Implementación de una red wifi con servidor Radius, para controlar el acceso y mejorar la seguridad de la red inalámbrica presente en la sala de docentes de la unidad educativa “camino del inca”

Poveda Espin, Welington Omar

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Monografía, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Moreta Changoluiza, Janneth Elizabeth

11 de agosto del 2022

Latacunga

COPYLEAKS

Monografia_ Poveda Welington.pdf

Scanned on: 12:32 August 10, 2022 UTC

Identical Words	274
Words with Minor Changes	199
Paraphrased Words	258
Omitted Words	0

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Certificación

Certifico que la monografía: "**Implementación de una red wifi con servidor Radius, para controlar el acceso y mejorar la seguridad de la red inalámbrica presente en la sala de docentes de la unidad educativa "Camino del Inca"**, fue realizado por el sr. **Poveda Espin, Welington Omar ,** la mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se la sustente públicamente.

Latacunga, 11 de agosto del 2022

.....

Ing. Moreta Changoluiza, Janneth Elizabeth

C.C.: 0503078974

Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Responsabilidad de Autoría

Yo, **Poveda Espin, Welington Omar,** con cédula de ciudadanía n° 1850144377, declaro que el contenido, ideas y criterios de la monografía: **Implementación de una red wifi con servidor Radius, para controlar el acceso y mejorar la seguridad de la red inalámbrica presente en la sala de docentes de la unidad educativa "Camino del Inca"** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 11 de agosto del 2022

.....

Poveda Espin, Welington Omar

C.C.: 1850144377

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

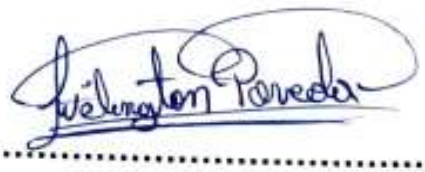
Departamento de Eléctrica y Electrónica

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Autorización de Publicación

Yo, **Poveda Espin, Welington Omar,** con cédula de ciudadanía n° 1850144377, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar la monografía: **Implementación de una red wifi con servidor Radius, para controlar el acceso y mejorar la seguridad de la red inalámbrica presente en la sala de docentes de la unidad educativa "Camino del Inca"**, en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga 11 de agosto del 2022



.....

Poveda Espin, Welington Omar

C.C.: 1850144377

Dedicatoria

A dios que me ha permitido seguir con constancia, esfuerzo y dedicación siempre adelante.

A mi madre Yolanda, y mi familia que con mucho amor y compresión han sido mi constante motivación para así haber llegado a cumplir mis metas para un futuro mejor y que siempre pondré al servicio del bien, la verdad, la justicia y la innovación.

Poveda Espin, Welington Omar

Agradecimiento

A la universidad de las fuerzas armadas ESPE- sede Latacunga, institución que se mantiene con un liderazgo positivo, garantizando la calidad de la educación superior y su progreso permanente formando profesionales humanísticos, lideres, emprendedores, competentes e innovadores, con valores enfocados en servir y apoyar en función de los requerimientos del desarrollo social y tecnológicos de la patria.

A las autoridades de esta noble institución quienes han sabido proyectarse con iniciativas importantes, en diferentes especialidades las cuales permiten elevar el nivel científico de las personas en busca de nuevos ideales.

A sus distinguidos catedráticos, mismos que con sus conocimientos, estuvieron prestos a compartir sus experiencias en el inter aprendizaje, logrando así que sus estudiantes sean entes creativos, reflexivos, críticos y de esa manera tengamos una educación de alto nivel.

A la Ing. Janeth Moreta, quien con su carisma y conocimientos supo guiar el desarrollo del presente trabajo hasta su culminación.

A mi familia por ser pieza fundamental para concluir con esta importante misión.

Poveda Espin Welington Omar

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

La Unidad Educativa “Camino del Inca” ubicada en la parroquia Turubamba -cantón Quito, actualmente cuenta con un equipo de enrutamiento de redes (router) el cual es el encargado de brindar la conexión tanto inalámbrica como cableada a las diferentes zonas y equipos presentes en la institución. Este equipo está configurado con el protocolo de seguridad WPA2 PERSONAL, esto representa un peligro de seguridad alto, más aún para una institución donde se maneja información sensible de cientos de individuos en etapa escolar y del personal que labora. El presente proyecto de titulación está enfocado en resolver los problemas de conexión wifi y seguridad en la red que presentan los individuos que forman parte de esta institución educativa fiscal, de forma específica los docentes que laboran en dicha institución, es por esto que, a través de una análisis teórico se ha determinado los elementos de software y hardware que presenten las mejores características para realizar la implementación de un punto de acceso situado en la sala de docentes, con esto se busca aumentar la cobertura de la red inalámbrica y además por medio de la configuración de un servidor de autentificación Radius, dotar a los educadores una conexión que sea segura, rápida y accesible.

Palabras clave: Red wifi, Servidor de autenticación, wpa2 Enterprise, Servidor Radius, Seguridad en las redes inalámbricas

Abstract

The Educational Unit "Camino del Inca" located in the parish Turubamba -cantón Quito, currently has a network routing equipment (router) which is responsible for providing both wireless and wired connection to different areas and equipment present in the institution. This equipment is configured with the WPA2 PERSONAL security protocol, which represents a high security risk, even more so for an institution where sensitive information of hundreds of individuals in school and staff is handled. This degree project is focused on solving the problems of wifi connection and network security presented by the individuals who are part of this fiscal educational institution, specifically the teachers who work in this institution, that is why, through a theoretical analysis has been determined the software and hardware elements that present the best features for the implementation of an access point located in the teachers' room, this seeks to increase the coverage of the wireless network and also through the configuration of a Radius authentication server, provide educators with a connection that is secure, fast and accessible.

Key words: wifi network, Authentication Server, wpa2 Enterprise, Radius Server, Security in Wireless networks.

Capítulo I

Planteamiento del problema

Tema

Implementación de una red wifi con servidor Radius, para controlar el acceso y mejorar la seguridad de la red inalámbrica presente en la sala de docentes de la unidad educativa “camino del inca”

Introducción

A lo largo de los últimos años se ha visto como la tecnología y la forma en que nos comunicamos ha ido evolucionando de forma exponencial y cada vez siendo está más accesible, así también, y a la par han ido creándose nuevas formas cada vez más innovadoras y fáciles de corromperlas; esto con la finalidad de acceder de forma ilegal y fraudulenta a información privada para generar algún tipo de beneficios.

Con la finalidad de que la información que se maneja en diversos sitios se encuentre protegida y en la era actual en la que vivimos donde la mayoría de comunicaciones se realiza a través de la red, ya sea esta inalámbrica o cableada, se busca evitar que dicho tráfico sea manipulado por personas ajenas a la red, es por esto que es de suma importancia crear métodos que permitan brindar seguridad a dicha red a través de equipos o software.

Debido a las vulnerabilidades que presentan en su mayoría las redes de telecomunicaciones inalámbricas, hacen que la implementación de mecanismos o métodos de seguridad cobren una mayor relevancia ya que de forma directa si se lograse monitorear y controlar de forma constante el acceso a una red wifi también se

estaría limitando el acceso a la información que se manejase dentro de esta, creando así en nuestro caso, a la comunidad educativa un ambiente más confiable respecto al manejo de sus datos.

A causa de esto florece el concepto de instalación de un servidor de autentificación Radius en la unidad educativa “Camino del Inca” localizada en la parroquia Turubamba de la Ciudad de Quito, para brindar a los docentes de la institución en cuestión una nueva red wifi, la cual aparte de brindarles un mayor alcance de cobertura de la red principal, también les prestara todas las seguridades al momento de navegar o compartir información sensible como lo es la de los niños y jóvenes que se forman aquí.

Antecedentes

Las redes inalámbricas wifi con el pasar del tiempo han contribuido eficazmente a la mejora continua de la conectividad en general beneficiando a empresas, hogares, entre otros, debido a que entre si principales beneficios esta la posibilidad de compartir recursos en red sin la necesidad de estar conectado físicamente mediante cables, facilitando la conectividad en lugares donde es imposible realizar una red alámbrica sea esto por factores físicos o climáticos. (Setephany & Serrano Anguieta, 2019-2020)

Las tecnologías de la información y las redes se están convirtiendo en recurso ubicuos, como sucedió con el agua y la electricidad. En consecuencia, la seguridad de las redes de comunicación y los sistemas de información, y en particular su disponibilidad, preocupa cada vez más a la sociedad, en particular debido a la

posibilidad de problemas en los sistemas de información clave, debido a la complejidad del sistema, errores o ataques de piratas informáticos. (Carolina, 2011)

"El WPA2 es el sistema de cifrado que se usa para proteger las redes inalámbricas desde hace más de una década. Por años había sido considerado uno de los protocolos más seguros que se habían creado, pero tal y como se ja comprobado, tenía una falla en su seguridad que ha sido descubierta y que esta, por lo menos potencialmente, a la mano de usuarios maliciosos". (Hidalgo, 2017)

En esta ocasión, se identificaron servicios de seguridad informática para la detección de control y acceso y el funcionamiento del sistema de seguridad, así como de emisiones entre las personas identificadas. (Pilicita, 2019)

Planteamiento del problema

Dado que la tecnología ha evolucionado con gran rapidez en los últimos años, a la par de esto ha surgido diversas nuevas problemáticas a la hora de salvaguardar los datos más prescindibles de una entidad pública o privada, en razón de esto es determinante analizar nuevas soluciones que ofrecen mejoras en cuanto a la seguridad en las redes.

La Unidad Educativa "Camino del Inca" situada en la parroquia Turubamba, en la ciudad de Quito al igual que en otras entidades de educación o de cualquier otro ámbito, necesitan hacer uso de internet para desarrollar actividades que van de la mano principalmente con la información de los estudiantes y de la demás comunidad educativa que labora en dicho establecimiento, por tal razón la implementación de una

red wifi en conjunto con un sistema de monitoreo y control de acceso en la sala de docentes de la institución en emisión cobran especial relevancia.

El protocolo de seguridad AAA (Radius) presenta la oportunidad de controlar el acceso a las redes, logrando así que solo el personal designado pueda manipular de forma correcta el flujo de datos que se manejan en la nueva red de telecomunicaciones, brindado así una alternativa confiable para el resguardo de la información.

En el Ecuador, el uso de este tipo de mecanismos de seguridad es implementados de forma minoritaria por entidades privadas y afines a rubros económicos. Es por esto que es sumamente importante que las unidades educativas y otras instituciones públicas que trabajan con datos sensibles de la población ecuatoriana implementen este tipo de redes seguras.

Justificación

Nuestra sociedad experimenta profundos cambios y transformaciones en el ámbito tecnológico y por ende en la manera en que las personas se comunican, es por esto que la implantación de una red wifi con un servidor Radius nos permite que los servicios de conexión, navegación y compartición de datos que se realicen dentro de esta red sean manejados de forma segura.

Este trabajo es pertinente ya que se dotará de una nueva red a la cual los docentes puedan conectarse para realizar sus actividades con la confianza de que su trabajo no podrá ser vulnerado o manipulado por un ente ajeno, además que nuestro perfil

profesional nos permite abordar temas como los planteados para el presente trabajo de titulación.

La ejecución del presente proyecto es factible ya que se cuenta con el apoyo de las autoridades, docentes que laboran en la institución y las facilidades que nos otorgarían, además se cuenta con los recursos y materiales necesarios para analizar y solucionar la problemática existente.

Por medio de entrevistas realizadas con las autoridades de la institución, se encontró con aspectos novedosos y a la vez se emiten sugerencias viables y seguras, lo cual ayudará de forma significativa en el manejo de información a través de esta red de forma competitiva, con los estándares de seguridad más altos en cuanto a redes inalámbricas, permitiendo así que la institución no tenga problemas se seguridad.

Objetivos

Objetivo General.

Diseñar e implementar un punto de acceso con un servidor Radius para brindar a la comunidad educativa de la institución “Camino del Inca” una conexión rápida y segura

Objetivos Específicos

- Realizar un análisis para selección de la zona que presente una mejor cobertura a los docentes de la unidad educativa “Camino del Inca”
- Analizar y elaborar una lista sobre los equipos físicos y software libre necesarios para la implementación.

- Desarrollar pruebas de conexión e infiltración para definir los niveles de seguridad que presenta la red creada.

Alcance

El presente trabajo busca implementar una nueva red wifi, misma que contará con un servidor Radius para monitorear y controlar el acceso a la red en mención, los usuarios beneficiarios con el proyecto serán los docentes que laboran en las dos jornadas laborales de esta institución, debido a que el alcance que provee la red inalámbrica con la que cuenta la institución no brinda cobertura total a la sala de docentes y esto ocasiona inconvenientes al momento de realizar actividades acordes a sus funciones.

Adicionalmente cabe mencionar que los docentes que acceden a la nueva red wifi, además de poder tener cobertura en su lugar de trabajo, también harán uso de una red segura gracias a la configuración de este protocolo de seguridad para redes inalámbricas.

Capítulo II

Marco Teórico

Redes de comunicación

Una red de comunicación se define como la unión de instalaciones técnicas las cuales permiten la comunicación remota entre dos o más computadores o también llamados ordenadores. Habitualmente hablamos de la trasmisión de datos, audio y video mediante ondas electromagnéticas que viajan por la atmosfera. La información puede transmitirse en forma analógica, digital o mixta, se realizan siempre de forma transparente para el usuario, que procesa la información exclusivamente en forma analógica. Las rede más comunes son las redes informáticas, las redes telefónicas y las redes de transmisión de audio y video.

Redes de datos

Una red de datos es un sistema de comunicaciones en el cual se emplea diversos equipos de telecomunicaciones y de cómputo, esto permite la transmisión y compartición de información entre los dispositivos que conforman la red. Una red de comunicación casi siempre esta conformadas por:

- Clientes
- Servidores
- Hardware
- Medio de transmisión
- Protocolos de Comunicación

Las redes de comunicación se clasifican según diferentes puntos de vista, entre las más famosas se encuentran los tipos de redes según su longitud, entre las que se distinguen las redes las redes LAN, MAN Y WAN.

Tipos de redes de acuerdo al medio por el que se transmiten

Otra de las formas en que se clasifican las redes de comunicación y las cuales formaran parte en este proyecto, hace referencia a la clasificación de las redes de acuerdo al medio por el que se transmiten.

Cuando se hace uso de las líneas de cables ya sean estos coaxial, de par trenzado, telefónico o de fibra óptica, a esto se le conoce como redes alámbricas. Por otra parte, se el medio por el que se transporta los datos es el aire, a esto se lo denomina redes inalámbricas. Para efecto de una mejor compresión a continuación se explica de forma detallada el funcionamiento de estas redes.

Redes alámbricas

Son aquellas en las que la comunicación se realiza a través de una conexión cableado entre los equipos presentes en la red como se ejemplifica en la figura 1, los cables de datos van conectados a las computadoras y otros dispositivos como switch o routers. Las redes alámbricas presentan una mejora considerable en cuanto al tema de seguridad y la transmisión de datos a altas velocidades, este tipo de redes son usados por gran parte de instituciones debido a la fiabilidad que proveen a sus datos. Algunas de las desventajas de este tipo de red son el manejo e instalación del cableado necesario para su funcionamiento, además pueden limitar la expansión de la red y para hacerlo se necesitaría de equipos adicionales.

Figura 1

Redes alámbricas

Nota. Esquema de una red alámbrica. Tomado de (ymant, 2016)

Tipos de redes alámbricas por su extensión

Según la distancia geográfica que pueden cubrir, las redes de telecomunicaciones se suelen clasificar tres grandes grupos que son LAN, MAN y WAN, de las cuales la red WAN es conocida como la más grande de todas las redes por el espacio geográfico que logra comprender, ya que además incluye todo el conjunto de equipos informáticos de red que se interconectan con cables o mediante protocolos para dar origen a lo que conocemos como internet.

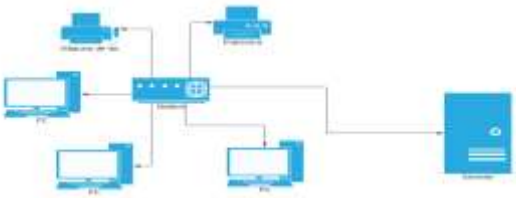
Local área network (LAN)

Este tipo de redes son las más comunes ya que se usan en nuestros hogares, instituciones educativas, oficinas o negocios pequeños, ya que al momento en que nuestro proveedor de servicios nos dota de un router y este conecta a varios equipos ya sea de forma cableada o inalámbrica a internet, además según Stallings (2004),´´Una LAN es una red de comunicaciones que interconecta varios dispositivos y proporciona un medio para el intercambio de información entre ellos´´ (pág. 17). Cabe recalcar que hay algunas diferencias entre las LAN y las WAN que se muestran en los siguientes puntos:

- Las redes WAN presentan mayor cobertura
- En una red LAN, casi siempre los equipos son de prioridad de los dueños de la red de ese lugar, esto no ocurre en una WAN porque este tipo de redes es la unión de múltiples LAN.
- Las velocidades de transmisión en una red LAN son mejor que las de una WAN

Figura 2

Representación de una Red LAN



Nota. Se presenta un ejemplo típico de cómo están formadas las redes de área local o LAN

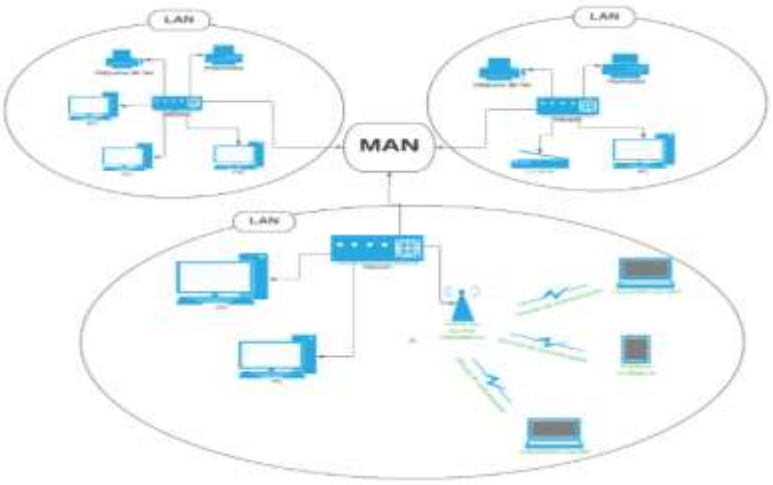
Metropolitan área network (MAN) (Red de área amplia)

Este es otro tipo de los tres que existen de las redes de acuerdo a la distancia que logran cubrir dentro de un territorio, de forma más técnica, se define que:

> Las MAN (Metropolitan área network) son entre las LAN y las WAN. La inclinación o gusto por las MAN ha surgido después de que se haya comprobado que las estrategias convencionales de conmutación y conexión factorial utilizadas en las técnicas convencionales de conmutación y conexión de factor a punto utilizadas en las WAN no estarían bien para las necesidades de desarrollo de las organizaciones. Mientras que la retrasmisión corporal y la ATM prometen satisfacer una enorme variedad de necesidades de los clientes dentro de un vasto espectro de deseos en cuanto a velocidades de transmisión, hay condiciones tanto en las redes personales como en las públicas que exigen una gran velocidad a valores de costo reducido. Para ello ha surgido nuevas soluciones como las redes wifi o extensión de redes metropolitanas. Sin duda que el mercado más importante para las redes MAN son los clientes que necesitan tener una cobertura extendida en toda un área metropolitana sin dejar de lado la velocidad y los costes bajos, con lo cual las MAN cumplen de forma idónea estas necesidades y además se podría implementar la telefonía fija o televisión por internet para mejorar la experiencia de este tipo de redes. (Stallings, 2004, págs. 17-18)

Figura 3

Representación de una red MAN



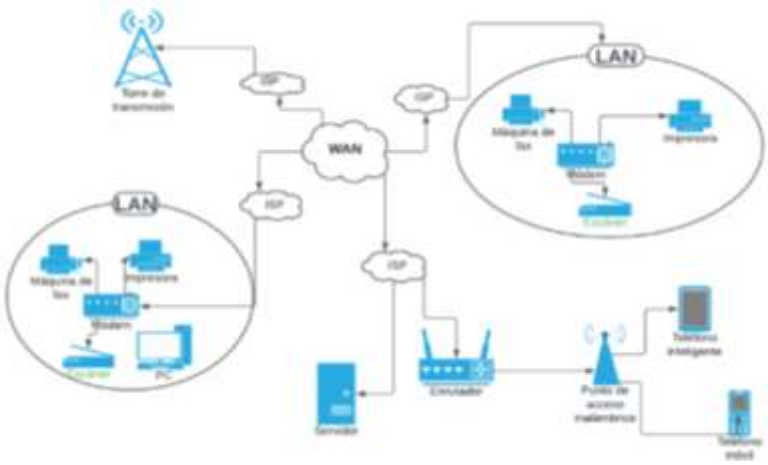
Nota. La imagen muestra un modelo típico de cómo están formadas las redes de área Metropolitana MAN

Wide área network (WAN) (Red de área amplia)

De igual manera este tipo de redes de forma global se define que cubren una gran área geográfica, además que para su implementación se necesita atravesar espacios públicos como parques, calles, edificios, etc. Se usarán por lo menos una pequeña fracción de la infraestructura que poseen las empresas proveedoras de servicios ya que así se logran formar la conexión entre las redes MAN ya que normalmente incluye unos numerosos dispositivos de conmutación interconectados. Estos nodos no están relacionados con el contenido, sino que de forma contraria su característica es la de ofrecer al proveedor las estadísticas de un nodo a otro. (Stallings, 2004)

Figura 4

Representación de una red WAN



Nota. La imagen muestra un modelo típico de cómo están formadas las redes de área amplia o WAN

Redes inalámbricas

Este tipo de redes como su nombre lo indica, son aquellas en las que el uso de cables para su funcionamiento es casi nulo, el medio que usa para la transmisión de datos entre los equipos que se encuentran dentro de su red es el aire o también llamado de forma técnica la atmosfera, esto al ser un medio que no puede ser controlado o manipulado presenta al administrador de la red una alta vulnerabilidad. Esta tecnología está basada en las normas 802.11 de la IEEE (Instituto de ingenieros eléctricos y electrónicos) y sus diferentes variables.

Figura 5

Redes Inalámbricas

Nota. Representación del funcionamiento de las redes inalámbricas. Tomado de (optical.pe, 2019)

Entre las ventajas que presentan estas redes encontraremos: la movilidad del usuario, la escalabilidad, el uso limitado de cables, menor costo en comparación con una red cableada.

Por otra parte, su principal desventaja en comparación con una red alámbrica, es la poca seguridad que presenta para los usuarios el uso de este tipo de redes.

Tipos de redes inalámbricas de acuerdo a su extensión

Redes WPAN

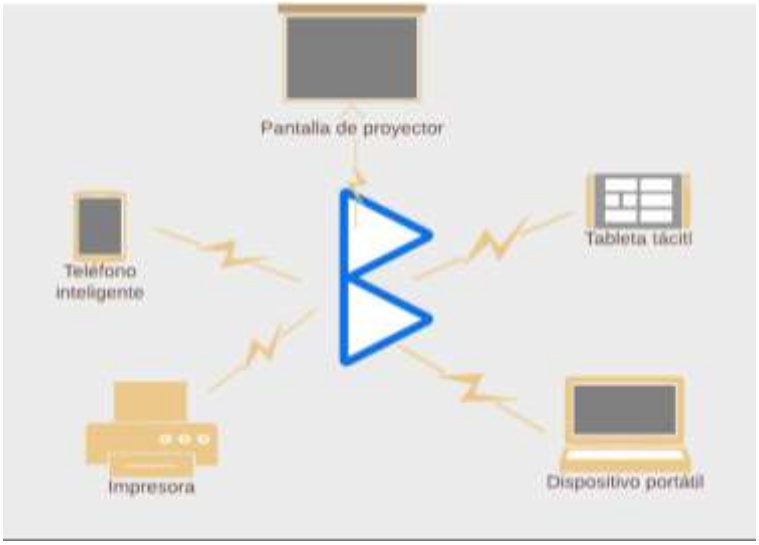
De manera inequívoca se puede decir que son el tipo de redes inalámbricas que menor cobertura logran abarcar y, además:

> “Las redes de área personal inalámbricas se basan en el estándar IEEE 802.15. Estas redes inalámbricas les servirán a los clientes para comunicarse en distancias muy cortas, aproximadamente en una forma ideal unos 10 metros. A diferencia de otras redes inalámbricas, la conectividad WPAN requiere poca o

ninguna infraestructura o conectividad directa fuera del canal que se haya establecido. Es esto por lo que permite crear pequeñas soluciones de bajo costo monetario y ahorro de energía se pueden implementar en una amplia variedad de dispositivos inteligentes, como celulares, PDA, tables, Laptops, entre otros. Un ejemplo claro de esta tecnología es Bluetooth". (Salazar, 2011, pág. 9)

Figura 6

Redes WPAN



Nota. La ilustración ejemplifica el funcionamiento de una red WPAN, tomando como tecnología de red a Bluetooth

Redes WLAN

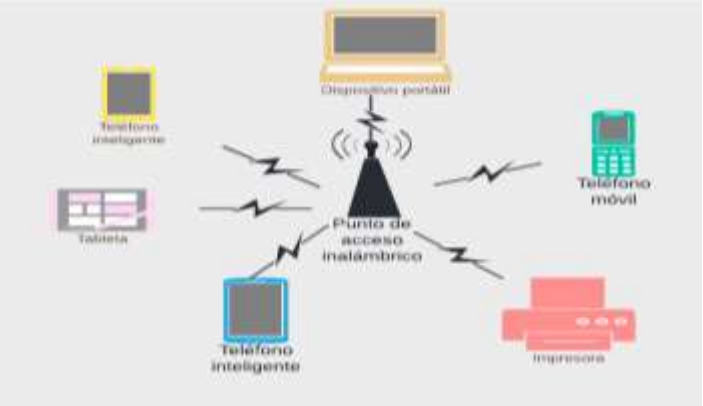
Las redes inalámbricas de área local por sus siglas en inglés:

Están diseñadas para brindar acceso sin la necesidad de usar cables en áreas con un alcance típico de hasta 100 metros siempre y cuando no existan obstáculos físicos como paredes y se utilizan principalmente en el hogar, la

escuela, el laboratorio de computación o en las oficinas. Esto brinda a los usuarios la capacidad de movilizarse dentro de su área de cobertura local y permanecer conectado a la red. Las WLAN se basan en el estándar IEEE 802.11 y se venden bajo la marce WiFi. Debido a la competencia, entre otros estándares como hiperLan nunca han tenido un uso comercial tan generalizado. El estándar IEEE 802.11 fue el más fácil de implementar y se comercializo más rápido aún. (Salazar, 2011, pág. 13)

Figura 7

Redes WLAN



Nota. La ilustración muestra el funcionamiento y algunos equipos usados en las redes WLAN.

Redes WMAN

Este tipo de redes son de mayor cobertura que las redes inalámbricas de área local**:**

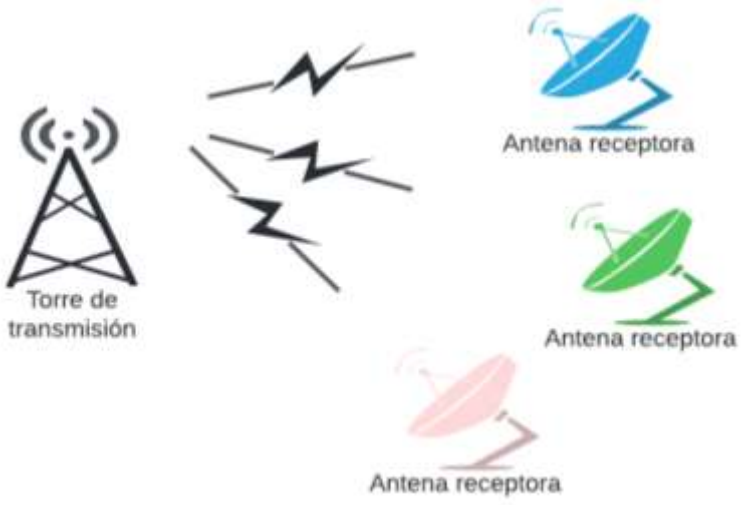
“Las redes inalámbricas de área metropolitana forman el tercer grupo de redes inalámbricas. Las WMAN se basan en el estándar IEEE 802.16, a menudo denominado

WIMAX. WIMAX es una tecnología de comunicaciones con arquitectura punto multipunto orientada a proporcionar una alta velocidad de transmisión de datos a través de redes inalámbricas de área metropolitana". (Salazar, 2011, pág. 13)

"Esto permite que las redes inalámbricas LAN más pequeñas pueda ser interconectadas por WIMAX creando así una gran WMAN. Por consiguiente, la creación de redes entre ciudades puede lograrse sin la necesidad de cableado costoso". (Salazar, 2011, pág. 13)

Figura 8

Redes WMAN



Nota. La imagen muestra cómo funcionan las redes WMAN

Redes WMAN

Usadas en diferentes lugares a lo largo del mundo por su versatilidad y facilidad de instalación y manejo, por otra parte:

“Las redes inalámbricas de área amplia logra alcanzar en condiciones ideales una distancia más allá de los 50 kilómetros y suelen utilizar frecuencias con licencia, es decir que requieren que se requiere de un permiso y costo económico para poder usar. Este tipo de redes se pueden usar en grandes áreas como ciudades o países, a través de los varios sistemas de satélites o ubicaciones con antena brindados por un proveedor de servicios de internet. Ejemplos más sobresalientes o importantes de este tipo de redes son la telefonía móvil y los satélites”. (Salazar, 2011, pág. 14)

Normativas

Las normativas son el conjunto de regles que se deben cumplir para realizar una determinada actividad, esto tiene como finalidad que los procesos se estandaricen y poder trabajar así de forma globalizada.

EIA/TIA 568A

Este estándar formula cada uno de los requisitos a implementar en este caso sería enfocado hacia el tópico de construir, diseñar y administrar un sistema de cableado estructurado. Establecen además una herramienta fundamental en el campo de las conexiones de redes o planeación e implementación del cableado de una red. Los dos extremos del cable UTP ya sean estos de la categoría 5 o categoría 6, que llevaran conectores RJ45 con un cierto orden de colores especificados por la norma los cuales, partiendo desde la izquierda hacia la derecha, blanco verde-blanco-blanco naranja-azul-blanco azul-naranja-blanco marrón- marrón. (Cortes, 2021)

EIA/TIA 568B

Este estándar es una herramienta útil para cada una de las implementaciones, encaminado de forma más específica hacia el diseño del cableado estructurado en un DataCenter. Cuenta con tres subcategorías las cuales son ANSI/TIA/EIA 568-B1, TIA/EIA 568-B2 y TIA/EIA 568-B3. (Cortes, 2021)

Estándar IEEE 802.11

Los estándares IEEE 802.11 son un conjunto de reglas o parámetros establecidos por el Instituto de ingenieros eléctricos electrónicos (IEEE), los cuales están enfocados en normar la forma en que se manejan o implementan las redes inalámbricas.

Figura 9

Estándares 802.11

Nota. Estándares IEEE 802.11 y sus variantes para Wifi. Tomado de (Oscar Ubierna Yubero, 2013)

Estándar 801.11a

“La primera carta después de la aprobación en junio del año 1997 del estándar 802.11, esta provista para operar en la frecuencia 5Ghz, con velocidades de transmisión de datos de hasta 54 Mbps.” (Shaw, 2018)

Contrariamente la norma 802.11 b, al ser publicada causo cierta confusión en el sector porque tendría aun teniendo una letra diferente al final como lo es la b, esta norma aún era compatible con la IEEE 802. 11a.

Estándar 802.11 b

“Publicado en el mes de septiembre del año 1999, proporcionaba a los equipos que tuvieran dicha norma el poder trabajar en la frecuencia 2,4 GHz y admitir una velocidad de hasta 11Mbps, esta normativa llega al mercado curiosamente antes que la norma 802.11 a.” (Shaw, 2018)

Estándar 802.11 g

Este estándar recibió la orden de aprobación para ser publicado en el mes de junio del año 2003 y se convirtió en el sucesor del estándar 802.11 b, capaz de alcanzar velocidades de transmisión de más de 54 Mbps en la banda de transmisión 2.4Ghz.

Estándar 802.11 n

Este estándar fue el primero en ser creado de forma específica para la tecnología MIMO que implementa el poder trabajar dentro de un equipo con dual band,

es decir tanto en la banda de 2.4Ghz como el 5ghz, con velocidades de hasta 600Mbps.

Estándar 802.11 i

El estándar 802.11i aborda muchas de las deficiencias de sus predecesores, tanto en términos de autenticación de usuarios como en la solidez de los métodos de cifrado. Y lo logra en el primer caso a través de su capacidad para trabajar en cooperación con 802.1X, y en el segundo caso al permitir el cifrado del Estándar de cifrado avanzado (AES). Además de mejorar en gran medida la seguridad de los entornos WLAN, también reduce en gran medida la complejidad y el tiempo necesario para que los usuarios se trasladen de un punto de acceso a otro. (COMPUTER WORLD, 2005)

Sin embargo, según usuarios y analistas, aunque el despliegue de 802.11i será inevitable a largo plazo, las empresas deberán sopesar cuidadosamente las ventajas y desventajas del nuevo estándar. Más aún, deberán distanciarse de la retórica de marketing de los proveedores y analizar con cabeza fría el momento más oportuno para implementarlo, especialmente si ya cuentan con infraestructuras que requieren actualizarse al estándar. (COMPUTER WORLD, 2005)

Tenga en cuenta que 802.11i no es un punto final. Es esencialmente una evolución de las tecnologías anteriores, principalmente WPA (Acceso protegido Wi-Fi), implementadas durante mucho tiempo en la industria, hasta el punto en que el nuevo estándar todavía se conoce como WPA2.

El primer protocolo de seguridad de redes inalámbricas reconocido por IEEE fue WEP (Privacidad equivalente por cable). Esto hizo posible utilizar claves cifradas de 40 bits según el algoritmo de cifrado RC4 y asignar una clave a cada máquina cliente por sesión. Pero desde que fue pirateado en el verano de 2001, se lo considera el talón de Aquiles de la cadena de seguridad inalámbrica.

La combinación de WEP con el protocolo de autenticación 802.1X mejoró un poco la situación, ya que en este esquema el cliente WEP se veía obligado a solicitar acceso a la red mediante EAP (Extensible Authentication Protocol), tal como lo establece el 802.1X.

Equipos de telecomunicaciones usados en redes inalámbricas

Punto de acceso

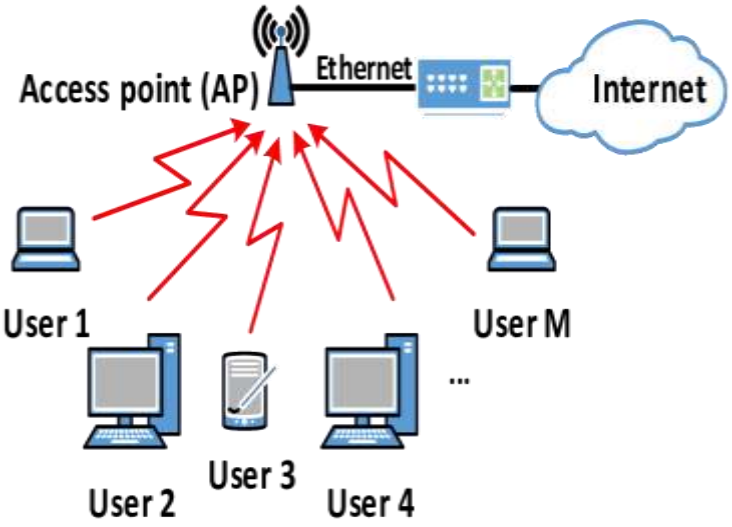
Son uno de los elementos más comunes en conjunto con los router inalámbricos por que presentan configuraciones interesantes que mejoran el acceso a la red, también se define que:

> Se considera que es el punto primordial de emisión y recepción en una red Wireless. Este punto de acceso centraliza la señal de todos los nodos inalámbricos y reúne el reparto de la información de toda la red local. También tiene que realizar el vínculo entre los nodos inalámbricos o clientes como celulares o tabletas, y la red cableada, por esto se le suele llamar en ocasiones como puente. Cuando se conecta varios puntos de acceso o WAP y los sincronizamos entre sí, se logrará crear una gran red sin la utilización de cables. Una idea practica para explicar el concepto de punto de acceso es que nos

podemos situar del lado del cliente y pensar que el punto de acceso provee un cable virtual o imaginario entre cada cliente y el AP. Así es como este cable inalámbrico virtual logra conectarnos a la red cableada que está ubicada luego de WAP y a los demás usuarios inalámbricos que se encuentren dentro de la red, sin causar complicaciones. (Salvetti, 2011, págs. 33-34)

Figura 10

Punto de acceso



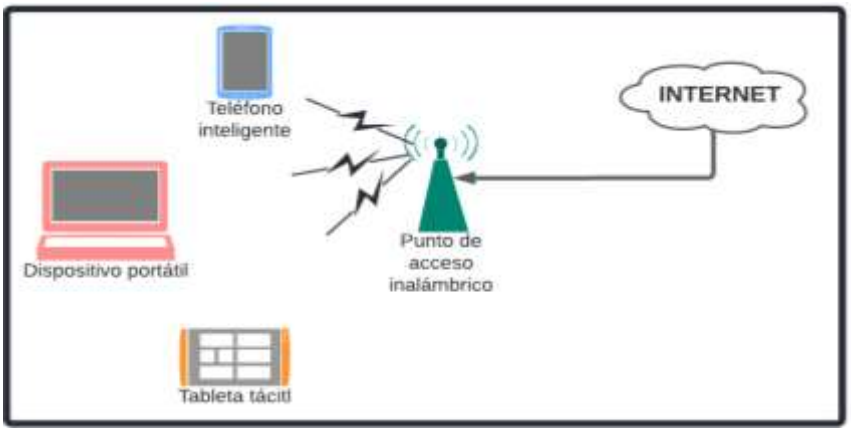
Nota. Diagrama de funcionamiento de un Punto de acceso. Tomada de (Martinez, 2021)

Existen de forma general dos características más sobresalientes de un punto de acceso, las cuales son la potencia que presente el transmisor y la otra seria la sensibilidad del receptor. La primera característica se refiere a que tan fuerte es la señal que irradia las antenas del equipo en dbm o mw. La segunda característica sobre la sensibilidad del receptor hace referencia a que tan débiles o bajos pueden ser los valores de potencia que puede receptar el equipo. Por tal razón se considera que un

equipo es bueno cuando su potencia de salida es alta y su sensibilidad de recepción permite detectar señales con potencias muy débiles.

Figura 11

Diagrama de funcionamiento de un AP



Nota. Diagrama de equipos que conforma un punto de acceso inalámbrico

Router inalámbrico

Si se tiene una conexión ADSL la cual os permita acceder a internet a través de nuestra línea telefónica, o por cable coaxial o fibra óptica, el dispositivo que es el encargado de conectarnos será el router. Pero esta no es la única forma de poder compartir internet a los clientes, ya que además de la función de compartir internet de forma cableada, también este tipo de dispositivos, gracias a la incorporación de antenas, pueden además brindar conexión inalámbrica. Es por esto que este tipo de equipos posee gran popularidad en el mercado ya que además de estas dos conexiones, también presentan un medio de configuración y monitoreo de la red que se puede realizar vía web. (Salvetti, 2011, pág. 35)

Figura 12

Funcionamiento de un router inalámbrico

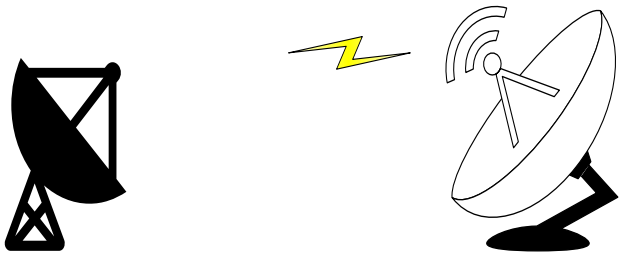
Nota. Funcionamiento de un router inalámbrico. Tomado de (redes inalambricas , s.f.)

Antenas

Son un elemento de gran importancia en las redes, ya que se encargan de transformar la energía de corriente alterna en campos electromagnéticos o viceversa, para ser irradiados hacia el cliente y captar la señal de estos. La calidad de estas influye directamente en la capacidad de los equipos para alcanzar una mayor o menor cobertura inalámbrica. (Salvetti, 2011, pág. 36)

Figura 13

Antenas



Nota. Antenas parabólicas usadas para formar conexiones PtP o PmP

Seguridad en las redes inalámbricas

Las redes inalámbricas presentan un alto inconveniente en cuanto a seguridad, la cual, a pesar de representar una alta gravedad, no ha recibo suficiente atención por parte de los desarrolladores de software y por consiguiente de los administradores de este tipo de redes.

En la actualidad la protección de la información y por consiguiente en flujo correcto de los datos se han convertido en un requisito imprescindible para los usuarios debido a que gran parte de la información que poseen se mueve a través de la red.

Debido a la alta vulnerabilidad de las redes inalámbricas, casi cualquier individuo que cuente con acceso a un equipo de cómputo y a información sobre el funcionamiento de las redes, podría hacer mal uso de esta información para vulnerar este tipo de redes con intenciones maliciosas logrando así conseguir datos personales, financieros o médicos del usuario. Sim embargo cabe recalcar que en la actualidad existen métodos y herramientas cada vez más sencillas y accesibles que ayudan hacer frente a este conflicto.

Como administradores de redes debemos tener en cuenta que este tipo de redes no debería ser más vulnerables en comparación con las redes cableadas y además que el nivel de seguridad de una red es directamente proporcional al coste económico.

Figura 14

Seguridad en redes inalámbricas

Nota. Representación gráfica de la seguridad en las redes inalámbricas. Tomado de (Martín, 2017)

Tipos de seguridad en redes inalámbricas

A lo largo de los últimos años se han desarrollado diferente técnicas, protocolos o algoritmos dirigidos principalmente a la protección de las redes inalámbricas los cuales se detallan a continuación.

WEP (Wired equivalen privacy)

Este es un algoritmo de seguridad opcional definido en el estándar IEEE 802.11, cuyos objetivos, según el estándar, son proporcionar confidencialidad, autenticación y control de acceso en las WLAN. La finalidad de este tipo de encriptación es

incrementar el nivel de seguridad en los equipos que lo tengan instalado o habilitado, con la finalidad de obtener un nivel de seguridad arecido al de los equipos cableados.

El protocolo de encriptación de datos para redes inalámbricas en mención fue desarrollado pensando en que su uso estaría dirigidos a equipos de costo bajo y que además sea de fácil configuración, es por esto que al usar WEP solo se usa una única clave de acceso para todos usuarios que se vayan a conectar a la red.

> “La funcionalidad de esta clave WEP es que se utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo externo que se encarga de la autenticación de claves, lo que obliga a escribir la clave de forma manual en cada cliente” (Suárez, 2012)

Esto a lo largo implica riesgos en la red ya que al tratarse de redes con gran cantidad de usuarios se toma el riesgo de que la clave de ingreso sea compartida con individuos ajenos lo cual derivara el aumento de control que debe manejar el individuo encargado de la administración de la red.

WPA (Wifi Protected Access)

El protocolo de acceso wifi corrige la mayoría de las falencias presentadas por el protocolo WEP y por ende se considera más confiable en cuanto a seguridad.

A diferencia de WEP en el cual solo se usaba una única clave para acceder a la red, en WAP se presenta al usuario o estaciones una variedad de claves lo cual lo vuelve más robusta y mejora así la integridad de los equipos y la información que se maneje.

WAP incluye las siguientes tecnologías:

IEEE 802.11 X

Es un estándar creado por la IEEE el cual está desarrollado para redes alámbricas y en el que se manifiesta el funcionamiento del control de acceso a la red a través de los puertos físicos de esta; de forma similar se tomaría para las redes inalámbricas en donde en punto de acceso seria símil de switch y los usuarios serían los clientes, funcionaria de la siguiente manera; las estaciones inalámbricas o usuarios para poder conectarse a la red necesitara de una clave para autentificarse y el punto de acceso a través de EAP y el uso de un servidor de autentificación puedan conocer y comprobar que la información ingresada por el usuario sea la correcta, el punto de acceso habilitaría su puerto.

EAP (Extensible Authentication Protocol)

Definido en el Registro federal de contribuyente o RFC número 2284 como el protocolo de autentificación extensible por sus siglas en el idioma inglés, en el que se tiene como meta llevar a cabo tareas de autentificación, autorización y contabilidad. El protocolo de autentificación extensible (EAP) fue diseñado inicialmente por el protocolo PPP, aunque WPA lo utiliza entre estación y el servidor de autenticación AAA Radius. Esta manera de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL. (Suárez, 2012)

Figura 15

Tipos de seguridad inalámbrica

Nota. Tipos de cifrado usados en redes wifi. Tomado de (acrylicwifi, 2019)

WPA2 Personal y Enterprise

WPA2 es un método de seguridad superpuesto sobre WPA, en la búsqueda de brindar una mayor protección de datos y capacidades relacionadas con el control de acceso a la red.

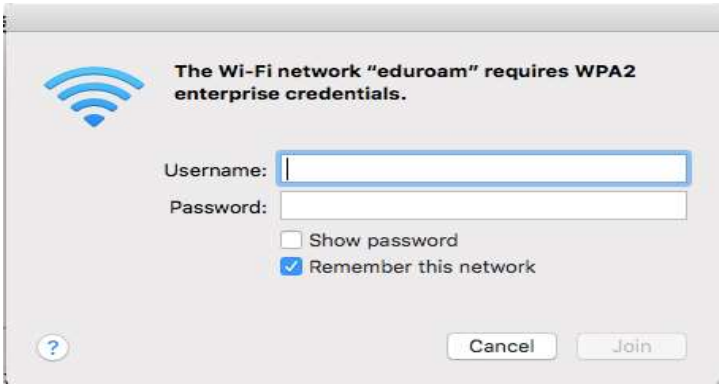
Otro autor ha afirmado lo siguiente:

> En la práctica, WPA2 ofrece a los usuarios de Wifi domésticos y empresariales la garantía de que únicamente sus usuarios autorizados van a poder acceder a la red inalámbrica**,** que es lo que se pretende en estos casos. Basado en el estándar IEEE 802.11i, WPA2 proporciona lo que se conoce como seguridad de nivel gubernamental. Lo hace gracias a la implementación del algoritmo de cifrado AES FIPS 140-2. Se trata de un algoritmo de cifrado compatible incluso con las exigencias del NIST, o Instituto Nacional de Estándares y Tecnología norteamericano. (Baldi, 2021)

Por otra parte, el cifrado para redes wifi según Bladi “Verifica a los usuarios de la red por medio de un servidor, siendo absolutamente compatible con las versiones previas de WPA. Alcanza, así un nivel de complejidad superior como alternativa”. (2021)

Figura 16

Autentificación para wpa2 Enterprise



Nota. Inicio de sesión en una red con cifrado wpa2-enterprise. Tomado de (MIE University , s.f.)

Medio de transmisión alámbricos

El canal es el medio de transmisión por el que viaja la señal portadora de la información que procede del emisor y es dirigida hacia el receptor. Actualmente los sistemas de comunicación tienen a su disposición, gracias a las investigaciones realizadas, multitud de tecnologías que nos permiten elegir un medio u otro en función de los requerimientos planteados en un proyecto.

En la actualidad, debido a los avances en la tecnología de las telecomunicaciones y la demanda de los usuarios por un acceso cada vez mayor a un mayor ancho de banda, se han inventado una gran variedad de medios de transmisión, ya sean alámbricos o inalámbricos. En el campo de los medios de transmisión físicos o alámbricos se pueden encontrar desde el cable telefónico, pasando por el cable coaxial y el par trenzado, hasta la invención de fibra óptica de vidrio o de plástico.

Figura 17

Formas de conexiones inalámbrica a internet

Nota. Equipos usados para conectarse a internet. Tomado de (econectia , 2017)

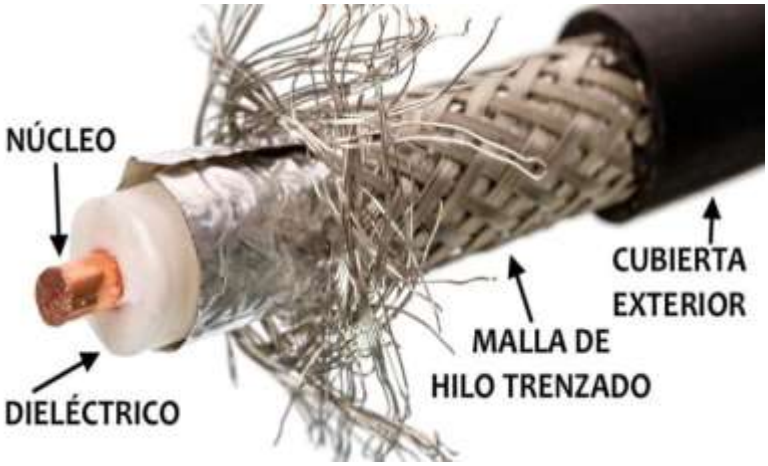
Por otra parte, en el campo de los medios de comunicación inalámbricos el medio que se sigue usando es sin duda alguna la atmosfera, aquí solo se ha evolucionado en cuanto al tipo de tecnología usada, empezando por el Bluethooth, el wifi, Wimax, hasta el Life, entre otras.

Cable coaxial

El cable coaxial consta de cinco capaz que se funden una con otra dando forma a un cable cilíndrico, el cual, desde el centro hacia afuera, está formado por un alambre de cobre, a su vez este está rodeado por un polímero de baja calidad que cumple con el papel de ser el aislante, una lámina fina de aluminio, una malla metálica la cual es el conductor externo y finalmente se coloca un plástico el cual será el recubrimiento o protección.

Figura 18

Partes de un cable coaxial



Nota. La imagen muestra las partes que forman un cable coaxial. Tomada de (Equipo editorial Etece, 2021)

Al ser unos de los primeros medios de trasmisión usados es de esperarse que su popularidad aún se mantenga y es por esto que aun entre los usos que se le dan encontramos los siguientes:

Tabla 1

Usos del cable Coaxial

USOS DEL CABLE COAXIAL	
Circuitos cerrados de videovigilancia	Se emplea en la conexión de cámaras dentro de un circuito cerrado de vigilancia
Entre el cable y Modem	Mezclan el uso de cable coaxial con otros tipos de cables para lograr establecer una conexión.
Distribución de señal de televisión	Ya sea en televisión analógica, digital o satelital, para llevar la señal desde la antena hasta en decodificar y luego hasta el televisor, se usa cable coaxial

Nota. La tabla presenta algunos de los usos más comunes del cable coaxial. Tomado de (Vásquez, 2015)

Tabla 2

Tipos de cable coaxial con su impedancia y uso

Tipo	Impedancia	Uso
RG-8	50 ohmios	10Base5
RG-11	50 ohmios	10Base5
RG-58	50 ohmios	10Base2
RG-62	93 ohmios	ARCnet
RG-75	75 ohmios	CTV (Televisión)

Nota. Se muestra algunos tipos de cables coaxial, su impedancia y sus usos comunes. Tomada de (Vásquez, 2015)

Par trenzado

Sin duda alguna este tipo de cable, son el medio físico que mayor popularidad tienen ya que son muy usados en los sistemas de comunicaciones en la actualidad, de forma más usual en las redes de datos como las de computadoras u ordenadores. Para explicar de mejor manera la estructura o forma en que esta diseñados el cable par trenzado es de forma simplificada la unión de dos cables de cobre u otro material conductor, que se trenzan o entrelazan entre si con el objeto de reducir el efecto electromagnético y de las diafonías.

Figura 19

Cable de par trenzado

Nota. Se observa los 4 pares de cables sin ningún tipo de blindaje. Tomada de (Castillo J. A., profesional review, 2020)

Tipos de cable de par trenzado

De acuerdo al tipo de pantalla o apantallamiento que presentes los cables de par trenzado, existirán también diferentes tipos de estos. Cuanto más apantallamiento o blindaje tengan los pares de cables de par trenzado, menor será el nivel de interferencia o diafonía que presenten.

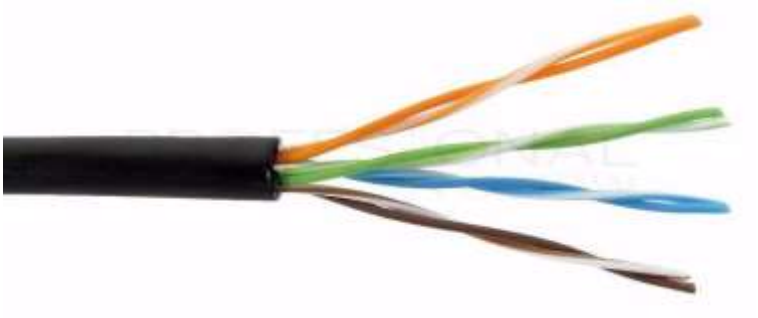
UTP (Unsshielded twisted pair) (Par trenzado sin apantallar)

Esta formados por un par de hilos aislados y trenzados entre sí, sin ningún tipo de recubrimiento metálico o pantalla que lo proteja frente a interferencias electromagnéticas o diafonías. Su costo económico es muy bajo, es fácil de manejar y su peso es reducido lo que lo convierte en un elemento fácil de instalar tanto en interiores como en exteriores donde no es recomendado ya que su exposición al medio lo destruiría rápidamente. (Castillo J. A., 2019)

Sim embargo, aunque mejora el comportamiento de las líneas abiertas frente a diafonías y emisión por ruido, se ve relativamente afectado por estos fenómenos y otros. Hoy en día se pueden encontrar ocho categorías de este tipo de cables, de las cuales mientras mayor es el numero de la categoría, mejor y más duradera será las protecciones que posean. (Castillo J. A., 2019)

Figura 20

Cable de red UTP



Nota. Cable de par trenzado sin apantallar. Tomado de (Castillo J. A., 2019)

FTP (Foiled Twisted Pair, Par Trenzado con pantalla)

Este tipo de cable de par trenzado presenta mejoras de protección, los 4 pares de cables se encuentran cubiertos de forma grupal por un recubrimiento plástico o de cualquier otro material que funcione como aislante y sobre este posee otro recubrimiento metálico encargado de evitar interferencias eléctricas. Sin duda que no es tipo de cable más óptimo, pero presenta mejorar con respecto al cable UTP.

Figura 21

Cable de red FTP

Nota. Se observa el blindaje plástico y metálico que recubren los 4 pares de cables. Tomado de (Castillo J. A., 2019)

STP (Shielded Twisted Pair, Par trenzado apantallado)

El cable de par trenzado es del siguiente tipo, cada par de cables tendrá una cubierta metálica diseñada para protegerlos. Presentan mejores prestaciones por lo cual están destinadas a ser usadas en redes donde se requiere mayor robustez en la seguridad, por lo que permiten instalaciones a mayores distancias sin causar muchas perdidas presentan un mayor costo económico.

Figura 22

Cable de red STP

Nota. Cable de par trenzado con apantallado individual para cada par de cables. Tomado de (Castillo J. A., profesional review, 2019)

SFTP (Screeened Foiled Twisted Pair) (Laminado apantallado individual)

Los cables de red SFTP se basa o toma como referencia la construcción del cable FTP, pero con un gran cambio ya que en este el apantallamiento presente mejoras, se agrega un laminado de malla metálica LSZH que recubra los pares de cuatro cables para aumentar la protección.

Figura 23

Cable de red SFTP

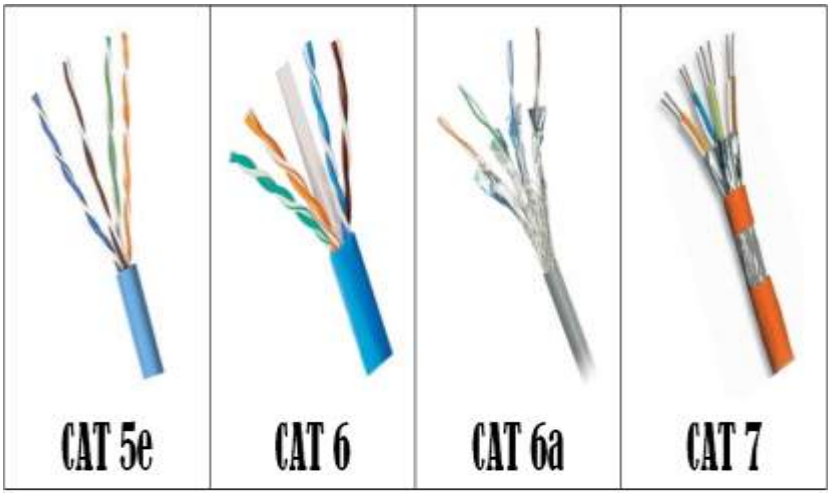
Nota. El cable posee una guía plástica ubicada en el centro y un apantallado metálico. Tomado de (Castillo J. A., profesional review, 2019)

Categorías de los cables de par trenzado

Cada vez los usuarios de las redes requieren de mejores velocidades de navegación y mayor seguridad en sus redes, es por esto que se han creado a lo largo de la historia diferentes tipos de cables, mismo que se han organizado por categorías.

Figura 24

Categorías de cables de par trenzado



Nota. Se muestra custro de las categorías más usadas de los cables. Tomada de (telectronika, 2018)

Tabla 3

Categorías de cable Ethernet

CATEGORÍA	VELOCIDAD	FRECUENCIA	VELOCIDAD DE DESCARGA
ETHERNET CAT 5	100 Mbps	100 MHz	15,5 MB/s

CATEGORÍA	VELOCIDAD	FRECUENCIA	VELOCIDAD DE DESCARGA
ETHERNET CAT 5E	1000 Mbps	100 MHz	150,5 MB/s
ETHERNET CAT 6	1000 Mbps	250 MHz	150,5 MB/s
ETHERNET CAT 6A	10000 Mbps	500 MHz	1.250 MB/s ó 1,25 GB/s
ETHERNET CAT 7	10000 Mbps	600 MHz	1,25 GB/s
ETHERNET CAT 7A	10000 Mbps	1.000 MHz	1,25 GB/s
ETHERNET CAT 8	40000 Mbps	2.000 MHz	5 GB/s

Nota. En la figura se muestra las categorías de cables Ethernet con la velocidad, frecuencia y velocidad de descarga que estos soportan. Tomado de (Fernández, 2022)

Cable de Fibra óptica

Una fibra óptica es un medio de transmisión por cable el cual es capaz de transmitir un haz de luz introducido en uno de sus extremos mediante una fuente láser o led. Cuando se introduce el haz de luz, esta queda retenida en su parte interior o núcleo evitando así que se escape de la fibra y pueda viajar largas distancias a velocidades mayores que la que pueden alcanzar sus homólogos.

Figura 25

Cable de fibra óptica

Nota. Se observa cómo está formado un cable con varios hilos de fibra óptica. Tomada de (Andrade, 2020)

Este medio de transmisión, al igual que el par trenzado y el cable coaxial, está formado por tres capaz las cuales son el núcleo o core, el revestimiento o cladding y la cubierta o buffer.

Núcleo o Core.

Está ubicado en el centro, es la parte más pequeña en dimensión del diámetro el cual mide de 8 a 12,5 micrómetros, es por donde viaja el haz de luz de forma confinada y rebotando en las paredes sin poder escaparse gracias a la diferencia de densidades que tienen el núcleo con respecto al revestimiento.

Revestimiento o Cladding.

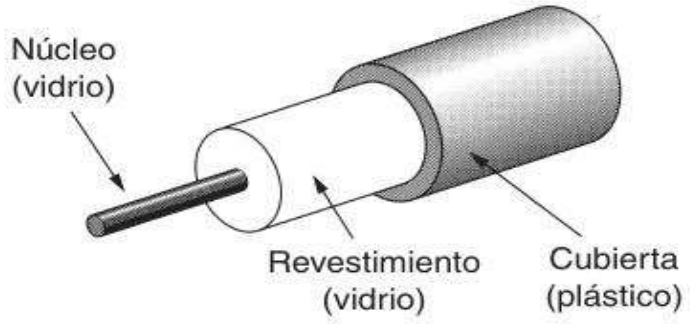
Esta capa, tiene como objetivo primordial el no permitir que el haz de luz que viaja por la fibra se escape del núcleo. Su diámetro es superior al del núcleo y va desde los 62.5 a los 125 micrómetros.

Cubierta o Buffer.

Está formada por un material plástico o polímero, cuya misión es la de proteger al núcleo y al revestimiento de posibles daños ocasionado por el manejo o manipulación de la fibra durante la instalación, además de acuerdo al color que se le asigne, en ocasiones donde existen múltiples cables de fibra óptica, como un diferenciador. Su diámetro es de 245 micrómetros.

Figura 26

Partes de un cable de FO



Nota. Se puede observar las partes de un hilo de fibra óptica con sus nombres en inglés y español. Tomado de (Mariana, 2015)

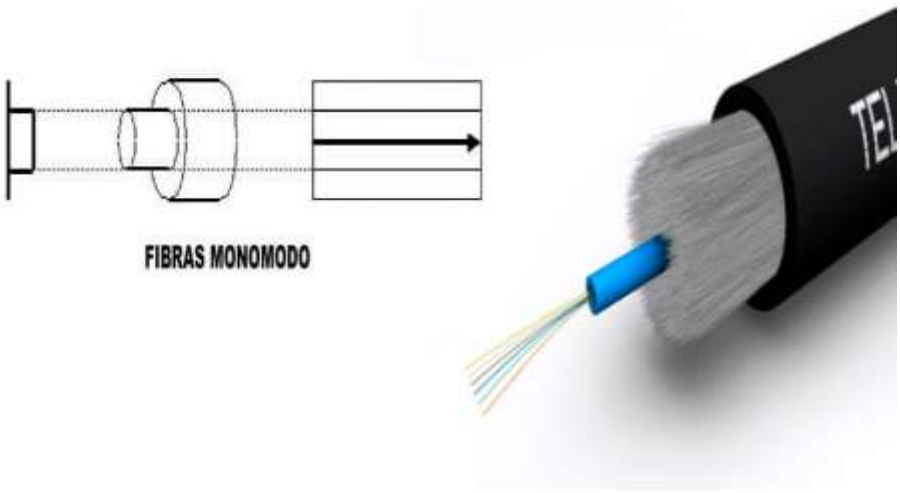
Tipos fibra óptica

Monomodo

Posee un núcleo de diámetro muy pequeño lo cual permite que los rayos de luz viajen por un solo trayecto, eliminan la dispersión modal por lo que es apta para transmisiones a altas velocidades a distancias mayores.

Figura 27

Fibras ópticas monomodo



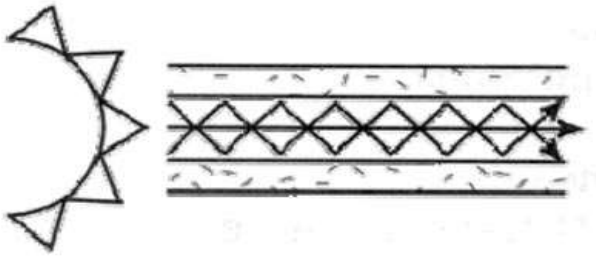
Nota. Se muestra un cable con varios hilos de fibra monomodo y como viaja un haz de luz por el núcleo de esta. Tomada de (Rico, s.f.)

Multimodo

Los rayos de luz generados por la fuente viajan dentro de la fibra a por diferentes trayectos lo cual produce dispersión modal el cual consiste en el ensanchamiento del pulso final con respecto al inicial, es por esto que se usa para distancias menores a los 4 kilómetros y además por que las velocidades de transmisión en comparación con las aceptadas por la fibra monomodo son mucho menores. El diámetro del núcleo es de 50 a 62,5 micrómetros.

Figura 28

Funcionamiento de fibra óptica multimodo



Nota. De esta manera viajan los haces de luz por el núcleo de una fibra multimodo. Tomada de (Rodriguez, 2014)

Servidor

Se entiende como servidor aquel elemento que es capaz de brindar un servicio a un usuario, de forma más detallada:

> Un servidor puede encontrarse en un local típico el cual ofrece un servicio de computadoras a sus clientes. La máquina que tiene un cajero da un servicio por lo tanto se podría considerar como un servidor, el cual estaría encargado de buscar los productos o actividades con sus valores o códigos asignados, y si este cajero dejase de funcionar entonces por consiguiente los servicios de facturación de esta entidad donde se esté usando dejarían de funcionar. Los servidores son grandes ordenadores o equipos que brindan un servicio al cliente que lo solicite, es por esto que, a diferencias de las computadoras normales usados por las personas, la arquitectura, hardware y software que estos posean deben ser de mejor calidad, capacidad y velocidad. (Marchionni, 2011, pág. 23)

Figura 29

Servidor

Nota. Cuarto de servidores. Tomada de (Etece, 2021)

Tipos de servidores

Debido a su versatilidad existen diferentes tipos de servidores los cuales pueden encontrarse instalados de forma físicos o de forma virtual. Además, estos también se clasifican de acuerdo a su capacidad, a los fabricantes o, por último, de acuerdo a los servicios que brindan al usuario. En base a esto a continuación se describen los diferentes tipos de servidores de acuerdo al servicio que prestan:

Servidores de impresión

En este tipo de servidores, un conjunto de impresoras se conecta a la red esperando a que los usuarios de dicha red empiecen a realizar sus peticiones de impresión, las cuales son realizadas de acuerdo al orden de llegada.

Figura 30

Diagrama de un servidor de impresión

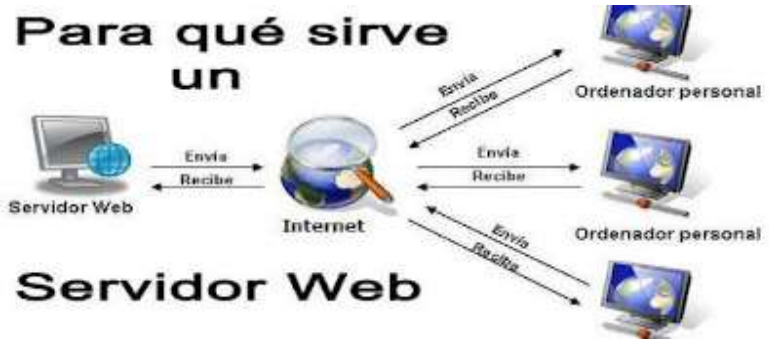
Nota. Equipos que conforman un servidor Tomado de (Marker, 2021)

Servidores Web

Este tipo de servidores tiene como una de sus funciones la de almacenar sitios web y posteriormente cumplir con otra de sus tareas que es la de devolver esta información a los clientes que lo soliciten

Figura 31

Topología de un servidor web



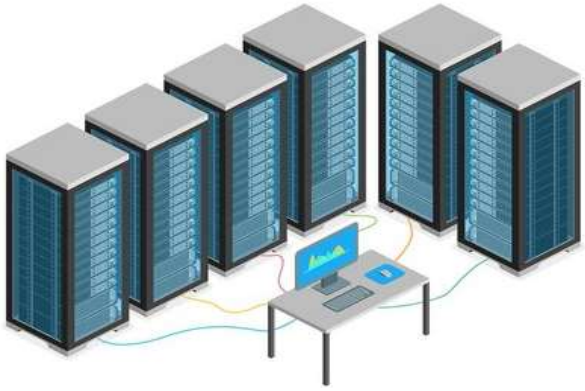
Nota. Equipos que conforman un servidor web. Tomado de (Torres, s.f.)

Servidores de base de datos

La importancia de este tipo de servidores radica en la capacidad de encausar enormes cantidades de datos y producir información. Para abarcar toda esta cantidad de información, suelen estar conectadas a u repositorio.

Figura 32

Servidor de base de datos



Nota. Equipos que forman un servidor de base de datos. Tomado de (comidoc, s.f.)

Servidores de correo electrónico

Pueden administrar todo el correo electrónico de la empresa en un solo lugar. Además, trabajan con almacenamiento como causa de que procesan una cantidad de datos grande. Los correos electrónicos se almacenan allí y se reenvían a clientes y servidores de seguridad, analizadores y replicadores. Algunos también brindan opciones de seguridad, como protección contra correo no deseado, listas blancas, listas negras y antivirus.

Figura 33

Servidor de correo electrónico

Nota. Equipos de un servidor de correo electrónico. Tomada de (area de soporte, 2014)

Servidores de directorio

Directory Service (DS) es una aplicación o conjunto de aplicaciones que almacenan y organizan información sobre los usuarios de la red informática y los recursos de la red, lo que permite a los administradores controlar el acceso de los usuarios a los recursos en una red específica.

Servidores de comunicaciones

Proporcionan chat, telefonía IP, teleconferencias, video y más. También pueden proporcionar servicios previos al servicio si están conectados a una consola telefónica.

Servidores de archivos

Nos permiten compartir y almacenar contenido de forma segura y ofrecen más espacio de almacenamiento adicional que lo que el de una computadora personal o de

escritorio. Se puede conectar a varias unidades de capacidades diferentes para mejorar su funcionalidad.

Servidores de seguridad

Están diseñados para escanear la red en busca de virus, máquinas desactualizadas por falta de parches del sistema operativo, computadoras con cierto software instalado y muchas otras acciones.

Servidores proxy

Brindan conexión a Internet. Por regla general, contienen cortafuegos para los que se crean reglas para permitir la visualización de determinadas páginas y bloquear otras. Pueden redirigir la navegación y mostrarnos una señal de advertencia o una violación de la política de la empresa.

Figura 34

Servidor proxy

Nota. Topología básica de un servidor proxy. Tomado de (Borges, 2019)

Servidores de servidores virtuales

Un servidor puede contener múltiples servidores virtuales, el conflicto de esto es que el usuario final no observa la diferencia. La única manera de poder usar todas sus características es a través de la gestión de estos y poder así hacer uso de las características que poseen.

Servidores particulares

Un servidor privado o particular tiene como tarea crear particiones virtuales separadas de un servidor físico, esto lo convierte en un pequeño servidor dedicado para una actividad personal. Al ser un servicio creado por uno mismo y para uso personal este elemento administra sus propios recursos, que no comparte con otros servidores, a diferencia del alojamiento de servidor compartido.

Radius

Radius son las siglas de Remote Authetication Dial-Up Server, misma que traducida al idioma español significaría Servidor de autentificación remota. De forma global RADIUS es un protocolo enfocado en cumplir las normas de seguridad en una red como lo son: la autorización, autentificación y el arqueo. Este protocolo es la continuación de AAA, la cual es una idea enfocada en la protección de las redes y que significa Authentication+ Authorization+ Accounting, con su traducción al idioma español de Autenticación+ Autorización+ Arqueo.

El protocolo en mención toma las bases de esta idea de AAA y además toma por una parte su código fuente y a parte del personal que trabajaba en dicha idea, es por

esto que se podría decir que es la versión mejorada de AAA. Estas tres directrices tomadas de la idea original lo que nos permiten es que al aplicar este protocolo el usuario o en si la red en la que se aplique, brinde al administrador de la red un control más minucioso del acceso, tráfico de la red, generación de reportes, estadísticas y demás mecanismos de control.

Figura 35

Topología de un servidor Radius

Nota. Funcionamiento de un servidor de autentificación Radius. Tomada de (Sanz, 2013)

Previo a la invención de este protocolo, la forma idea de AAA era algo que se debía realizar de forma individual y aislada una de la otra ya que en el caso de necesitar que un usuario autentifique, luego se le autorice el acceso y demás; la forma de configurar esto era a través de la configuración manual de cada uno de los servicios por separado, lo cual alargaba el tiempo para acceder a una red y además la puesta en marca en sí de dicha red. Gracias a la estandarización de este protocolo se logró mejorar de forma exponencial la vida de los administradores de red y por consiguiente la de los usuarios.

Tipos de servidores radius

A causa de su versatilidad, los servidores Radius son ampliamente usados a lo largo del mundo, con mayor relevancia en entornos UNIX, Al compartir un código fuente cada variante de estos servidores comparten la esencia y características muy parecidas entre sí, la diferencia es que cada nuevo servidor está enfocado en mejorar o superar a su antecesor u homologo y esto será una de las características que los diferencia ya que, al contar con mejoras tecnológicas, esto potencia sus ventajas.

Al igual que con los sistemas operativos u otras herramientas de ofimática o en forma general de software, existen tantos servidores de licencia libre, es decir sin costo para su uso, y por otro lado aquellos que para su implementación se requiere hacer uso de una licencia con un coste económico.

Servidores radius no licenciados

Servidor Free radius

Este tipo de servidor de autenticación AAA es uno de los conocidos en la actualidad, además se puede decir que:

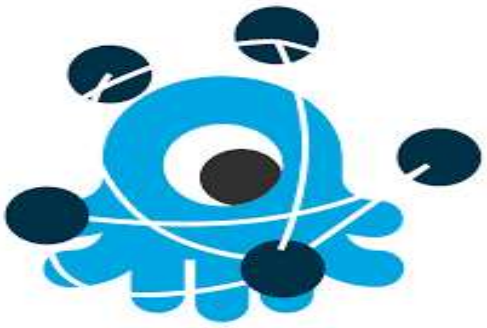
Free RADIUS es un paquete estándar el cual es soportado por múltiples sistemas operativos ya sean estos licenciados o gratuitos, permite realizar instalaciones de gran envergadura empleando múltiples servidores AAA. (Carlos A. Vásquez, 2015, pág. 6)

Soporta conexiones con diferentes clases de bases de datos, tanto para la autorización como para la contabilidad, es compatible con una gran cantidad de métodos de autenticación que en conjunto forman un sistema AAA muy robusto y

confiable. Una de las grandes ventajas que representa utilizar Ubuntu Server como sistema operativo base es el manejo de un repositorio actualizado constantemente por los desarrolladores, esto agiliza el proceso de instalación de cualquier software y sus dependencias, además que supone un ahorro para los individuos que quieran usarlo porque no deberá hacer uso de una licencia para su uso. (Carlos A. Vásquez, 2015, pág. 6)

Figura 36

Freeradius



Nota. Logo del servidor freeradius creado por los desarrolladores de este servicio. Tomada de (freeradius, s.f.)

Cistron

"Cistron RADIUS era un servidor de autenticación y contabilidad para servidores de terminales que hablan el protocolo RADIUS. El autor es Miquel van Smoorenburg . Cistron Radius tuvo una buena racha durante bastantes años, pero es viejo y ya no recibe mantenimiento. Deberías usar su sucesor, Freeradius." (Smoorenburg, 2012) Algunas de las características de este servidor son:

- Es gratis (bajo la GNU GPL).
- Admite acceso basado en HuntGropus.
- El archivo de usuario se procesa en orden, por defecto son posibles múltiples entradas y todas las entradas pueden ser "fallidas" opcionalmente.
- Intercepta todos los archivos de configuración en memoria, incluidos los archivos de usuario.
- Mantiene una lista de usuarios para iniciar sesión.
- Admite el uso simultáneo de parámetros X.
- Admite atributos especificados por el proveedor, incluidos los USR no estándar.
- Soporta proxy.
- Admite el paquete "en vivo"
- Puede replicar datos de uso de cuentas entre servidores.

XtRadius

Según (xtRadius, s.f.) XtRadius es una implementación gratuita de servidor de radio, La principal diferencia entre XtRadius y otros servidores Radius es que le permite ejecutar comandos para gestionar la autenticación y la contabilidad de los usuarios. Una ventaja de esta función es que, en lugar de usar el archivo de usuarios de Radius o el archivo de contraseña del sistema para la autenticación, puede llamar a un script/aplicación que puede consultar cualquier fuente (como una base de datos SQL) y verificar las condiciones válidas antes. permitir que un usuario inicie sesión. A diferencia de otras soluciones, no se requieren parches. Basado en el radio de Cistron.

Servidores radius licenciados

Radiator

Radiator Server es uno de los mejores servidores Radius, permite comprobar y controlar de forma segura el acceso a redes alámbricas e inalámbricas a la vez que se puede configurar de forma muy sencilla y adaptarse a trabajar con diferentes dispositivos de fabricantes distintos lo que les permite una mayor adaptación a los requisitos presente y futuros de las redes, además es uno de los servidores que ofrece gran variedad de métodos de autentificación EAP.

Figura 37

Radiator

Nota. Logo del servidor radiator. Tomada de (radiatorsoftware, s.f.)

Software libre

Se conoce como software libre a todos los programas en los que se permita la modificación de su código fuente, además su descarga, uso o compartición es totalmente libre de costos económicos. Sim embargo esta definición no es del todo acertada ya que se tiene la idea que al ser libre por consiguiente es gratis y esto no es así.

Existen varios programas o aplicaciones que son gratis, pero esto no quiere decir que sean libres, ya que gratis lo es solo para que el usuario pueda usar el producto como tal, pero no podrá bajo ninguna circunstancia copiar, modificar sin el permiso de su desarrollador.

Sin duda que la comprensión sobre lo que implica que un software sea libre esta ha libre albedrio de los interesados, ya que como explicamos anteriormente, muchos son los puntos de vista sobre que es el software libre. Ejemplos de estos son que algunos individuos entienden que un software es libre porque su código fuente está a disposición de todos lo que lo necesiten, otros por su parte entienden que un software es libre cuando dentro de sus objetivos está el de hacer libres a los usuarios.

En fin, desde el punto de vista que se intente definir este término, muchas serán sus variaciones, pero sim embargo hay algo en lo que coinciden la mayoría de personas, y es que un software es libre cuando este pueda ser usado, modificado, estudiado y distribuido sin ninguna clase de impedimentos. El ejemplo más claro de esto es Linux.

Figura 38

Software libre

Nota. Ejemplo de un código fuente libre creado por un desarrollador. Tomado de (Etece, 2019)

Ubuntu server

Ubuntu server es un sistema operativo desarrollado por la empresa canonical, es de licencia libre, es decir que para su utilización no se necesita disponer de una licencia con un costo económico para realizar su activación, solo basta con ingresar a las paginas oficiales de descarga de Ubuntu y buscar la versión que se desea instalar.

Ubuntu generalmente es reconocido por los usuarios gracias a su versión de escritorio debido a que es sin duda el más usado en cuanto a sistemas de GNU Linux, pero Ubuntu server está enfocado en la utilización y manejo de servicios.

Existen un sinfín de versiones de este sistema operativo, siendo en el año 2022 la versión 222.04 la más actual. Al igual que las versiones para escritorios, Ubuntu server también ha tenido que sufrir cambios y es por esto que ha dejado de lado la creación de sistemas o versiones enfocadas en trabajar con procesadores de arquitectura de 32 bits.

Ubuntu server al funcionar como un servidor tiene la función de dar servicios, programas, archivos o datos a otros equipos que lo soliciten los cuales se denominan consumidores. Su función es la guardar los archivos para luego compartirlos, en conclusión, un servidor es un homólogo de un equipo de cómputo personal, solo que a niveles de almacenamiento y procesamiento más elevado.

Figura 39

Ubuntu server 20.04 LTS

Nota. Imagen de la ISO 20.04 LTS de Ubuntu server. Tomada de (Rodríguez, 2020)

Capitulo III

Desarrollo del tema

Mediante un estudio técnico realizado por medio de visitas a la Unidad Educativa “Camino del Inca”, que es una institución fiscal de la parroquia Turubamba cuyo ingreso a dicha institución se muestra en la figura 40, se pudo conocer el área donde se encuentra ubicada la infraestructura de telecomunicaciones y los equipos que conforman dicha red, los cuales son un router cisco, un switch de 48 puertos y un router Tp-link TL-WR940 N como se muestra en la figura 41.

Figura 40

Unidad educativa fiscal "Camino de Inca"

Nota. Imagen frontal de ingreso a la institucion de educacion fiscal.

Figura 41

Caja de equipos de red de la UECI

Nota. Caja donde están colocados los equipos de red que posee la institución.

También se pudo conversar con varios docentes, como se muestra en las figuras 42 y 44, sobre la cobertura, conectividad y calidad del servicio; se reconoce el área designada por las autoridades, Figura 43, en la cual se necesita la instalación de un punto de acceso con mejores características

Figura 42

Sala de docentes UECI

Nota. Docentes de la institución reunidos en la sala de docentes

Figura 43

Zona de la Instalación del AP

Nota. Se muestra en un círculo color rojo el lugar de la institución donde se instalará el punto de acceso

Figura 44

Sala de docentes

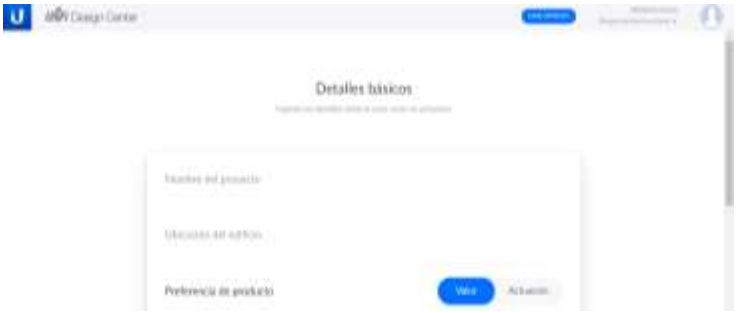
Nota. Vista panorámica de la sala de docentes

UniFi Design Center

Como punto inicial para la implementación de la nueva red wifi en la Unidad Educativa “Camino del Inca” situada en la ciudad de Quito, haremos uso de la herramienta de diseño de redes inalámbricas de la empresa UBIQUITI cuyo nombre es UniFi Design Center, para esto debemos crear una cuenta en Ubiquiti y posteriormente, abrimos en un navegador de nuestra preferencia el software UniFi Design Center y seleccionamos en el apartado de nuevo proyecto como le muestra en la figura 45.

Figura 45

Creación de nuevo proyecto en UniFi Design Center

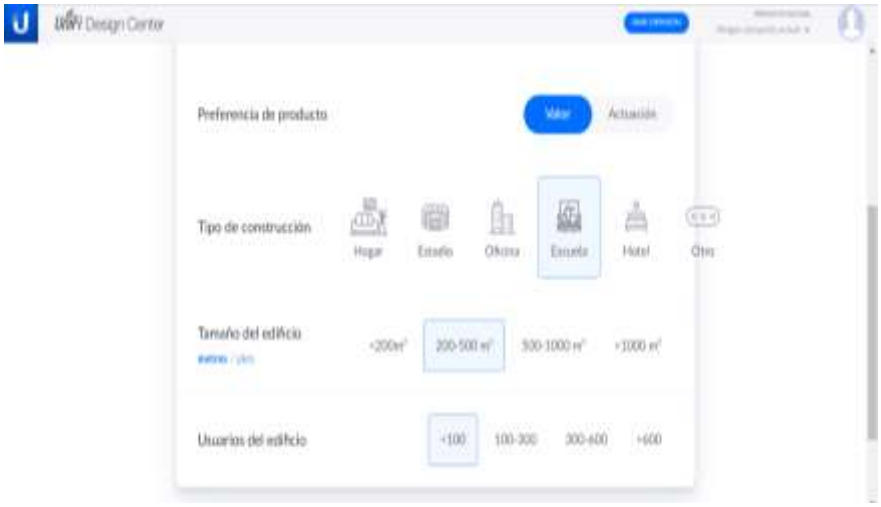


Nota. Al crear un nuevo proyecto en UniFi Design Center, se deben colocar datos como el nombre y la ubicación del edificio para que la herramienta pueda mejorar la simulación.

Una vez dentro del software empezaremos un nuevo proyecto, aquí debemos colocar datos acordes al diseño de la red que vamos a simular, como el nombre, tipo de construcción, tamaño, entre otros

Figura 46

Parámetros del nuevo proyecto



Nota. Se debe seleccionar el tipo de edificio, un área aproximada y la cantidad de usuarios para los que se va a diseñar la red wifi.

A continuación, seleccionaremos las casillas acordes al proyecto que se desea simular, para nuestro caso en específico seleccionamos la primera opción correspondiente a gestión de redes cableadas y Wifi, acto seguido pulsamos en crear proyecto como se muestra en la figura 47.

Figura 47

Tipo de red que se desea simular

Nota. Se debe seleccionar el tipo de red que se pretende simular, ya sea esta wifi o de videovigilancia

Para realizar el diseño del edificio o construcción, tenemos las opciones de ayudarnos con una imagen, mapa o plano de la estructura, o podemos dibujar desde cero todo como se observa en la figura 48. En nuestro caso nos ayudamos de un mapa de la institución educativa donde se va a implementar la red.

Figura 48

Mapa de la UECI

Nota. Se debe subir un archivo en formato imagen para guiarnos con el diseño del recinto.

Con ayuda de las herramientas que posee el software, establecemos una escala de medición para alguna pared conocida, y a continuación en el icono (martillo) dibujamos las paredes y las puertas de las aulas y oficinas que existen en la estructura. Como se observa en la figura 49.

Figura 49

Gráfico de paredes en el mapa de la UECI

Nota. Dibujamos con una herramienta del software, las paredes, puertas y ventanas presentes en el reciento educativo.

Para la simulación usaremos un equipo que posee caracteristicas similares al equipo que se planea adquirir como en la figura 50, el cual sera dual band, de 450 Mbps en 2.4 Ghz y de 800Mbps en 5Ghz.Colacamos el equipo en el punto donde se ha dispuesto la instalacion y observamos como de difrerentes colores las areas donde existen meyor cobertura.

Figura 50

Simulación de la cobertura wifi

Nota. Ubicamos un equipo y observamos la zona donde brinde mayor cobertura.

Adicionalmente, escogemos el cable y lo dibujamos por donde será la ruta del cableado de red y nos arroja una medición muy aproximada al valor real de los metros de cable UTP que se necesitará para la instalación como se muestra en la figura 51. Cabe mencionar que en este caso no toma en consideración que el equipo que vamos a usar posee una conexión desde el switch principal hasta el puerto LAN del PoE y desde el puerto Poe hasta el equipo que se colocara en el techo.

Figura 51

Simulación de la red con equipos AP y el cableado de red

Nota. Podemos colocar elementos a la red y ver las distancias u otras características de estos.

Gracias a esta simulación podemos conocer las zonas donde los docentes podrán tener una mejor cobertura de la red inalámbrica que crearemos y además una idea estimada de la cantidad de materiales que se necesitarán para la implementación.

Equipos

Mediante la investigación realizada se logró determinar que la institución debe contar con un dispositivo de redes el cual será usado para implementar un punto de acceso que brinde al usuario, en este caso los docentes, mayor cobertura y sobre todo seguridad al momento de navegar por internet, es por esto que se ha realizado una tabla de los elementos necesarios para la implementación de la red con el servidor de autentificación y otras tablas comparativas en la cual se muestran varios equipos.

Tabla 4

Equipos que se usaran

Nombre	Cantidad
Punto de acceso	1
Cable de par trenzado	20 m
Conectores RJ45	8 unidades
PoE	1
Canaletas	3 unidades
Tornillos	12 unidades
Gabinete	1
Disco HDD	1 (mínimo 50 GB de almacenamiento)
CPU	1 (Arquitectura de 64 bits)
Memorias RAM	1 (mínimo 1GB DDR2)
Placa madre	1
Cable de poder AC	2 unidades
Cable HDMI	1
Monitor	1
Grapas plásticas	12 unidades

Nota. En la tabla se enlistan los equipos que se usaran, con sus respectivas características

Características de hardware

Para analizar entre diferentes opciones, el mejor equipo tanto de software como de hardware que se instalara en la institución, se usaron tablas en las cuales se enlistan las características de estos elementos como lo muestra la tabla 5.

Tabla 5

Puntos de acceso con cifrado Wpa2 Enterprise

Tp-Link EAP 225 AC135	
Interfaz	Gigabit Ethernet (RJ-45) Puerto × 1 (Soporte IEEE802.3af PoE y PoE pasivo)
Bloqueo de Seguridad	Si
Botón	Restablecer
Fuente de alimentación	802.3af/atPoE PoE pasivo de 24V (+ 4,5 pinos; -7,8 pinos. Adaptador de PoE incluido)
Consumo de Energía	UE: 10.5 W EE. UU: 12.6 W
Dimensiones	8.1 × 7.1 × 1.5 in (205.5 × 181.5 × 37.1 mm)
Tipo de Antena	3 Omni interno - 2.4 GHz: 4 dBi - 5 GHz: 5 dBi
Montaje	Techo / montaje en pared (kits incluidos)

Tp-Link EAP 225 AC135

Características inalámbricas

Estándares inalámbricos	IEEE 802.11ac / n / g / b / a
Frecuencia	2.4 GHz y 5 GHz
Velocidad de la señal	- 5 GHz: hasta 867 Mbps - 2.4 GHz: hasta 450 Mbps
Funciones Inalámbricas	- Múltiples SSID (hasta 16 SSID, 8 para cada banda) - Habilitar / Desactivar la radio inalámbrica - Asignación automática de canales - Transmitir control de potencia (ajustar la transmisión de energía en dBm) - QoS (WMM) - itinerancia sin costos - Omada Mesh - Dirección de banda - Saldo de carga - MU-MIMO - Equidad de tiempo aire - Beamforming

Tp-Link EAP 225 AC135	
Seguridad Inalámbrica	- Límite de tarifas - Reiniciar horario - Horario inalámbrico - Estadísticas interiores básicas en SSID / AP / Cliente - Autenticación del portal cautivo * - Control de acceso - Filtrado inalámbrico de direcciones Mac - Aislamiento inalámbrico entre clientes - SSID un mapeo VLAN - Detección de AP rebelde - Soporte 802.1X - CE
Poder de transmisión	≤20 dBm (2.4 GHz, EIRP) ≤23 dBm (5 GHz, EIRP) - FCC: ≤24 dBm (2.4 GHz) ≤22 dBm (5 GHz)

Tp-Link EAP 225 AC135	
Gestión	
Aplicación Omada	Si
Control LED de encendido / apagado	Si
Control de acceso MAC de gestión	Si
SSH	Si
Gestión basada en la web	HTTP/HTTPS
Gestión VLAN	Si
Otros	
Certificación	CE, FCC, RoHS
Contenido del paquete	- AC1350 Punto de acceso inalámbrico de montaje en techo Gigabit MU-MIMO EAP225 - Adaptador de PoE pasivo - Cable de alimentación - Kits de montaje - Guía de instalación

Tp-Link EAP 225 AC135	
Requisitos del Sistema	Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows10, Linux
Medio Ambiente	- Temperatura de funcionamiento: 0–40 ° C (32–104 ° F) - Temperatura de almacenamiento: -40–70 ° C (-40–158 ° F) - Humedad de funcionamiento: 10–90% HR sin condensación - Humedad de almacenamiento: 5–90% HR sin condensación

Tp-Link EAP 115	
Características de hardware	
Interface	1 puerto Fast Ethernet (RJ-45) Soporta PoE IEEE802.3af）
Botón	Reset
Fuente de alimentación	PoE o Fuente de Alimentación de 9VDC / 0.6A
Consumo de Energía	2.8W
Dimensiones	189.4×172.3×29.5mm. (7.5×6.8×1.2 in.)
Tipo de antena	2 antenas Internas Omnidireccionales de 4dBi
Montaje	Montaje de Techo / Pared (Kits incluidos)

Tp-Link EAP 115	
Características inalámbricas	
Estándares Inalámbricos	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Frecuencia	2.4-2.4835GHz
Tasa de señal	- 11n: Hasta 300Mbps(dinámico) - 11g: Hasta 54Mbps(dinámico) - 11b: Hasta 11Mbps(dinámico)
Sensibilidad de recepción	- 300M: -71dBm@10% PER - 150M: -75dBm@10% PER - 54M: -78dBm@10% PER - 11M: -93dBm@8% PER - 6M: -92dBm@10% PER - 1M: -96dBm@8% PER
Funciones inalámbricas	- Múltiples SSIDs （Hasta 8 SSIDs） - Habilitar/Deshabilitar la Emisión Inalámbrica - Asignación de Canal Automático - Control de Potencia de Transmisión (Potencia de Transmisión Ajustable en dBm） - QoS (WMM) /-Limitador de Velocidad - Reboot Agendado /-Horario Inalámbrico - Estadísticas Inalámbricas basadas en SSID/AP/Cliente

Tp-Link EAP 115	
Seguridad inalámbrica	- Autenticación mediante Portal Cautivo -Control de Acceso Filtrado de Direcciones MAC Inalámbrico - Aislamiento Inalámbrico entre Clientes - Mapeo SSID a VLAN - Detección de Punto de Acceso No Autorizado - Soporta 802.1X WEP 64/128/152-bit / WPA / WPA2-Enterprise, WPA-PSK / WPA2-PSK
Potencia de transmisión	CE: <19dBm FCC: <21dBm
Administración	
Omada app	Si
Led ON/OFF	Si
Telnet	Si
SSH	Si
Web- based management	HTTP/HTTPS
Gestión VLAN	Si
Otros	
Certificación	CE, FCC, RoHS

Tp-Link EAP 115	
Contenido del paquete	- Punto de Acceso de Montaje en Techo Inalámbrico N a 300Mbps EAP115 - Adaptador de Corriente - Kit de Montaje - Guía de Instalación
Requisitos del Sistema	Microsoft Windows 10/8/7/Vista/XP
Medio Ambiente	- Temperatura de Funcionamiento: 0℃~40℃ (32℉~104℉) - Temperatura de Almacenamiento: -40℃~70℃ (-40℉~158℉) - Humedad de Funcionamiento: 10%~90% sin condensación - Humedad de Almacenamiento: 5%~90% sin condensación

Tp-Link TL-WR941HP	
Características de hardware	
Procesador	Single-Core CPU
Puertos Ethernet	- 1× 10/100 Mbps WAN Port - 4× 10/100 Mbps LAN Ports
Botones	- Wi-Fi On/Off Button, -Power On/Off Button - WPS Button/-Reset Button

Tp-Link TL-WR941HP	
Energía	12 V ⎓ 1.5 A
Características inalámbricas	
Estándares	IEEE 802.11n/b/g 2,4 GHz
Velocidad Wifi	2,4 GHz: 450Mbps (802.11n)
Capacidad Wifi	Legado
Modos de trabajo	- Modo de enrutador, - Modo de punto de acceso, - Modo extensor de rango
Seguridad	
Cifrado Wifi	- WEP / WPA/ WPA2 - WPA/WPA2-Empresa (802.1x)
Seguridad de la red	- SPI Firewall - Control de acceso Enlace de IP y MAC - Gateway de capa de aplicación
Red de invitados	1 × red de invitados de 2,4 GHz
Servidor VPN	- Open VPN, - PPTP
Otros	
Requisitos del sistema	- Internet Explorer 11+, Firefox 12.0+, Chrome 20.0+, Safari 4.0+ u otro navegador habilitado para JavaScript Módem por cable o DSL (si es necesario)

Tp-Link TL-WR941HP	
	- Suscripción con un proveedor de servicios de Internet (para acceso a Internet)
Certificaciones	FCC CE RoHS
Ambiente	- Temperatura de funcionamiento: 0 ℃~40 ℃ (32 ℉ ~104 ℉) - Temperatura de almacenamiento: -40 ℃~70 ℃ (-40 ℉ ~158 ℉) - Humedad de funcionamiento: 10 %~90 % sin condensación - Humedad de almacenamiento: 5 %~90 % sin condensación

Nota. La tabla muestra las características de 3 equipos que podrían ser usados para la creación de la red wifi con cifrado wpa2 Enterprise. Tomado de (tp-link, s.f.)

Se ha seleccionado el equipo EAP 225 indor, mostrado en la figura 52, ya que es un equipo especializado en interiores, presenta mejores prestaciones de cobertura para los usuarios, puede trabajar tanto en la banda 2.4Ghz así también como en la banda 5Ghz, a su vez también se ha tomado en consideración que es un equipo relativamente actual, lo cual facilitará la migración a tecnologías que pudiesen surgir en un futuro próximo.

Figura 52

Punto de acceso seleccionado para la instalación

Nota. Este equipo brindara un gran salto tecnológico a la institución en materia de equipos de telecomunicaciones.

Como parte del aporte realizado por la institución, se nos entregó un equipo de cómputo, en el cual se montaría el servidor radius. Para esto se analizó entre un grupo de PCs que se encontraban en el laboratorio de la institución y se decantó por uno que posee las características de hardware necesarias para el óptimo funcionamiento de servidor de autentificación.

Tabla 6

Equipo para servidor

PC /SERVIDOR	
Almacenamiento	HDD 80 GB
RAM	2 GB DDR2

PC /SERVIDOR	
CPU	INTEL CORE 2 DUO E4500 -1.1GHZ
Sistema operativo	Ubuntu Server 20.04 LTS
Puertos	USB 2.0, RJ45, VGA, PS2, paralelo, Jack audio, Jack micrófono, Jack entrada audio.
Arquitectura del sistema operativo	64 bits
Arquitectura del CPU	64 bits
Tipo de placa madre	Micro ATX
Fuente de poder	Genérica

Nota. En la figura se pueden observar las características del equipo donde se montará el servidor de autentificación.

Una vez realizado el análisis sobre los equipos que se iban a usar, se pasó al análisis del Software que cumplan con las características necesarias para un correcto funcionamiento.

Tabla 7

Sistemas operativos

UBUNTU SERVER 20.04	
Versión	20.04.4 Lts
Desarrollador	Canonical Ltd /Fundación Ubuntu
Tipo de software	Libre
Requisitos mínimos	• 2.5 GB en disco • 512 MB RAM • Procesador 1GHz o superior
Tipo de Interfaz	Unity (11.04- 17.04) GNOME Shell (17.10-+)
Medio de instalación	USB, DVD
Arquitecturas soportadas	64 bits
Soporte	Hasta 2025
UBUNTU SERVER 22.04 LTS	
Versión	Ubuntu 22.04 LTS "Jammy Jellyfish"
Fabricante	Canonical Ltd /Fundación Ubuntu
Tipo de software	Libre

UBUNTU SERVER 22.04 LTS	
Requisitos mínimos de hardware	• 25 GB almacenamiento • 4GB RAM • Procesador Velocidad de 2Ghz y dos núcleos
Medio de instalación	USB, DVD
Arquitecturas de CPU soportadas	64 bits
WINDOWS SERVER 2022	
Versión	Microsoft Windows Server 2022
Fabricante	Microsoft
Tipo de software	Paga
Requisitos mínimos de hardware	Almacenamiento 32GB 512MB A 2GB RAM Procesador 1.4 bits a 64GHz
Medio de instalación	USB, DVD
Arquitecturas de CPU soportadas	64 bits

Nota. Esta tabla muestra tres sistemas operativos con sus características.

En este caso luego de haber comparado entre tres sistemas operativos en los cuales se puede posteriormente realizar la instalación del servidor radius, se ha seleccionado el sistema operativo Ubuntu server V 20.04.4 LTS por sus características las cuales se pueden observar en la figura 53, en este caso no se optó por la versión

más actual de este sistema operativo debido a que este tipo de software necesitan un periodo de pruebas luego de haber sido lanzados al público, periodo en el cual los programadores se enfocan en corregir errores , parches, y demás. En el caso del sistema operativo Windows Server, este fue descartado porque es un sistema de licencia y esto implicaría un gasto adicional a una institución en la cual no se percibe los ingresos suficientes.

Figura 53

Sistema operativo seleccionado

Nota. Usando el comando neofetch podemos visualizar algunos de los datos más relevantes de un sistema operativo.

Como parte final en la selección de software para la implementación de una red wifi con un servidor de autentificación AAA, se optó por escoger al servidor de licencia libre Freeradius versión 3.0.20, ya que está acorde a las características del equipo de cómputo dispuesto por la institución y como lo mencionamos con anterioridad al ser de licencia libre limitara los gastos que tenga que abarcar la institución. Se muestra el logo de este servidor en la figura 54.

Tabla 8

Servidor de autentificación AAA

Freeradius	
Tipo de licencia	Libre
Version	3.0.20
Kernel	5.4.0-122-generic

Nota. Esta tabla muestra las caracteristicas del servidor de autenftificacion AAA.

Figura 54

Servidor de autentificación AAA seleccionado

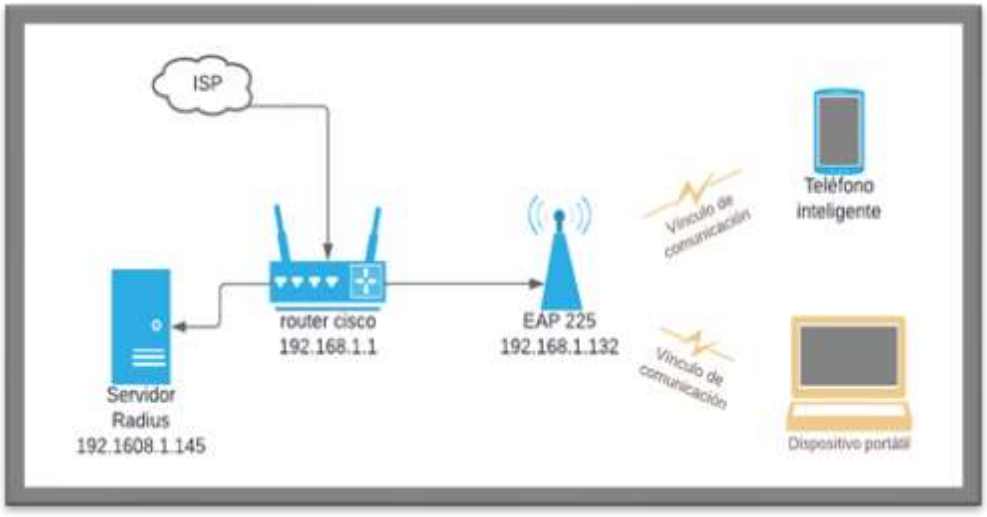
Nota. Logo del servidor freeradius

Diagrama de topología del proyecto

El Punto de acceso de la marca TP-LINK, modelo EAP2 225 Dual Band AP AC 1350, y el PoE que dotará de energía y conexión a la red estará colocado en la sala de docentes, y el servidor estará ubicado en el laboratorio de computación que se encuentra junto a la sala de docente como se muestra en la figura 55.

Figura 55

Topología de red del proyecto de implementación



Nota. Topología de red con las direcciones Ip y los equipos que se van a usar.

Instalación del Cableado de red

Primero inspeccionamos la ruta por la cual se realizará nuestro cableado de red, misma que ya fue definida en un principio durante la simulación de la cobertura de red con la herramienta Ubiquiti Design Center, para esto se usara los siguientes materiales:

Tabla 9

Materiales para cableado de la red

Nombre	Cantidad
Cable UTP cat 6	20 m
Conectores RJ45	6 unidades
Taco Fisher F-6	12 unidades
Tornillos TR, Pato 8x1	12 unidades

Nombre	Cantidad
Canaleta Lisa 20X12	3 unidades
Grapa Plástica 6mm	3 unidades

Nota. Se detalla los materiales y la cantidad que se usara de estos para realizar el cableado de la red.

Para la instalación del cableado de red dispuesto para el punto de acceso, se usó las normas de cableado de red EIA/TIA 568A para el ponchado de cables y cableado de red. Iniciamos por taladrar varios agujeros a lo largo de la ruta por donde se colocará las canaletas que contendrá al cable utp y colocar dentro de estos los taco Fisher F-6 como se muestra en la figura 56.

Figura 56

Perforación de agujeros para fijación de canaletas

Nota. Con la ayuda de un taladro se realizó los agujeros para la fijación de las canaletas

Luego de preparar los puntos de anclaje de las canaletas lisas, procedemos a marcar estos puntos donde coinciden con los agujeros realizados como se muestra en

la figura 57, y además a realizar un agujero para pasar por estos los tonillos TR Pato8x1.

Figura 57

Acondicionamiento y medición de canaletas para fijación en pared

Nota. Acondicionamiento de las canaletas

A continuación, retiramos el adhesivo de las canaletas y las atornillamos a los agujeros realizados como se muestra en la figura 58, además colocamos de forma ordenada el cable de red y aplicando un poco de fuerza logramos sellar las canaletas lisas.

Figura 58

Fijación de canaletas

Nota. Medimos, cortamos y colocamos dentro de las canaletas el cable de red.

Para el funcionamiento del punto, este necesita de un Poe, mismo que ya viene incluido en el kit del equipo adquirido, por lo cual marcamos los puntos donde se fijara este mecanismo que dota de energía al equipo de red, Figura 59, y lo aseguramos a la pared con la ayuda de unos tacos 2 tacos Fisher y dos tornillos como se observa en la figura 60.

Figura 59

Perforación de agujeros para instalación de PoE

Nota. Marcamos y perforamos dos agujeros para sujetar el PoE a la pared.

Figura 60

Fijación del PoE

Nota. Colocamos los pernos en los agujeros para dejar sujeto el PoE a la pared.

Como parte culminante de la instalación del cableado de red, nos ayudamos de una placa plástica que será el punto de anclaje entre el techo y el dispositivo, marcamos en el techo los 3 puntos donde ira anclada el equipo EAP 225 como se muestra en la figura 61.

Figura 61

Perforación de agujeros para AP

Nota. Marcamos y perforamos tres agujeros en el techo.

A continuación, basándonos en la norma EIA /ITA T568A para ponchado de cable directo, realizamos el pelado, peinado, colocación de cables de acuerdo al código de colores, y con ayuda de una ponchadora y un conector RJ45 realizamos el ponchado de los cables como se presenta en la figura 62, estos cables van desde el switch principal hacía el puerto LAN del Poe, desde el Poe hasta el Equipo de red.

Figura 62

Ponchado de cables usando Normas TIA 568A

Nota. Usamos la Norma TIA 568 A para ponchado de cable directo

Mostramos el estado del equipo Tp Link EAP 225 AC1350 a varios de los docentes presentes al momento de la instalación como se observa en la figura 63, y además explicamos algunas características técnicas de este equipo.

Figura 63

Presentación del AP a los docentes de la UECI

Nota. Se enseño el equipo a los docentes de la institución

Respetando la disposición de las ranuras que presentan tanto el AP como la placa plástica, pulsamos hacia arriba, y después con un giro hacia en sentido horario logramos colocar el equipo en el punto asignado como se muestra en la figura 64.

Figura 64

Fijación del equipo EAP 225 en el techo

Nota. Conectamos el cable de red al equipo y lo colocamos en el techo.

Como último paso en la estación del cableado de red y del equipo que funcionara como punto de acceso para la sala de docentes, como se muestra en la figura 65 se ponchó el cable de red de acuerdo a la norma EIA /ITA T568A y se conectó en un puerto libre del switch presente en el rack.

Figura 65

Conexión del cable de red al switch principal

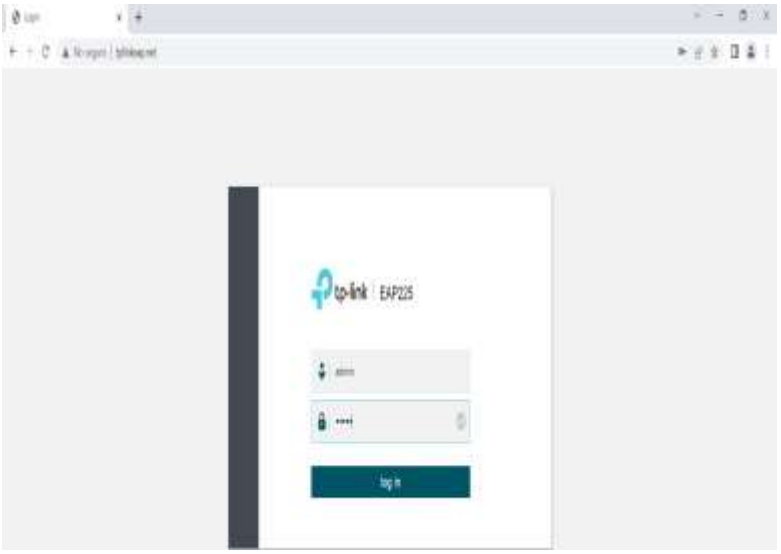
Nota. Se conecto el cable Utp a un puerto libre del Switch presente en la caja de equipos de telecomunicaciones.

Implementación de red wifi con cifrado wifi WPA2 personal

Al momento de conectar a la red eléctrica el PoE del equipo EAP 225 de Tp Link, este nos mostrara dos redes inalámbricas abiertas, tanto para la frecuencia 2.4 GHz como para la frecuencia 5GHz. Para configurar el equipo desde la web, ingresamos en un navegador la dirección **http://tplinkeap.net** y a continuación se muestra una ventana enseñada en la figura 66, en la cual debemos ingresar las credenciales que vienen dadas por defecto, en el apartado de usuario **admin** y el clave **admin.**

Figura 66

Página de ingreso a configuración del AP



Nota. Escribimos las credenciales por defecto “admin” y “admin”.

Antes de permitirnos ingresar al modo de configuración del equipo, tendremos que configurar la creación de una nueva cuenta como se enseña en la figura 67, esto con la finalidad de brindar mejoras en la seguridad de ingreso al equipo.

Figura 67

Configuración de nueva cuenta del AP

Nota. Creamos un nuevo usuario y clave de ingreso

En este caso procederemos con la configuración de la red inalámbrica como se detallad en la figura 68, para la cual hemos escogido trabajar con la frecuencia 2.4 GHz, le asignamos el nombre a la red “UECI SALA DOCENTES”, en este caso trabajaremos con el tipo de seguridad inalámbrica WPA2-PERSONAL, y le asignaremos una clave provisional “CAMINO23”.

Figura 68

Creación de una red con cifrado Wpa2 Personal

Nota. Se creo una red nueva que funciona en la banda 2,4 GHz

Al ingresar a la configuración del equipo, en la ventana Management (Administrador), se configura la dirección ip de forma estática, la cual será para este equipo la 192.168.1.132 con mascará de res 255.255.255.0, Gateway 192.168.1.1 y el servidor DNS de Google el cual posee la dirección 8.8.8.8 como se señala en la figura 69.

Figura 69

Configuración Ip Estática

Nota. Se le asigno una ip estática al punto de acceso.

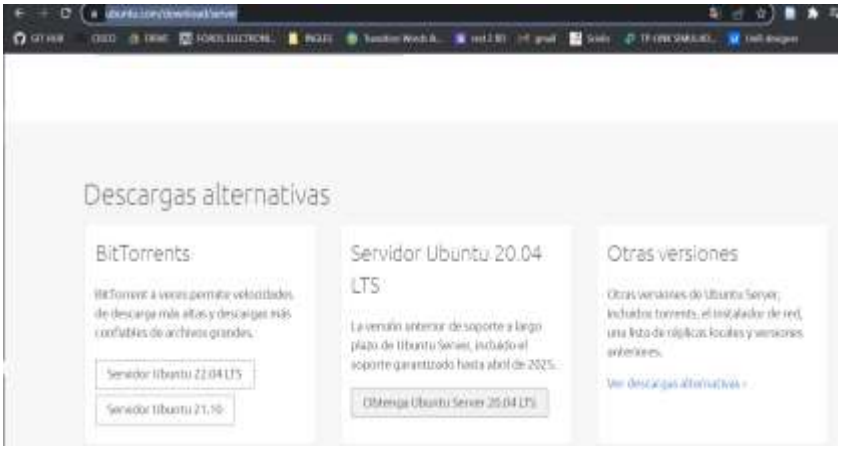
Esta configuración servirá de forma temporal, ya que el objetivo de este trabajo de titulación es, el de crear una red wifi y configurar un servidor radius que brinde una red segura y rápida a los docentes de la institución educativa en cuestión.

Instalación de Ubuntu server v 20.04.4 LTS

Para la instalación del sistema operativo en el equipo de cómputo designado, como se presenta en la figura 70, descargamos desde la página oficial https://ubuntu.com/download/server de Ubuntu la versión 20.04.4 LTS.

Figura 70

Página oficial de descarga para Ubuntu Server 20.04.4 LTS

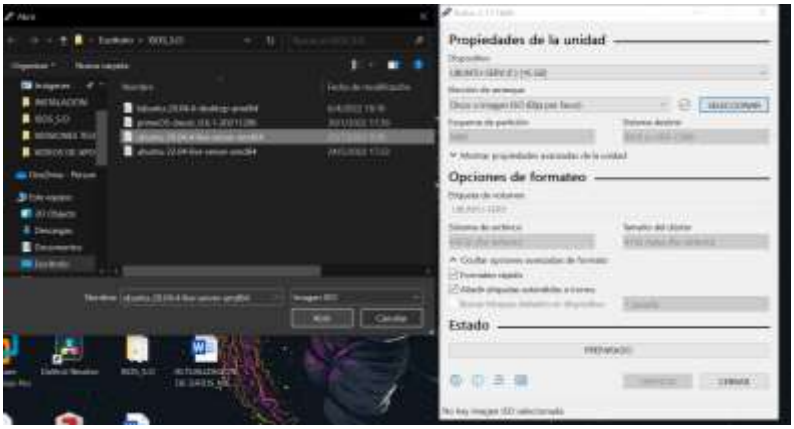


Nota. Desde la página oficial de Ubuntu podemos descargas las versiones más actuales del sistema operativo.

Necesitaremos una unidad de almacenamiento USB de 8 Gb o superior y el programa Rufus, el cual nos servirá para hacer al USB una unidad booteable e instalar desde esta el sistema operativo en cualquier equipo como se muestra en la figura 71.

Figura 71

Creación de unidad bootable



Nota. El programa Rufus es usado para la creación de unidades bootables

Para iniciar con la instalación se Ubuntu server en la PC, antes de encenderla, conectamos la unidad de almacenamiento USB, al pulsar el botón de encendido, dependiendo del Pc, como se observa en la figura 72 deberemos seleccionar la unidad de arranque, es este caso la memoria USB.

Figura 72

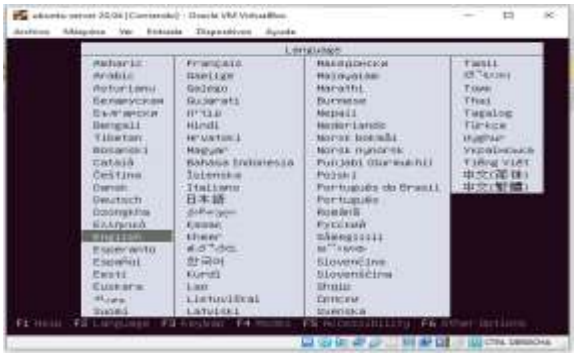
Selección de unidad de arranque

Nota. Con la tecla f9 ingresamos a la BIOS del PC y seleccionamos la unidad desde la que se desea iniciar.

Empezaremos con el proceso de instalación de este sistema operativo, seleccionaremos el idioma del sistema como se puede ver en la figura 73, el del teclado, el nombre que le asignaremos al equipo, la clave para super usuario, entre otras

Figura 73

Selección de idioma del sistema operativo



Nota. Con las teclas direccionales del teclado podemos seleccionar como el que va a trabajar nuestro sistema operativo

Para terminar con la instalación que se puede observar en la figura 74, deberemos apagar de forma directa el equipo y retirar la unidad USB del puerto en el cual lo hemos ubicado, y a continuación volver a encender el equipo; luego de que carguen todos los archivos de arranque del sistema operativo, nos pedirá que ingresemos el nombre que le hemos asignado y la contraseña de ingreso.

Figura 74

Proceso de instalación de Ubuntu server 20.04.4 LTS

Nota. Descarga de archivos necesarios para la instalación de Ubuntu server

Configuración de servidor Radius

Una vez hemos instalado el sistema operativo, procederemos con la instalación del servidor de autentificación AAA freeradius, para esto lo primero que debemos hacer es digitar el comando **sudo apt update** como se expone en la figura 75, esto con la finalidad de que Ubuntu actualice algunos archivos en caso de que existiesen nuevas modificaciones.

Figura 75

Actualización de archivos de Ubuntu

Nota. Se usa el comando **sudo apt update** para actualizar los repositorios, paquetes y archivos del sistema operativo.

Para que se instale el servidor digitaremos el comando **sudo apt install freeradius** y a continuación digitaremos la clave de super usuario para que proceda con el proceso de instalación como se puede observar en la figura 76.

Figura 76

Instalación del servidor freeradius

Nota. Se usa el comando **sudo apt install** seguido del nombre del servicio o programa que se necesita instalar.

Para poder conocer la versión de freeradius que se nos ha instalado en nuestro equipo, usaremos el comando **sudo ls /etc/freeradius**, además con el comando **sudo ls /etc/freeradius/3.0/** podremos observar el directorio de radius con sus diferentes archivos tales como el de usuario y clientes como se muestran en las figuras 77 y 78.

Figura 77

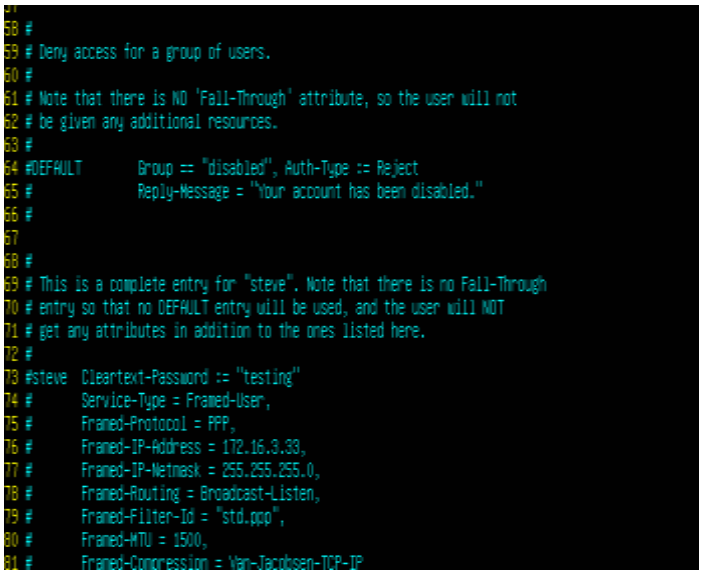
Comandos para visualizar la versión de Freeradius y archivos

Nota. Se observa la versión del servidor freeradius y sus archivos.

Una de las partes más importantes sin duda es la creación de los usuarios y las claves de acceso que se les designara para el ingreso a la red “UECI SALA DOCENTES”, para ello, el comando **sudo vim /etc/freeradius/3.0/users** nos mostrara el archivo como el que se muestra en la figura 78, en el cual podremos agregarlos. Pulsando la tecla **esc +: + set number** podremos observar de forma numerada las líneas de código.

Figura 78

Archivo Users



Nota. Archivo donde se podrá ingresar o modificar el nombre y claves de los usuarios.

Pulsamos la tecla **i** para insertar y con ayuda de las teclas direccionales no ubicamos debajo de la línea 82 y procedemos a crear el nombre de los usuarios seguido de la intrusión **Cleartext-Password: = “**clave del usuario**”** como se muestra en la figura 79, y crearemos así tantos usuarios como sean necesarios, para nuestro caso serán 50.

Figura 79

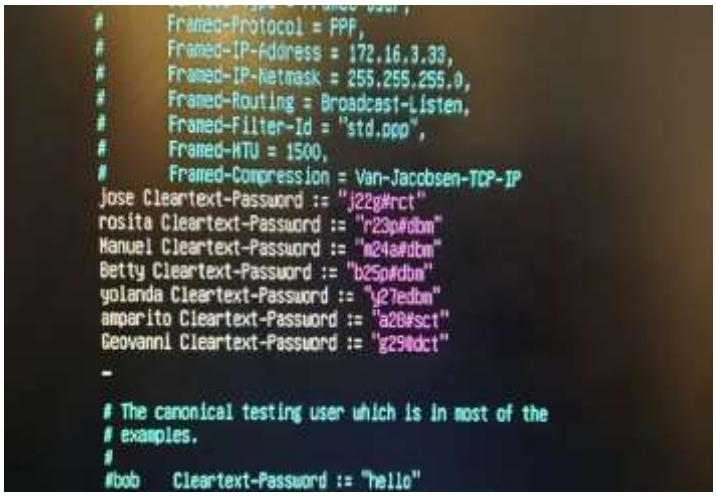
Creación de usuarios y contraseñas

Nota. Se muestra las líneas de código configuradas en el servidor para la creación de usuarios.

Una vez que hemos creado todos los usuarios con sus respectivas claves como se manifiesta en la figura 80, pulsamos la tecla **esc +: + wq** para salir al modo de usuario en el cual procederemos con las configuraciones restantes.

Figura 80

Salir del archivo users

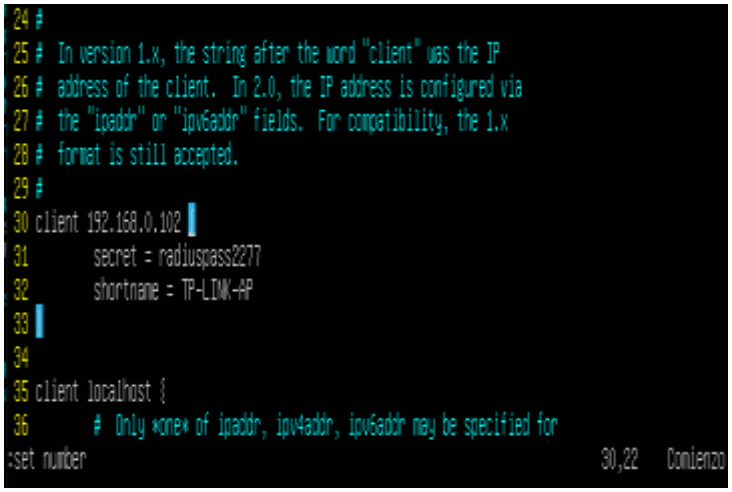


Nota. Se muestra un ejemplo de la creación de usuarios.

Para la asignación de equipo de red a los cuales el servidor va brindar el servicio de autentificación, escribimos el comando **sudo vim /etc/freeradius/3.0/clients.conf,** una vez dentro de este archivo podremos agregar, modificar o eliminar a los clientes como se puede observar en la figura 81. Para salir del archivo **clientes.conf** usando la tecla **esc +: + wq.**

Figura 81

Configuración de clientes

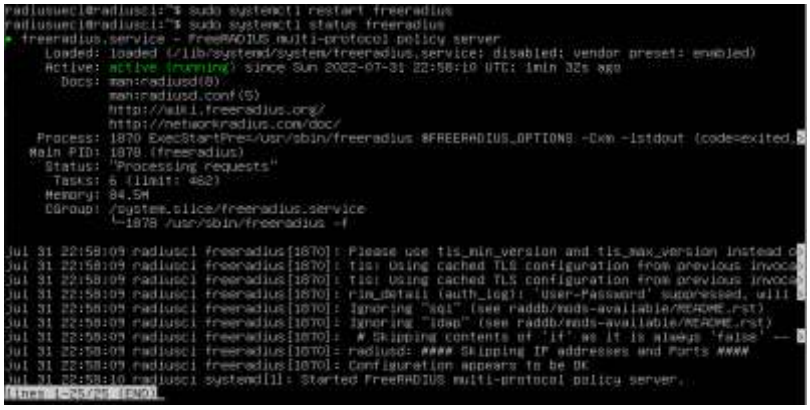


Nota. Se agrega un cliente al servidor radius por medio de la dirección Ip del Equipo.

Realizadas estas configuraciones, es momento de iniciar el servidor, para esto usamos en comando **sudo systemctl restart freeradius** y a continuación escribiremos la clave de super usuario para iniciar el servidor con los cambios realizados tanto para cliente como para los usuarios. Para comprobar el estado del servidor se usa el comando **sudo systemctl status freeradius** como se muestra en la figura 82.

Figura 82

Estado del servidor



Nota. En letras de color verde se puede observar el estado del servidor.

Figura 83

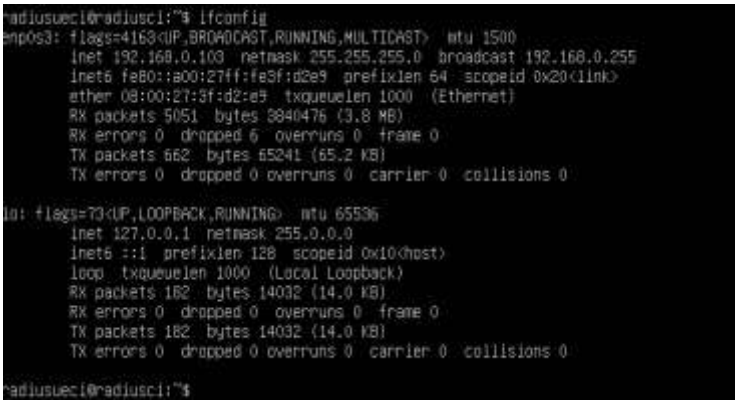
Visita del rector para conocer los avances de la implementación

Nota. La autoridad de la institución realiza una visita para conocer y observar lo que se está realizando (configuración de freeradius)

Ingresamos el comando **if config**, el cual es usado para saber la dirección ip que se le ha asignado para nuestro servidor como se exhibe en la figura 84, esta dirección Ip debemos ingresar posteriormente dentro de las configuraciones del punto de acceso al momento de habilitar el tipo de seguridad inalámbrica Wpa2 Enterprise.

Figura 84

Dirección ip asignada al servidor



Nota. Otro de los comandos que se puede usar para conocer la Ip del servidor es ip address

Figura 85

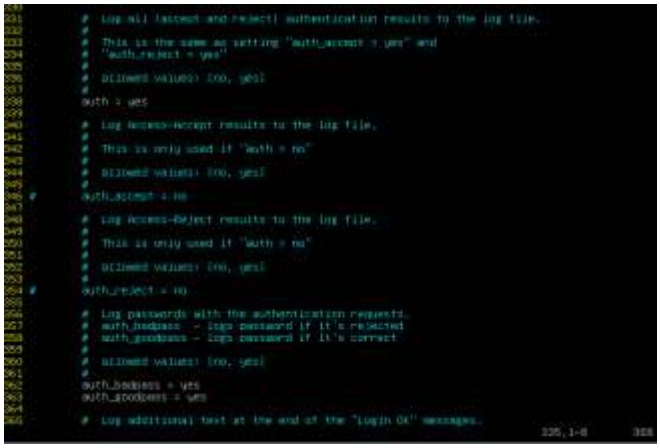
Revisión de las configuraciones para la instalación del servidor

Nota. Se comprueba que las configuraciones realizadas no presenten errores

Para habilitar la activar el registro de los usuarios usamos el comando **sudo vim /etc/freeradius/3.0/radiusd.conf**, en la línea de comando número 338, 362 y 363 debemos cambiar los parámetros de autentificación del estado no a yes como se muestra en la figura 86, esto permitirá monitorear a los usuarios que se conecten a la red.

Figura 86

Activación del registro de usuarios



Nota. Se cambia de no a yes la autenticación, autenticación correcta e incorrecta.

Tabla 10

Datos del servidor freeradius instalado

Puerto	1812
Ip asignada	192.168.*. ***
Clave sudo	r**********3
Número de usuarios configurados	50
Número de equipos configurados	1

Nota. En la tabla se muestran algunos datos del servidor freeradius.

Configuración de WPA2 Enterprise

Para la configuración del cifrado WPA2-Enterprise en el dispositivo de red instalado en la sala de docentes, abrimos un navegar, en el cual debemos ingresar la dirección ip del punto de acceso y luego de esto ingresar las credenciales de acceso al equipo creadas anteriormente como se indica en la figura 87.

Figura 87

Ingreso al AP

Nota. Pestaña de inicio de sesión del equipo.

Una vez dentro de la configuración del equipo nos dirigiremos a la pestaña de Wireless (inalámbrico) como se muestra en la figura 88, dentro de esta en la sub ventana de Wireless settings en la cual se podrá observar la red creada con cifrado wpa2 personal.

Figura 88

Ventana de configuración para redes inalámbricas

Nota. La tabla ubicada en la parte inferior de la imagen muestra todas las redes creadas por el AP.

En la tabla que muestra la red, se encuentra en la parte izquierda, dos botones los cuales sirven para eliminar la red y el otro que usaremos es el de editar la configuración de dicha red, para esto ingresamos a las configuraciones y se mostrara lo que se ve en la figura 89 que se presenta a continuación.

Figura 89

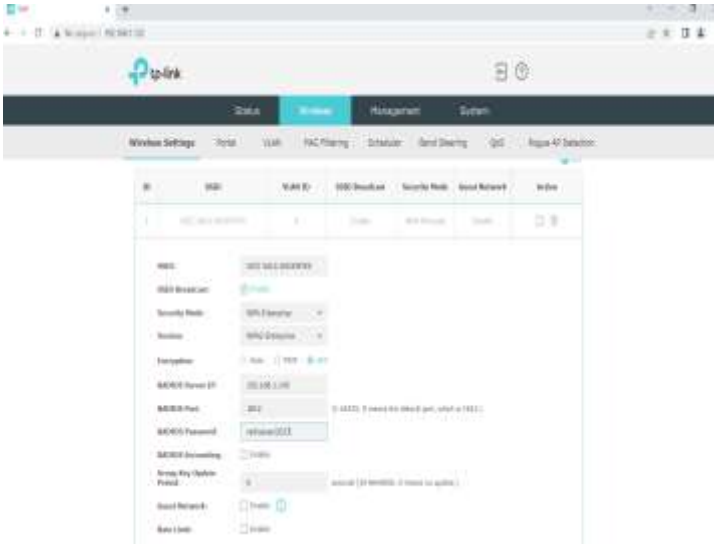
Edición del tipo de cifrado de la red wifi

Nota. En la opción de Security mode se muestran los cuatro tipos de seguridad wifi más comunes, WPA, WEP, WPA2 Personal y Wpa2 Enterprise

Dentro de esta configuración, como se presenta en la figura 90, tendremos que seleccionar el tipo de seguridad wpa2 Enterprise, la versión wpa/wpa2-Enterprise, el tipo de encriptación AES, y colocaremos la dirección ip del servidor, el puerto 1812 por defecto, y la clave que le hemos asignado dentro del archivo **clients.conf** a nuestro equipo.

Figura 90

Ingreso de datos del servidor radius



Nota. Se ingresan la dirección Ip generada para el servidor, el puerto y la contraseña del equipo.

Una vez realizados todos los cambios, la configuración de wpa2-enterprise habrá concluido y para comprobar que se ha realizado de forma correcta, nos conectaremos desde un de cómputo para visualizar los requerimientos que deberemos ingresar al momento de querer conectarse a esta red como se observa en la figura 91.

Figura 91

Requerimientos solicitados para conexión a la red wifi

Nota. Para ingresar a la red con cifrado wpa2 Enterprise se necesita colocar un usuario y su respectiva contraseña

Para conocer algunos datos sobre los usuarios que se conectan a la red wifi y monitorear el ingreso a esta red inalámbrica, desde el servidor de autentificación, escribimos el comando **sudo tail -f /var/log/freeradius/radius.log** para poder ver si los usuarios se conectaron de forma correcta o incorrecta. Como se presenta en la figura 92, dentro de los parámetros que podemos observar con este comando está el nombre del usuario, a que equipo cliente se conectó, porque vía, a través de que cliente, entre otras.

Figura 92

Lista de usuarios que acceden al a red wifi vista desde el servidor

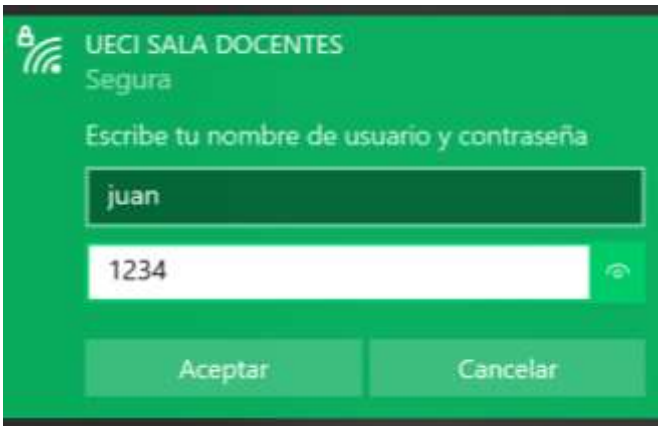
Nota. El comando descrito en este párrafo sirve para monitorear el ingreso correcto o incorrecto de los usuarios a la red

Pruebas de vulnerabilidad de la red

Para acceder a una red inalámbrica con el tipo de cifrado wpa2- Enterprise de forma idónea se deberá ingresar el usuario y contraseña correcto, lo cual limita que personas ajenas a los docentes pueden conectarse a la red, ya que, si se ingresa un usuario, contraseña o carácter diferente a los que se han creado como el ejemplo mostrado en la figura 93, entonces el servidor de autentificación no les permitirá el acceso y se mostrara un mensaje de error de conexión a la red como se muestra en la figura 94. Con esto se logra crear una red segura y que permita trabajar y navegar por internet de forma fluida.

Figura 93

Ingreso de usuarios inválidos



Nota. Ya sea que ingresemos el nombre del usuario o la clave incorrecta, el servidor de autentificación no permitirá la conexión a la red wifi.

Figura 94

Mensaje de login incorrecto

Nota. Si las credenciales de autenticación son incorrectas o diferentes a las generadas para una red, nos mostrara un error de conexión a la red

Elaboración de manual

Con la finalidad de brindar una herramienta que facilite el manejo del servidor en caso de que este se apague, ya sea por fallos de la red eléctrica o por manipulación errónea de los cables conectores, se elaboró un manual básico para el inicio del servidor freeradius cuya portada del documento se presenta en la figura 95. Así también como el listado de los usuarios y claves de acceso, y las hojas de datos de los equipos de hardware instalados mostrados en las figuras 96 y 97.

Figura 95

Lista de usuarios y claves creadas

Nota. El documento con el listado, manual, y hoja de datos, fueron entregados de forma física y digital al rector de la institución.

Figura 96

Manual para iniciar el servicio de freeradius

Nota. Este documento servirá para que cualquier docente designado puede iniciar el servicio.

Figura 97

Hojas de datos de los equipos de Hardware usados

Nota. Este documento servirá para dar a conocer las diferentes características de los equipos instalados.

Luego de una explicar a la autoridad de esta institución sobre el contenido de estos documentos, se procedió con la entrega física de estos documentos como se muestra en la figura 98, y además se le solicito el correo institucional para poder por medio de este medio compartir de igual manera los documentos en cuestión de forma digital.

Figura 98

Entrega de documentos al rector de la institución

Nota. Todos los documentos fueron compilados en un solo modulo para facilitar el archivo y manejo de este.

Capitulo IV

Conclusiones

- Se logró determinar por medio de la utilización de un software de Ubiquiti, cuál sería la zona de implementación más óptimo dentro de la sala de docentes, y poder colocar el equipo; esto con la finalidad de brindar a los docentes la mejor cobertura posible en este sitio que funge como zona de trabajo para realizar diferentes temas relacionados al ámbito de su trabajo.
- Mediante un análisis exhaustivo de los materiales que intervienen en el proyecto, se logró determinar el software y hardware que presentan las mejores características y prestaciones para la implementación de este proyecto
- Se realizó la respectiva instalación y configuración, tanto del punto de acceso, así como también, la del servidor de autentificación AAA freeradius, esto servirá de gran ayuda para que los docentes puedan acceder de forma segura a una red inalámbrica, y que, además, al limitar el acceso a esta red por medio del servidor, se logra tener una mejor estabilidad en términos de conexión.
- Con las pruebas de conexión realizadas y la elaboración de documentos sobre el funcionamiento y datos técnicos de los equipos, se logra que el personal directivo, como lo es, el rector de esta institución, adquiera conocimiento necesario para poder administrar esta nueva red que se ha implementado en la institución.

Recomendaciones

- Es recomendable que, en los próximos años, tanto el servidor freeradius como el sistema operativo instalado, sea actualizado por una versión nueva y estable de estos softwares, permitiendo así tener mejoras en el funcionamiento de los equipos y en la seguridad y soporte que se les brinde por parte de los desarrolladores.
- Para el manejo adecuado de la red y los equipos, se le recomienda usar la hoja de datos técnicos de los equipos y el manual de usuario, con esto se logra prevenir una mala manipulación del sistema o desconfiguración, además, existe un sinnúmero de características que aún no fueron usadas y que podrían ser puestas en práctica a futuro.
- Se recomienda a los docentes pertenecientes al área de informática, realizar cada seis meses un manteniendo preventivo del equipo Pc Servidor, esto con el afán de prolongar aún más la vida útil del equipo y la fluidez con que este trabaje.

Glosario:

Autenticación: Es el acto, proceso o conjunto de actividades que se deben desarrollar para confirmar que algo es lo que se dice.

Usuario: Es aquel individuo que necesita acceder o utilizar un servicio.

Servidor: Equipo o conjunto de equipos capaces de brindar un servicio y atender las peticiones solicitadas por un usuario.

Acces Point: Punto de acceso

Radius: Es un protocolo de autenticación AAA, usado para controlar y monitorear el acceso a una red wifi.

WPA2 ENTERPRISE: Es un tipo de cifrado de seguridad usado en redes inalámbricas, que permite vincular un servidor radius para la autentificación de usuarios

UTP: Cable de par trenzado sin blindaje

STP: Par trenzado apantallado

FTP: Cable de par trenzado apantallado

SFTP: Par trenzado apantallado totalmente blindado

DHCP: Protocolo de configuración dinámica de host

PoE: Alimentación a través de ethernet

WLAN: Red de área local inalámbrica

MAN: Red de área metropolitana

LAN: Red de área local

WAN: Red de área amplia

PC: Computadora personal

WIFI: Tecnología móvil para conectar dispositivos a internet (Wireless Fidelity)

IP: Protocolo de internet

LINUX: Sistemas operativos, en su mayoría con licencia libre

ACCES POINT O WAP: Punto de acceso inalámbrico

Gateway: Puerta de enlace

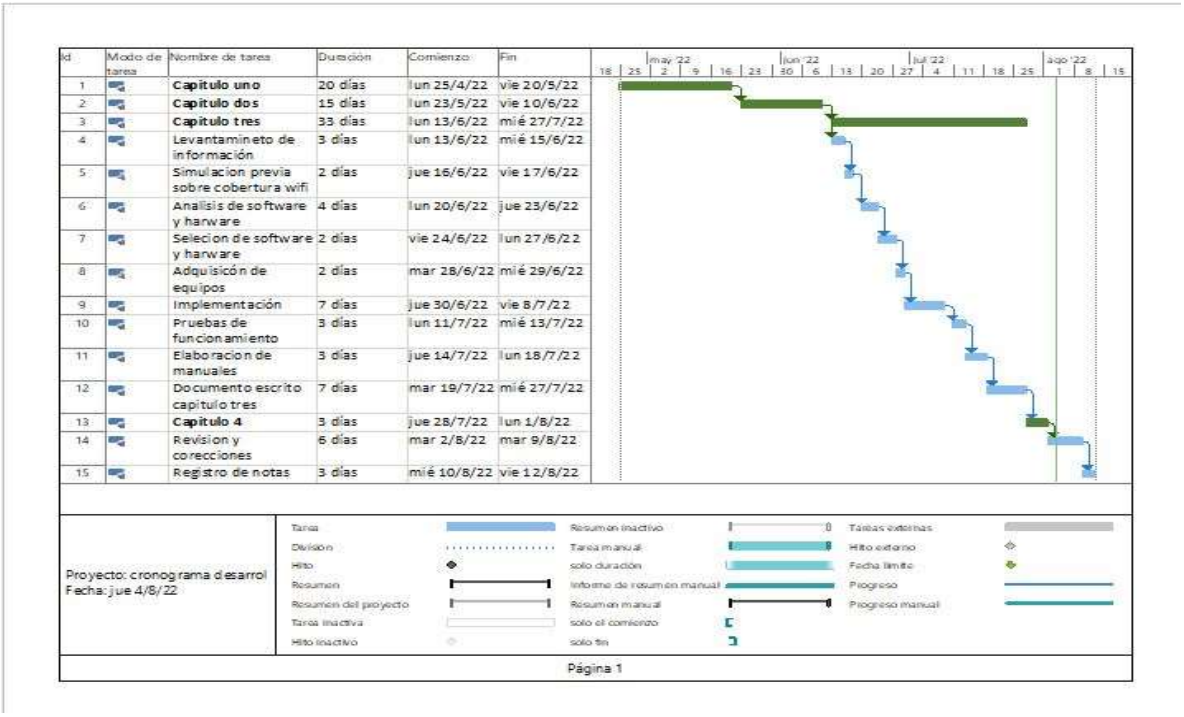
CPU: Unidad de procesamiento central

RAM: Memoria de acceso aleatorio

Cronograma

Figura 99

Cronograma de presentación del proyecto de titulación



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Capitulo uno**	20 días	lun 25/4/22	vie 20/5/22
2		**Capitulo dos**	15 días	lun 23/5/22	vie 10/6/22
3		**Capitulo tres**	33 días	lun 13/6/22	mié 27/7/22
4		Levantamineto de información	3 días	lun 13/6/22	mié 15/6/22
5		Simulacion previa sobre cobertura wifi	2 días	jue 16/6/22	vie 17/6/22
6		Analisis de software y harware	4 días	lun 20/6/22	jue 23/6/22
7		Seleccion de software y harware	2 días	vie 24/6/22	lun 27/6/22
8		Adquisicón de equipos	2 días	mar 28/6/22	mié 29/6/22
9		Implementación	7 días	jue 30/6/22	vie 8/7/22
10		Pruebas de funcionamiento	3 días	lun 11/7/22	mié 13/7/22
11		Elaboracion de manuales	3 días	jue 14/7/22	lun 18/7/22
12		Documento escrito capitulo tres	7 días	mar 19/7/22	mié 27/7/22
13		**Capitulo 4**	3 días	jue 28/7/22	lun 1/8/22
14		Revision y corecciones	6 días	mar 2/8/22	mar 9/8/22
15		Registro de notas	3 días	mié 10/8/22	vie 12/8/22

Nota. Se muestra las actividades con las fechas en que fueron realizadas.

Presupuesto

Tabla 11

Presupuesto del proyecto

Descripción	Cantidad	Precio Unitario	Valor total
Tp-Link EAPE 225 indor	1	$ 89,95	$89,95
Cable UTP cat 6	20 m	$0,35	$ 7,00
Tacos Fisher F-6	12 unidades	$0.08	$0,96
Tornillo TR PATO 8X1	12 unidades	$0.03	$ 0,36
Canaleta lisa 20x12	3 unidades	$2,80	$8,40
RJ45	7 unidades	$ 0,20	$ 0,60
Grapa plástica 6mm	12 unidades	$0,06	$ 0,72
Ángulos para canaletas 20x12 mm	4 unidades	$ 0,45	$ 1,80
		Valor Total	**$ 109,79**

Nota. Esta tabla muestra los gastos realizados para la implementación del proyecto

Bibliografía

acrylicwifi. (22 de enero de 2019). Obtenido de acrylicwifi: https://www.acrylicwifi.com/blog/es-segura-red-wifi-wpa-wpa2/

Andrade, F. (17 de agosto de 2020). Obtenido de cablecom: https://www.cablecom.com.ec/post/qu%C3%A9-es-el-cable-de-fibra-%C3%B3ptica

Angon, E. M. (2014). *Mecanismos y estrategias de seguridad en redes Wifi.* Zumpango , Mexico: Universidad Autonoma del estado de Mexico. Recuperado el 14 de julio de 2022, de http://ri.uaemex.mx/bitstream/handle/20.500.11799/40492/tesinaFinal.pdf?sequence=1&isAllowed=y

area de soporte. (13 de octubre de 2014). Obtenido de area de soporte: https://areadesoporte.com/que-es-un-correo-corporativo-y-como-funciona/

Baldi, A. (18 de octubre de 2021). Recuperado el 29 de julio de 2022, de islabit: https://www.islabit.com/153256/que-es-wpa2-o-wifi-protected-access-2.html

Borges, S. (27 de agosto de 2019). Obtenido de infranetworking: https://blog.infranetworking.com/servidor-proxy/

Carlos A. Vásquez, W. E. (2015). Control de acceso y administración de recursos de red mediante un servidor AAA en el GAD Municipal de Urcuquí usando software libre. *Universidad Tecnica del norte* , 9.

Carolina, P. P. (2011). *Investigacion del servidor radius para la seguridad en redes Lan inalambricas.* Riobamba, Ecuador. Recuperado el 4 de mayo de 2022, de

http://dspace.unach.edu.ec/bitstream/51000/627/1/UNACH-EC-ISC-2011-0005.pdf

Castillo, J. A. (26 de enero de 2019). Obtenido de profesional review: https://www.profesionalreview.com/2019/01/26/cables-utp-cables-stp-cables-ftp/

Castillo, J. A. (26 de enero de 2019). Recuperado el 16 de julio de 2022, de PROFESIONAL review: https://www.profesionalreview.com/2019/01/26/cables-utp-cables-stp-cables-ftp/

Castillo, J. A. (12 de septiembre de 2020). Obtenido de profesional review: https://www.profesionalreview.com/2020/09/12/cable-par-trenzado-caracteristicas/

comidoc. (s.f.). Obtenido de comidoc: https://comidoc.net/udemy/servidores-con-linux

COMPUTER WORLD. (01 de julio de 2005). Recuperado el 2 de Agosto de 2022, de COMPUTER WORLD: https://www.computerworld.es/archive/seguridad-wlan-80211i

Cortes, W. J. (2021). Recuperado el 02 de julio de 2022, de issuu: https://issuu.com/wendyjohanaestebancortes/docs/manual_de_normatividad/s/12470082

econectia . (22 de mayo de 2017). Obtenido de econectia : https://www.econectia.com/blog/tipos-de-conexiones-a-internet-cual-te-conviene-mas

Equipo editorial Etece. (16 de julio de 2021). Obtenido de concepto: https://concepto.de/cable-coaxial/

Etece. (5 de agosto de 2019). Obtenido de concepto: https://concepto.de/software-libre/#ixzz7ZuK8XIY0

Etece. (5 de agosto de 2021). Obtenido de concepto: https://concepto.de/servidor/#ixzz7ZuC0UNA7

Fernández, Y. (26 de julio de 2022). Obtenido de xataka: https://www.xataka.com/basics/cable-red-ethernet-categorias-protecciones-como-saber-cual-comprar

freeradius. (s.f.). Obtenido de freeradius : https://freeradius.org/

Hidalgo, S. (16 de octubre de 2017). Recuperado el 7 de mayo de 2022, de codigo espageti: https://codigoespagueti.com/noticias/internet/alerta-todas-las-redes-wifi-del-mundo-estan-en-peligro/

Marchionni, E. A. (2011). *ADMINISTRADOR DE SERVIDORES* (Primera ed.). Buenos Aires, Argentina : Fox Andina. Recuperado el 17 de julio de 2022

Mariana. (28 de septiembre de 2015). Obtenido de pandaancha: https://www.pandaancha.mx/noticias/fibra-optica-caracteristicas-ventajas.html

Marker, G. (2021). Obtenido de tecnologia + informatica: https://www.tecnologia-informatica.com/servidor-impresion/

Martín, I. (16 de agosto de 2017). Obtenido de topes de gama: https://topesdegama.com/noticias/apps-software/aumenta-seguridad-conversaciones-telegram-android

Martinez, J. C. (15 de septiembre de 2021). Obtenido de ymant: https://www.ymant.com/blog/que-es-un-ap-access-point-y-que-usos-y-modos-tiene/

MIE University . (s.f.). *MIE University* . Obtenido de MIE University : https://www.cc.mie-u.ac.jp/cc/eduroam_mac_e.html

Open. (s.f.). Obtenido de OPEN SYSTEM CONSULTANTS PTY LTD: https://www.open.com.au/radiator/Radiator-AAA-server-brochure-A4-print-resolution-es.pdf

optical.pe. (31 de Octubre de 2019). Obtenido de optical.pe: https://www.optical.pe/blog/tipos-de-redes-inalambricas/

Oscar Ubierna Yubero,. (26 de abril de 2013). Obtenido de https://www.comunicacionesinalambricashoy.com/wireless/802-11-ac-el-nuevo-estandar-wifi/

Pilicita, J. S. (2019). *Diseño e implementación de seguridad AAA (Autehentication Authorization and Accounting) en las redes wi-fi del GAD municipal del cantón Mejia .* Latacunga , Ecuador . Recuperado el 7 de mayo de 2022, de http://repositorio.utc.edu.ec/bitstream/27000/5337/1/PI-001357.pdf

radiatorsoftware. (s.f.). Obtenido de radiatorsoftware: https://radiatorsoftware.com/products/radiator/

redes inalambricas . (s.f.). Obtenido de redes inalambricas : https://www.redesinalambricas.es/

Rico, M. (s.f.). Obtenido de telecocable: https://www.telecocable.com/blog/tipos-de-fibra-optica-monomodo/1577

Rodriguez, A. (18 de marzo de 2014). Obtenido de fibra optica hoy: https://www.fibraopticahoy.com/tipos-de-cables-de-fibra-optica/

Rodríguez, M. (2020). Obtenido de viva ubuntu : https://vivaubuntu.com/instalar-ubuntu-server-20-04-lts/

Salazar, J. (2011). *Redes Inalámbricas* (prueba ed.). Praga, Republica Checa: Universidad Tecnica Checa de Praga. Recuperado el 22 de junio de 2022, de https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

Salvetti, D. (2011). *Redes Wireless Instalación , Configuración y Mantenimiento* (Primera ed.). Buenos Aires, Argentina : Fox Andina , Dalaga. Recuperado el 15 de Julio de 2022

Sanz, J. M. (6 de noviembre de 2013). Obtenido de security art work: https://www.securityartwork.es/2013/11/06/seguridad-wi-fi-empresarial-servidores-radius-i/

Setephany, G., & Serrano Anguieta, C. R. (2019-2020). *Diseño e implementación de una red wireless con alta disponibilidad basado en la tecnologia lifi(light fidelity)para optimizar la tasa de transferencia y el nivel de seguridad de conexion haciendo uso de un servidor radius AAA en el departamento.* Guayaquil. Recuperado el 5 de mayo de 2022

Shaw, K. (3 de febrero de 2018). Recuperado el 5 de julio de 2022, de COMPUTER WORLD: https://www.computerworld.es/wifi/80211-estandares-de-wifi-y-velocidades

Smoorenburg, M. V. (1 de febrero de 2012). Obtenido de miquels.cistron.nl: http://www.miquels.cistron.nl/cistron-radius/

Stallings, W. (2004). *Comunicaciones y redes de computadoras* (septima ed.). Madrid, España: PEARSON EDUCACION S.A. Recuperado el 12 de junio de 2022

Suárez, M. G. (2012). *Mecanismos de seguridad en redes inalámbricas .*

telectronika. (22 de junio de 2018). Obtenido de telectronika: https://www.telectronika.com/articulos/ti/categoria-8/

Torres, C. (s.f.). Obtenido de tado informatica: https://www.tadoinformatica.com/2017/05/servidor-web-que-es-y-para-que-sirve.html

tp-link. (s.f.). Obtenido de tp-link: https://www.tp-link.com/ec/business-networking/omada-sdn-access-point/

Vásquez, S. G. (2015). *Elementos de sistemas de telecomunicaciones.* Madrid: Paraninfo S.A. Recuperado el 29 de junio de 2022, de https://qdoc.tips/elementos-de-sistemas-de-telecomunicaciones-2-pdf-free.html

xtRadius. (s.f.). Obtenido de XTRAdius: http://xtradius.sourceforge.net/index.html

ymant. (12 de enero de 2016). Obtenido de ymant : https://www.ymant.com/blog/ventajas-redes-cableadas/

Anexos