UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE ADMINISTRACIÓN, AUTENTICACIÓN Y CONTROL EN EL ESTÁNDAR 802.11 EN EL CENTRO DE COMUNICACIONES DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO"

TESIS

PRESENTADA POR

LUÍS JESÚS REYNALDO MAMANI HERRERA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PUNO - PERU

2019

UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE ADMINISTRACIÓN, AUTENTICACIÓN Y CONTROL EN EL ESTÁNDAR 802.11 EN EL CENTRO DE COMUNICACIONES DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO

TESIS PRESENTADA POR:

MAMANI HERRERA LUIS JESUS REYNALDO

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

APROBADO POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE : .....

Dr. EUDES RIGOBERTO APAZA ESTAÑO

PRIMER MIEMBRO : .....

Mg. TEOBALDO RAUL BASURCO CHAMBILLA

SEGUNDO MIEMBRO : .....

M.Sc. EDDY TORRES MAMANI

DIRECTOR DE TESIS : .....

Dr. JOSE EMMANUEL CRUZ DE LA CRUZ

TEMA: REDES DE COMPUTADORAS

ÁREA: TELECOMUNICACIONES

FECHA DE SUSTENTACIÓN 18 DE SETIEMBRE DEL 2019

DEDICATORIA

Dedico este proyecto de tesis a dios, a mis padres y hermanas quienes me apoyaron en todo momento, teniendo en cuenta, que estuvieron conmigo moralmente y me acompañaron desde siempre

AGRADECIMIENTOS

A los docentes de la escuela profesional de ingeniería electrónica de la universidad nacional del altiplano, por haber compartido sus conocimientos a lo largo de mi vida universitaria.

INDICE

INDICE DE FIGURAS

TABLAS

ACRÓNIMOS

WEP: (Wired Equivalent Privacy o Privacidad Equivalente a Cableado)

LAN: (Local Area Network o Red de Área Local)

RC4: (Rivest Cipher 4 o Cifrado rivest 4)

CRC: (Cyclic Redundancy Check o Verificación por Redundancia Cíclica)

ARP: (Address Resolution Protocol o Protocolo de Resolución de Direcciones)

WPA: (Wi-Fi Protected Access o Acceso Wi-Fi Protegido)

TKIP: (Temporal Key Integrity Protocol o Protocolo de Integridad de Clave Temporal)

MIC: (Pulse Code Modulation o Modulación por Impulsos Codificados)

EAP: (Extensible Authentication Protocol o Protocolo de autenticación extensible)

AP: (Access Point o Puntos de Acceso)

AES: (Advanced Encryption Standard o Estándar de Cifrado Avanzado)

PSK: (Phase Shift Keying o modulación por desplazamiento de fase)

PMK: (Pair-wise Master Key o Clave maestra por pares)

MK: (Key Master o Clave maestra)

CCMP: (Counter Mode with Cipher Block Chaining Message Authentication Code o Modo Contador con Código de Autenticación de Mensaje de Encadenamiento de Bloques).

UDP: (User Datagram Protocol o Protocolo de Datagramas de Usuario)

NAS: (Network Access Server o Servidor de Acceso a la Red)

LDAP: (Lightweight Directory Access Protocol O Protocolo Ligero de Acceso a Directorios)

RFC2251: (Request for Comments Publication o Solicitud de Publicación de Comentarios)

NIC: (Network Interface Controller o Tarjeta de Interfaz de Red)

TELNET: (Telecommunication Network o Red de telecomunicaciones)

SSH: (Secure Shell o Cubierta segura)

TLS: (Transport Layer Security o Seguridad de la Capa de Transporte)

RESUMEN

Las empresas que implementen redes WI-FI en sus ambientes, no pone atención en temas de seguridad, exponiendo así, que información personal llegue a manos equivocadas, y puedan darle mal uso. RADIUS tuvo que cerciorarse que los usuarios de una red W-FI se encontraron enlazados a esta red de una manera fiable, observando que ahora el medio de transmisión fueron ondas electromagnéticas. RADIUS comprobó que los datos ingresados pertenecen a un usuario en específico (autenticación), que solo pueda ingresar a cierto contenido (autorización) y llevar un registro de lo que haga en la red (contabilidad); realizando todo esto de una manera confidencial, sin el temor de que personas ajenas al centro de labores, accedan a la información personal. Se plantea el diseño e implementación del servidor RADIUS, para la para una red WI-FI segura, y que administre a los usuarios por medio de una plataforma de protocolo SSH. Se verifico los las principales actividades en redes Wi-Fi, poniendo atención a la seguridad WPA2, (IEEE 802.11i), 802.1X, EAP, RADIUS, entre otros. Se examina la autenticación y autorización para usuarios conectados a una red WI-FI. Explica los protocolos AAA y el objetivo del protocolo, protocolos de autenticación y estándares de seguridad informática. Como resultado, se crea la red privada, y RADIUS que autentica a los usuarios conectados de forma inalámbrica. La contabilidad reúne el resultado del comportamiento de RADIUS y así tomar decisiones para cada usuario en específico.

PALABRAS CLAVE

Seguridad, estándar 802.11, autenticación, autorización, administración.

ABSTRACT

Companies that implement WI-FI networks in their environments do not pay attention to security issues, exposing that personal information reaches the wrong hands, and may misuse it. RADIUS had to make sure that the users of a W-FI network were linked to this network in a reliable way, noting that the transmission medium was now electromagnetic waves. RADIUS verified that the data entered belongs to a specific user (authentication), who can only access certain content (authorization) and keep a record of what they do in the network (accounting); doing all this in a confidential way, without the fear that people outside the work center, access to personal information. In this thesis, the design and implementation of the RADIUS server was proposed, for a secure WI-FI network, and administered to users through an SSH protocol platform. We verified the main activities in Wi-Fi networks, paying attention to the security WPA2, (IEEE 802.11i), 802.1X, EAP, RADIUS, among others. The purpose of this thesis examined authentication and authorization for users connected to a WI-FI network. The thesis explained the AAA protocols and the purpose of the protocol, authentication protocols and computer security standards. The practice explained the implementation in the private network. As a result, the private network was created, and RADIUS authenticated the connected users wirelessly. Accounting gathers the result of RADIUS behavior and thus makes decisions for each specific user.

KEYWORDS

Security, 802.11 standard, authentication, authorization, administration.

CAPÍTULO I

INTRODUCCIÓN

En la actualidad, muchas personas, incluso objetos dependen de Internet.

Internet ha estado evolucionando exponencialmente**,** y podemos dividirlos en dos grupos, los que requieren el servicio de internet, que son los clientes, y esto incluye a las personas que han usado navegadores simples, y los que proporcionan internet, que son los servidores que también pueden incluir a algunos de nosotros, principalmente debido al intercambio de archivos que hacemos de vez en cuando. Al momento de hablar de servidores también hablamos de computadoras, pero con un propósito en específico. Los servidores tienen como objetivo satisfacer los deseos de los clientes, virtualmente hablando, y para responder a sus consultas cuando lo deseen.

En el capítulo I se establece los problemas que involucra la falta de conocimiento acerca de la seguridad informática, planteando así hipótesis que nos ayude a solucionarlos, enfocándonos en los objetivos tal como implementar un servidor RADIUS.

En el capítulo II menciona los antecedentes, y el marco teórico de referente al proyecto de investigación.

En el capítulo III indica los materiales y métodos utilizados, incluyendo el procedimiento del proyecto. La autenticación es necesaria tanto en redes cableadas como inalámbricas. En las redes inalámbricas, la autorización es mucho más importante, ya que, en las redes cableadas, el acceso está limitado de alguna manera a través de los cables, mientras que cualquier dispositivo con capacidad inalámbrica puede conectarse al

servidor y, sin la autenticación adecuada, puede causar daños graves al entrometerse en el sistema.

En el capítulo IV se establece los resultados obtenidos en este proyecto, teniendo en cuenta las diferencias que existen entre otros proyectos y la eficiencia de RADIUS frente a situaciones adversas, brindando así, diferentes recomendaciones para su uso efectivo.

1.1. Planteamiento del Problema

El problema es que existen personas malintencionadas, que, a fin de lograr objetivos perjudiciales, acceden a información personal, teniendo en cuenta que actualmente todos tenemos medios que nos identifican, para adaptarnos en la sociedad, así hablando en el mundo real como en el mundo virtual.

Los servidores actuales de la Universidad Nacional del Altiplano, no tienen un monitoreo para cada usuario, y eso no garantiza desconfianza para los usuarios, ya que, personas ajenas a la Universidad Nacional del Altiplano podrán interferir en la red WI-FI, ocasionando deficiencias en la red.

Para acceder a los servicios, RADIUS solicita las credenciales del usuario que compara con la base de datos que tiene y emite un veredicto basado en la comparación. Si la identificación y la autorización son correctas, el servidor le permite al usuario recibir los servicios que desea, según las prioridades que tenga el usuario.

1.2. Formulación del Problema

Falsos usuarios están al asecho de robar información, y acceder a sitios de internet restringidos, teniendo en cuenta la saturación del ancho de banda que existe, y el impedimento de navegar por internet con fluidez.

Cuando tocamos el tema de servidores hablamos de computadoras, sobre estos que tienen un propósito mayor que uno personal, los servidores están ahí para satisfacer las necesidades de los deseos de los clientes y responder a sus consultas.

Los servidores son parte muy esencial de la red, brindan a los demás servicios disponibilidad y rendimiento rápido, son las claves para tener un servicio confiable, sin embargo, existen problemas al acceder a la red, como lentitud al abrir paginas educativas, o al intentar acceder a cuentas personales ya sea estudiantes, docentes o personal administrativo.

El problema está dado por el excesivo uso de personas ajenas a la Universidad Nacional del Altiplano, ya que al acceder a la red inalámbrica limitan el ancho de banda, causando así, deficiencias al navegar por la red.

Hay variedades de servidores web, como, por ejemplo, servidores de correo y servidores de juegos, etc. La mayoría de las veces estos servicios se combinan en una sola máquina, siempre que no afecten el rendimiento de la máquina. Pero la idea principal detrás de todos y cada uno de ellos es proporcionar algún tipo particular de servicio.

1.3. Hipótesis de la Investigación

1.3.1. Hipótesis General

Proporcionar información acerca de la seguridad informática y tecnologías de la información en la Universidad Nacional del Altiplano

1.3.2. Hipótesis Específica

El presente proyecto llevará a generar certeza entre las personas que trabajan en el Centro de Comunicaciones de la Universidad Nacional del Altiplano y, de esta manera, trabajar de manera segura a nivel de computadora, manteniendo la información personal y brindando confianza entre los usuarios que ingresan a la red WI-FI implementada.

1.4. Justificación del Estudio

La autenticación es útil tanto en redes cableadas como inalámbricas. En las redes inalámbricas, la autorización es de mayor prioridad, ya que en las redes cableadas la accesibilidad es únicamente mediante cables, mientras que, en redes inalámbricas, cualquier equipo móvil puede conectarse.

Sin la autenticación adecuada posiblemente causaría daños al ingresar al sistema. La conexión cableada mantiene prácticamente atado a un usuario, por ende, las personas no estarán de acuerdo en no ser libres así que buscarán una conexión libre de cables. En otras palabras, esto explica el repentino auge de la tecnología inalámbrica.

1.5. Objetivos

1.5.1. Objetivos Generales

- Informar a los usuarios sobre la importancia de la seguridad en redes inalámbricas, teniendo en cuenta, la desconfianza existente en un entorno laboral con los falsos usuarios.

1.5.2. Objetivos Específicos

- Implementar RADIUS en el Centro de Comunicaciones de la Universidad Nacional del Altiplano
- Autenticar a cada usuario para el uso correcto de la red inalámbrica de la Universidad Nacional del Altiplano – Puno.
- Informar a los usuarios la importancia de usar contraseñas seguras, mayor a 12 caracteres, uso de mayúsculas y minúsculas, uso de números y letras, para una mayor fiabilidad.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. Antecedentes

Implementación de un Prototipo de Red Inalámbrica que Permita Elevar los Niveles de Seguridad a Través de la Autenticación de un Servidor Radius para los Usuarios que Accedan a Internet en El Edificio Francisco Morazán de la Utec.

Carlos Miranda Fuentes, Kevin Villatoro Derás, Rolando Hernández Hernández – Universidad Tecnológica de El Salvador – El Salvador 2012

Resumen:

Esta tesis describe la introducción de las redes inalámbricas en todos los ámbitos de nuestras vidas, debido a las empresas que hacen uso de estas tecnologías.

Como parte del proyecto de investigación se plantea la implementación de un prototipo de red inalámbrica que cubra el área del edificio Francisco Mozarán y que brinde control de acceso a los usuarios, ya que un punto importante en las redes inalámbricas es el factor seguridad, debido a ellos el prototipo pretende elevar los niveles de seguridad a través de la validación y autenticación usando el servidor RADIUS.

En el capítulo I, describe el edificio Francisco Morazán, que consta de 5 niveles, existe una estructura de red inalámbrica ya instalada que brinda acceso solo al primer y

segundo nivel, dejando de lado los demás niveles, porque los AP (Access Point), está ubicado en el primer y segundo nivel

Dentro de la red inalámbrica existe un servidor RADIUS, bajo la plataforma Linux el cual funciona a través de un portal educativo que es el que autentica a cada usuario que acceda a la red, pero este no brinda la suficiente seguridad a la red, ya que cualquier persona puede tener acceso a esta estructura que forma parte de la red institucional de la Universidad Tecnológica y no deja ningún registro cuando establece una conexión.

Con el planteamiento del proyecto de investigación se pretende incrementar los niveles de seguridad en el ingreso a la red inalámbrica del edificio Francisco Morazán de la Universidad Tecnológica de El Salvador, al mismo tiempo se pretende mantener un control más directo sobre los usuarios que se conecten a dicha red, esto se logrará por medio de un servidor RADIUS de autenticación, el cual validará y autenticará al usuario al momento que intente ingresar a la red inalámbrica.

En el capítulo II, implementa un prototipo de servidor de autenticación dentro de la red inalámbrica del edificio Francisco Morazán de la UTEC, este permitirá proporcionar nuevos niveles de escalabilidad en la seguridad dentro de la red, a la vez se llevará un mayor control de los usuarios que accedan a la red. El servidor RADIUS es un equipo que maneja un protocolo de autenticación y autorización para aplicaciones de acceso a la red.

RADIUS facilita una administración centralizada de usuarios cuando se maneja una enorme cantidad de usuarios, continuamente cientos de ellos son agregados o

eliminados a lo largo del día y la información de autenticación cambia continuamente; en este sentido la administración centralizada de usuarios es un requerimiento operacional fundamental.

En el capítulo III se configura un prototipo de servidor de autenticación dentro de la red inalámbrica del edificio Francisco Morazán de la UTEC. El servidor RADIUS brindará una mejor seguridad en la red de todo el edificio, permitirá un mayor control de los usuarios. El servidor RADIUS es un equipo que maneja un protocolo de autenticación y autorización para aplicaciones de acceso a la red.

Conclusiones

La presente investigación se ha dedicado a la implementación de un servidor RADIUS, que permite la validación y autenticación de usuarios para el mejoramiento de la seguridad de la red inalámbrica del edificio Francisco Morazán de la UTEC.

El aplicar políticas de seguridad no es tarea sencilla; sin embargo, actualmente, se cuenta con herramientas que ayudan a la realización de tan importante tarea, Esta tesis es un ejemplo de ellos.

En el desarrollo del trabajo de investigación que ha dado lugar a la presente tesis se han alcanzado los adjetivos inicialmente planeados en cuanto a:

Verificar la infraestructura de red inalámbrica existente en el Edificio Francisco Morazán para determinar requerimientos adicionales que se puedan utilizar.

Diseñar el modelo y la topología de la nueva red inalámbrica que se implementará en el edificio Francisco Morazán la cual brindará una cobertura total dentro del edificio.

Diseño e Implementación de un Sistema de Gestión de Accesos a una Red Wi-Fi Utilizando Software Libre

Jorge Alonso López Mori – PUCP – Lima – Perú 2008

Resumen

La presente tesis describe que la implementación de redes inalámbricas obliga a contemplar con más cuidado el aspecto de la seguridad. Así como en el caso de las típicas redes de datos con cables (siendo la tecnología Ethernet la más utilizada para estos casos), tiene que asegurarse que los usuarios de una red inalámbrica se encuentren conectados a ésta de una manera segura, teniendo en cuenta que ahora el medio de transmisión ya no se restringe a un cable, sino que se encuentra en todo el ambiente que lo rodea.

Debe de comprobarse que el usuario sea quien dice ser (autenticación), que solo tenga acceso a los recursos que le corresponda (autorización) y también llevar a cabo un registro de las actividades que haga dentro de la red (contabilidad); realizando todo esto de una manera segura y sin que sujetos ajenos a la red puedan estar leyendo información confidencial ni mucho menos tratar de modificarla.

En el capítulo I la tesis presenta los objetivos, tales como:

Estudiar la tecnología Wi-Fi (IEEE 802.11), enfocándonos en el análisis de los aspectos de seguridad que en ella se contemplan.

Diseñar e implementar una red inalámbrica considerando los más altos grados de seguridad: con autenticaciones y comunicaciones seguras.

Implementar una plataforma de gestión y contabilidad de los usuarios para el acceso de la red inalámbrica.

Llevar a cabo un análisis de costo-beneficio entre los distintos equipos disponibles en el medio para la implementación de la red inalámbrica segura.

En el capítulo II menciona que una organización cuenta con una red LAN en su oficina principal, siendo esto una gran traba para sus usuarios móviles que cuentan con computadoras portátiles (notebooks) y se encuentran en constante movimiento dentro de dicho local; ya que requieren ubicar un punto de red cercano a donde se encuentren para poder descargar sus correos o buscar alguna información en la Internet, lo que trae consigo incomodidad y una disminución en el desempeño de dicha persona al perder tiempo realizando este proceso; tiempo que se traduce en una disminución de su productividad.

En el capítulo III se detalla los procesos para la solución propuesta.

El primer proceso, denominado “Conexión de un usuario móvil a la red inalámbrica” se explica el flujo de operaciones que se realizan desde el momento en el que un cliente intenta acceder a la red inalámbrica hasta el acceso concedido a dicho usuario.

Para ello, se inicia con la aparición del cliente inalámbrico dentro del área de cobertura de la red inalámbrica (pudiendo el AP ser capaz de reconocerlo y empezar a intercambiar información).

Luego, el cliente identifica a la red inalámbrica como una posible red a la que puede acceder e intenta conectarse a ella. Para ello, el equipo de dicho usuario se comunica con el AP y lo primero que realiza es la asociación a dicho punto de acceso.

Una vez realizado esto, se inicia la sesión 802.1X con el cliente, solicitándole su nombre de usuario y contraseña. Acceso de un cliente a la Internet; segundo proceso en donde se explica el flujo de operaciones que se realizaría de contar con un servidor Web Proxy como fue mencionado anteriormente. Desde el momento en el que un cliente intenta acceder a la Internet hasta el acceso concedido a dicho usuario. Para ello, se inicia con la ejecución de algún explorador Web (Web browser) desde el equipo del cliente.

En el capítulo IV menciona que la implementación será con prototipo (piloto) como se ha mencionado anteriormente y se contempla dentro de los alcances de la tesis; buscando que dicho prototipo cumpla con las metas propuestas a lo largo de esta tesis a manera funcional; es decir, que cumpla con realizar las funciones u operaciones planteadas sin buscar necesariamente presentar un acabado final. Podemos dividir la implementación del prototipo en etapas:

Primera etapa: Implementación del servidor FreeRADIUS

Segunda etapa: Implementación del servidor OpenLDAP

Tercera etapa: Implementación del servidor MySQL

Cuarta etapa: Implementación del servidor de gestión Web

Quinta etapa: Configuración de los puntos de acceso

Sexta etapa: Configuración de los usuarios móviles

En el capítulo V menciona los factores económicos que traen consigo los distintos equipos (puntos de acceso) y de acuerdo a estas características poder reconocer cuales de éstas aportan un beneficio significativo para la solución y cuanto sería la diferencia en costos con respecto a la que no lo tenga. Así, podemos encontrar varios equipos Wi-Fi en el mercado; para los cuales hemos tenido la oportunidad de analizar hasta 03 diferentes equipos: Zyxel Prestige 660HW-T1, Linksys WRT54G, D-Link DWL-3200AP.

Conclusiones

Tras haber logrado la implementación de un prototipo para la solución planteada, se ha podido llegar a las siguientes conclusiones:

Es posible la integración de todas las herramientas de software libre utilizadas en la presente tesis (FreeRADIUS, OpenLDAP, SAMBA, MySQL) con un dominio desarrollado con Microsoft Windows. Es decir, en el caso de que se le desee implementar en una red ya existente y que utilice herramientas comerciales (tales como MS Windows 2003 Server y/o MS Active Directory) bastaría con modificar algunos parámetros en los archivos de configuración de las herramientas de software libre utilizadas para poder lograr la integración y trabajo entre todos estos.

La implementación de este prototipo no contempla mecanismos de seguridad que aseguren ataques provenientes desde el interior de la red (la red cableada). Lo que se plantea aquí es garantizar un medio de acceso seguro entre el cliente móvil y el punto de acceso a la red (AP); más no entre éste y los elementos de la red interna (tales como servidores de correo, Web, archivos, entre otros).

2.2. Protocolos y Estándares de Red

Conexiones alámbricas o inalámbricas requieren de ciertas medidas, para alcanzar una comunicación optima.

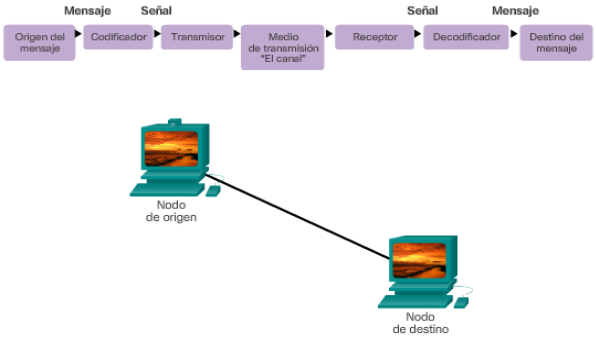
El envío de información, a través de una red, está dado por "protocolos".

En primer lugar, para establecer una conexión y enviar mensajes, se necesitará codificar.

La codificación es el procedimiento en el cual la información se transforma en otra, aceptable y compatible con los protocolos de red. La decodificación revierte este proceso para interpretar la idea.

El dispositivo o host emisor, transforma en bits los mensajes digitados. Cada bit se codifica en un patrón de sonidos, ondas de luz o impulsos electrónicos, según el medio de transmisión. El host de destino recibe y decodifica las señales para interpretar el mensaje. El mensaje enviado a través de la red es encapsulado en un especifico formato denominado trama.

Figura Nº 2. 1: Codificación de Mensajes



Fuente: CCNA. (2017)

La interrelación de protocolos consta entre él envió de mensajes entre un servidor web y un cliente web. Por ejemplo:

HTTP: Es protocolo de la capa de aplicación que es encargado de la interacción entre un servidor web y un cliente web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor web implementan el HTTP como parte de la aplicación.

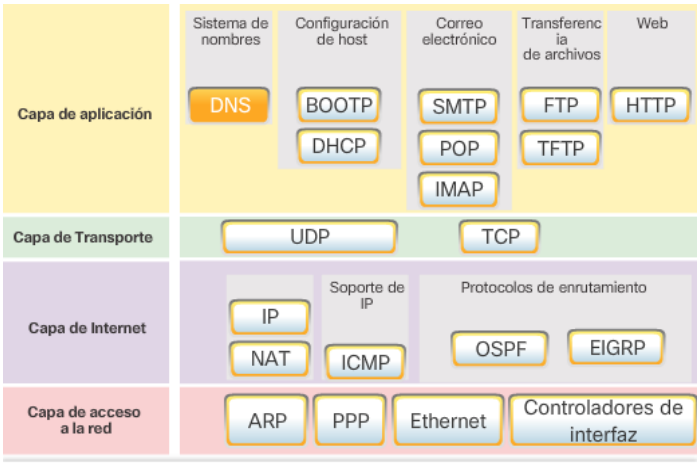
TCP: Es el protocolo de la capa de transporte que define envío de mensajes personales. TCP segmenta los mensajes HTTP en pequeñas partes. Los segmentos son controlados en tamaño e intervalos para la correcta interacción entre cliente y servidor.

IP: Protocolo de la capa de red encargado de tomar los segmentos TCP, proporciona direcciones y deriva la información por la ruta más conveniente para llegar al host de destino.

ETHERNET: Es un protocolo de acceso a la red que define la interrelación por medio de un enlace de datos y la transferencia física de datos en los medios de red. Los protocolos de acceso a la red toman los paquetes de IP para transmitirlos por los medios.

TCP/IP se implementa en los hosts emisores y receptores para que la recepción de datos sea completa a través de la red. Los protocolos Ethernet se utilizan para transmitir el paquete IP a través de un medio físico que utiliza la LAN.

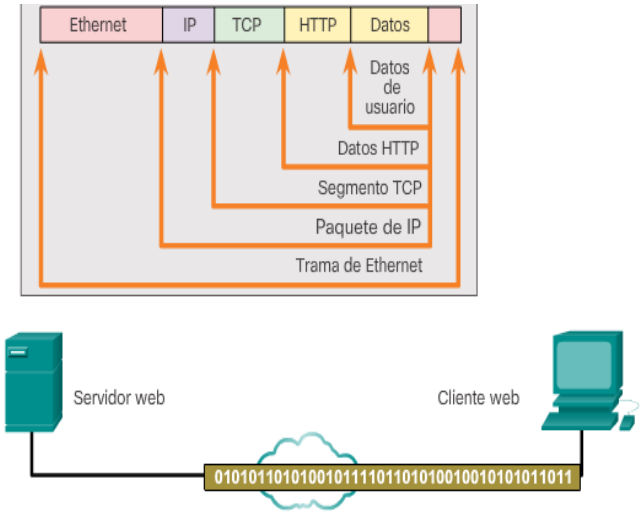
Figura Nº 2. 2: Conjunto de Protocolos TCP/IP y Proceso de Comunicación



Fuente: CCNA. (2017)

El servidor web dispone la página de lenguaje de marcado de hipertexto (HTML) para predeterminar los datos que se mandaran a través de la red.

Figura Nº 2. 3: Términos de Encapsulamiento de Protocolos



Fuente: CCNA. (2017)

El header o encabezado HTTP predetermina los datos HTML. El header contiene información diversa, incluyendo la versión HTTP que usa el servidor e indica que tiene información para el cliente web.

HTTP suministra los datos de la página web con formato HTML a la capa de transporte.

IP asigna las direcciones IP determina direcciones de origen y destino, dicha información se conoce como paquete IP.

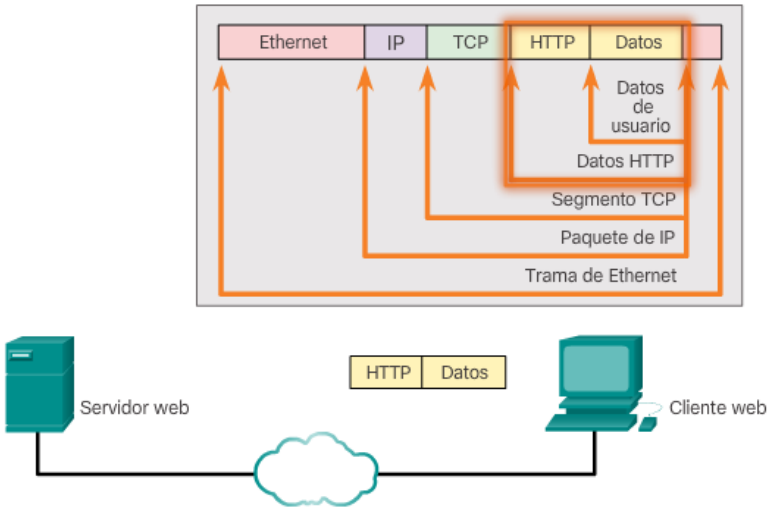
Ethernet emite mensajes en ambos extremos del paquete IP, denominados "trama de enlace de datos". La ruta se traza desde el router más cercano, a lo largo de la ruta hacia el cliente web. Este router descarta la información de Ethernet, verifica el paquete IP, analiza y define la mejor ruta para el paquete, coloca el paquete en una trama nueva y lo envía al siguiente router vecino hacia el destino. Cada router elimina y agrega información de enlace de datos nueva antes de reenviar el paquete.

Estos datos viajan a través de la internetwork, que consta de medios y dispositivos intermediarios.

El host receptor recibe las tramas de la capa de enlace de datos que contiene la información. Cada encabezado de protocolo se procesa y luego se elimina en el orden inverso al que se agregó. La información de Ethernet se procesa y se elimina, seguida por la información del protocolo IP, luego la información de TCP y, finalmente, la información de HTTP.

A continuación, la información de la página web se transfiere al software de navegador web del cliente.

Figura Nº 2. 4: Operación del Protocolo para Enviar y Recibir un Mensaje



Fuente: CCNA. (2017)

2.3. Normas Abiertas

Los estándares abiertos hacen posible las comunicaciones a través de la red, la competencia y la innovación. Garantizan la no monopolización del mercado.

Existen diversas alternativas en equipos de diferentes proveedores, y todas ellas con estándares como IPv4, DHCP, 802.3 (Ethernet) y 802.11 (LAN inalámbrica). Estos estándares abiertos también permiten que un cliente con el sistema operativo de Apple descargue una página web de un servidor web con el sistema operativo Linux. Esto se debe a que ambos sistemas operativos implementan los protocolos de estándar abierto, como los de la suite TCP/IP.

Figura Nº 2. 5: Organizaciones de Estandarización

Fuente: CCNA. (2017)

Las organizaciones de estandarización generalmente son organizaciones sin fines de lucro y neutrales en lo que respecta a proveedores, que se establecen para desarrollar y promover el concepto de estándares abiertos.

2.4. Estándares de Internet

Las organizaciones de estandarización generalmente respectan a proveedores, que desarrollan y promueven estándares abiertos.

Las organizaciones de estandarización son:

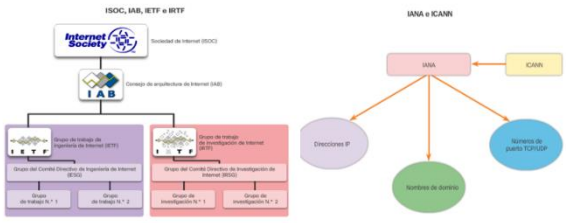
- **Sociedad de Internet (ISOC):** Es responsable de promover el desarrollo, la evolución y el uso abierto de Internet en todo el mundo.
- **Consejo de Arquitectura de Internet (IAB):** Es responsable de la administración y el desarrollo general de los estándares de Internet.
- **Grupo de Trabajo de Ingeniería de Internet (IEFT):** desarrolla, actualiza y

mantiene las tecnologías de Internet y de TCP/IP. Esto incluye el proceso y documentación para el desarrollo de nuevos protocolos y la actualización de los protocolos existentes.

- **Grupo de Trabajo de Investigación de Internet (IRTF):** Está enfocado en la investigación a largo plazo en relación con los protocolos de Internet y TCP/IP, como los grupos Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG) y Peer-to-Peer Research Group (P2PRG).
- **Corporación de Internet para la Asignación de Nombres y Números (ICANN):** Tiene base en los Estados Unidos, coordina la asignación de direcciones IP, la administración de nombres de dominio y la asignación de otra información utilizada por los protocolos TCP/IP.
- **Autoridad de Números Asignados de Internet (IANA):** Responsable de supervisar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.

Otras organizaciones de estandarización tienen responsabilidades de promoción y creación de estándares de comunicación y electrónica que se utilizan en la entrega de paquetes IP como señales electrónicas en medios inalámbricos o por cable.

Figura Nº 2. 6: Otras Organizaciones de Estandarización



Fuente: CCNA. (2017)

- **Instituto de Ingenieros en Electricidad y Electrónica (IEEE):** Organización de electrónica e ingeniería eléctrica dedicada a avanzar en innovación tecnológica y a elaborar estándares en una amplia gama de sectores, que incluyen energía, servicios de salud, telecomunicaciones y redes.
- **Asociación de Industrias Electrónicas (EIA):** Es conocida principalmente por sus estándares relacionados con el cableado eléctrico y los conectores.
- **Asociación de las Industrias de las Telecomunicaciones (TIA):** Es responsable de desarrollar estándares de comunicación en diversas áreas, entre las que se incluyen equipos de radio, torres de telefonía móvil, dispositivos de voz sobre IP (VoIP) o comunicaciones satelitales.
- **Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T):** Es uno de los organismos de estandarización de comunicación más grandes y más antiguos. El UIT-T define estándares para la compresión de vídeos, televisión de protocolo de Internet y comunicaciones de banda ancha, como la línea de suscriptor digital.

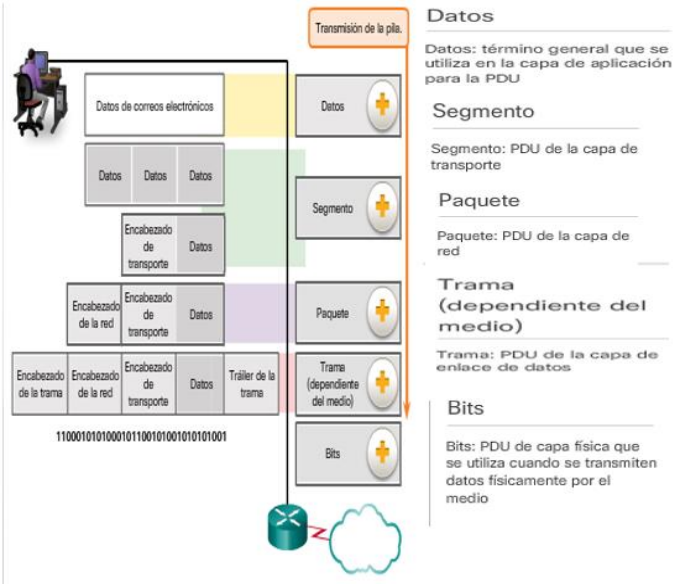
2.5. Segmentación del Mensaje y Encapsulamiento

Es fraccionar los datos en pequeñas partes para enviarlas por la red. Al momento de segmentar los datos de origen al destino, se pueden intercalar diversas conversaciones en la red, llamadas multiplexión. Se puede retransmitir los mensajes en caso los datos no lleguen al destino final.

2.6. Unidades de Datos de Protocolo

Mientras los datos de la aplicación bajan a la pila del protocolo y se transmiten por los medios de la red, se agrega diversa información de protocolos en cada nivel. Esto comúnmente se conoce como proceso de encapsulamiento. Cada fragmento de datos que ocupa cada capa se denomina unidad de datos del protocolo (PDU). En el proceso de encapsulamiento, cada capa almacena las PDU que obtiene de la capa inferior de acuerdo al protocolo usado. Según el proceso cada capa tiene un PDU diferente.

Figura Nº 2. 7: Proceso de Encapsulamiento



Fuente: CCNA. (2017)

2.7. Desencapsulamiento

Proceso inverso al encapsulamiento en el host receptor. Elimina los encabezados del protocolo usando los dispositivos receptores. Los datos se desencapsulan hacia la aplicación del usuario final.

2.8. Acceso a la Red

2.8.1. Capa Física

En el modelo OSI, la capa física transporta los bits a través de un medio de red. El objetivo de la capa física es codificar y decodificar la información en señales eléctricas, ondas de radio u ópticas que representan los bits. Los medios de la capa física son: Cable de cobre, la información es transmitida en forma de señales eléctricas; cable de fibra óptica, la información es transmitida en forma de ondas de luz y conexión inalámbrica, la información es transmitida en forma de ondas de radio

Estándares de la Capa Física

La capa física está definida por circuitos electrónicos y eléctricos, por ende, es necesario que organizaciones especializadas en ingeniería eléctrica y telecomunicaciones estandaricen este hardware. Algunos de estas organizaciones son:

Unión Internacional de Telecomunicaciones (ITU)

Instituto Nacional Estadounidense de Estándares (ANSI)

Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

FUNCIONES DE LA CAPA FÍSICA

Componentes físicos: Dispositivos electrónicos y conectores que transmiten la información representada en bits

Codificación y decodificación: Transforma los datos en códigos predefinidos, teniendo en cuenta que los códigos establecidos entre dispositivos electrónicos son representados por impulsos 1 o 0.

Señalización: la capa física establece, que tipo de señal es definida como 1 o como 0.

Figura Nº 2. 8: Cable UTP y conector RJ 45

Fuente: Yela, P. (2014). Protocolos de Telecomunicaciones Capa Física y Capa de Enlace de datos. PDF. Recuperado de: https://pabloyela.files.wordpress.com/2014/01/clase2_protocolos.pdf

2.8.2. Capa de Enlace de Datos

El host que emite la información, el objetivo principal de la capa de enlace de datos es alistar los datos para la correcta transmisión e inspeccionar los datos que accedan a los medios físicos.

En el host receptor, la capa física recepciona la información, a través de medios de transmisión, después de decodificar la señal y convertirla en bits.

Tarjeta de Interfaz de Red

Las tarjetas de interfaz pueden conectar a la red a cualquier dispositivo.

Las NIC ethernet son usadas para conexiones alámbricas.

Las NIC de red de área local inalámbrica (WLAN) se usan para transmisiones inalámbricas.

DIRECCIÓN MAC

Son direcciones únicas en cada dispositivo, para identificar origen y destino real de la información, y evitar sobrecarga excesiva para el procesamiento de cada trama.

SWITCH

Los switches se utilizan para conectar varios dispositivos a través de la misma red. De esta manera, un switch puede conectar varias computadoras, impresoras y servidores para crear una red de servicios compartidos dentro de una oficina o edificio.

El switch actúa como un controlador que permite que diferentes dispositivos compartan información entre sí.

Dispositivo que se encuentra en la capa de enlace de datos, por ende, utiliza dirección MAC para reenviar información a través de sus puertos.

Figura Nº 2. 9: Tarjeta de Interfaz de Red y Dirección MAC

Fuente: HASLAB IG. Networks and the effects of using them. Recuperado de: http://haslab.co.uk/IG%20ICT/unit4_networks_2.html

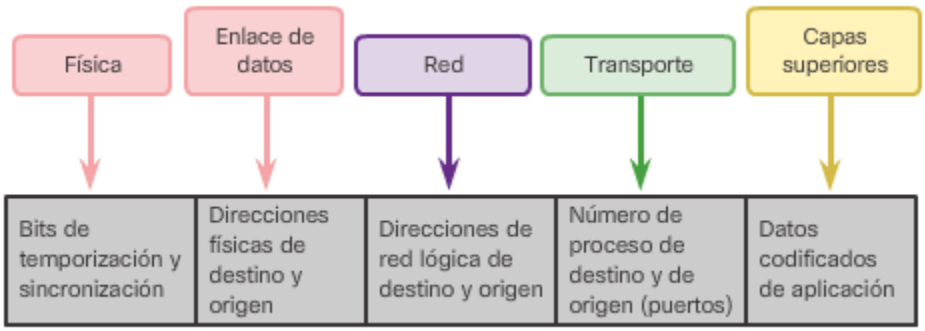
2.8.3. Capa de Red

La capa de red es responsable de enviar los datos desde el dispositivo de origen o emisor hasta el dispositivo de destino o receptor con una dirección IP. Los protocolos de las dos capas contienen las direcciones de origen y de destino, pero sus direcciones tienen objetivos distintos.

Los paquetes IP contienen dos direcciones IP:

- **Dirección IP de origen:** La dirección IP del dispositivo emisor, el origen del paquete.
- **Dirección IP de destino:** La dirección IP del dispositivo receptor, es decir, el destino final del paquete.

Figura Nº 2. 10: Direcciones de Red



Fuente: CCNA. (2017)

DISPOSITIVOS EN UNA RED REMOTA

Funciones de la dirección de la capa de red y de la dirección de la capa de enlace de datos cuando un dispositivo se comunica con un otro en una red remota.

FUNCIÓN DE LAS DIRECCIONES DE LA CAPA DE RED

Cuando el emisor del paquete se encuentra en una red distinta de la del receptor, las direcciones IP de origen y de destino representan los hosts en redes diferentes. Esto lo indica la porción de red de la dirección IP del host de destino.

- Dirección IP de origen: La dirección IP del dispositivo emisor, es decir, el equipo cliente.
- Dirección IP de destino: La dirección IP del dispositivo receptor, es decir, el servidor web.

ROUTING

Un router es el encargado de procesar el paquete IP, para enviar información correctamente de host a host. El router es encargado de elegir el mejor camino para llegar a un host de destino

CARACTERÍSTICAS DEL PROTOCOLO IP

Una dirección IPv4 es un número de 32 bits formado por cuatro octetos (números de 8 bits) en una notación decimal, separados por puntos. Un bit puede ser tanto un 1 como un 0 (2 posibilidades), por lo tanto, la notación decimal de un octeto tendría 2^8 posibilidades (256 de ellas para ser exactos). Ya que nosotros empezamos a contar desde el 0, los posibles valores de un octeto en una dirección IP van de 0 a 255. Ejemplos de direcciones IPv4: 192.168.0.1, 66.228.118.51, 173.194.33.16

Si una dirección IPv4 está hecha de cuatro secciones con 256 posibilidades en cada sección, para encontrar el número de total de direcciones IPv4, solo debes de multiplicar 256 x 256 x 256 x 256 para encontrar como resultado 4,294,967,296 direcciones.

Las direcciones IPv6 están basadas en 128 bits. Usando la misma matemática anterior, nosotros tenemos 2^{128} para encontrar el total de direcciones IPv6 totales, se tendría 2^{32}

Para permitir el uso de esa gran cantidad de direcciones IPv6 más fácilmente, IPv6 está compuesto por ocho secciones de 16 bits, separadas por dos puntos (:). Ya que cada sección es de 16 bits, tenemos 2 elevado a la 16 de variaciones (las cuales son 65,536 distintas posibilidades). Usando números decimales de 0 a 65,535, tendríamos representada una dirección bastante larga, y para facilitarlo es que las direcciones IPv6 están expresadas con notación hexadecimal (16 diferentes caracteres: 0-9 y a-f). Ejemplo de una dirección IPv6: 2607: f0d0: 4545: 3: 200: f8ff: fe21: 67cf

GATEWAY PREDETERMINADO

Enruta el tráfico hacia otras redes y lo puede hacer fuera de la red local.

Un gateway (puerta de enlace) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Una puerta de enlace o gateway es normalmente un equipo informático configurado para hacer posible a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones.

Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

La dirección IP de un gateway (o puerta de enlace) a menudo se parece a 192.168.1.1 o 192.168.0.1 y utiliza algunos rangos predefinidos, 127.x.x.x, 10.x.x.x, 172.x.x.x, 192.x.x.x, que engloban o se reservan a las redes locales.

En caso de usar un ordenador como gateway, necesariamente deberá tener instaladas 2 tarjetas de red.

MÁSCARA DE SUBRED

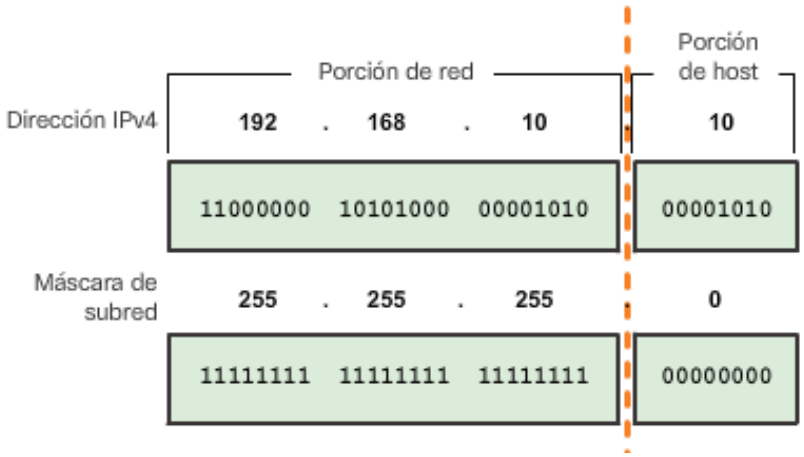
Se usa para identificar la porción de red/host de la dirección IPv4.

Cuando se asigna una dirección IPv4 a un dispositivo, la máscara de subred se usa para determinar la dirección de red a la que pertenece el dispositivo. La dirección de red representa todos los dispositivos de la misma red.

Para identificar las porciones de red y de host de una dirección IPv4, se compara la máscara de subred con la dirección IPv4 bit por bit, de izquierda a derecha.

Los 1 de la máscara de subred identifican la porción de red, mientras que los 0 identifican la porción de host. Se debe tener en cuenta que la máscara de subred no contiene en efecto la porción de red o de host de una dirección IPv4, sino que simplemente le dice a la PC dónde buscar estas porciones en una dirección IPv4 dada.

Figura Nº 2. 11: Comparación de la Dirección IP y la Máscara de Subred



Fuente: CCNA (2017)

2.8.4. Capa de Transporte

La función principal es fijar una sesión entre dos aplicaciones y transmitir información entre estas.

Para lograr la transmisión de datos con las aplicaciones adecuadas, la capa de transporte identifica la aplicación con la que desea comunicarse el usuario, y asigna un numero de puerto para que los dates pasen a través de él.

Protocolos de la Capa de Transporte

TCP: Es un protocolo confiable ya que hace seguimiento al momento de enviar datos, y los pasos que sigue son los siguientes:

- Numeración y seguimiento de los datos segmentados y transmitidos hasta una aplicación especifica
- Reconocimiento de los datos aceptados
- Retransmisión de los datos sin reconocimiento después de un tiempo de espera

Las aplicaciones que transmiten audio y vídeo almacenado utilizan TCP. Por ejemplo, si de repente la red no puede admitir el ancho de banda necesario para ver una película, la aplicación detiene la reproducción, durante la pausa, es posible que vea un mensaje de "almacenando en búfer" mientras TCP intenta restablecer la transmisión. Una vez que todos los segmentos estén en orden y se restaure un nivel mínimo de ancho de banda, la sesión TCP se reanuda y la película comienza a reproducirse.

UDP: otorga segmentación de datos con muy poca sobrecarga y revisión de datos, sin embargo, eso lo hace una entrega más rápida que TCP.

A diferencia de TCP, UDP no tiene control de flujo, en caso los datos se pierdan, estos no se vuelven a retransmitir, por lo que lo hace un protocolo simple

UDP se usa en la telefonía IP, las transmisiones en vivo.

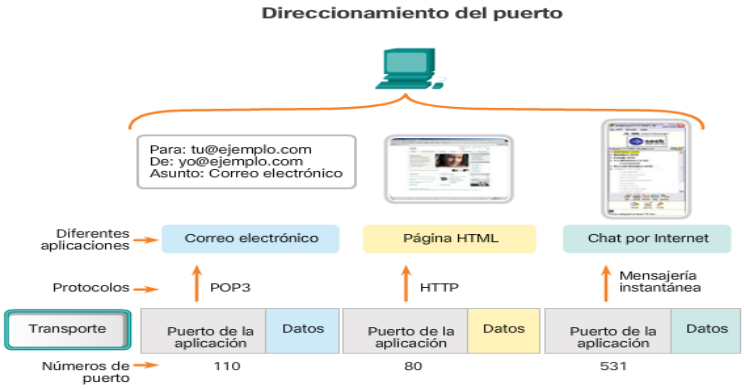
NÚMEROS DE PUERTO

El número de puerto de origen está asociado con la aplicación que origina la comunicación en el host local. El número de puerto de destino está asociado con la aplicación de destino en el host remoto.

El número de puerto de origen es generado de manera dinámica por el dispositivo emisor para identificar una conversación entre los dispositivos. Este proceso permite establecer varias conversaciones simultáneamente. Resulta habitual para un dispositivo enviar varias solicitudes de servicio HTTP a un servidor web al mismo tiempo. El seguimiento de cada conversación HTTP por separado se basa en los puertos de origen.

El cliente coloca un número de puerto de destino en el segmento para informar al servidor de destino el servicio solicitado, como se muestra en la figura. Por ejemplo, cuando un cliente especifica el puerto 80 en el puerto de destino, el servidor que recibe el mensaje sabe que se solicitan servicios web. Un servidor puede ofrecer más de un servicio de manera simultánea, por ejemplo, servicios web en el puerto 80 al mismo tiempo que ofrece el establecimiento de una conexión FTP en el puerto 21.

Figura Nº 2. 12: Direccionamiento de Puerto



Fuente: CCNA (2017)

2.8.5. Capa de Sesión

Como su nombre lo indica, las funciones de la capa de sesión crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos y para reiniciar sesiones que se interrumpieron o que estuvieron inactivas durante un período prolongado.

Protocolos de la Capa de Sesión

SQL: Es un leguaje de consulta estructurado, surgido de un proyecto de investigación para acceso a base de datos

NFS: Permite acceder y compartir archivos de una red, siguiendo la estructura cliente-servidor. NFS comparte directorios seleccionados con condiciones de seguridad concretas.

2.8.6. Capa De Presentación

La capa de presentación tiene tres funciones principales:

- Dar formato a los datos en el dispositivo de origen, o presentarlos, en una forma compatible para que los reciba el dispositivo de destino.
- Comprimir los datos de forma tal que los pueda descomprimir el dispositivo de destino.
- Cifrar los datos para la transmisión y descifrarlos al recibirlos.

La capa de presentación da formato a los datos para la capa de aplicación establezca estándares para los formatos de archivo. Dentro de los estándares más conocidos para vídeo encontramos QuickTime y Motion Picture Experts Group (MPEG).

Algunos formatos gráficos de imagen conocidos que se utilizan en redes son el formato de intercambio de gráficos (GIF), el formato del Joint Photographic Experts Group (JPEG) y el formato de gráficos de red portátiles (PNG).

PROTOCOLOS DE LA CAPA DE PRESENTACIÓN

XDR (External Data Representation): Es un protocolo de presentación de datos. Según el modelo OSI permite la transferencia de datos entre máquinas de diferentes arquitecturas y sistemas operativos.

SMB (Server Message Block): Permite compartir archivos e impresoras entre nodos de una red. Es utilizado principalmente en ordenadores Microsoft Windows y DOS.

2.8.7. Capa de Aplicación

La capa de aplicación es la más cercana al usuario final, es la capa que proporciona la interfaz entre las aplicaciones utilizada para la comunicación y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino.

Protocolos de la Capa de Aplicación

Existen muchos protocolos de capa de aplicación, y están en constante desarrollo. Algunos de los protocolos de capa de aplicación más conocidos incluyen:

- HTTP (protocolo de transferencia de hipertexto)
- FTP (protocolo de transferencia de archivos)
- TFTP (protocolo trivial de transferencia de archivos)
- IMAP (protocolo de acceso a mensajes de Internet)
- DNS (protocolo del sistema de nombres de dominios).

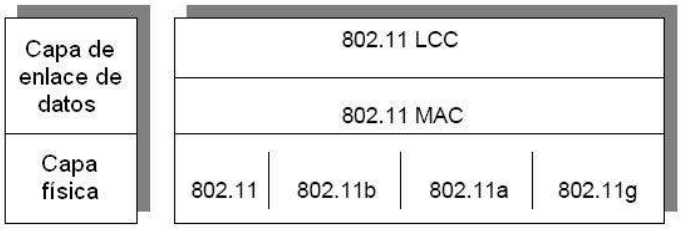
2.9. Estándar 802.11

Las redes inalámbricas actualmente son un componente muy importante entre las redes informáticas y continúa en crecimiento. Por la realización del estándar LAN inalámbrica IEEE 802.11.

Las redes inalámbricas no necesitan guiarse por cables para lograr conectarse a equipos, si no que usa el aire como medio, para poder transmitir y recibir datos gracias a las ondas electromagnéticas que son capaces de propagarse en diversos medios.

El estándar 802.11 es parte de Instituto de Ingeniería Eléctrica y Electrónica (IEEE) desarrollado en 1990 y conocido con el nombre de WI-FI (Wireless Fidelity Alliance, que es una organización que promueve la tecnología WI-FI y certifica los productos WI-FI, si se ajustan a ciertas normas de interoperabilidad).

Figura Nº 2. 13: Dos Capas Inferiores del Modelo OSI



Fuente: López, J. (2008), Diseño e Implementación de un Sistema de Gestión de Accesos a una Red WI-FI Utilizando Software Libre

El IEEE 802.11 utiliza la banda ISM (Industrial, Scientific and Medical, banda reservada internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica).

2.9.1. 802.11 b

IEEE 802.11b fue la primera versión en desarrollarse, admite una tasa de transmisión teórica de hasta 11 Mbps.

802.11b utiliza frecuencia de señalización de radio no regulada 2.4 GHz. IEEE 802.11b usa la tecnología FSHH, esta técnica toma la señal de transmisión y modula una señal portadora que, va saltando de frecuencia en frecuencia, dentro del ancho de la banda asignado, en función del tiempo. Este cambio reduce la interferencia producida por otra señal, afectando solo si ambas señales se transmiten en la misma frecuencia y en el mismo momento.

Un patrón de salto (hopping code), determina las frecuencias por las que se transmitirá y el orden de uso de estas. Para recibir correctamente la señal, el receptor debe disponer del mismo patrón de salto que el emisor y escuchar la señal en la frecuencia y el momento correcto.

IEEE amplió el estándar 802.11 original en julio de 1999, creando la especificación 802.11b. 802.11b admite una velocidad teórica de hasta 11 Mbps. Se debe esperar un ancho de banda más realista de 5.9 Mbps (TCP) y 7.1 Mbps (UDP).

802.11b utiliza la misma frecuencia de señalización de radio no regulada (2.4 GHz) que el estándar 802.11 original. Los vendedores a menudo prefieren usar estas frecuencias para reducir sus costos de producción.

Al no estar regulado, el equipo 802.11b puede incurrir en interferencia procedente de hornos de microondas, teléfonos inalámbricos y otros dispositivos que utilizan el mismo rango de 2,4 GHz. Sin embargo, al instalar el engranaje 802.11b a una distancia razonable de otros dispositivos, la interferencia puede evitarse fácilmente.

2.9.2. 802.11a

IEEE 802.11a utiliza la banda de 5 GHz, IEEE creó una segunda extensión para el estándar 802.11 original llamado 802.11a. Debido a que 802.11b ganó popularidad mucho más rápido que 802.11a, algunas personas creen que 802.11a se creó después de 802.11b. De hecho, 802.11a se creó al mismo tiempo.

802.11a admite ancho de banda de hasta 54 Mbps y señales en un espectro de frecuencia regulado de alrededor de 5 GHz. La frecuencia más alta también significa que las señales 802.11a tienen más dificultades para penetrar paredes y otras obstrucciones.

Mientras 802.11b estaba en desarrollo, IEEE creó una segunda extensión para el estándar 802.11 original llamado 802.11a. Debido a que 802.11b ganó popularidad mucho más rápido que 802.11a, algunas personas creen que 802.11a se creó después de 802.11b. De hecho, 802.11a se creó al mismo tiempo. Debido a su costo más alto, 802.11a se encuentra generalmente en redes comerciales, mientras que 802.11b sirve mejor al mercado interno.

Como 802.11a y 802.11b utilizan frecuencias diferentes, las dos tecnologías son incompatibles entre sí. Algunos proveedores ofrecen equipos híbridos de red 802.11a / b, pero estos productos simplemente implementan los dos estándares uno al lado del otro (cada dispositivo conectado debe usar uno u otro).

IEEE 802.11a usa la tecnología OFDM, la multiplexación por división de frecuencia ortogonal (OFDM) es un esquema de modulación que se ha vuelto virtualmente omnipresente en el mundo de las comunicaciones inalámbricas.

2.9.3. IEEE 802.11g

Intenta combinar lo mejor de 802.11a y 802.11b. 802.11g admite ancho de banda de hasta 54 Mbps, y utiliza la frecuencia de 2,4 GHz para un mayor alcance. 802.11g es compatible con 802.11b, lo que significa que los puntos de acceso 802.11g funcionarán con adaptadores de red inalámbricos 802.11b y viceversa.

Ventajas de 802.11g: compatible con prácticamente todos los dispositivos inalámbricos y equipos de red actualmente en uso; La opción menos cara.

Desventajas de 802.11g: toda la red se ralentiza para coincidir con cualquier dispositivo 802.11b en la red; estándar más lento / más viejo todavía en uso.

2.9.4. IEEE 802.11n

Opera en la banda dual de 2.4GHz y 5GHz. 802.11n (también conocido como Wireless N) se diseñó para mejorar 802.11g en la cantidad de ancho de banda admitida al utilizar múltiples señales y antenas inalámbricas en lugar de una. Los grupos de estándares industriales ratificaron 802.11n en 2009 con especificaciones que proporcionan hasta 300 Mbps de ancho de banda de red. 802.11n también ofrece un rango algo mejor que los estándares Wi-Fi anteriores debido a su mayor intensidad de señal, y es compatible con versiones anteriores con 802.11b / g.

Ventajas de 802.11n: mejora significativa del ancho de banda de estándares anteriores; amplio soporte en dispositivos y equipos de red

Desventajas de 802.11n: más costoso de implementar que 802.11g; el uso de señales múltiples puede interferir con redes cercanas basadas en 802.11b / g

2.10. Aspectos de Seguridad en IEEE 802.11

2.10.1. Seguridad Wep

La seguridad WEP (Wired Equivalent Privacy o Privacidad Equivalente a Cableado) implica dos partes, autenticación y cifrado. La autenticación en WEP implica la autenticación de un dispositivo cuando se une por primera vez a la LAN (Local Area Network o Red de Área Local). El proceso de autenticación en las redes inalámbricas que usan WEP consiste en evitar que los dispositivos / estaciones se unan a la red a menos que conozcan la clave WEP.

En la autenticación basada en WEP, el dispositivo inalámbrico envía la solicitud de autenticación al punto de acceso inalámbrico, luego el punto de acceso inalámbrico envía 128 bits aleatorios en un texto claro al cliente solicitante.

El dispositivo inalámbrico utiliza la clave secreta compartida y lo envía al punto de acceso inalámbrico. El punto de acceso inalámbrico descifra el mensaje usando la clave secreta compartida y es verificado. Si la clave coincide con los 128 bits enviados por el punto de acceso inalámbrico, entonces la autenticación tiene éxito de lo contrario no.

Desafortunadamente, en web la misma clave secreta o clave compartida se usa tanto para la autenticación como para el cifrado. Así que no hay manera de saber si los mensajes posteriores provienen del dispositivo de confianza o de un impostor. Este tipo de autenticación es propenso al ataque de "man in the middle" (hombre en el medio).

2.10.2. Encriptación WEB

Una encriptación WEP es un tipo de cifrado, implementado en el protocolo de conexión WI-FI 802.11, se encarga de cifrar la información que vamos a transmitir entre dos puntos, de forma que solo sea posible tener acceso a ellos e interpretarlos a aquellos puntos que tengan la misma clave.

La encriptación WEP utiliza el cifrado de flujo RC4 (Rivest Cipher 4 o Cifrado Rivest 4) para cifrar los datos entre el punto de acceso y el dispositivo inalámbrico.

WEP utiliza RC4 de 8 bits y opera en valores de 8 bits creando una matriz con 256 valores de 8 bits para una tabla de búsqueda.

WEP utiliza CRC (Cyclic Redundancy Check o Verificación por Redundancia Cíclica) para la integridad de los datos. Es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos

2.10.3. Vulnerabilidad WEB

El principal problema radica en que no implementa adecuadamente el vector de iniciación del algoritmo RC4, ya que utiliza un enfoque directo y predecible para incrementar el vector de un paquete a otro. Además, existe un problema con el tamaño de los vectores de iniciación.

A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación. Aumentar los tamaños de las claves de cifrado aumenta el tiempo necesario para romperlo, pero no resulta imposible el descifrado.

Para atacar una red Wi-Fi se suelen utilizar los llamados Packet sniffers y los WEP Crackers. Para llevar a cabo este ataque se captura una cantidad de paquetes determinada (dependerá del número de bits de cifrado) mediante la utilización de un Packet sniffer y luego mediante un WEP cracker o key cracker se trata de "romper" el cifrado de la red.

Un key cracker es un programa basado generalmente en matemáticas estadísticas que procesa los paquetes capturados para descifrar la clave WEP. Crackear una llave más larga requiere la interceptación de más paquetes, pero hay ataques activos que estimulan el tráfico necesario como envenenadores de ARP (Address Resolution Protocol o Protocolo de Resolución de Direcciones).

2.10.4. Seguridad WPA

El acceso protegido Wi-Fi WPA (Wi-Fi Protected Access o Acceso Wi-Fi Protegido) es compatible con un algoritmo de cifrado fuerte y la autenticación de usuario. El estándar WPA emplea el TKIP (Temporal Key Integrity Protocol o Protocolo de Integridad de Clave Temporal) con RC4, para el cifrado y la verificación de integridad del mensaje **MIC (**Pulse Code Modulation o Modulación por Impulsos Codificados) utilizando claves de 128 bits que se generan dinámicamente para el cifrado. En una empresa, las claves se generan aprovechando el protocolo de autenticación 802.1X con el **EAP** (Extensible Authentication Protocol o Protocolo de autenticación extensible).

El protocolo 802.1X es un método de control de acceso a la red que se utiliza tanto en redes cableadas como inalámbricas. El uso del protocolo 802.1X de EAP permite la compatibilidad con una variedad de tipos de credenciales de usuario, incluidos el nombre de usuario / contraseña, las tarjetas inteligentes, las identificaciones seguras o cualquier otro tipo de identificación de usuario.

Los clientes y los AP (Access Point o Puntos de Acceso) se autentican frente a un servidor de servicio de usuario de acceso telefónico de autenticación (RADIUS) que, valida el acceso de los clientes a la red, y permite a los clientes conectados saber que están hablando con puntos de acceso válidos una vez que están en la red.

En el estándar WPA, si se emplea seguridad empresarial, un usuario proporciona credenciales al servidor RADIUS que autentica al usuario, o si no, se emplea seguridad empresarial, suministra un PSK ingresado manualmente en el dispositivo cliente y el Punto de Acceso. Una vez que un usuario se autentica, se crea una clave maestra única para la sesión.

En resumen, las mejoras en WPA sobre WEP son: el aumento en la longitud de la clave de 40 bits a 128 bits; el aumento de la longitud del vector de inicialización para el cifrado RC4 de 24 bits a 48 bits; el uso de una clave secreta recién generada para el cifrado de cada paquete; comprobación de integridad del mensaje (MIC).

2.10.5. Seguridad WPA 2

El estándar WPA2 tiene dos componentes, cifrado y autenticación que son cruciales para una **LAN** inalámbrica segura. La parte de encriptación de WPA2 exige el uso de AES (Advanced Encryption Standard o Estándar de Cifrado Avanzado).

2.10.6. Autenticación WPA2

Uno de los principales cambios introducidos con el estándar WPA 2 es la separación entre la autenticación del usuario y el cumplimiento de la integridad y privacidad de los mensajes, proporcionando así una arquitectura de seguridad más escalable y robusta adecuada para redes domésticas o redes corporativas con la misma destreza.

La autenticación en el modo personal WPA2, que no requiere un servidor de autenticación, se realiza entre el cliente y el AP generando un PSK (Phase Shift Keying o Modulación por Desplazamiento de Fase) de 256 bits a partir de una frase de contraseña de texto sin formato (de 8 a 63 caracteres). El PSK junto con el Identificador de conjunto de servicios y la longitud del SSID (Service Set Identifier o Identificador de Conjunto de Servicios), forman la base matemática para el PMK (Pair-wise Master Key o Clave maestra por pares) que se usará más adelante en la generación de claves. La autenticación en el modo WPA2 Enterprise se basa en el estándar de autenticación IEEE 802.1X.

Los componentes principales son el abonado (cliente) que se une a la red, el autenticador (el AP sirve como autenticador) que proporciona control de acceso y el servidor de autenticación (RADIUS) que toma las decisiones de autorización.

El autenticador (AP) divide cada puerto virtual en dos puertos lógicos, uno para el servicio y el otro para la autenticación, que forma el PAE (Physical Address Extension o Physical Address Extension). La autenticación PAE está siempre abierta para permitir el paso de marcos de autenticación, mientras que el servicio PAE solo está abierto si el servidor RADIUS realiza una autenticación exitosa. El suplicante y el autenticador se comunican utilizando la capa 2 (EAP sobre LAN). El autenticador lo convierte en mensajes RADIUS y luego los reenvía al servidor RADIUS. El servidor de autenticación (RADIUS), que debe ser compatible con los tipos de EAP del solicitante, recibe y procesa la solicitud de autenticación. Una vez que se completa el proceso de autenticación, el suplicante y el autenticador tienen una MK (Key Master o Clave maestra).

2.10.7. Cifrado WPA2

El AES utilizado por WPA2 "es un cifrado de bloque, un tipo de cifrado de clave simétrica que utiliza grupos de bits de una longitud fija, llamados bloques". Un cifrado de clave simétrica es un conjunto de instrucciones o algoritmo que utiliza la misma clave tanto para el cifrado como para el descifrado.

Los bits se cifran (utilizando una longitud de clave de 128 bits) en bloques de texto sin formato, que se calculan de forma independiente, en lugar de una secuencia de clave que actúa a través de una secuencia de entrada de datos de texto sin formato. El cifrado AES incluye 4 etapas que forman una ronda y cada ronda se itera 10 veces.

AES utiliza el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code o Modo Contador con Código de Autenticación de Mensaje de Encadenamiento de Bloques).

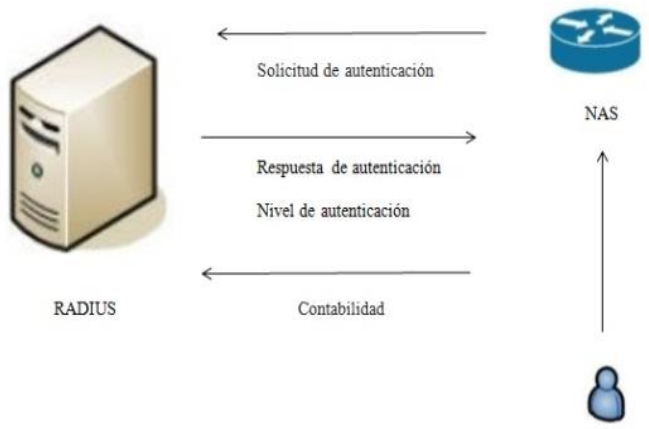
CCM es un nuevo modo de operación para un cifrado de bloque que permite utilizar una sola clave para el cifrado y la autenticación (con diferentes vectores de inicialización).

2.11. RADIUS

RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores NAS, más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos, etc.

RADIUS es un protocolo AAA y la principal alternativa para proporcionar acceso centralizado, que utiliza el protocolo UDP (User Datagram Protocol o Protocolo de Datagramas de Usuario), usa los puertos 1812/1645, para autenticación y los puertos 1813/1646, para contabilizar, todo este proceso es para la comunicación entre NAS (Network Access Server o Servidor de Acceso a la Red) o "cliente RADIUS" y el servidor RADIUS.

Figura Nº 2. 14: Secuencia de Autenticación RADIUS



Fuente: Dmitry. O (2015). RADIUS server as centralized authentication

Una de las ventajas de RADIUS es que, si la solicitud al servidor de autenticación principal falla, el servidor no necesita esperar los paquetes de respuesta (UDP no tiene conexión).

Los temporizadores de retransmisión deben configurarse, o el usuario simplemente puede intentar autenticarse con la ayuda de un servidor de autenticación secundario, si está disponible. RADIUS es compatible con muchos proveedores.

Se incluyen algunas limitaciones, lo que significa que es bastante interoperable, pero solo mientras estén en uso los mismos atributos.

2.12. PUTTY

PuTTy es de licencia libre, es un cliente de red que soporta los protocolos SSH, Telnet y Rlogin y sirve principalmente para iniciar una sesión remota con otra máquina o servidor.

2.13. Diferencias entre SSH, TELNET y RLOGIN

SSH, TELNET y RLOGIN son tres formas de hacer lo mismo: iniciar sesión en una computadora multiusuario desde otra computadora, a través de una red.

Al utilizar este tipo de interfaz, no es necesario que esté en la misma máquina. Los comandos y las respuestas se pueden sentir a través de una red, por lo que puede sentarse en una computadora y dar órdenes a otra, o incluso a más de una.

2.14. TELNET

TELNET (Telecommunication Network o Red de Telecomunicaciones). Es el nombre del protocolo de red y del programa informático que implementa el cliente. Un servidor telnet permite a los usuarios acceder a un ordenador huésped para realizar tareas como si estuviera trabajando directamente en ese ordenador.

Pertenece a la familia de protocolos de Internet. Sigue un modelo cliente/servidor. El puerto TCP que utiliza el protocolo telnet es el 23. Telnet es un protocolo del nivel aplicación y va sobre TCP/IP. TELNET sólo sirve para acceder remotamente en modo terminal, es decir, sin gráficos. Útil para Arreglar fallos a distancia, de forma remota, consultar datos a distancia.

Telnet ha tenido y tiene un fuerte uso en sistemas UNIX-LINUX y en equipos de comunicaciones (configuración de routers). Permite abrir una sesión con una máquina UNIX, de modo que múltiples usuarios con cuenta en la máquina, se conectan, abren sesión y pueden trabajar utilizando esa máquina.

2.15. SSH

SSH (Secure Shell o Cubierta segura), Cifra la información antes de transmitirla, autentica la máquina a la cual se conecta y puede emplear mecanismos de autenticación de usuarios más seguros. ™ SSH permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas) y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH. Se utiliza TCP en el puerto 22.

SSH trabaja de forma similar a como se hace con telnet. ™ La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

2.16. RLOGIN

Rlogin (Remote Login) es una aplicación TCP/IP que comienza una sesión de terminal remoto sobre el anfitrión especificado como host.

El comando rlogin le permite iniciar sesión en un sistema remoto. Una vez iniciada la sesión, puede navegar a través del sistema de archivos remoto y manipular su contenido (sujeto a autorización), copiar los archivos o ejecutar comandos remotos.

Si el sistema en el que inicia sesión es un dominio remoto, asegúrese de anexar el nombre de dominio al nombre del sistema.

Ejemplo: rlogin pluto.(nombre del dominio del sistema)

Además, puede interrumpir una operación de inicio de sesión remoto en cualquier momento al escribir Control-d.

2.17. La Integridad de la Comunicación SSH entre dos Host

Se lleva a cabo un 'handshake' (apretón de manos) encriptado para que el cliente pueda verificar que se está comunicando con el servidor correcto.

La capa de transporte de la conexión entre el cliente y la máquina remota es encriptada mediante un código simétrico.

El cliente se autentica ante el servidor.

El cliente remoto interactúa con la máquina remota sobre la conexión encriptada.

CAPITULO III

MATERIALES Y METODOS

3.1. Ubicación Geográfica del Estudio

Actualmente se ha visto muchos lugares en donde un puede conectarse a una red inalámbrica, sin embargo, no tienen la seguridad de la confidencialidad de su información y, por lo tanto, tienden a desconfiar de la seguridad de la red WI-FI. En el Centro de Comunicaciones de la Universidad Nacional del Altiplano de Puno, el personal tendrá privacidad en el acceso a la red, debido a que contarán con un servidor RADIUS a su disposición.

Los resultados del proyecto nos permitirán promover el uso de las tecnologías de la información ente los estudiantes y docentes universitarios, y así generar conocimiento sobre la seguridad informática.

La implementación del servidor RADIUS generará alta seguridad entre docentes y estudiantes del Centro de Comunicaciones de la Universidad Nacional del Altiplano, lo cual no permitirá acceso a intrusos.

3.2. Periodo de Duración del Estudio

Tabla Nº 3. 1: Periodo de Elaboración del Estudio

Actividad	Tiempo (Meses)					
	Febrero	Marzo	Abril	Mayo	Junio	Julio
Revisión bibliográfica	x	x	x	x	x	x
Planteamiento del problema e implementación del proyecto			x			
Ejecución del proyecto				x		
Análisis e interpretación de resultados					x	
Presentación de informe final						x

Elaboración Propia

3.3. Procedencia del Material de Estudio

En este proyecto se usó materiales y equipos relacionados a redes e internet para lograr una correcta conectividad entre usuario y una red WI-FI. Entre los equipos usados son:

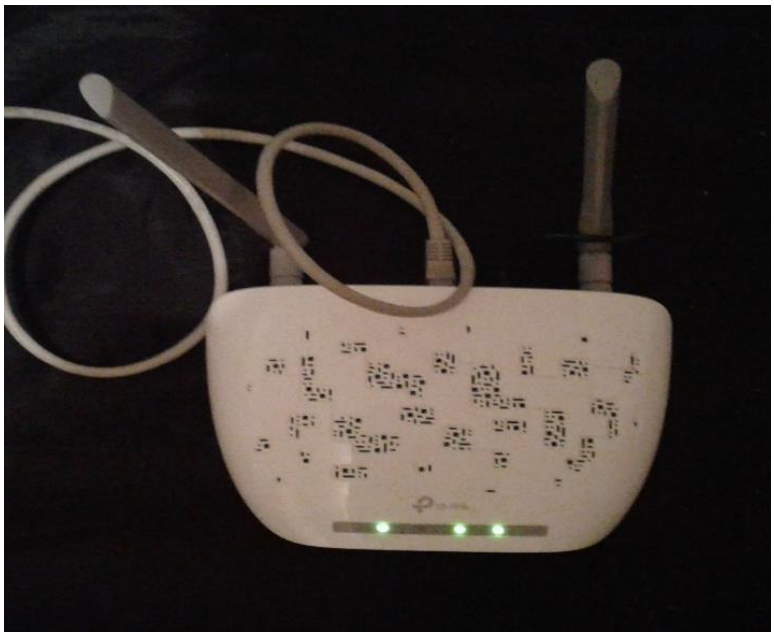
Figura Nº 3. 1: Router MOVISTAR y Cables UTP

Elaboración Propia

Figura Nº 3. 2: Switch TPLink y Cables UTP

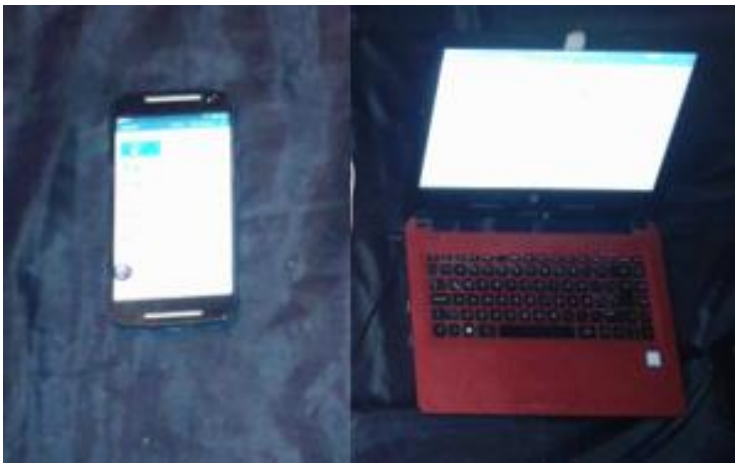
Elaboración Propia

Figura Nº 3. 3: Access Point



Elaboración Propia

Figura Nº 3. 4: Celular y Laptop como Usuarios



Elaboración Propia

3.4. Población y Muestra del Estudio

El diseño e implementación de RADIUS está destinado al Centro de Comunicaciones de la Universidad Nacional del Altiplano – Puno. (CECUNA)

Figura Nº 3. 5: CECUNA

Elaboración Propia

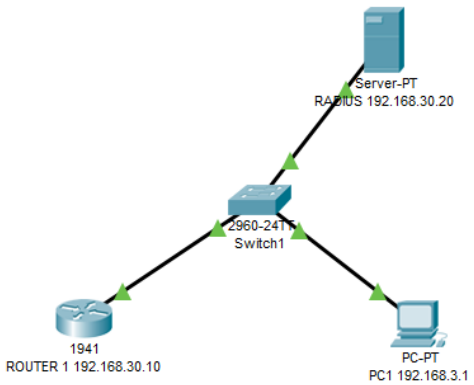
3.5. Procedimiento

3.5.1. Virtualización de AAA en Packet Tracer

3.5.2. Arquitectura de la Red

La arquitectura de red es el marco completo de la red informática de una organización. El diagrama de la arquitectura de red proporciona una imagen completa de la red establecida con una vista detallada de todos los recursos accesibles. Incluye componentes de hardware utilizados para comunicación, cableado y tipos de dispositivos, diseño de red y topologías, conexiones físicas e inalámbricas, áreas implementadas y planes futuros.

Figura Nº 3. 6: Arquitectura de Red de la Virtualización



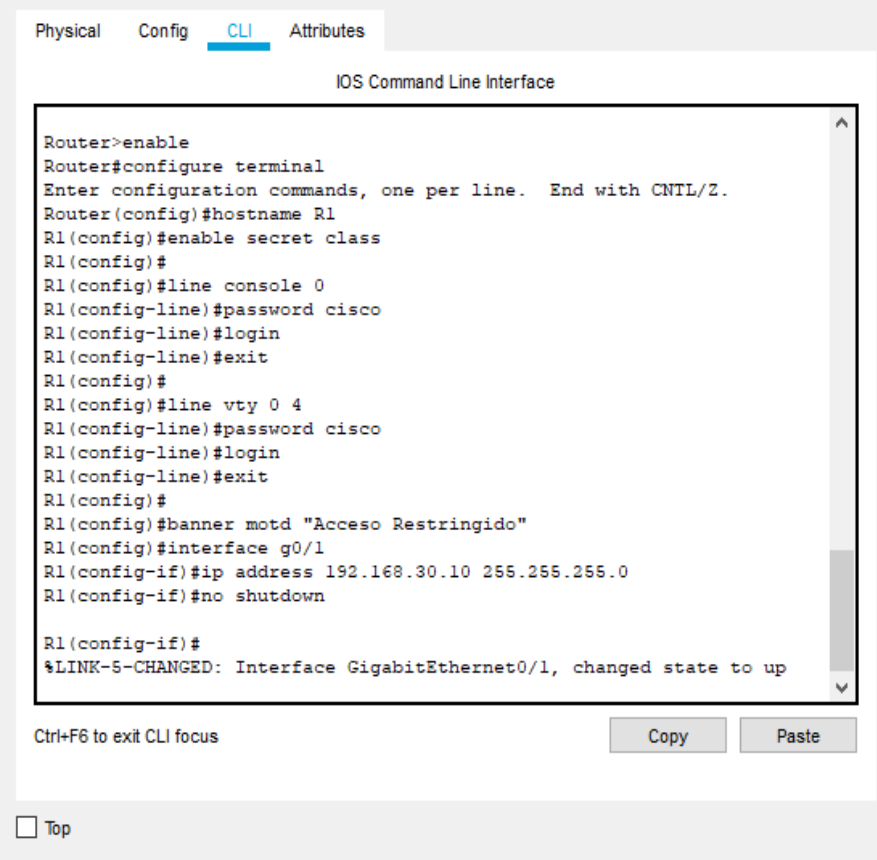
Elaboración Propia

3.5.3. Configuracion del Router

Paso1: Configuración básica de router y asignación de dirección IP, se usa los siguientes comandos:

enable:	Ingresa a EXEC privilegiado
configure terminal:	Ingresa al modo de configuración global
hostname:	Agrega un nombre a router, en este caso fue “R1”
enable secret:	Coloca una clave al modo EXEC en este caso fue class
line console 0:	para ingresar al modo de configuración de línea de la consola
login:	IOS incluye el comando login en las líneas VTY. Esto impide el acceso al dispositivo mediante Telnet sin autenticación
banner motd:	Coloca un mensaje, en caso el usuario sea incorrecto
interface g0/1:	Coloca una dirección IP y una máscara de subred a gigabit 0/1, en este caso la IP fue 192.168.30.10 y máscara de subred fue 255.255.255.0

Figura Nº 3. 7: Asignación de Direcciones IP al Router



Elaboración Propia

Paso2: Habilitación del Servidor RADIUS, se usa los siguientes comandos:

radius-server host: Conecta el router con el servidor RADIUS, para este caso usamos la dirección de servidor RADIUS 192.168.30.20

radius-server key: Agrega una clave al servidor RADIUS, en este caso fue radius1

aaa new-model: Habilita el protocolo RADIUS

aaa authentication login default

groups

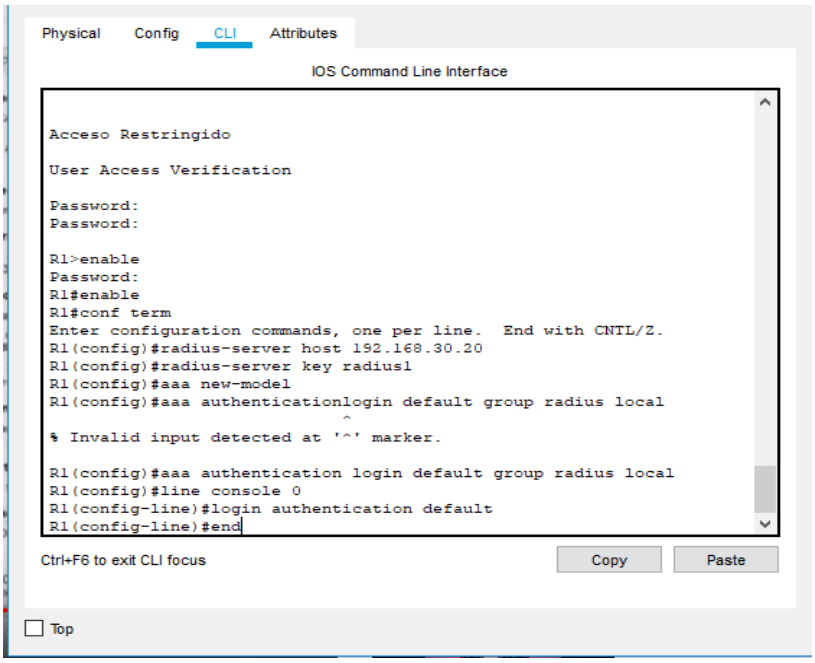
radius local: La consola, empezara a usar servidor RADIUS para la autenticación. El comando habilita la sesión de RADIUS para todos los accesos de inicio de sesión al enrutador en una red local

line console 0: Ingresa al modo de configuración de línea de la consola. El cero se utiliza para representar la primera interfaz de consola.

login authentication

default: Habilita AAA en R1 y configura la autenticación AAA para que el inicio de sesión de la consola use la lista de métodos predeterminados.

Figura Nº 3. 8: Habilitación del Servidor RADIUS

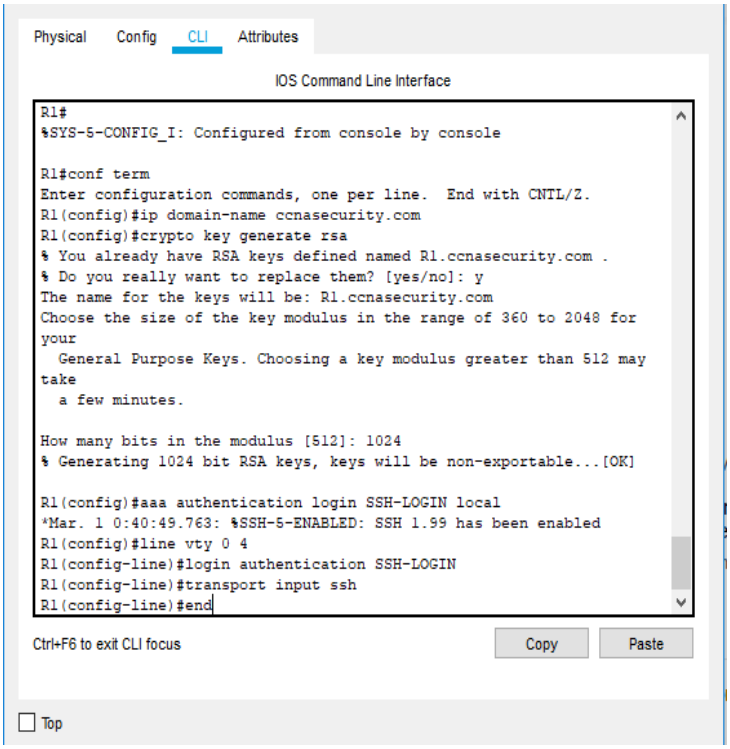


Elaboración Propia

Paso3: Activación del protocolo SSH en router, se usa los siguientes comandos:

ip domain-name:	Configura el nombre de dominio del servidor de nombres de dominio (DNS), en este caso se usó ccnasecurity.com.
crypto key generate rsa:	Genera una llave pública de 1024 bits. El protocolo SSH cifra todos los datos enviados y recibidos a través del puerto 22. Para esto fines, se utiliza el algoritmo de cifrado asimétrico RSA.
aaa authentication login ssh-login local:	Logra la autenticación de SSH en un área local, Para autorizar que los usuarios de la base de datos local pueden ejecutar comandos en el modo privilegiado (EXEC).
login authentication SHH-LOGIN:	Activa la autenticación para inicios de sesión del Authentication, Authorization, and Accounting (AAA), utilice el comando.
line vty 0 4:	Habilita 5 puertos virtuales para las conexiones SSH.
transport input ssh:	Establece que el protocolo a utilizar para conexiones remotas será SSH.

Figura Nº 3. 9: Asignación del Protocolo SSH a Router



Elaboración Propia

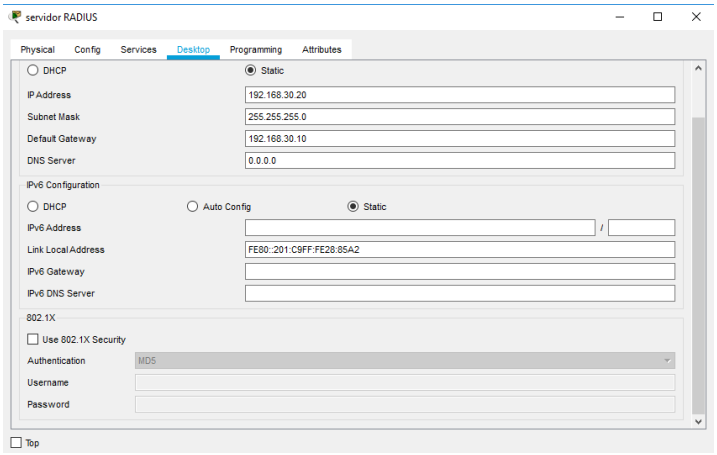
3.5.4. Configuración del Servidor RADIUS

Paso1: Asignación de dirección IP al servidor RADIUS

Una asignación de dirección IP determinará la localización de cualquier dispositivo. Esta información es utilizada para encontrar el propietario exacto de cualquier dirección IPv4 o IPv6.

La ubicación IP se puede encontrar utilizando nuestra herramienta de búsqueda de IP. Ninguna herramienta de búsqueda de IP es 100% precisa debido a muchos factores diferentes. Algunos de esos factores incluyen dónde está registrado el propietario de la IP, dónde está ubicada la agencia que controla la IP, los representantes, las IP celulares, etc. Si se encuentra en los EE. UU. Y la agencia controladora de la IP está ubicada en Canadá, lo más probable es que los resultados de búsqueda de direcciones IP se muestren como Canadá. Mostrar una IP canadiense en el norte de los EE. UU. Es muy común entre los usuarios de dispositivos móviles en la red Verizon.

Figura Nº 3. 10: Asignación de Dirección IP al Servidor RADIUS

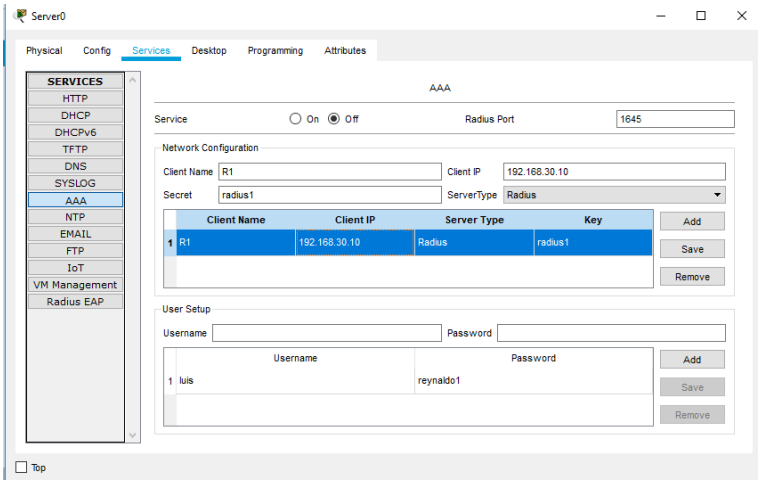


Elaboración Propia

Agregaremos como cliente al Router

También se observa que se agrega un pc como usuario, lo identificamos como, Usuario: luis y Password: reynaldo1. Para este caso se asigna como nombre del cliente el hostname del Router, la dirección IP del ROUTER y la contraseña que usamos en el comando radius-server key, para que R1 esté conectado con el servidor RADIUS.

Figura Nº 3. 11: Anexo de Cliente

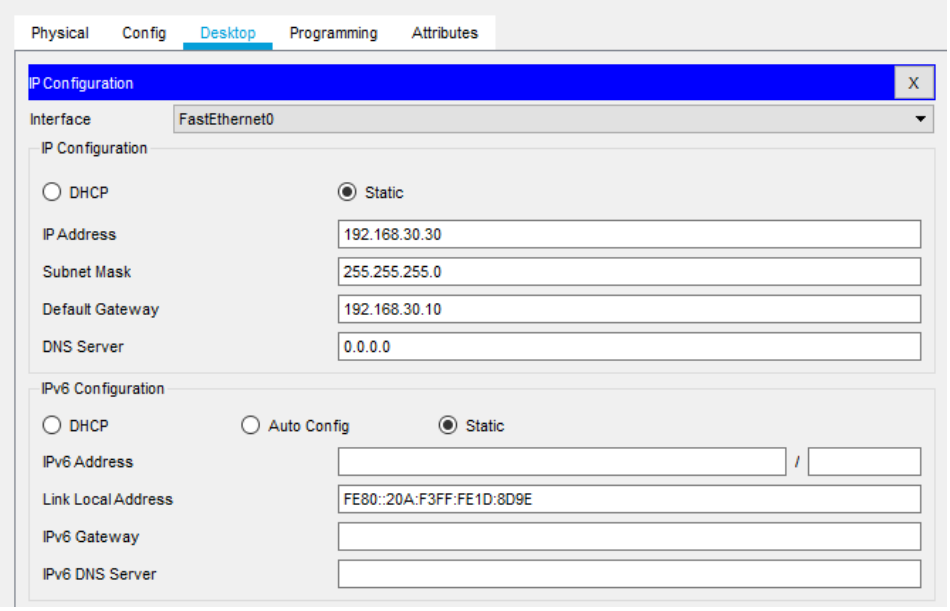


Elaboración Propia

3.5.5. Configuración de la PC

Cuando instala un nuevo dispositivo o programa, necesita configurarlo, lo que significa configurar varios interruptores y puentes (para hardware) y definir valores de parámetros (para software). Por ejemplo, el dispositivo o programa puede necesitar saber qué tipo de adaptador de video tiene y qué tipo de impresora está conectada a la computadora. Algunos parámetros son: Direccion IP, mascara de red o puerta de enlace, gran parte de esta configuración se realiza automáticamente.

Figura Nº 3. 12: Configuración de PC Usuario

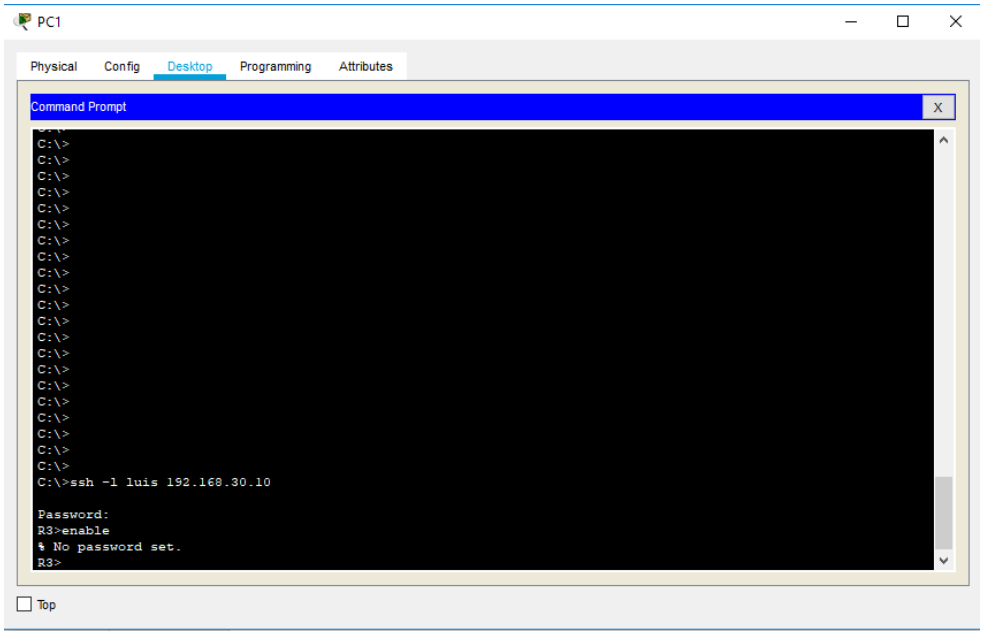


Elaboración Propia

Paso1: Acceso al router mediante el protocolo SSH

SSH en dispositivos Cisco. Podemos acceder a un enrutador Cisco o cambiarlo a través de un cable de consola o mediante acceso remoto a través de protocolos conocidos SSH (Secure Shell). SSH son protocolos de capa de aplicación utilizados para tomar acceso remoto y administrar un dispositivo.

Figura Nº 3. 13: Acceso al Router, Mediante Protocolo SSH



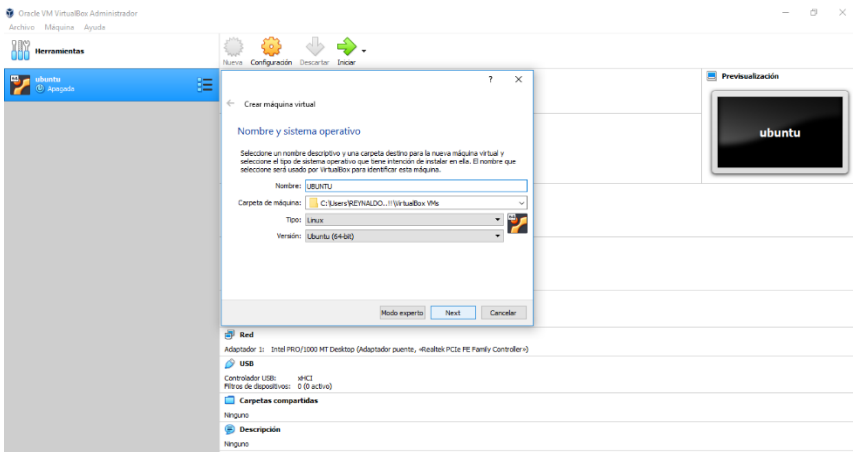
Elaboración Propia

3.5.6. Virtualización en Virtual Box

Se crea una máquina virtual, en este caso se precederá a crear un servidor UBUNTU 19.04.

Una máquina virtual, conocida como invitado, se crea dentro de un entorno informático, llamado host. Pueden existir varias máquinas virtuales en un host a la vez. Los archivos clave que componen una máquina virtual incluyen un archivo de registro, un archivo de configuración de NVRAM, un archivo de disco virtual y un archivo de configuración.

Figura Nº 3. 14: Inicio de la Creación de una Máquina Virtual

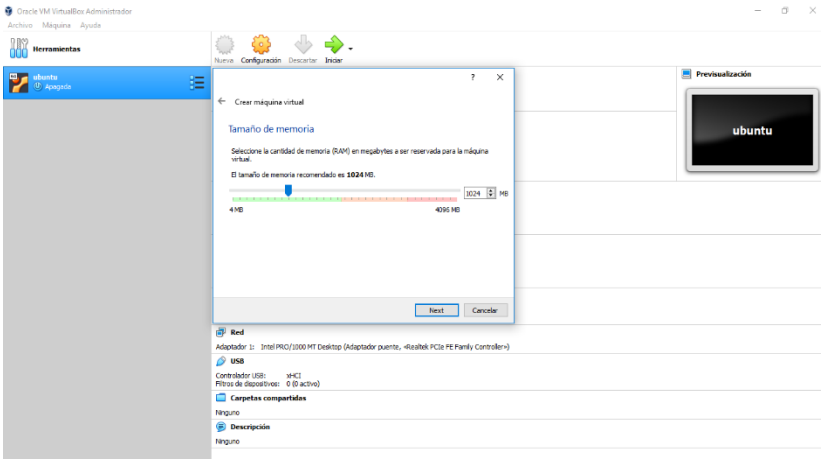


Elaboración Propia

- Selección de memoria, 1024 MB de RAM

Las máquinas virtuales son computadoras de software que proporcionan la misma funcionalidad que las computadoras físicas. Al igual que las computadoras físicas, ejecutan aplicaciones y un sistema operativo. Sin embargo, las máquinas virtuales son archivos de computadora que se ejecutan en una computadora física y se comportan como una computadora física. En otras palabras, las máquinas virtuales se comportan como sistemas informáticos separados.

Figura Nº 3. 15: 1024 MB DE RAM

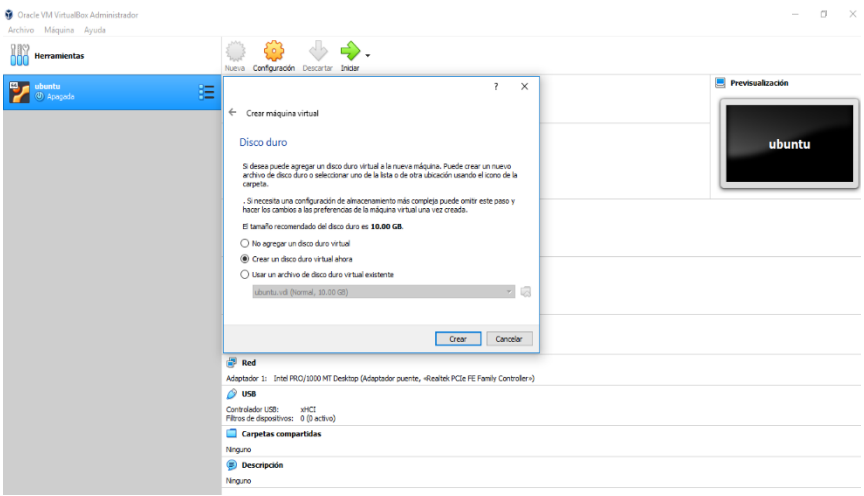


Elaboración Propia

- Se crea la máquina virtual

Las máquinas virtuales se crean para realizar tareas específicas que son riesgosas de realizar en un entorno host, como acceder a datos infectados por virus y probar sistemas operativos. Dado que la máquina virtual está aislada del resto del sistema, el software dentro de la máquina virtual no puede alterar la computadora host. Las máquinas virtuales también se pueden utilizar para otros fines, como la virtualización del servidor.

Figura Nº 3. 16: Creación de la Máquina Virtual

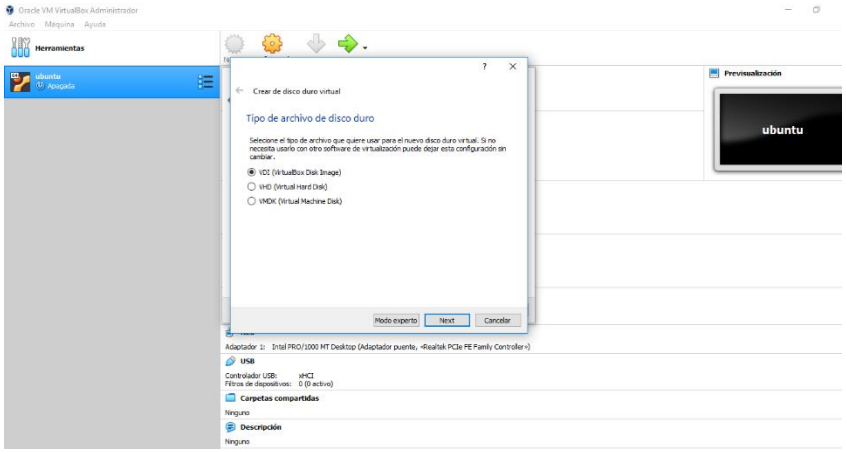


Elaboración Propia

- Se crea un disco duro virtual

Los discos duros virtuales son archivos de disco duro virtualizados que, una vez montados, aparecen y funcionan de manera casi idéntica en un disco duro físico. En este caso usaremos Virtual Box

Figura Nº 3. 17: Virtualbox Disk Image

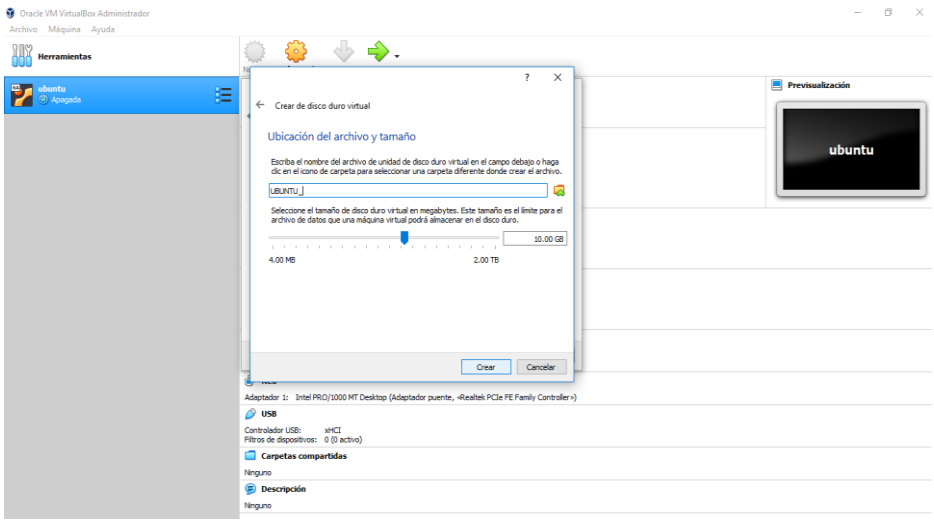


Elaboración Propia

El disco duro virtual es un formato de archivo de imagen de disco para almacenar el contenido completo de un disco duro. La imagen del disco, a veces llamada máquina virtual, replica un disco duro existente e incluye todos los datos y elementos estructurales. Se puede almacenar en cualquier lugar al que pueda acceder el host físico.

Hay dos tipos principales de discos duros virtuales: tamaño fijo y expansión dinámica. Ambos tipos tienen un valor de tamaño máximo que especifica qué tan grande será el disco para las máquinas virtuales. Sin embargo, los disco duros virtuales de tamaño fijo ocuparán automáticamente la cantidad especificada de espacio físico en el disco en el sistema de archivos de la computadora host, mientras que los discos en expansión dinámica asignarán espacio solo cuando sea necesario.

Figura Nº 3. 18: 10 GB de Disco Duro Virtual

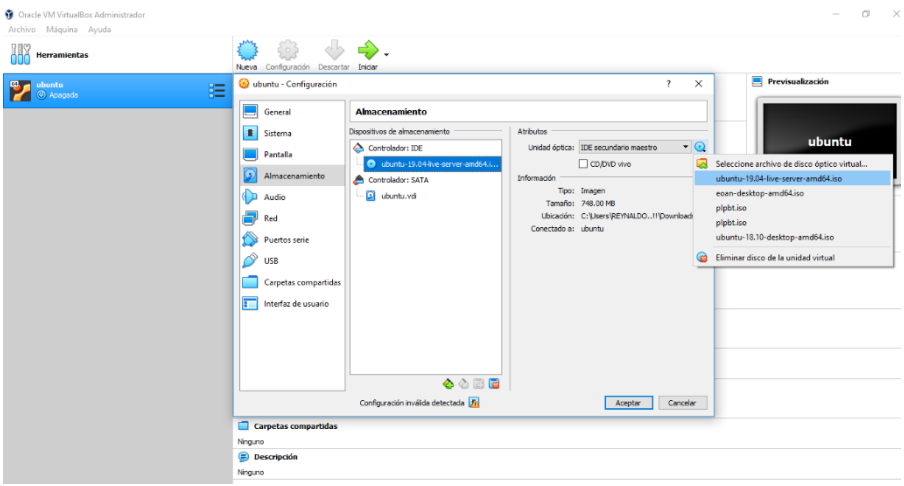


Elaboración Propia

- Selección de la imagen ISO de UBUNTU 19.04

La imagen ISO es un archivo de computadora que es una copia exacta de un sistema de archivos existente. Un ISO puede contener todo el contenido de un disco CD-ROM o medio CD. Los archivos ISO generalmente se crean a través de una aplicación de software que abrirá, creará, editará y extraerá archivos de imagen de CD o DVD, luego convertirá la imagen extraída en un archivo ISO, permitiendo fácilmente a los usuarios grabar una copia exacta del original en CD o DVD.

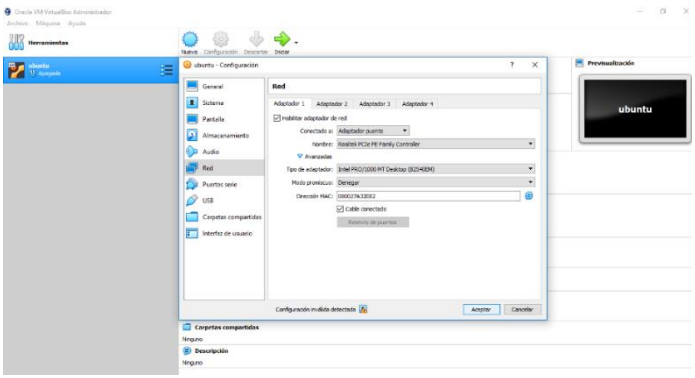
Figura Nº 3. 19: Selección de la Imagen ISO de UBUNTU 19.04



Elaboración Propia

Se agrega un adaptador puente y seleccionamos el controlador de red correspondiente, teniendo en cuenta que el cable de red debe de estar conectado.

Figura Nº 3. 20: Configuración de Red

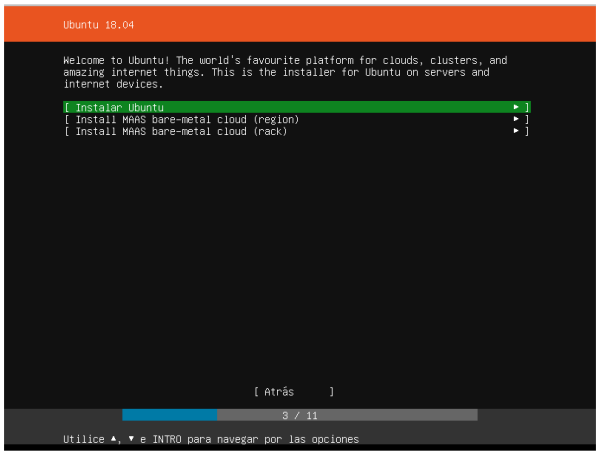


Elaboración Propia

3.5.7. Arranque de UBUNTU 19.04

Ubuntu es un sistema operativo basado en Linux, son de código abierto, lo que significa que cualquiera puede hacer lo que quieren con ellos, gratis. Es un concepto de compartir que es bastante raro en el mundo cerrado de distribución de software.

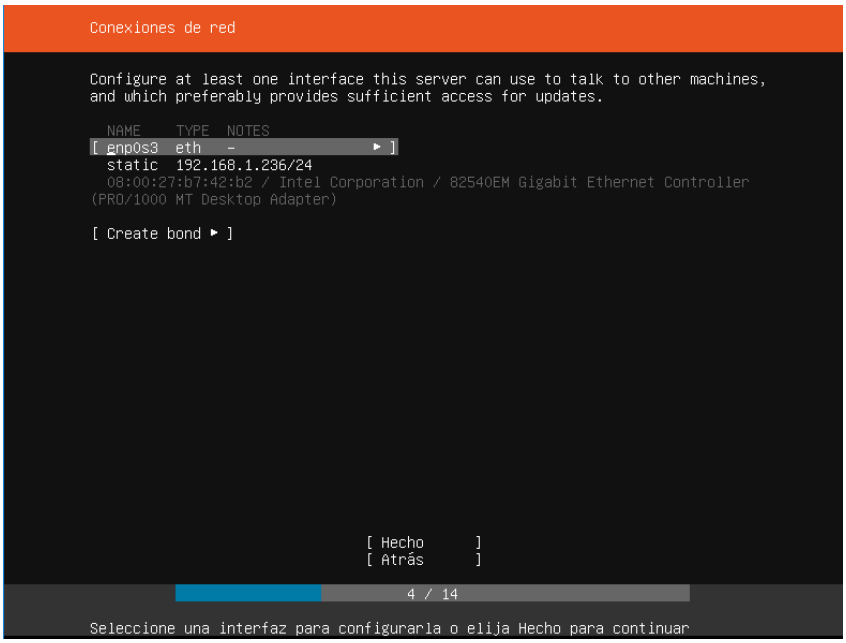
Figura Nº 3. 21: Proceso de Instalación de Ubuntu 19.04



Elaboración Propia

Se agrega direcciones IP y mascara de sub red respectivas Se requiere al menos 10 gb de espacio libre en su disco duro para instalarlo. Esto asegurará que tener mucho espacio para instalar aplicaciones adicionales más adelante, así como almacenar tus propios documentos, música y fotos.

Figura Nº 3. 22: Asignación de Direcciones IP

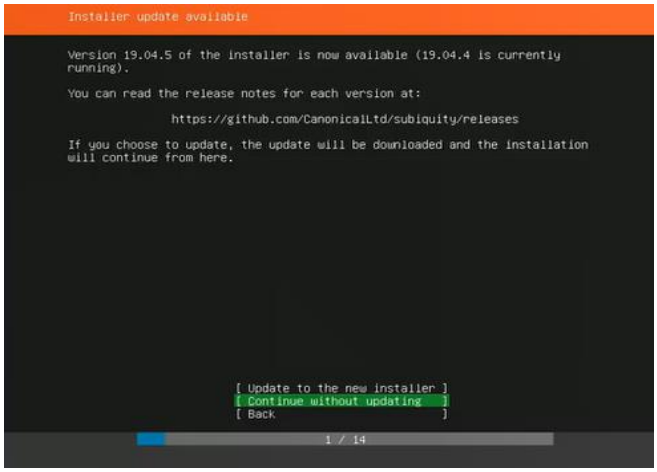


Elaboración Propia

Selección de la opción de actualizar e instalar

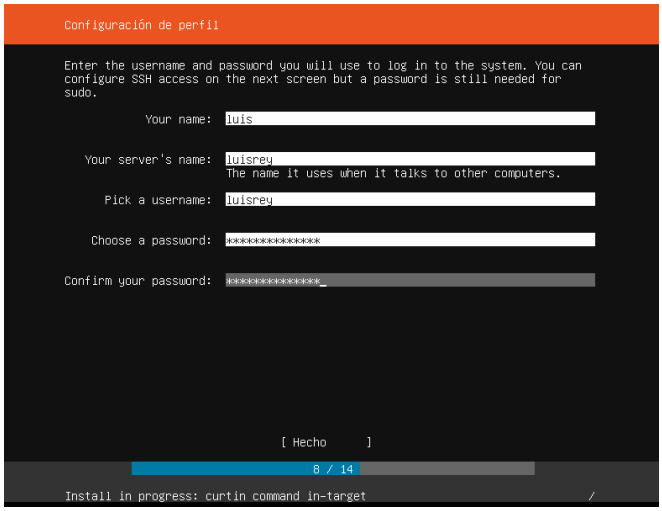
Si desea buscar actualizaciones manualmente, puede hacerlo haciendo clic en el submenú Administración del menú Sistema y luego seleccionando la entrada Administrador de actualizaciones. Cuando se abre el Administrador de actualizaciones, haga clic en el botón Comprobar para ver si hay actualizaciones disponibles.

Figura Nº 3. 23: Actualización e Instalación de UBUNTU 19.04



Elaboración Propia

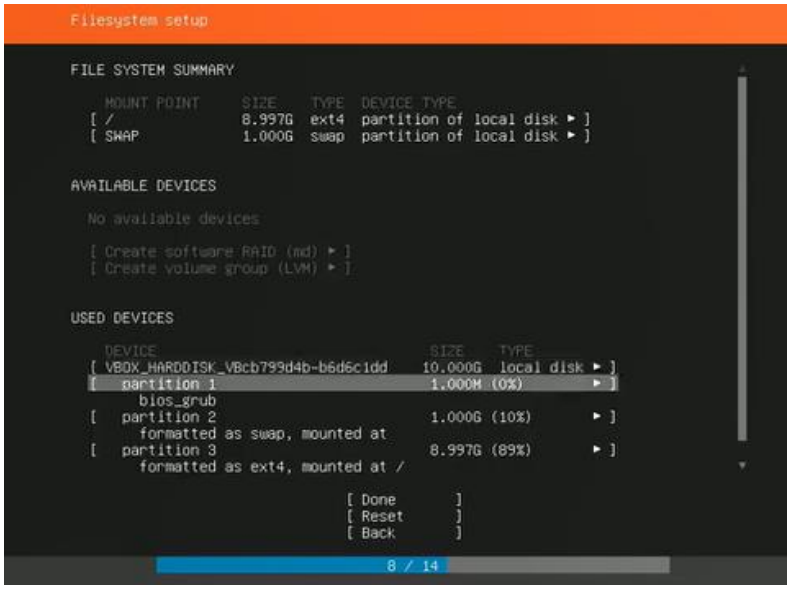
Figura Nº 3. 24: Asignación de Nombre al Servidor RADIUS



Elaboración Propia

Cuando hablamos de "unidades" etiquetadas C :, D :, y así sucesivamente, en realidad estamos hablando de particiones, secciones de la unidad física. Cada disco duro en uso tiene al menos una partición. Puede reducir esa partición y crear otras nuevas a partir del espacio extra. Esto le resultará útil si desea instalar más de un sistema operativo, o si realmente desea separar los programas y los datos. Se crea particiones tal como se ve en la imagen

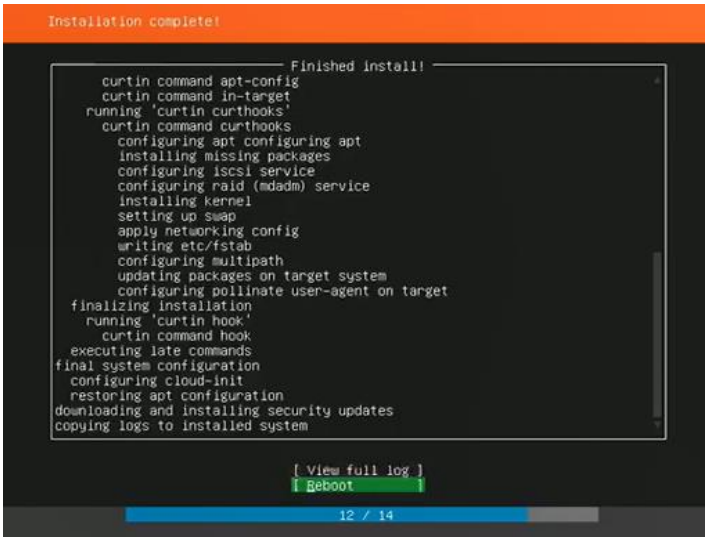
Figura Nº 3. 25: Creación de Particiones



Elaboración Propia

Reinicio del sistema después de instalar el servidor UBUNTU 19.04

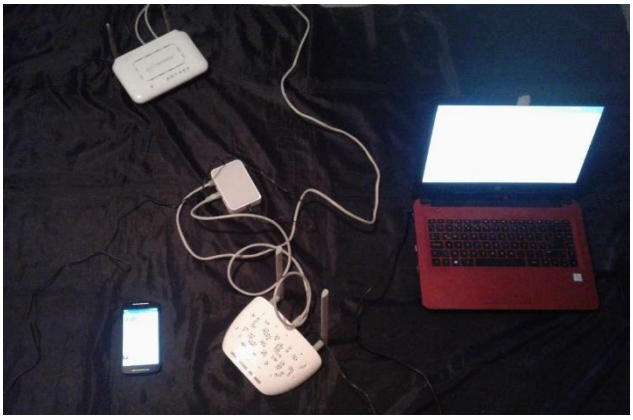
Figura Nº 3. 26: Finalización de la instalación de UBUNTU SERVER 19.04



Elaboración Propia

3.5.8. Implementación de Equipos para Instalar RADIUS

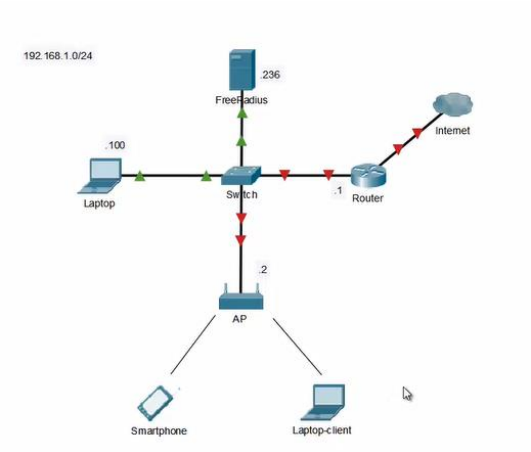
Figura Nº 3. 27: Equipos Usados Para Instalación del Servidor RADIUS



Elaboración Propia

3.5.9. Arquitectura de Red

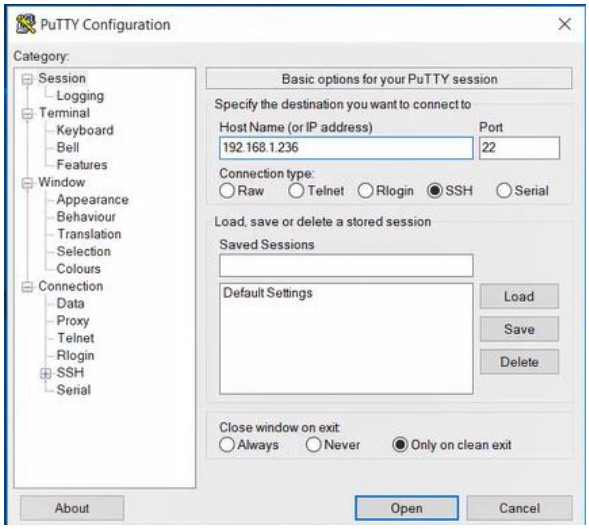
Figura Nº 3. 28: Arquitectura de Red Para la Implementación del servidor RADIUS



Elaboración Propia

3.5.10. Configuración de SSH Mediante PUTTY

Figura Nº 3. 29: Programa PUTTY, Agregando la IP del Servidor

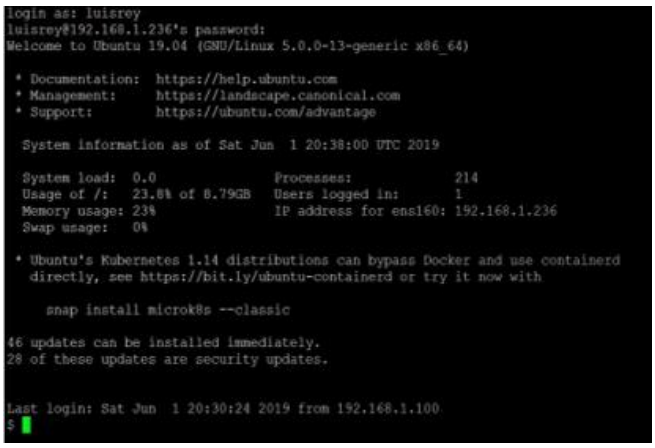


Elaboración Propia

3.5.11. Acceso al Servidor

En este caso se accede con el nombre de usuario “luisrey”

Figura Nº 3. 30: Acceso al Servidor

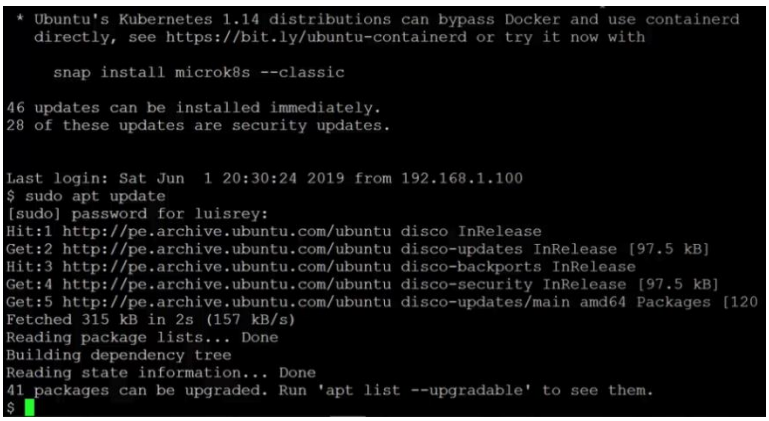


Elaboración Propia

3.5.12. Actualización de Repositorios

Es la actualización del software disponible en los repositorios de internet, se usa el comando: “sudo apt update”

Figura Nº 3. 31: Actualización de los Repositorios

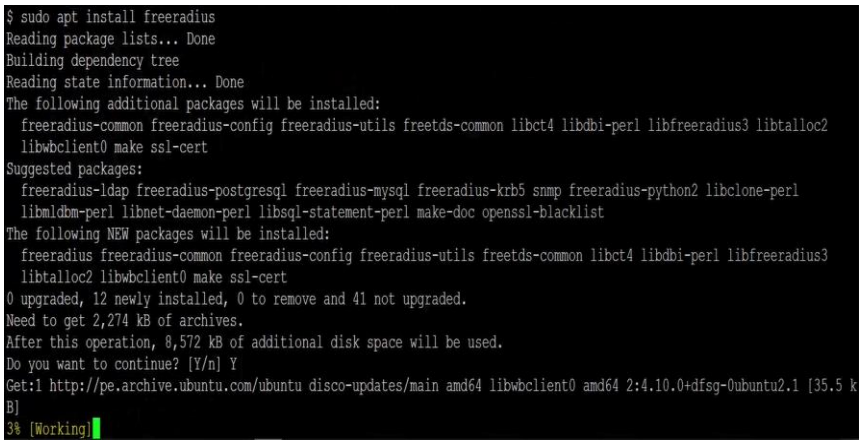


Elaboración Propia

3.5.13. Instalación de FREE RADIUS

Se usa el comando “sudo apt install freeradius”

Figura Nº 3. 32: Instalación de FREERADIUS



Elaboración Propia

3.5.14. Comando para Registro de Usuarios

Se usa el comando “sudo vim/etc/freeradius/3.0/users”

sudo es para privilegios de root

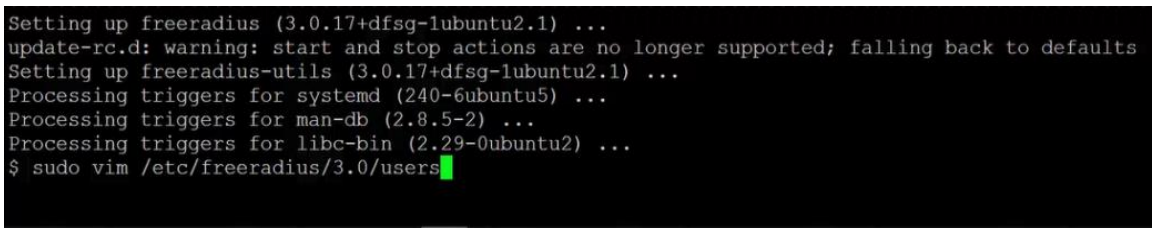
vim es un editor de línea de comandos

etc es el directorio

freeradius en su versión 3.0 es el directorio del software

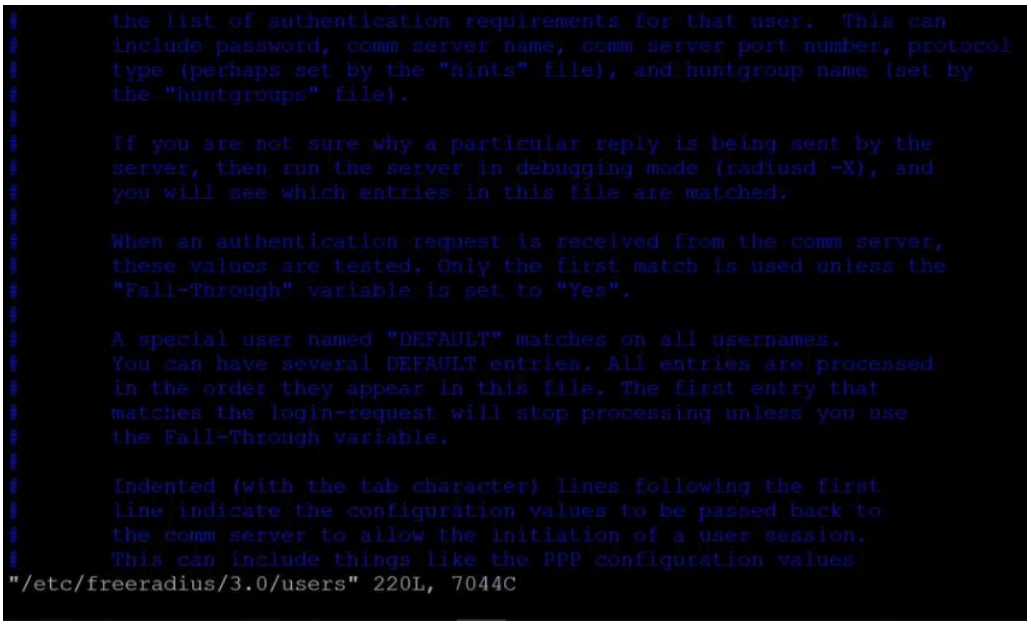
user es el archivo

Figura Nº 3. 33: Comando para Incorporación de Nuevos Usuarios



Elaboración Propia

Figura Nº 3. 34: Desarrollo del Comando “sudo vim/etc/freeradius/3.0/users”



Elaboración Propia

REGISTRO DE USUARIOS

Se agrega dos usuarios: “luisrey” y “adminunap”, con sus respectivas contraseñas

Figura Nº 3. 35: Inserción de Nuevos Usuarios al Servidor RADIUS

Elaboración Propia

El comando “: wq” se usa para guardar y salir

3.5.15. Comando para Registro de Cliente

Es muy diferente usuarios y cliente, en este caso agregaremos un equipo cliente que será un Access Point, que conectará a los usuarios, como laptops o celulares.

Con el comando "sudo vim /etc/freeradius/3.0/cliente.conf", podremos agregar usuarios a la red inalámbrica.

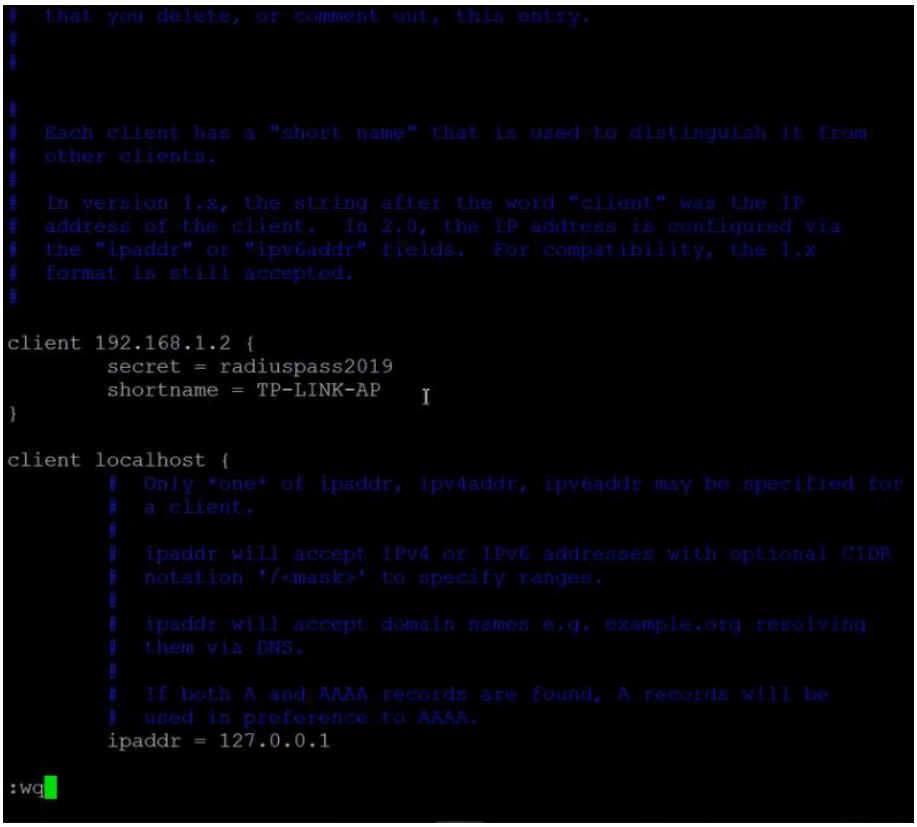
Figura Nº 3. 36: Comando para Agregar a Cliente

Elaboración Propia

3.5.16. Registro de Cliente

Se agrega al AP con la dirección 192.168.1.2 con una contraseña: radiuspass2019 y una pequeña descripción, shortname: TP-LINK-AP

Figura Nº 3. 37: Anexo de Access Point como Cliente

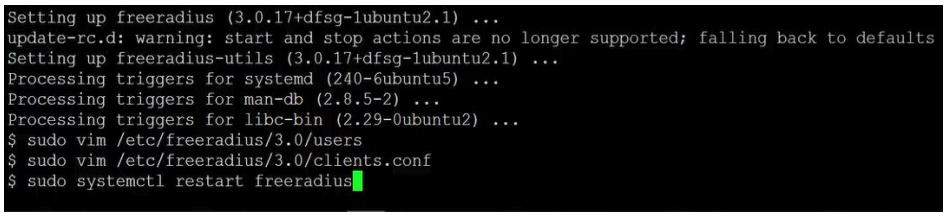


Elaboración Propia

3.5.17. Reinicio de Servidor RADIUS

Es indispensable reiniciar el servidor RADIUS para aplicar los cambios. Se usará el comando “sudo systemctl restart freeradius”

Figura Nº 3. 38: Comando para Reiniciar en Servidor RADIUS

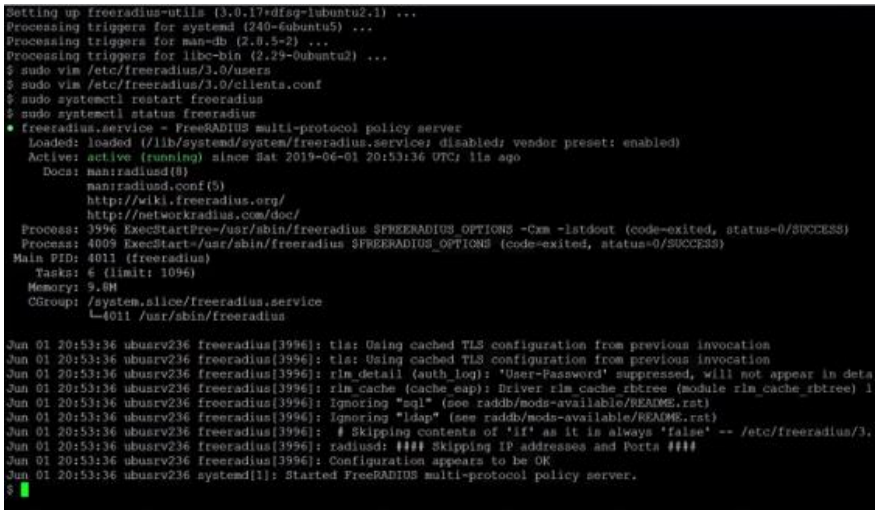


Elaboración Propia

3.5.18. Verificación del Estado de FREE RADIUS

Se observa que el estado de FREERADIUS está activo, observando la parte seleccionada en verde.

Figura Nº 3. 39: Estado del Servidor FREE RADIUS

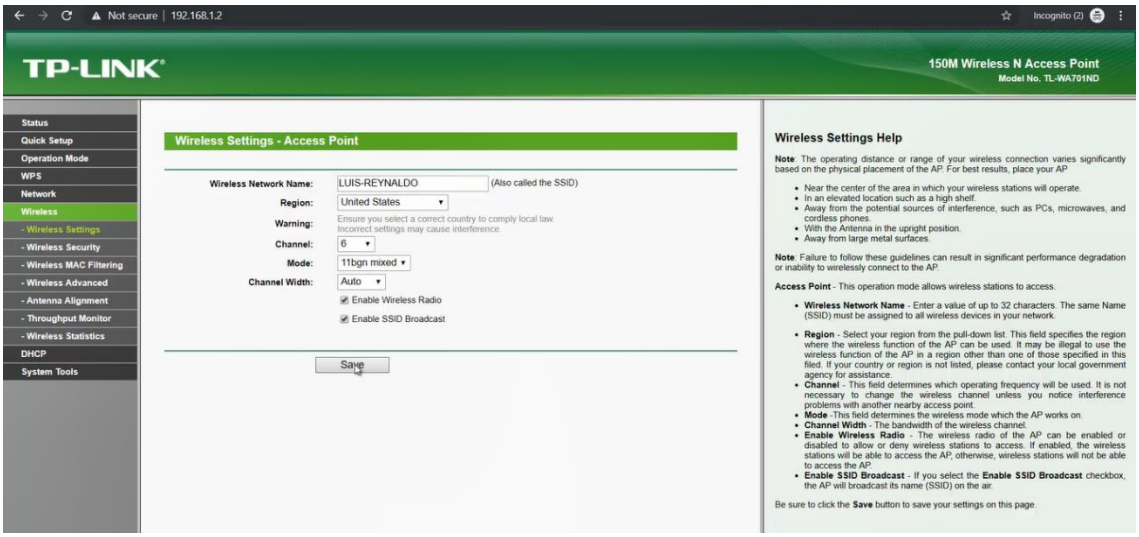


Elaboración Propia

3.5.19. Acceso al Access Point para su Configuración

Acceso al AP mediante su IP: 192.168.1.2 y se configurara según lo predispuesto. En este caso se usa como nombre de la red WI-FI "luis-reynaldo"

Figura Nº 3. 40: Configuración de Access Point

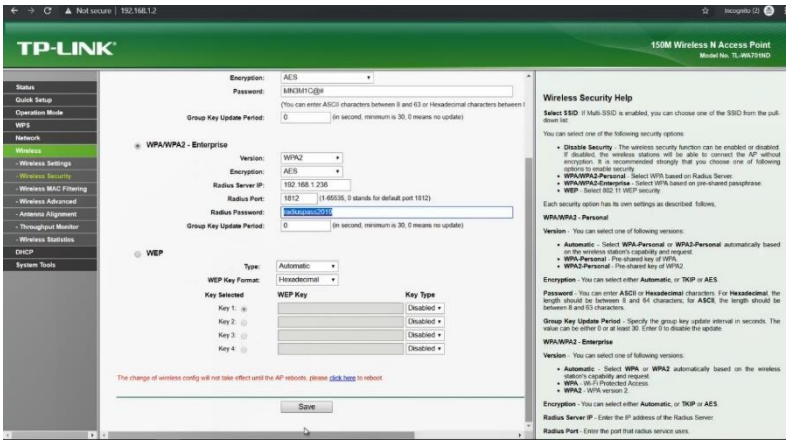


Elaboración Propia

Se usa la seguridad WPA2-Eterpise, ya que es propia para RADIUS, con una encriptación AES, colocaremos también la clave IP del servidor RADIUS la cual es: 192.168.1.236 con el puerto 1812 y se pondrá la clave que se ha puesto anteriormente en el servidor RADIUS, la cual fue: radiuspass2019.

Luego se procede a reiniciar el equipo guardando todas las configuraciones establecidas.

Figura Nº 3. 41: Configuración de la Seguridad de Red en el Access Point

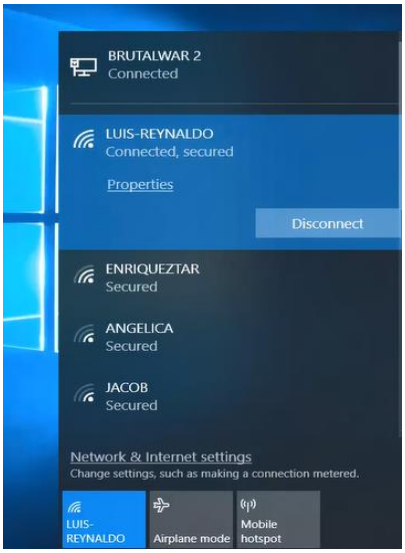


Elaboración Propia

3.5.20. Conexión de Usuarios al Access Point

Se procede a conectar una laptop al servidor RADIUS usando el Access Point.

Figura Nº 3. 42. Conexión de una Laptop al Servidor RADIUS por AP

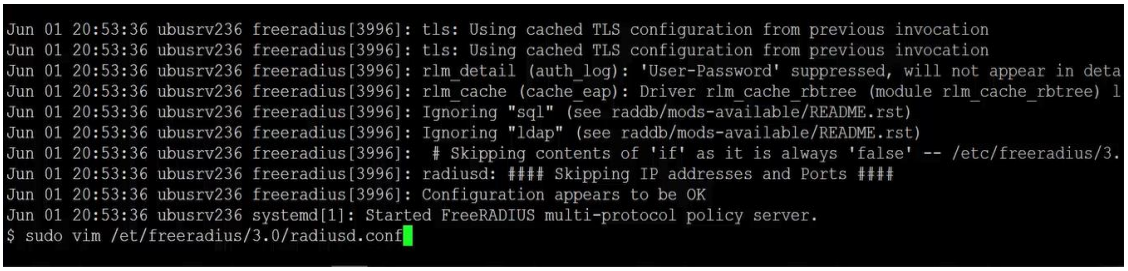


Elaboración Propia

3.5.21. Verificación de Registro de Usuarios

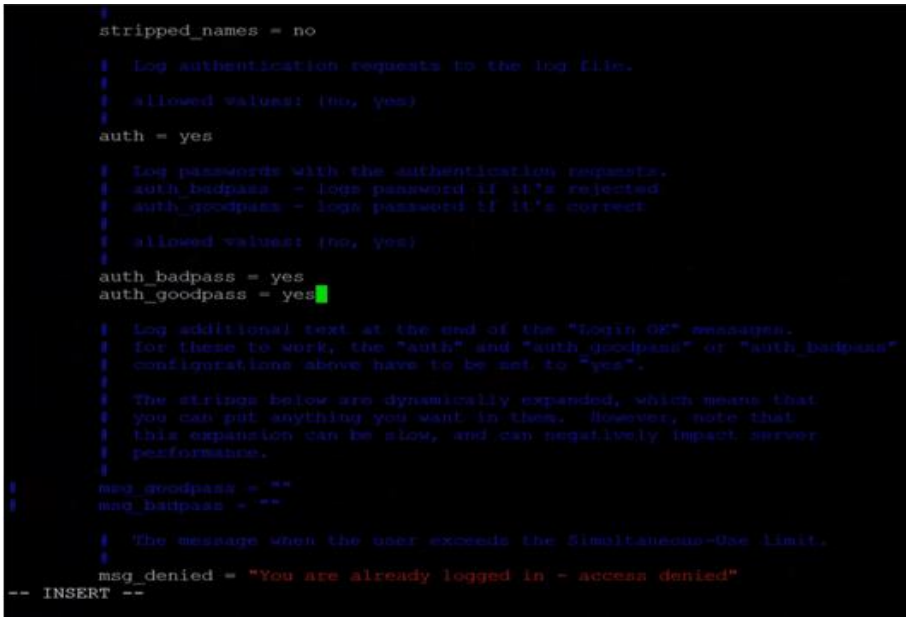
En este paso se usa el comando en el archivo radiusd.conf "sudo vim /et/freeradius/3.0/radiusd.conf"

Figura Nº 3. 43: Comando para Registro de Usuarios



Elaboración Propia

Figura Nº 3. 44: Palabra "YES" Permite la Interacción de RADIUS con el Usuario



Elaboración Propia

3.5.22. Verificación de Actividades de FREE RADIUS

En este momento se verifica el archivo radius.log que está dentro del directorio de var/log/freeradius, el comando es: “sudo tal -f /var/log/freeradius/radius.log”

Sudo es para acceder a privilegios de administrador

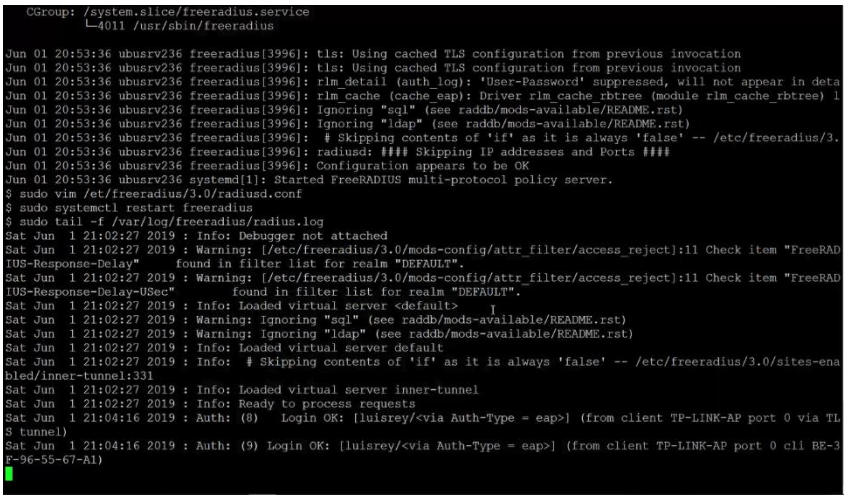
Tail es para ver las últimas líneas del archivo radius.log

-f es para verlo en tiempo real

Figura Nº 3. 45: Observación de Actividades en FREERADIUS

Elaboración Propia

Figura Nº 3. 46: Registro de Actividades FREERADIUS



Elaboración Propia

En la imagen anterior podemos ver algunos detalles:

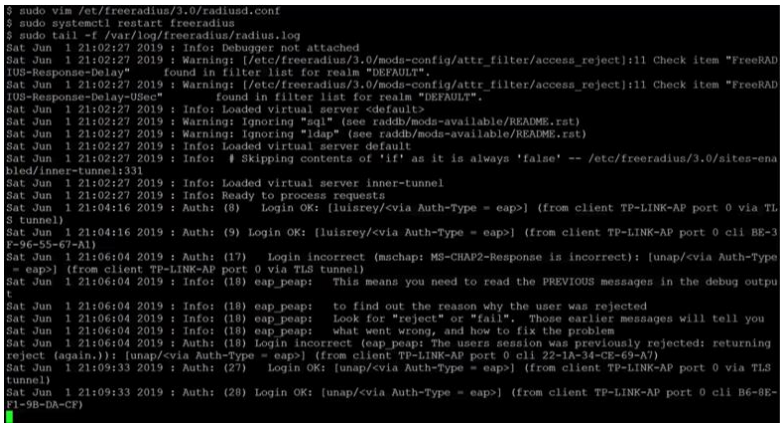
Login ok: luisrey está accediendo vía EAP (protocolo de comunicación extensible) usando un túnel TLS (TransportLayer Security) y con la MAC: F:96:55:67:A1

3.5.23. Autenticación con otro Usuario

Figura Nº 3. 47: Acceso con el Usuario "unap" a RADIUS Mediante el AP

Elaboración Propia

Figura Nº 3. 48: Autenticación con el Usuario “unap”

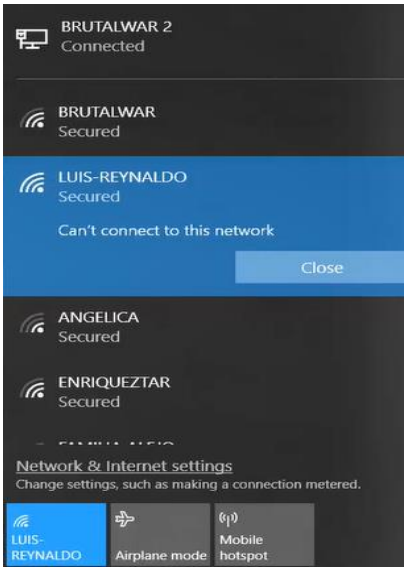


Elaboración Propia

3.5.24. Acceso de un Falso Usuario

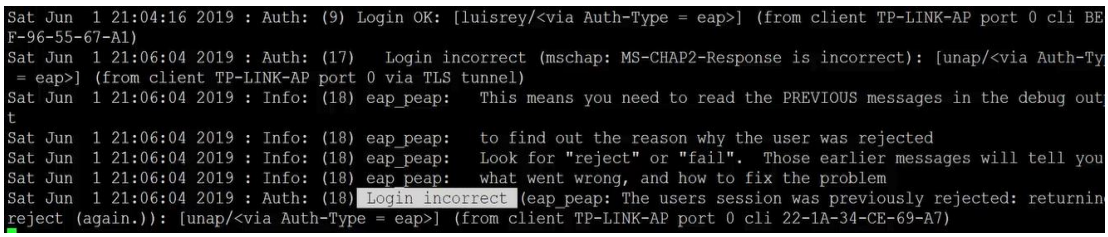
Se accede al servidor RADIUS con una contraseña falsa, el servidor no lo reconocerá y denegará el servicio, observando así su comportamiento.

Figura Nº 3. 49: Denegación de Falso Usuario



Elaboración Propia

Figura Nº 3. 50: Comportamiento del Servidor RADIUS a falso Usuario



Elaboración Propia

3.6. Variables

3.6.1. Variable Independiente

- Implementación de un servidor de seguridad y control de acceso con RADIUS

3.6.2. Variable Dependiente

- Nivel de autenticación, autorización del control en el entorno WI – FI

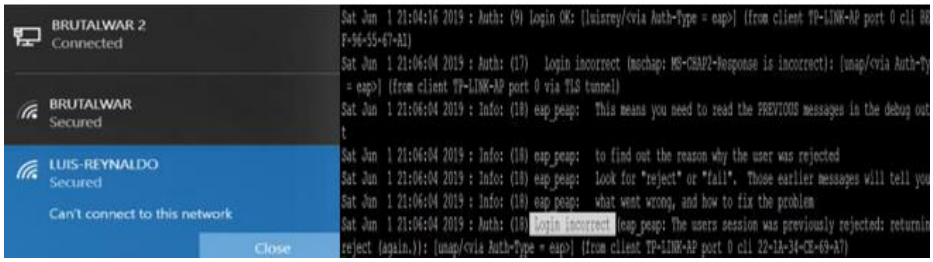
CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. Resultados

- La implementación del sistema RADIUS logró un resultado óptimo, ya que permitió al 100% el acceso los usuarios que estaban registrados a la red y denegar a quienes no lo estaban.

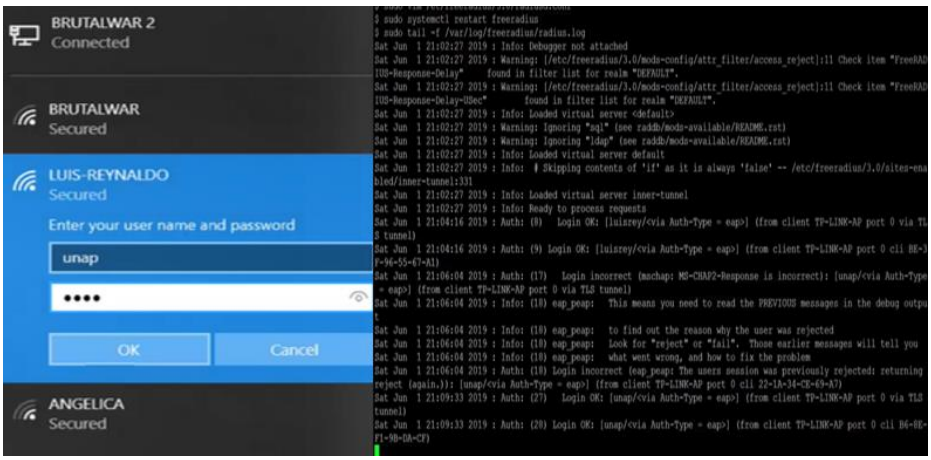
Figura Nº 3. 51: Resultado de la Denegación a un Falso Usuario



Elaboración Propia

- Se logró autenticar a los usuarios con sus respectivas contraseñas y de esta manera verificar su autenticidad en la red.

Figura Nº 3. 52: Resultado de Autenticación de Usuario



Elaboración Propia

- Lista de usuarios con acceso a la red

Tabla Nº 4. 1: Lista de usuarios con acceso a la red

Nombres	DNI	CONTRASEÑA ENCRIPTADA
Sucasaca Sucasaca, Vanessa Erika	71215341	●●●●●●●●●●●
Calsin Churata, Igner Bruno	43869673	●●●●●●●●●●●
Macedo Mamani, Wiliam Max	46982673	●●●●●●●●●●●
Zeballos Machaca, Karla Michelle	70002817	●●●●●●●●●●●
Quispe Calsin, Flor Angela	71040183	●●●●●●●●●●●
Colque Chayña, Sindy Pilar	72919388	●●●●●●●●●●●
Quispe Javier, Hubert Cristian	47263239	●●●●●●●●●●●
Sucto Cucho, Nayer Richart	48117685	●●●●●●●●●●●
Ruelas Sullo, Teofilo	73222468	●●●●●●●●●●●
Atencio Alanoca, Aderlyn	45525784	●●●●●●●●●●●
Quispe Gordillo, Richard	44234707	●●●●●●●●●●●
Ponce De Leon Quispe, Hochimin	42554031	●●●●●●●●●●●
Condori Sevillanos, Karen	48345608	●●●●●●●●●●●
Mamani Aguilar, Ruben	70761577	●●●●●●●●●●●
Puma Quinallata, Ruth Veronica	44552637	●●●●●●●●●●●
Humpire Carita, Aydee	46893006	●●●●●●●●●●●
Apaza Quispe, Jakeline Ivonne	70142897	●●●●●●●●●●●
Huanca Poma, Vanesa	47232983	●●●●●●●●●●●
Cordova Canaza, Flaniver Roscio	72047779	●●●●●●●●●●●
Calcina Paredes, Mijael Santiago	47992940	●●●●●●●●●●●
Maquera Apaza, Arnaldo Elvis	71804075	●●●●●●●●●●●
Coila Coaquira, Sol De María	71736721	●●●●●●●●●●●
Rivas Barra, Grecia Adeline	76089128	●●●●●●●●●●●
Zuniga Apaza, Dania Flor	47844649	●●●●●●●●●●●
Ccuno Aruquipa, Tatiana	70317525	●●●●●●●●●●●
Hancco Herrera, Roxana	71582269	●●●●●●●●●●●
Arpasi Quispe, Lisbeth	73371497	●●●●●●●●●●●
Rivera Valeriano, Edgar	73762436	●●●●●●●●●●●
Caceres Chura, Rayin Dbeto	70162513	●●●●●●●●●●●
Yucra Saraya, Isidro	40208614	●●●●●●●●●●●
Ramos Ramos, Luis Antonio	74067181	●●●●●●●●●●●
Ccamapaza Coapaza, Martin	44796361	●●●●●●●●●●●
Macedo Chislla, Carlos Erickson	47596581	●●●●●●●●●●●
Flores Quispe, Jorge Luis	44851346	●●●●●●●●●●●
Gamarra Calle Sergio Aurelio	74158957	●●●●●●●●●●●

Continua		
Quiñones Pilco Adrian Rodrigo	70136544	●●●●●●●●●●●
Ramos Rosel Walker Alexis	72681813	●●●●●●●●●●●
Hanco Montesinos Luis Anthony	71059943	●●●●●●●●●●●
Ortega Gonzales Karen Haydee	45736581	●●●●●●●●●●●
Saavedra Colquehuanca Yuly Marilyn	77289750	●●●●●●●●●●●
Quispe Caceres Reynaldo	70610147	●●●●●●●●●●●
Yanapa Ramos Monica Yurley	77692209	●●●●●●●●●●●
Villarreal Chambi Jean Paul	72690485	●●●●●●●●●●●
Cruz Andrade Yesenia	76947822	●●●●●●●●●●●
Cano Payva Carlos	75364535	●●●●●●●●●●●
Ponce Romero Laura Diana	76931837	●●●●●●●●●●●
Calcina Charca Edwin	70292521	●●●●●●●●●●●
Vilca Chagua Jhon Fidel	74841066	●●●●●●●●●●●
Condori Zapana Yimy Cristian	70076484	●●●●●●●●●●●
Mamani Mollocondo Laura Cecilia	70865872	●●●●●●●●●●●
Mamani Oscalla Liz Mashiel	71347612	●●●●●●●●●●●
Yapuchura Apaza Renan	72910890	●●●●●●●●●●●
Alca Apaza Ronald	74450790	●●●●●●●●●●●
Frias Quilca Esmeralda	70942253	●●●●●●●●●●●
Jilapa Chura Luis Fernando	70405179	●●●●●●●●●●●
Luque Justo Anyely Teresa	73022548	●●●●●●●●●●●
Montiel Canaza Deysy Patricia	75322830	●●●●●●●●●●●
Nina Alarcon Jimena Rubi	70941498	●●●●●●●●●●●
Istaña Contreras Dennys	70280099	●●●●●●●●●●●
Velarde Yana Wendy Melissa	72656922	●●●●●●●●●●●
Zaraza Fernandez Kevin Jampier	72305134	●●●●●●●●●●●
Colque Espinoza Lesly Evelyn	71791832	●●●●●●●●●●●
Amanqui Lipe Gilder Yulem	73694243	●●●●●●●●●●●
Valeriano Huaman Michelle Nadia	73477347	●●●●●●●●●●●
Apaza Quispe Alex	71011902	●●●●●●●●●●●
Toro Ruelas Andre de Jesus	70398283	●●●●●●●●●●●
Jaliri Mamani Magy Rosario	70155914	●●●●●●●●●●●
Zuñiga Apaza, Marilyn	74174280	●●●●●●●●●●●
Aruhuanca Nina, Olinda	47334127	●●●●●●●●●●●
Vilca Valero, Vladimir Santos	70208459	●●●●●●●●●●●

Elaboración Propia

- Lista de usuarios sin acceso a la red

Tabla Nº 4. 2: Lista de usuarios sin acceso a la red

Nombres	DNI	CONTRASEÑA ENCRIPTADA
Arohuanca Galindo, Haldhana Katherine	70311783	●●●●●●●●●●●●
Villar Morales, Victor Ivan	70445817	●●●●●●●●●●●●
Tite Ambrosio, Abed De La Cruz	70076862	●●●●●●●●●●●●
Pancca Turpo, Nely Antonieta	76274629	●●●●●●●●●●●●
Villanueva Condori, Yeny Danitsa	70846863	●●●●●●●●●●●●
Pancca Turpo, Nely Antonieta	76274629	●●●●●●●●●●●●
Ticona Villalta, Jhon Erick	47689183	●●●●●●●●●●●●
Gamarra Condori, Jorge Alberto	73199039	●●●●●●●●●●●●
Mamani Canaza, Felix	47657106	●●●●●●●●●●●●
Humpiri Vargas, Esthefany	70002046	●●●●●●●●●●●●
Quispe Mamani, Ruben	46381089	●●●●●●●●●●●●
Ticona Huahuasoncco, Sayda Yovana	70172728	●●●●●●●●●●●●
Quispe Mamani, Ruben	46381089	●●●●●●●●●●●●
Hanco Pinto, Ana Lucero	70169577	●●●●●●●●●●●●
Galindo Condori, Redy	76821175	●●●●●●●●●●●●
Colque Limachi, Edwin	70414056	●●●●●●●●●●●●
Nina Segovia, Yenifer Kely	70317534	●●●●●●●●●●●●
Curtihuanca Lima, Aurelia Viviana	47810225	●●●●●●●●●●●●
Mamani Mamani, Jesus Ivan	75998992	●●●●●●●●●●●●
Suarez Vela, Kristel Margot	72476908	●●●●●●●●●●●●
Mamani Apaza, Yenni Edelmira	71847925	●●●●●●●●●●●●
Mamani Ramos, Yoely Lisbeth	72837316	●●●●●●●●●●●●
Calcina Calcina, Ivan Percy	70331181	●●●●●●●●●●●●
Quenta Belisario, Milagros Marleny	76055624	●●●●●●●●●●●●
Castillo Cuchuyrumi, Gloria	70495096	●●●●●●●●●●●●
Tacuri Valdez, Carmen Rosa	72011770	●●●●●●●●●●●●
Montesinos Llano, Indira Milena	76947794	●●●●●●●●●●●●
Puerta Olivera, Antonella Briyanet	72631445	●●●●●●●●●●●●
Ramos Turpo, Kely Jhanira	46826057	●●●●●●●●●●●●
Valeriano Turpo, Edgar	71044885	●●●●●●●●●●●●

Elaboración Propia

- **Proceso de intentos de usuarios que intentan conectarse a la red wi-fi**

Tabla Nº 4. 3: Resumen de los casos de usuarios

	Numero de Intentos					
	Resultados Positivos		Resultados Negativos		Total	
Sistema de Autenticacion y nivel de acceso controlado	Usuarios	Porcentaje	Usiarios	Porcentaje	Usuarios	Porcentaje
El control en seguridad relacionado a servicios de internet, y teneiedo en cuenta las numerosas conexiones que se hace a la red inalambrica, nos damos cuenta que el rendimiento de internet disminuye considerablemente, debido a que, los usuarios ajenos al CECUNA se conectaban a la red innecesariamente, saturando la red, despues de la instalacion del servidor RADIUS, mejoro el rendimiento, debido a la distribución del ancho de banda para todos los usuarios.	70	70%	30	30%	100	100%

Elaboración Propia

4.2. Discusión

RADIUS permiten la autenticación desde el inicio, y es redirigido a un portal cautivo en donde tendrá que introducir datos de identificación, teniendo en cuenta, las ventajas que tiene sobre algunos protocolos como LDAP, que funcionan únicamente como directorio o base de dato, RADIUS es un servidor de autenticación, ya que corrobora los datos del usuario.

Haciendo mención a la tesis de PAREDES VASQUEZ, EDWIN ESTUARDO, "MEJORAMIENTO DE LA SEGURIDAD DE LA INFORMACION EN LA RED DE MICREDITO SAC", que define el uso de un servidor, ACTIVER DIRECTOR, usando protocolos como LDAP O DHCP, funcionando como directorio o base de datos.

Se afirma que el servidor RADIUS tiene más garantía al momento de brindar seguridad, ya que, proporciona, administración, autenticación y contabilidad de los usuarios.

Haciendo mención a la tesis de Gladis Sofía Asadovay Lema y Liliana Mercedes Caiza Ortiz, Titulado "Análisis Comparativo de Servidores de Autentificación Radius y Ldap con el Uso de Certificados Digitales para Mejorar la Seguridad en el Control de Acceso a Redes Wifi" que define un servidor LDAP, LDAP es un directorio, LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas. Habitualmente, almacena la información de login o acceso a un sistema (usuario y contraseña) y es utilizado para autentificarse, aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.). y RADIUS un servidor de autenticación y autorización con soporte para diversos mecanismos de autenticación: contraseña, certificado, biometría.

Teniendo en cuenta a TACACS (Terminal Access Controller Access control system) que es un protocolo de autenticación remota que permite a un servidor de acceso remoto comunicarse con un servidor de autentificación pata determinar si un usuario tiene acceso a la red. Se opto en usar servidor RADIUS pr que es de libre acceso y compatible con diferentes sistemas y TACACS se usa exclusivamente en equipos CISCO.

Tabla Nº 4.4: Diferencias entre TACACS Y RADIUS

TACACS	RADIUS
- TACACS utiliza el puerto 49 del Protocolo de control de transmisión (TCP) para comunicarse entre el cliente y el servidor. - Tiene la capacidad de separar la autenticación, la autorización y la contabilidad como funciones separadas e independientes. Esta es la razón por la cual se usa con tanta frecuencia para la administración de dispositivos. - La comunicación TACACS + entre el cliente y el servidor utiliza diferentes tipos de mensajes según la función. En otras palabras, se pueden usar diferentes mensajes para la autenticación que los que se usan para la autorización y la contabilidad. Otro punto muy interesante para saber es que la comunicación TACACS cifrará todo el paquete. - TACACS cifra toda la comunicación - TACACS es un protocolo pesado que consume más recursos - TACACS admite 15 niveles de privilegio - Utilizado principalmente para la administración de dispositivos	- RADIUS se use entre el dispositivo inalámbrico y el servidor AAA, este es el caso porque RADIUS es el protocolo de transporte para el Protocolo de autenticación extensible (EAP), junto con muchos otros protocolos de autenticación. - RADIUS todavía es capaz de proporcionar la administración de dispositivos AAA. - Con IEEE 802.1X, RADIUS se usa para extender el Protocolo de autenticación extensible de capa 2 (EAP) del usuario final al servidor de autenticación. - Es un protocolo AAA compatible con todos los proveedores. - RADIUS usa el puerto UDP 1812 para la autenticación RADIUS y el puerto UDP 1813 para la contabilidad RADIUS. Algunas otras implementaciones usan el puerto UDP 1645 para mensajes de autenticación RADIUS y el puerto UDP 1646 para contabilidad RADIUS - RADIUS cifra solo las contraseñas

Elaboración Propia

4.3. Tipo de Investigación

Es tecnológica, ya que su finalidad es desarrollar los efectos que produce un sistema con protocolos AAA de seguridad de autenticación con RADIUS.

Es una correlacional porque analiza el nivel de relación entre las variables de estudio de control de acceso con el servidor RADIUS y el nivel de autenticación y autorización, en un entorno wi-fi.

CONCLUSIONES

- Se informó a todos los usuarios del Centro de Comunicaciones de la Universidad Nacional del Altiplano sobre la importancia de la seguridad que existe en una red inalámbrica, y su apropiado uso.
- Se implementó el sistema RADIUS, con 70 usuarios registrados como trabajadores del Centro de Comunicaciones de la Universidad Nacional del Altiplano.
- Se autenticó a los usuarios con una efectividad del 100%, teniendo en cuenta que, se logró la denegación de acceso al servicio a 30 usuarios quien no estaba registrado en el servidor.
- Se verificó que cada usuario use contraseñas seguras, mayor a 12 caracteres; las contraseñas usadas fueron alfanuméricas, con caracteres especiales, usando mayúsculas y minúsculas, y usando la barra espaciadora, para más confiabilidad.

RECOMENDACIONES

- Tener en cuenta políticas de seguridad, fomentar amplia difusión abarcando temas de Seguridad de la Información con el propósito de general confianza al personal del CECUNA.
- En base al diseño de RADIUS es necesario se recomienda formular un plan de trabajo, verificando los recursos tecnológicos, que soporten tecnologías actualizadas y teniendo en cuenta las nuevas tecnologías de la información.
- Se recomienda a todos los usuarios usar contraseñas alfanuméricas con uso de mayúsculas y minúsculas, mayor a ocho caracteres, para garantizar seguridad al momento de navegar por la red.
- Teniendo en cuenta la cantidad de personas que quieran tener acceso a la red WI-FI de la Universidad Nacional del Altiplano, se recomienda clasificar a los usuarios que tengan relación con la universidad mencionada, ya sean estudiantes docentes o administrativos.
- Realizar copias de seguridad en los servidores y equipos intermediarios
- Monitorear continuamente la auditoría de red para obtener previo conocimiento de la situación.
- El personal debe estar capacitado en el área de TI para el correcto uso de los equipos de red.

REFERENCIAS

- Alonso, C. (2006). Proteger una red Wireless, PC World Profesional, IDG. España.

- Baghaei, N. (2003). IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients. 2003.

- Ceja, E. (2012). Implementación de un Servidor RADIUS . Mexico.

- Gast, M. (2005). 802.11 Wireless Networks: The Definitive Guide, O'Reilly . Estados Unidos.

- Jhony, B. (2017). Seguridad y Control del Acceso a las Redes Inalámbricas en la UNSM. Mediante Servidores de Autentificación Radius con el Uso de Certificados Digitales. Universidad Nacional de San Martin, Tarapoto, Perú. . Peru.

- Lopez, J. (2008). Sistema e Implementación de un Sistema de Gestión de Accesos a una Red Wi–Fi Utilizando Software Libre. Peru.

- Miranda, C. (s.f.). Implementación de un Prototipo de Red Inalámbrica que Permita elevar los niveles de seguridad a través de la Autenticación de un Servidor RADIUS para los Usuarios que Accedan Internet en el Edificio Francisco Morazán de la UTEC.

- Morand, L. (2014). Adding bandwidth specification to a AAA Sever. England.

- Osmar, A. (2016). Diseño de un Sistema de Seguridad de Red Basado en la Integración de los Servidores RADIUS - LDAP en Linux para Fortalecer el Acceso de la Red de la Clínica MILLENIUM. Peru.

- Paredes, E. (2016). Mejoramiento de la Seguridad de la Informacion en la Red de Mi Credito S.A.C. Peru.

- Pedro, G. (2017). Diseño de un Modelo de Autenticación RADIUS para Reforzar los Niveles de Seguridad en el Diseño de Redes Inalámbricas IEEE 802.11x para la Cooperativa de Ahorro y Crédito Tumán. Peru.

- Said, S. (2010). Design and Performance Optimization of Authentication, Authorization, and Accounting (AAA) Systems in Mobile Telecommunications Networks. Germany.

- Singh, A. (2017). An Analytical and Experimental Study of AAA Model with Special Reference to RADIUS and TACACS+. India.

- Vesa, I. (2002). Secure Network Access with IPSec Tunnels. Findland.

ANEXOS

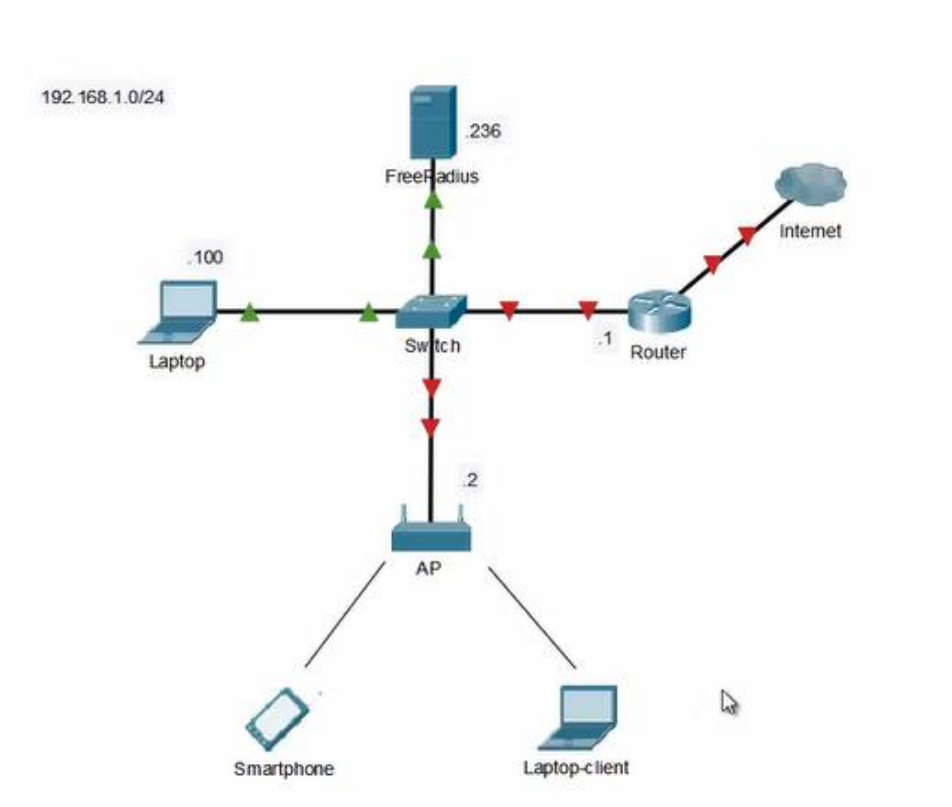
ANEXO A.

FIg. 1: Equipos Usados

Elaboración Propia

ANEXO B.

FIg. 1: Topología de Red



Elaboración Propia