para los dispositivos controlados por el UDM Pro.

Para realizar esta prueba, se establecen 4 lugares diferentes en la provincia de Santa Elena, estos lugares serán los sitios remotos y el Laboratorio de Telecomunicaciones será el lugar donde se va a establecer la conexión VPN. La siguiente tabla muestra las coordenadas de cada dispositivo móvil.

Tabla 13

Coordenadas de cada usuario remoto

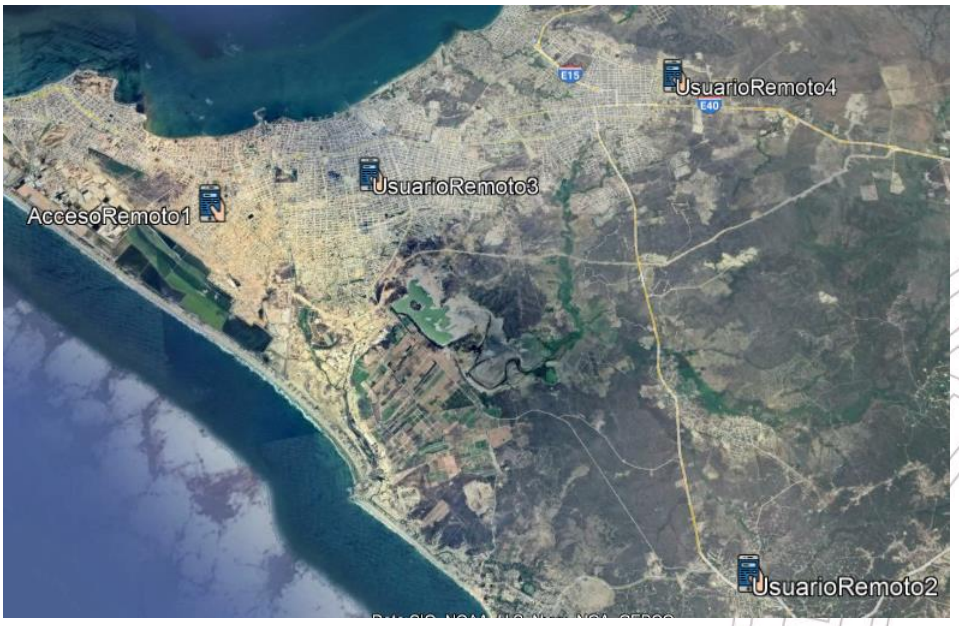
	Latitud	**Longitud**
Usuario1	2°14'7.60"S	80°56’00.3”W
Usuario2	2°19'06.3"S	80°51'06.2"W
Usuario3	2°14'05.5"S	80°54'13.2"W
Usuario4	2°13'29.1"S	80°50'37.3"W
Laboratorio	2°14'1.96"S	80°52'50.33"W

Nota. Elaborado por el autor

La siguiente figura muestra la ubicación de los sitios remotos

Figura 65

Ubicación del sitio remoto



Nota. Tomado de Google Earth Pro

Por otra parte, la Universidad Estatal Península de Santa Elena se encuentra ubicada en la Avda. principal La Libertad - Santa Elena, La Libertad con coordenadas 2°14′00″S 80°52′40″O, el laboratorio de Telecomunicaciones se encuentra ubicado por los siguientes componentes de vector 2°14'1.96"S 80°52'50.33"W

Figura 66

Ubicación del laboratorio de Telecomunicaciones

Nota. Tomado de Google Earth Pro

Se mide la distancia de los Accesos Remotos y el Laboratorio de Telecomunicaciones, de los cuales se obtiene la siguiente table

Tabla 14

Distancia de Accesos Remotos al Laboratorio

	Usuario1	**Usuario2**	**Usuario3**	**Usuario4**
Distancia	5,87Km	9,89Km	2,56Km	4,24Km

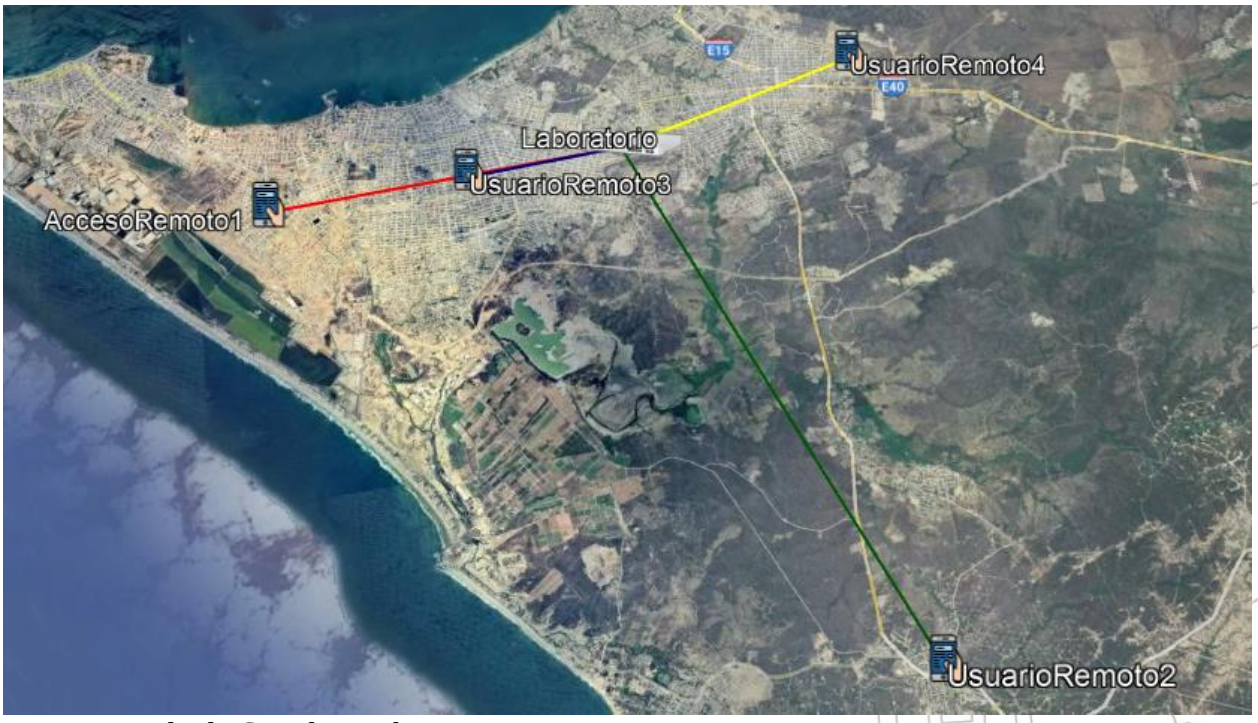
Nota. Elaborado por el autor

La distancia de 9,89Km está situada en la parroquia San José de Ancón, le sigue la distancia 5,87Km que está situada en el cantón Salinas; por consiguiente, la menos corta es de 4,24Km en Santa Elena y la más corta comprende de 2,56Km situado en el cantón de La Libertad.

Al analizar estos parámetros de distancia, podemos analizar que la movilización en transporte no es directa hacia su destino (laboratorio), por lo que tomaría más tiempo en llegar al establecimiento académico.

Figura 67

Distancia entre los Accesos Remotos y el Laboratorio



Nota. Tomado de Google Earth Pro

El dispositivo celular a usar en el Acceso Remoto tiene las siguientes características presentadas en la siguiente tabla:

Tabla 15

Características del dispositivo móvil de cada usuario

Características	Usuario1	Usuario2	Usuario3	Usuario4
Marca	Xiaomi	One Plus	Xiaomi	Huawei
Modelo	Redmi Note 9 Pro	NTN-LX3	Redmi Note 9 T	Poco X3
ISP del hogar	CNT	CNT	CNT	CONECEL S.A.
WiFiman	Instalado	Instalado	Instalado	Instalado
UniFi Network	Instalado	Instalado	Instalado	Instalado

Nota. Elaborado por el autor

Antes de realizar la conexión VPN verificamos las IP que nos detalla el aplicativo WiFiman, estos datos se muestran en la Figura 68 y las demás capturas de los otros usuarios se encuentran en el Anexo 6.

Figura 68

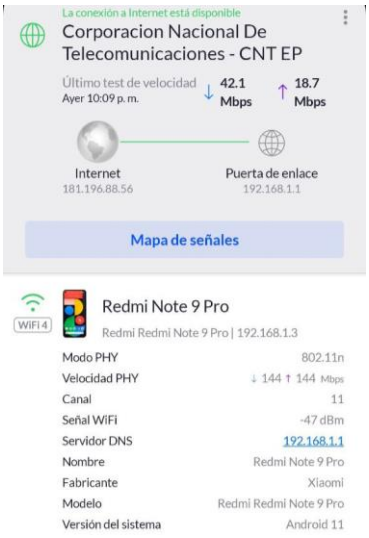
Direcciones proporcionadas del Acceso Remoto

Nota. Elaborado por el autor

En la parte inferior de la aplicación WiFiman se encuentra una opcion de estado, en donde nos brinda algunos detalles técnicos del dispositivo móvil, estos parámetros se encuentran en la siguiente figura

Figura 69

Detalles técnicos del dispositivo móvil



Nota. Elaborado por el autor

Procedemos a realizar la respectiva conexión VPN y verificamos los cambios que se pueden observar en la Figura 70 y Figura 71.

Figura 70

Conexión VPN del Acceso Remoto y Laboratorio

Nota. Elaborado por el autor

Antes de realizar la conexión VPN, se realiza la siguiente taba donde se presentan los parámetros de cada usuario, con el fin de visualizar los cambios que se generan luego de realizar la conexión VPN.

Tabla 16

Parámetros de cada usuario antes de la VPN

Parámetros	Usuario1	Usuario2	Usuario3	Usuario4
IP Pública	181.196.88.56	181.211.217.9	181.196.88.92	200.7.246.49
IP del móvil	192.168.1.3	192.168.1.52	192.168.1.3	192.168.178.50
Servidor DNS	192.168.1.1	192.168.1.1	192.168.1.1	192.168.178.113
Modo PHY	802.11n	802.11n	802.11n	---
Velocidad PHY	↓ 144 ↑ 144 Mbps	↓ 72 ↑ 72 Mbps	↓ 72 ↑ 72 Mbps	72 Mbps
Canal	11(20Mhz)	3(20Mhz)	3(20Mhz)	13(20Mhz)
Señal WIFI	-47dBm	-67dBm	-53 dBm	-47 dBm

Nota. Elaborado por el autor

A continuación, se crean los enlaces para el acceso VPN que se detallan en la siguiente tabla, estos enlaces tienen una duración de 24 horas.

Tabla 17

Enlaces VPN para cada usuario

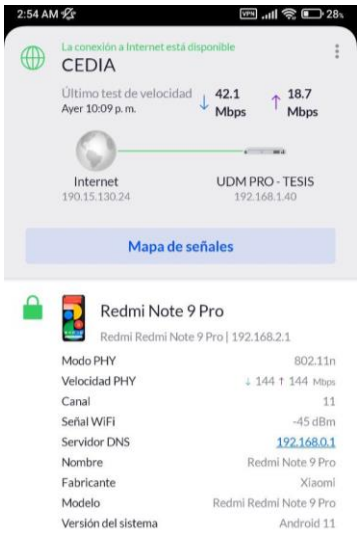
Cliente	Llave pública
Usuario1	https://teleport.ui.link/b8c80b11-da8d-40a4-a511-8fc8425bd065
Usuario2	https://teleport.ui.link/c9486327-9d54-4d5f-ba17-ceb6f37b19fe
Usuario3	https://teleport.ui.link/b91c8b5c-61a6-4b80-b70b-c56cdc293362
Usuario4	https://teleport.ui.link/39ac4c5d-b7bb-4a09-b1f6-4fc96b1223bc

Nota. Elaborado por el autor

Los usuarios proceden a establecer la conexión VPN de los cuales se genera la siguiente tabla, las figuras de las capturas generadas por los demás dispositivos están en el Anexo 2.

Figura 71

Detalles técnicos del dispositivo móvil al establecer el túnel VPN



Nota. Elaborado por el autor

De las siguientes figuras en donde se muestran los detalles técnicos, podemos realizar la siguiente tabla para su respectiva comparación:

Tabla 18

Detalles técnicos al establecer la VPN

Parámetros	Usuario1	Usuario2	Usuario3	Usuario4
IP Pública	190.15.130.24	190.15.130.24	190.15.130.24	190.15.130.24
IP del móvil	192.168.2.1	192.168.2.2	192.168.2.3	192.168.2.4
Servidor DNS	192.168.0.1	192.168.0.1	192.168.0.1	192.168.0.1
Modo PHY	802.11n	802.11n	802.11n	---
Velocidad PHY	↓ 144 ↑ 144 Mbps	↓ 72 ↑ 72 Mbps	↓ 72 ↑ 72 Mbps	72 Mbps
Canal	11(20Mhz)	3(20Mhz)	3(20Mhz)	13(20Mhz)
Señal WIFI	-45dBm	-60dBm	-47 dBm	-47 dBm

Nota. Se analizan los parámetros técnicos más relevantes

De la tabla podemos se puede constatar que la IP Pública de los ISP de cada usuario cambia al establecer la conexión VPN, y esta toma la dirección IP Pública de la Universidad Estatal Península de Santa Elena 190.15.130.24. Por otra parte, el Usuario4 accede al internet a través de datos móviles de la operadora Claro (CONECEL), teniendo una IP Pública de 200.7.246.49. De igual manera la dirección IP del dispositivo electrónico toma la dirección que se le asigna a la interfaz de red cuando se conecta a la VPN, en este caso la dirección 192.168.2.1 para Usuario1, 192.168.2.2 para Usuario2, 192.168.2.3 para Usuario3 y 192.168.2.4 para Usuario4; del mismo modo, la dirección del servidor DNS cambia y toma la dirección que le brinda el EdgeRouter 4 al UDM Pro que es 192.168.0.1.

El modo PHY nos muestra la cobertura sobre los protocolos 802.11 que están presentes en el área de escaneo, en este caso el protocolo 802.11n, la velocidad subida y bajada no varía en la tabla comparativa. Por lo tanto, el uso de este protocolo hace referencia al uso de Wi-Fi 4, es decir, estos dispositivos tienen la tecnología para usar dos frecuencias como: 2,4 GHz y 5 GHz, con velocidades que pueden alcanzar hasta los 600 Mbps.

Del mismo modo, se encuentra la velocidad de internet con la cual operan los dispositivos electrónicos que usan el protocolo 802.11n o Wi-Fi 4, para el Usuario1 esta comprende de 144Mbps de subida y bajada, mientras que para el Usuario 2 y Usuario3 tienen una velocidad de subida y bajada de 72Mbps; el Usuario 4 al utilizar datos móviles, la velocidad con la que navega este dispositivo es de 72Mbps.

La banda de 2,4GHz tiene un ancho de banda disponible limitado. Si bien es cierto, se enumera 11 canales diferentes, cada canal tiene solo unos 5MHz de ancho. Además, el Wi-Fi necesita un mínimo de 20MHz. Por lo tanto, se puede observar que los equipos electrónicos usan diferentes canales y con el mínimo de 20MHz requerido. Por otra parte, para el Usuario4 al usar internet por datos móviles, el canal 13 se debe a que esta operadora está usando la frecuencia VHF.

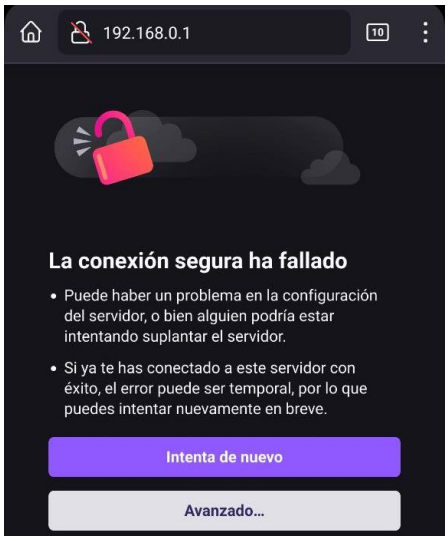
El lo que corresponde a la señal Wi-Fi, esta no tiende a variar, ya que el uso de la VPN al ser de Open Source no genera algún retardo y no se puede visualizar alguna lentitud mientras se navega por internet.

3.4.1 Acceso al UDM Pro a través de la VPN

Estando conectados a la VPN nos dirigimos a nuestro navegador preferido, en este caso, intentaremos acceder a la interfaz de UDM Pro con la siguiente dirección IP 192.168.0.1 como se muestra en la siguiente figura:

Figura 72

Acceso al UDM Pro a través del navegador

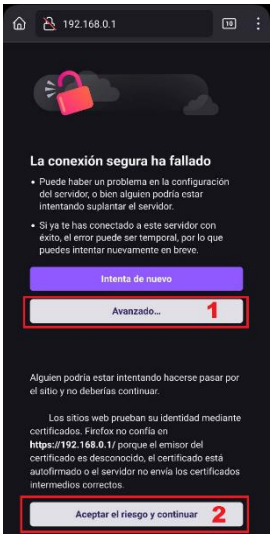


Nota. Elaborado por el autor

Como siguiente paso, seleccionamos “Avanzado” (1) y “Aceptar el riesgo y continuar” (2) como se muestra en la figura

Figura 73

Activar conexión segura para 192.168.0.1

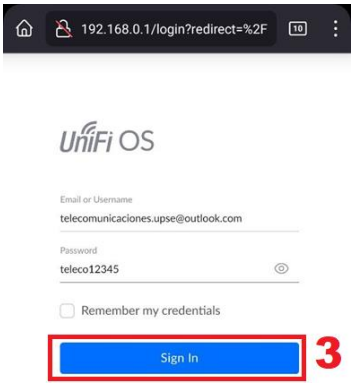


Nota. Elaborado por el autor

La siguiente figura muestra la interfaz de bienvenida al UDM Pro, donde es necesario agregar nuestras credenciales de acceso.

Figura 74

Ingreso de credenciales para el acceso al UDM Pro



Nota. Elaborado por el autor

Estas credenciales fueron creadas para acceder a los equipos Ubiquiti de la línea UniFi, las cuales son:

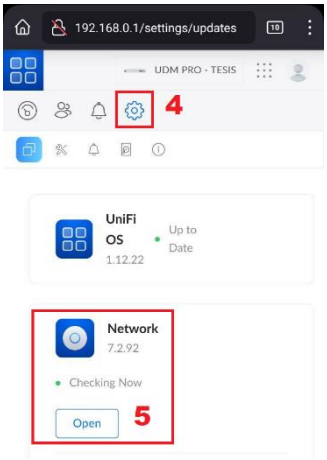
Usuario: telecomunicaciones.upse@outlook.com

Contraseña: teleco12345

Al ingresar las credenciales de acceso y seleccionar “Sing In” (3), se carga la pina al inicio de la interfaz del UDM Pro, donde seleccionaremos la opción de Network, esta se encuentra Configuración (4) > Updates (5)

Figura 75

Pasos para el acceso a la interfaz Network



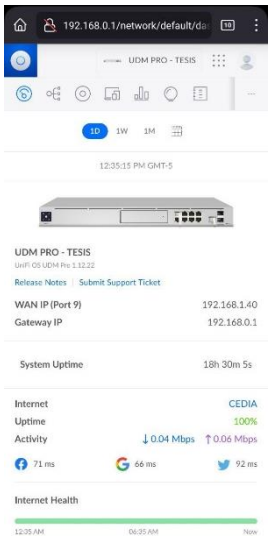
Nota. Elaborado por el autor

La Figura 76, nos muestra la interfaz de Network del UDM Pro, donde podemos realizar diferentes configuraciones como el control de acceso de usuarios, control de acceso a aplicaciones y cualquier otra regla de firewall, ya que este dispositivo en lo que corresponde a firewall resulta ser muy altamente eficaz e intuitivo a través de su software.

Otra forma de acceso a la interfaz Network, es descargar la aplicación UniFi Network, para hacer uso de esta herramienta dentro del acceso remoto, es necesario primero conectarse a la VPN, luego abriremos la aplicación UniFi Network y nos aparece una interfaz donde reconoce el dispositivo sin la necesidad de realizar manualmente figura

Figura 76

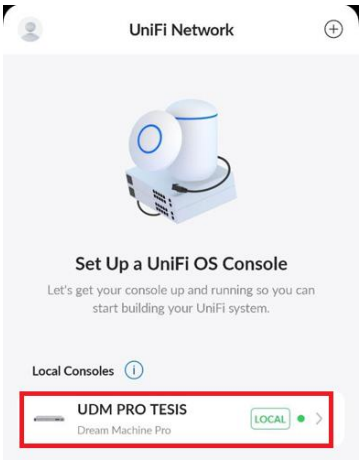
Acceso al UDM Pro desde el navegador



Nota. Elaborado por el autor

Figura 77

Reconocimiento del UDM Pro en UniFi Network



Nota. Elaborado por el autor

Se realiza el mismo procedimiento en ingresar las credenciales de acceso, ingresamos y tendremos acceso a la interfaz Network con el uso del aplicativo instalado (figura)

Figura 78

Interfaz Network a través de UniFi Network

Nota. Elaborado por el autor

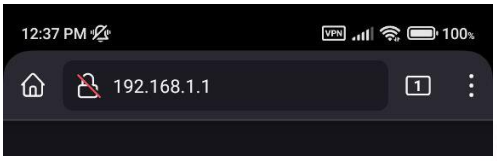
En la aplicación UniFi Network, se pueden realizar diferentes operaciones de configuraciones del UDM Pro como si estuviéramos conectados en el navegador, la principal diferencia es que presenta otro tipo de interfaz un poco similar al de la web del celular.

3.4.2 Acceso al EdgeRouter 4 a través de la VPN

Para acceder al enrutador de Ubiquiti de nuestra topología, estando conectados a la VPN nos dirigimos a nuestro navegador preferido, en este caso, intentaremos acceder a la interfaz de EdgeRouter 4 con la siguiente dirección IP 192.168.1.1 como se muestra en la siguiente figura:

Figura 79

Acceso al EdgeRouter 4 a través del navegador

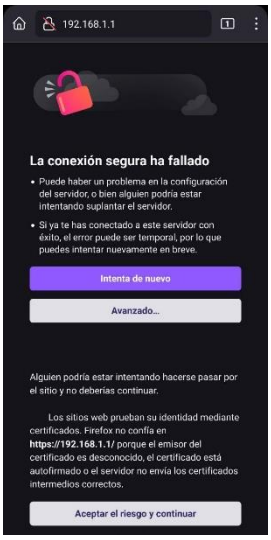


Nota. Elaborado por el autor

Como siguiente paso, se nos abre una pestaña en donde, al igual que el UDM Pro se necesita aceptar las condiciones de navegación para poder acceder a la interfaz del EdgeRouter 4

Figura 80

Activar conexión segura para el ER-4



Nota. Elaborado por el autor

La siguiente figura muestra la interfaz de bienvenida al EdgeRouter4, donde es necesario agregar nuestras credenciales de acceso, estas credenciales fueron creadas para acceder a los equipos la línea Edge de Ubiquiti,

Figura 81

Ingreso de credenciales para el acceso al ED-4

Nota. Elaborado por el autor

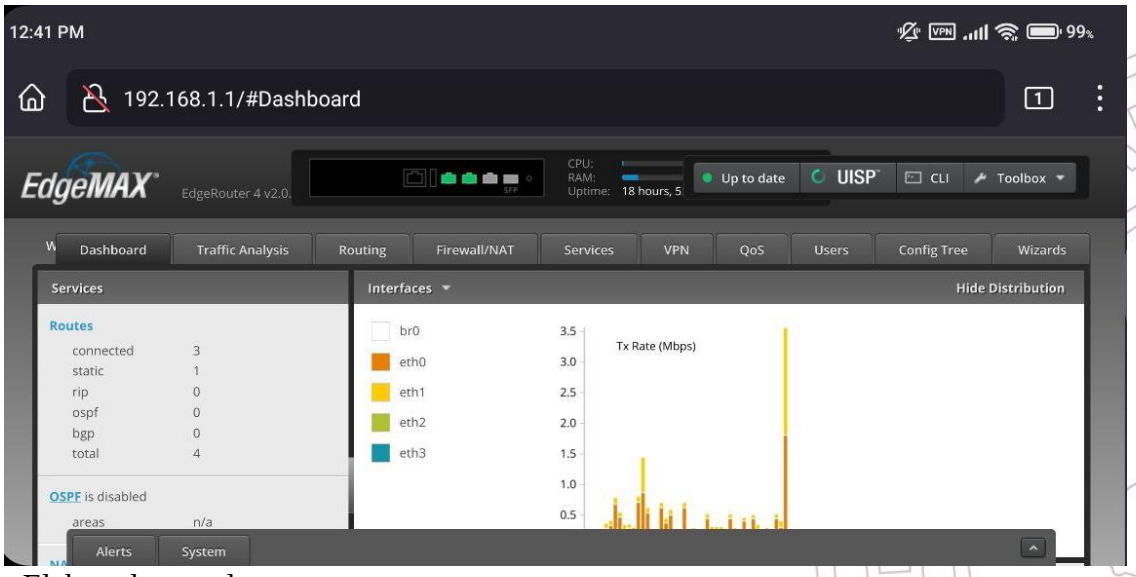
Usuario: ubnt

Contraseña: ubnt

Al ingresar las credenciales de acceso, se carga la pina al inicio de la interfaz del ED-4 como se muestra en la siguiente figura

Figura 82

Acceso a la interfaz ED-4



Nota. Elaborado por el autor

EdgeRouter4 a diferencia del UDM Pro no cuenta con una aplicación intuitiva como por ejemplo el UniFi Network. Hasta el momento de realizar esta propuesta, no se ha lanzado una aplicación para la línea Edge de Ubiquiti.

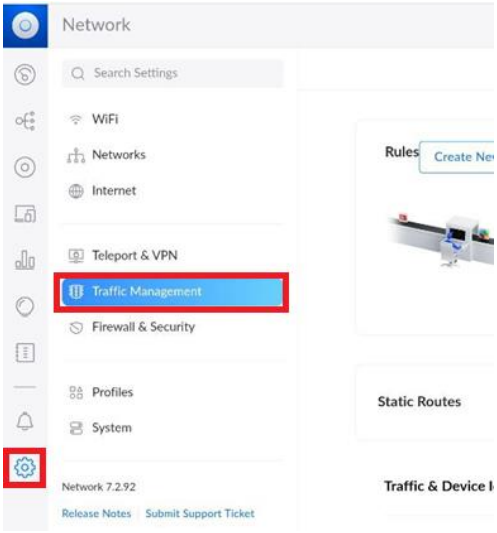
3.4.3 Gestión de tráfico DPI con el UDM Pro a través de VPN

La inspección profunda de paquetes o deep packet inspection (DPI), es un tipo de filtrado que se realiza para localizar los paquetes, realiza una identificación y las clasifica para redireccionar o bloquear paquetes. Comúnmente se los encuentra como una función de firewall.

Para comenzar nos dirigimos a Network del UDM Pro, seleccionamos el icono de configuración y nos dirigimos a la opción Traffic Management o Gestión de Tráfico.

Figura 83

Gestión de tráfico



Nota. Elaborado por el autor

La siguiente figura, nos muestra dos tipos de opciones de gestión de tráfico. En Rules o Normas nos permite elegir los dominios, puertos y aplicaciones a los que se pueden acceder en la red y especificar con qué frecuencia se va a realizar en el transcurso del día.

Figura 84

Crear regla para cada usuario

Nota. Elaborado por el autor

A modo de ejemplo: si se desea bloquear Netflix en el IPhone de Gonzalo todos los días entre las 10 am y las 12pm, se crearía la siguiente regla mostrado en la siguiente tabla:

Tabla 19

Ejemplo de Gestión de Tráfico DPI

Parámetros	Descripción
Acción	Bloquear
Categoría	Netflix
Objetivo	IPhone de Gonzalo
Calendario	10am – 12pm. Diario

Nota. Elaborado por el autor

Para nuestro ejemplo, se va aplicar una regla en general para todos los dispositivos, bloqueando aplicaciones como Facebook y Youtube de manera indefinida, entonces se realiza la siguiente tabla.

Tabla 20

Bloqueo de aplicaciones a todos los usuarios

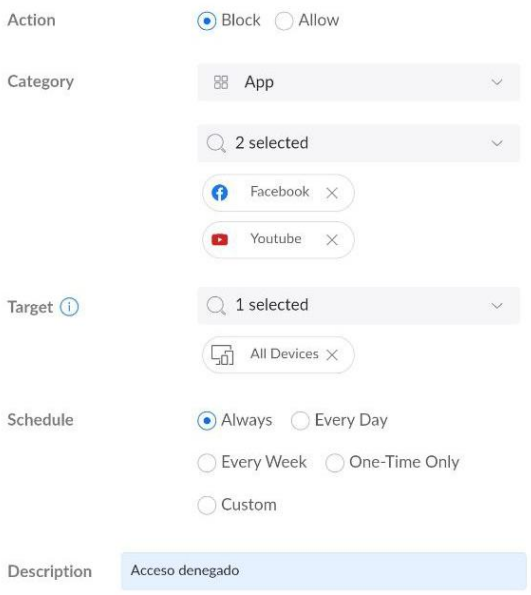
Parámetros	Descripción
Acción	Bloquear
Categoría	Facebook, Youtube
Objetivo	Todos los dispositivos
Calendario	Siempre

Nota. Elaborado por el autor

La siguiente configuración se muestra en la figura, donde tenemos dos tipos de acciones: bloquear y permitir. En la categoría nos ofrece diferentes opciones como: aplicación, grupo de aplicaciones, nombre de dominio, dirección IP, región, Internet, Red local; cada una de estas opciones tiene sus propios filtros correspondientes, en lo que corresponde a aplicación podemos seleccionar todas o buscar el tipo de aplicación que en este caso serán Facebook y Youtube.

Figura 85

Parámetros a configurar DPI por app



Nota. Elaborado por el autor

En la opción objetivo, se selecciona un dispositivo al que se desea que se le aplique la regla, nos brinda opciones para aplicar a todos los dispositivos, por defecto para los dispositivos de grupo y por último seleccionar el dispositivo móvil. En calendario tenemos opciones como: siempre, todos los días, cada semana, solo una vez, a medida; en nuestro caso se aplica la opción siempre, en las demás opciones nos permite elegir días y la hora; por último, se tiene una etiqueta de descripción la cual es opcional. Realizado los ajustes podemos observar los resultados que se muestran en el Anexo 3.

Por otra parte, también nos permite crear una nueva ruta de tráfico, la opción se puede visualizar en la figura; esto nos permite definir cómo se enrutará el tráfico de la red; es decir, puede enrutar todo el tráfico a través de la conexión WAN. Por ejemplo: si se desea que todo el tráfico de juegos y Skype se enrute a través de la WAN se debe crear la siguiente regla detallado en la Tabla 21.

Figura 86

Crear nueva ruta de tráfico

Nota. Elaborado por el autor

Tabla 21

Ejemplo de regla de tráfico

Parámetros	Descripción
Categoría	Skype, juegos en línea
Dispositivo	Macbook de Gonzalo
Interfaz	WAN1

Nota. Elaborado por el autor

Para nuestro ejemplo práctico, se desea enrutar todo el tráfico en la interfaz WAN1 y el dispositivo cliente estará configurado por todos los dispositivos. Por lo tanto, se tiene la siguiente tabla:

Tabla 22

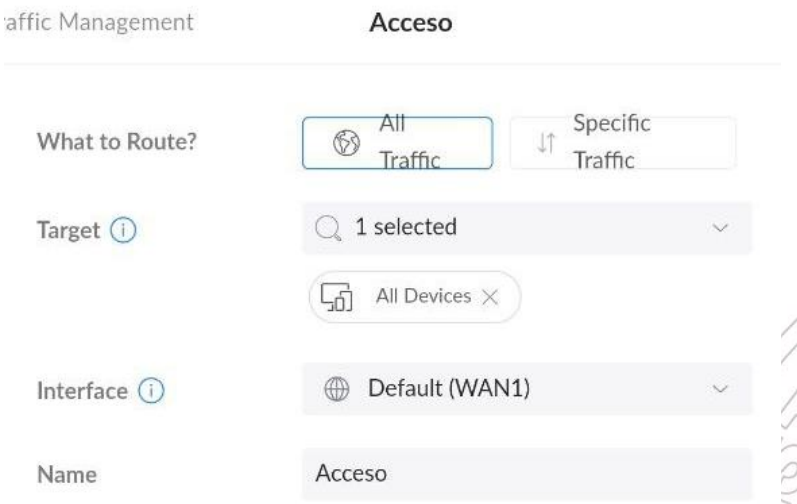
Nueva regla de tráfico

Parámetros	Descripción
Categoría	Facebook, Redes Sociales
Dispositivo	Todos los equipos
Interfaz	WAN1

Nota. Elaborado por el autor

Figura 87

Configuraciones para la gestión de tráfico



Nota. elaboado por el autor

En la gráfica nos muestra ¿Qué enrutar? Donde tenemos las opciones de seleccionar Todo el tráfico o un tráfico en especifico; al seleccionar un tráfico específico nos muestra opciones de categoría para: nombre de dominio, direccion IP y región, dependiendo del parametro elegido hay que llenar las opciones correspondientes; al seleccionar Todo el tráfico, tendremos que seleccionar el objetivo, en este caso, todos los dispositivos serán enrutados a través de la interfaz WAN1, por último se escribe un detalle y aceptamos los cambios.

Como podemos observar, UDM Pro nos presenta diversas funcionalidades a escala de red empresarial, mediante una VPN se puede hacer acciones que se pueden realizar a través de un acceso remoto mediante internet sin la necesidad de encontarse en el lugar de ubicación del equipo.

CONCLUSIONES

Al analizar la situación actual de la universidad, donde por razones de seguridad no otorga acceso VPN a los estudiantes para trabajar de forma remota por cuestiones de seguridad, en base a las investigaciones realizadas sobre los diferentes protocolos VPN, se optó por utilizar un tipo de protocolo de código abierto que nos permita la comunicación segura al laboratorio de telecomunicaciones sin la necesidad de recurrir a la IP Pública de la UPSE, de los cuales eran muy necesarios en los tipos de VPN, PPTP, L2TP y IPSec.

Existen diferentes tipos de topologías VPN, en la cual para realizar el túnel VPN el enrutador debe ser el principal punto de acceso que recibe Internet del ISP y este reparte este servicio a los demás equipos instalados en sus puertos LAN; sin embargo, en la topología de acceso remoto que utiliza protocolo de código abierto, pudimos constatar que esto no fue un impedimento al encontrarse en un nivel no principal siendo éste el EdgeRouter 4; por lo tanto, esto nos facilita en cuanto a conexión de equipos ya que no se necesita estar conectada directamente al ISP de la UPSE.

Para la implementación del diseño propuesto, se determinaron los requerimientos que se presentaron antes de implementar la VPN, logrando así optar por hardware y software de alto rendimiento, de bajo costo e interfaz intuitiva, haciendo uso de un acceso software libre que nos permitió acceder a la intranet de la UPSE con seguridad.

El protocolo WireGuard es el tipo de VPN que utiliza la función Teleport en sus equipos controladores en la línea UniFi de la marca Ubiquiti; en cuanto a su función, necesita instalarse la aplicación WiFiman para establecer la comunicación VPN en los dispositivos móviles celulares siendo un proceso más intuitivo; lo cual, nos llevó a proponer el uso de esta VPN siendo de bajo

presupuesto solucionando diferentes adversidades que se presentaron al momento de realizar con diversas arquitecturas de Redes Privadas Virtuales.

Se demostró la implementación de la VPN haciendo pruebas como el acceso de diferentes usuarios y analizando el cambio de direcciones IP al momento de realizar este proceso; de igual forma, se realizaron pruebas en gestión de control de aplicaciones DPI, que es usado para administrar grandes redes empresariales en el mundo de las Telecomunicaciones y que es posible realizar estos cambios a través de un solo hardware controlador.

RECOMENDACIONES

Por diferentes motivos de conocimiento en redes de seguridad, se recomienda que el uso de este software VPN dentro del hardware controlador, este administrado por un experto en redes o ingeniero de la carrera de telecomunicaciones para gestionar los perfiles de acceso de cada usuario.

Para el uso de los usuarios, se recomienda el uso de la herramienta “WiFiman”, que presenta una interfaz gráfica intuitiva, la misma que solo se encuentra en sistemas operativos Android y iOS.

Los docentes tutores deben crear un plan de clase basado en las configuraciones haciendo pruebas de funcionamiento que se puedan realizar a través del uso de equipos de la marca Ubiquiti, dando acompañamiento, evaluación y retroalimentación sobre las prácticas que efectúen los estudiantes mediante el acceso remoto al laboratorio de Telecomunicaciones.

Se sugiere a las autoridades de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, que se realice un análisis profundo sobre el uso de acceso remoto al laboratorio de Telecomunicaciones, determinando las necesidades en el proceso de enseñanza-aprendizaje con el uso prácticas experimentales ante adversidades de crisis nacional y mundial.

Como es de conocimiento las VPN nos brindan seguridad en un medio que no es confiable como lo es el Internet; además, de que la implementación representa un bajo costo para su operación; sin embargo, para mantener una comunicación optima de conexión se recomienda que el dispositivo móvil tenga una buena conexión estable a Internet y con una buena velocidad de carga y descarga.

BIBLIOGRAFÍA

Älvarez Delgado, D., Jorquera Cáceres, C., Sepúlveda Jorquera , G., y Zamora Esquivel, C. (2014). *Redes Privadas Virtuales (VPN).* Universidad Técnica Federico Santa María. https://bit.ly/3A3KLx8

Calazacón Aguavil, J. A. (2015). *Desarrollo de un prototipo de una red VoIP segura mediante VPN utilizando Software libre, para la comunicación de la Pontificia Universidad Católica del Ecuador, Sede Santo Domingo PUCE SD* [Tesis de grado, PUCE SD]. Repositorio Institucional PUCE. https://bit.ly/3dwmkAF

Choto, E., García, R., Jiménez, I., Urueta, D., y Varelo, P. (2007). *Implementación de una Red Virtual para teleoperación a través de internet* [Tesis de grado, Universidad Tecnológica de Bolívar]. Repositorio Institucional UNAB. https://bit.ly/3QTWW6z

De La Cruz Bernilla, S. M., y Vera Cruz, R. S. (2019). *Implementación de una VPN con open source para la gestión* [Tesis de grado, Universidad Nacional "Pedro Ruíz Gallo"]. Repositorio Institucional UNPRG. https://bit.ly/3SZUexU

Delgado, A. (09 de Sep de 2020). *¿Qué es un HUB y para qué sirve?* Geeknetic: https://bit.ly/3AtuV00

Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. https://bit.ly/3AtK2GZ

Gómez Estrada, A. I. (2013). *Redes Privadas Virtuales* [Tesis de grado, Universidad Linda Vista]. Repositorio Institucional ULV. https://bit.ly/3QB37g6

Google Trends. (s.f.). *Interés a lo largo del tiempo de la VPN*. https://bit.ly/3QPb2G1

Guerrero Panchana, J. F. (2017). *Estudio y diseño de una IP VPN en un entorno MPLS con tunelización para enlazar de manera segura y proveer conectividad al cuerpo docente*

hacia la red de la Facultad de Administración a través de un emulador [Tesis de grado, Universidad de Guayaquil]. Repositorio UG. https://bit.ly/3Qx7ZCV

Heradio, R., de la Torre, L., Galán, D., Cabrerizo, F. J., Herrera Viedma, E., y Dormido, S. (2016). Laboratorios virtuales y remotos en educación: un análisis bibliométrico. *Informática y Educación, 98*, 14-38. https://bit.ly/3T1RtfB

Hernández, J. F., Alonso, J., Figueroa, C. G., y Zazo, Á. F. (2006). *Redes privadas virtuales.* Universidad de Salamanca. https://bit.ly/3Gf668D

Iza Ninasunta, M. M., y Vera Zambrano, C. S. (2020). *Implementación de la Red Privada Virtual VPN en la Universidad Técnica de Cotopaxi - Extensión "La Maná"* [Tesis de grado, Universidad técnica de Cotopaxi]. Repositorio Institucional UTC. https://bit.ly/3A6UfYk

Jauniškis , P. (03 de Mar de 2022). *Surfshark*. https://bit.ly/3wcQlMy

Limari Ramirez, V. H. (2004). *Protocolos de Seguridad para Redes Privadas Virtuales (VPN).* [Tesis de Grado, Universidad Austral de Chile], Respositorio UACh. https://bit.ly/34UQ2Ll

Martel Velasquez, V. R. (2019). *Diseño de una red de comunicación VPN sobre internet para un Distribuidor Autorizado de Claro basado en el RFC 2764* [Tesis de grado, Universidad Peruana de Ciencias Aplicadas]. Repositorio Académico UPC. http://dx.doi.org/10.19083/tesis/625693

Microsoft. (10 de Oct de 2009). *Protocolo de tunelización punto a punto (PPTP)*. Microsoft: https://bit.ly/3QqlbJD

Ministerio de Educación. (2020). *Instructivo para la Implementación de Educación Abierta en el subnivel de Educación General Básica Superior y el nivel de Bachillerato.* Quito. https://bit.ly/3dA4g8U

Monge Nájera, J., y Méndez Estrada, V. (2007). Ventajas y desventajas de usar laboratorios virtuales en educación a distancia: la opinión delestudiantado en un proyecto de seis años de duración. *Educación, 31*(1), 91-108. https://bit.ly/3ps83HX

Quezada Lozano, H. D. (2016). *Diseño de una VPN para el acceso a las bases de datos científicas de la Universidad Nacional de Loja* [Tesis de grado, Universidad Nacional de Loja]. Repositorio Institucional UNL. https://bit.ly/3wcoA6B

Ramos Dillón, L. M. (2016). *Diseño de una red VPN para la integración de los servicios de VoIP y video vigilancia para los Infocentros Comunitarios* [Tesis de postgrado, Pontificia Universidad Católica del Ecuador]. Repositorio Institucional PUCE. https://bit.ly/3Ca4rSv

Riofrío Herrera, J. C. (2020). *Acceso web a recursos institucionales mediante VPN-SSL*. Universidad Nacional de Loja. https://bit.ly/3c2RLCg

Rivera, J. (23 de Julio de 2021). *Tendencias del acceso remoto en la educación*. UPINFORMA: https://bit.ly/3Cefuue

Ruiz Rivas, J. A., y Reina Toranza, F. (2002). *Redes de Ärea Local*. Universidad Nacional de Nordeste. https://bit.ly/3dsccZK

Salazar, J. (2016). *Redes Inalámbricas.* TechPedia. https://bit.ly/3dscik4

Triana Ortiz, K. N., Herrera Muñoz, D. C., y Mesa mendoza, W. N. (2020). Importancia de los laboratorios remotos y virtuales en la educación superior. *Documentos De Trabajo ECBTI, 1*(1). https://bit.ly/3Khahnr

Ubiquiti. (2022). *EdgeRouter 4.* Guía de inicio rápido ER-4. https://bit.ly/3AvnvJC

Ubiquiti. (2022). *UAP-AC-LITE.* Guía de acceso rápido. https://bit.ly/3SWPPMe

Ubiquiti. (2022). *UAP-AC-Pro.* Guía de acceso rápido. https://bit.ly/3Cdwbpj

Ubiquiti. (2022). *Unifi Dream Machine Pro.* Guía de acceso rápido. https://bit.ly/3AaW3zQ

Ubiquiti. (2022). *Unifi Switch 16 PoE*. Guía de inicio rápido. https://bit.ly/3dGkA7W

Ubiquiti. (2022). *UniFi Video Camera G3 DOME*. Quick Start Guide. https://dl.ubnt.com/guides/unifivideo/UVC-G3-DOME_QSG.pdf

UNAE Ecuador [@UNAEcuador]. (30 de Jun de 2020). *Te contamos cómo acceder a la biblioteca virtual*. [Tweet]. Twitter. https://bit.ly/3wbnDvy

VPN Unlimited. (2022). *¿Qué es el protocolo VPN WireGuard®?* https://bit.ly/3poOHDN

Wikipedia. (22 de enero de 2022). *Ubiquiti Networks*. Wikipedia. https://bit.ly/3oeBvRE

ANEXOS

Anexo 1

Especificaciones técnicas de EdgeSwitch 10X

Características	Filtros
estándar LAN	Ethernet Gigabit 10/100/1000 Mb/s
Número de puertos LAN	8x [10/100/1000M (RJ45)] , 2x SFP (1,25G) ,
Cantidad de puertos Ethernet básicos de conmutación RJ-45	8
Tipo de puertos Ethernet RJ-45 de conmutación básica	Ethernet Gigabit (10/100/1000)
Certificación	CE, FCC, CI
Puerto de consola	RJ-45
Voltaje de entrada de CC	24
Profundidad	90
Características de DHCP	Espionaje de DHCP
Tasa de reenvío	14.88
Altura	31.1
Compatibilidad con fotogramas gigantes	Y
Indicadores LED	Actividad, Enlace, Velocidad, Estado
administración	Interfaz de línea de comandos CLI , por navegador web ,
Humedad relativa de funcionamiento (HH)	5 - 95
Temperatura de funcionamiento (TT)	-10 - 50
Consumo de energía (máx.)	8
Alimentación a través de Ethernet (PoE)	Y
Cantidad de puertos Power over Ethernet (PoE)	1
color del producto	Negro
Montaje en bastidor	Y
Cantidad de ranuras para módulos SFP	2
Protocolo de árbol de expansión	Y
Cambiar de capa	L2
Tipo de interruptor	Administrado

Capacidad de conmutación	20
capa de conmutación	2
tipo de caso	Escritorio
compatibilidad con VLAN	Y
Gestión basada en web	Y
Peso	500
Ancho	207

Nota. EdgeSwitch 10X. Tomado de (Ubiquiti, 2022)

Anexo 2

Especificaciones técnicas del EdgeRouter 4

Característica	Descripción
Dimensiones	229 x 136,5 x 31,1 mm (9,02 x 5,37 x 1,22")
Peso	795 g (1,75 lb)
Consumo máximo de energía	13W
Método de alimentación	Cable de alimentación de CA universal (C13)
Fuente de alimentación	Adaptador de alimentación de CA/CC interno, 30 W de CC
Rango de tensión admitido	100-240 V CA, Adaptador universal de 50/60 Hz
Botón	Restablecer
Luces LED	
Puertos de datos	Velocidad/enlace/actividad
Puerto de datos SFP	Enlace/Actividad
Procesador	4-Core 1 GHz MIPS64
Memoria del sistema	1 GB de RAM DDR3
Almacenamiento flash incorporado	EMMC de 4 GB, 8 MB SPI NOR
Protección ESD/EMP	Aire: ± 24 kV, contacto: ± 24 kV
Interfaces	
Gestión	(1) puerto serie RJ45 (4) puertos Ethernet (eth0 predeterminado)
Red	(3) puertos RJ45 10/100/1000 (1) puerto SFP de 1 Gbps
Temperatura de funcionamiento	De -10° C a 50° C (de 14° F a 122° F)
Humedad de funcionamiento	10 - 90% sin condensación
Certificaciones	CE, FCC, IC

Nota. Tomado de (Ubiquiti, 2022)

Anexo 3

Especificaciones técnicas del UDM Pro

Características	Descripción
Dimensiones	442.4 x 43.7 x 285.6 mm (17.42 x 1.72 x 11.24")
Peso	3.90 kg (8.60 lb)
Con soporte de montaje	3.99 kg (8.80 lb)
Interfaces de Redes de gestión	(8) 10/100/1000 RJ45 LAN Ports
Red	(1) 10/100/1000 RJ45 WAN Port (1) 1/10G SFP+ LAN Port (1) 1/10G SFP+ WAN Port
Gestión	Ethernet en banda (1) Bluetooth BLE
Rendimiento IDS/IPS	3.5 Gbps
Procesador	Quad ARM Cortex-A57 Core a 1.7 GHz
Memoria de sistema	4 GB DDR4
Almacenamiento flash integrado	16 GB eMMC
Consumo máximo de energía	33W
Rango de voltaje	100 a 240VAC
Método de potencia	(1) Universal AC Input, 100-240VAC, 50/60 Hz (1) RPS DC Input
Fuente de alimentación	Interno 50W/12V
LEDs	
HDD	Activo
RJ45	Enlace/velocidad/actividad
SFP+	Enlace/velocidad/actividad
Memoria del Sistema	DDR4 de 4 GB
Temperatura de operación	-10 to 40° C (14 to 104° F)
Humedad de funcionamiento	5 a 95% sin condensación
Certificaciones	CE, FCC, IC

Nota. Tomado de (Ubiquiti, 2022)

Anexo 4

Especificaciones técnicas del UAP-AC-Pro

Características	Descripción
Dimensiones	196,7 x 196,7 x 35 mm (7,74 x 7,74 x 1,38")
Peso • con kit de montaje	350 g (12,35 oz) 450 g (15,87 oz)
Interfaz de red	(2) puertos Ethernet 10/100/1000
Botones	Restablecer
Método de alimentación	PoE 802.3af/802.3at
Fuente de alimentación	48 V, adaptador Gigabit PoE, 0,3 A
Consumo máximo de energía	9W
Frecuencia operativa	2,4 GHz 5 GHz
Potencia de transmisión máxima • 2,4 GHz • 5 GHz	• 22 dBm • 22 dBm
Antenas	(3) antenas de banda dual de 3 dBi cada una
Estándares Wi-Fi	802.11 a/b/g/n/ac
Seguridad inalámbrica	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
Montaje	Pared/techo (kits incluidos)
Temperatura de funcionamiento	De -10 a 70° C (de 14° F a 158° F)
Humedad de funcionamiento	5 a 95 % sin condensación
Certificaciones	CE, FCC, IC

Nota. tomado de (Ubiquiti, 2022)

Anexo 5

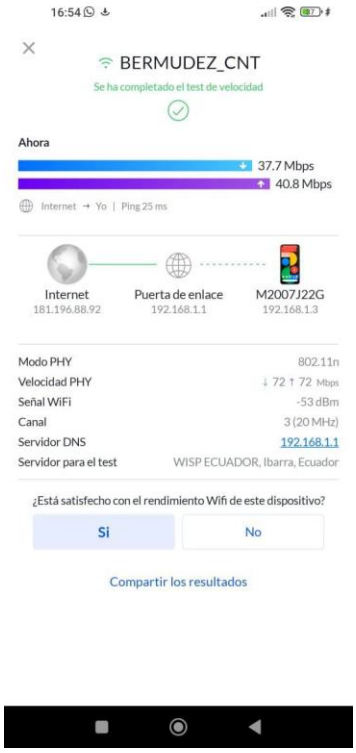
Especificaciones técnicas del UAP-AC-LITE

Características	Descripción
Dimensiones	160 x 160 x 31,45 mm (6,3 x 6,3 x 1,24")
Peso • Con kit de montaje	170 g (6,0 oz) 185 g (6,5 oz)
Interfaz de red	(1) puerto Ethernet 10/100/1000
Botones	(1) Restablecer valores predeterminados
Método de alimentación	PoE pasivo (pares 4, 5+ para la ida y 7, 8 para el retorno)
Fuente de alimentación	24 V, adaptador Gigabit PoE, 0,5A
Consumo máximo de energía	6,5W
Potencia de transmisión máxima • 2,4 GHz • 5 GHz	 • 20 dBm • 20 dBm
Antenas	(2) antenas de banda dual de 3 dBi cada una
Estándares Wi-Fi	802.11 a/b/g/n/ac
Seguridad inalámbrica	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
BSSID	Hasta cuatro por radio
Montaje	Pared/techo (kits incluidos)
Temperatura de funcionamiento	De -10 a 70° C (de 14 a 158° F)
Humedad de funcionamiento	5 a 95 % sin condensación
Certificaciones	CE, FCC, IC

Nota. Tomado de (Ubiquiti, 2022)

Anexo 6

Usuarios remotos antes de establecer la comunicación VPN


16:54
BERMUDEZ_CNT
Se ha completado el test de velocidad
Ahora
37.7 Mbps
40.8 Mbps
Internet → Yo | Ping 25 ms
Internet
181.196.88.92
Puerta de enlace
192.168.1.1
M2007J22G
192.168.1.3
Modo PHY 802.11n
Velocidad PHY ↓ 72 ↑ 72 Mbps
Señal WiFi -53 dBm
Canal 3 (20 MHz)
Servidor DNS 192.168.1.1
Servidor para el test WISP ECUADOR, Ibarra, Ecuador
¿Está satisfecho con el rendimiento Wifi de este dispositivo?
Si
No
Compartir los resultados


CNT
5:00
La conexión a Internet está disponible
Otecel S.A.
Internet
200.7.246.49
Puerta de enlace
192.168.178.113
Mapa de señales
STK-LX3
HUAWEI STK-LX3 | 192.168.178.50
SSID POCO X3 GT
Velocidad PHY ↓ 72 Mbps
Canal 13 (20 MHz)
Señal WiFi -47 dBm
Servidor DNS 192.168.178.113
Nombre STK-LX3
Fabricante HUAWEI
Modelo HUAWEI STK-LX3
Versión del sistema Android 10
Señal Wifi
Señal móvil
-40
-60
-80
dBm
-20s
-10s
Ahora
Google 268 ms
Facebook –
8.8.8.8 268 ms
Puerta de en... 4 ms
Test de
Estado
Inalámbrico
Buscar
Teleport

Anexo 7

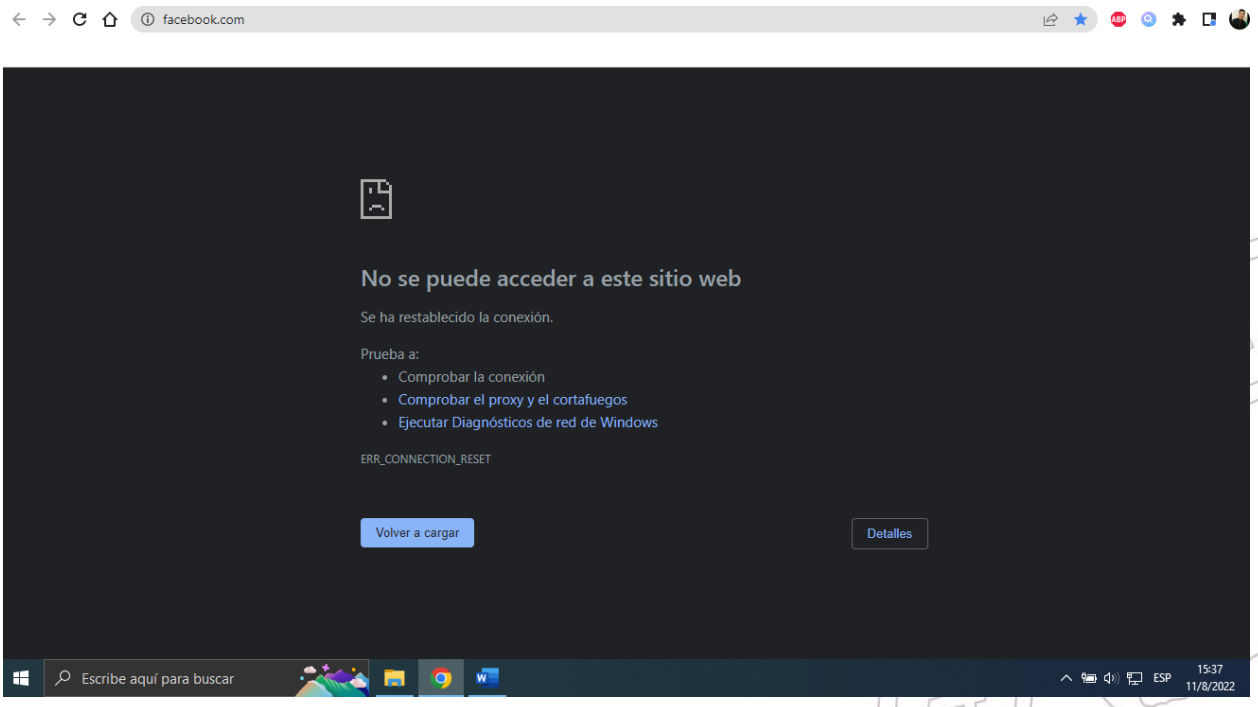
Usuarios remotos después de establecer la comunicación VPN

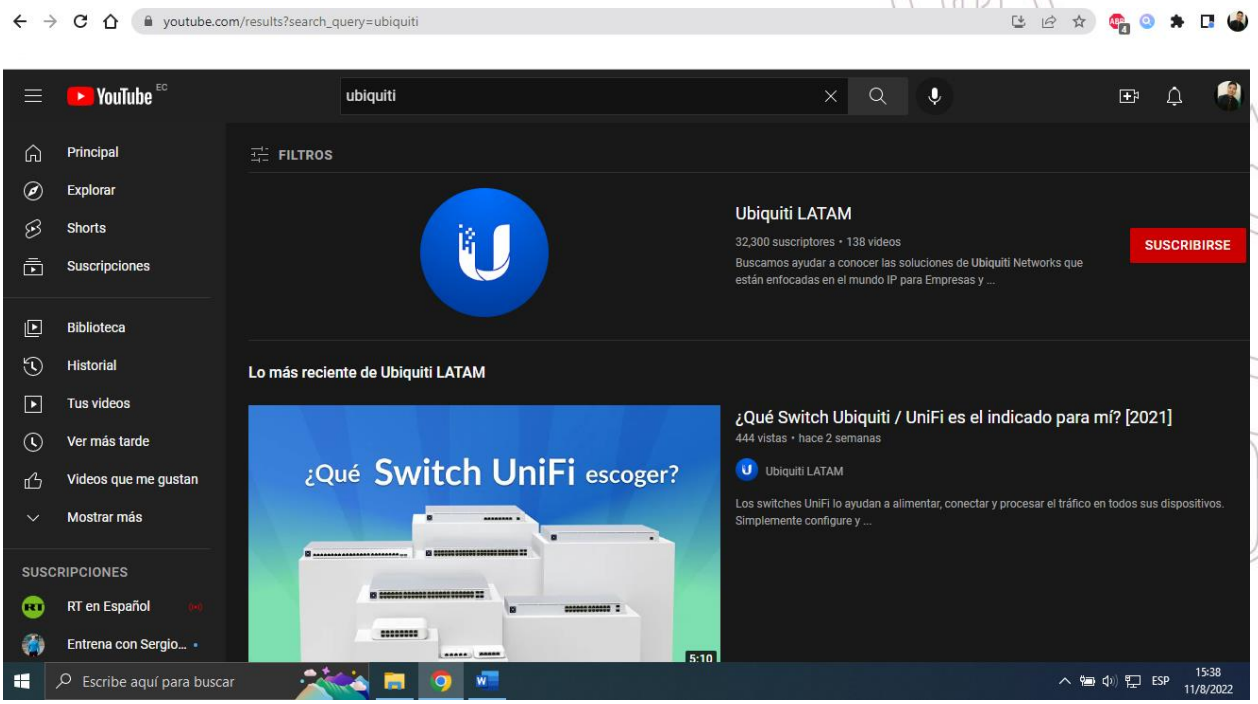

CNT
4:49
La conexión a Internet está disponible
CEDIA
Último test de velocidad
11 ago. 15:20
29.8 Mbps
10.9 Mbps
Internet
190.15.130.24
UDM PRO - TESIS
192.168.1.40
STK-LX3
HUAWEI STK-LX3 | 192.168.2.4
Servidor DNS
192.168.0.1
Nombre
STK-LX3
Fabricante
HUAWEI
Modelo
HUAWEI STK-LX3
Versión del sistema
Android 10
Señal móvil
Debe dar permisos de acceso al estado del teléfono para obtener información sobre la calidad de la señal móvil.
Solicitar permisos
Google
449 ms
Facebook
449 ms
8.8.8.8
386 ms
Puerta de en...

Test de
Estado
Inalámbrico
Buscar
Teleport

Anexo 8

Bloqueo a aplicaciones





Anexo 9

Instalación de equipos en el laboratorio