UNIVERSIDAD NACIONAL DE HUANCAVELICA

(CREADA POR LEY N°25265)

FACULTAD DE INGENIERÍA ELECTRÓNICA – SISTEMAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

TESIS

“SERVIDOR RADIUS EN EL CONTROL DE ACCESO A LA RED INALÁMBRICA DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA”

LÍNEA DE INVESTIGACIÓN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PRESENTADO POR:

Bach. RAMOS AYUQUE, Luis Ángel

Bach. TORRES LANDEO, Daniel

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

HUANCAVELICA, PERÙ

2021

UNIVERSIDAD NACIONAL DE HUANCAVELICA

(Creada por Ley N ° 25265)

FACULTAD DE INGENIERÍA ELECTRÓNICA – SISTEMA

ACTA DE SUSTENTACIÓN DE TESIS

Mediante el aplicativo Google Meet con enlace: **meet.google.com/gbi-ckoz-sht; Unirse por teléfono (US) +1 507-533-5067 PIN: 322 221 255# #**, habilitado por Secretaría Docente de la Facultad de Ingeniería Electrónica – Sistemas, en mérito a la **Resolución de Consejo de Facultad Nº 247-2021-FIES-UNH** de fecha 28 de octubre de 2021, a los 17 días del mes de noviembre del año 2021, a las 16:00 horas y, ante la ausencia del Dr. Fernando Viterbo SINCHE CRISPÍN quien formaba parte del jurado titular y en mérito al "Reglamento único de Grados Y títulos de la Universidad Nacional de Huancavelica, aprobado con Resolución N° 0330-2019-CU-UNH (29/03/2019); Modificado con Resolución Nº 0552-2021-CU-UNH (14/05/2021), Art 12º De la sustentación del trabajo de investigación; 12.8. Si en la fecha, hora y lugar señalado para el acto de sustentación, faltara por razones justificadas y documentadas uno de los miembros del jurado titular, será remplazado automáticamente por el docente accesitario, quien remplazará al miembro faltante; la reestructuración de los miembros debe constar en el acta de sustentación. Si faltan dos miembros del jurado, el titular presente suspende el acto de sustentación, suscribiendo el acta correspondiente en el que se fijará la nueva fecha y hora dentro de las 24 horas, no requiere nuevo acto resolutivo, comunicando al o los interesados, al decano y a los miembros del jurado". En consecuencia, se reunieron; el Jurado Calificador, **y asumiendo** el **accesitario en calidad de secretario**, la misma que está conformado de la siguiente manera:

Presidente: Dr. John Fredy, ROJAS BUJAICO
Secretario: Dr. Rafael Wilfredo ROJAS BUJAICO
Vocal: Mg. Roly Alcides, CRISTOBAL LARA

Designados con Resolución Nº 064-2019-DFIES-UNH, de fecha 30 de diciembre de 2019 del proyecto de investigación, Titulado:

"SERVIDOR RADIUS EN EL CONTROL DE ACCESO A LA RED INALÁMBRICA DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA"

Cuyos autores son los graduados: Bachilleres:

Luis Ángel, RAMOS AYUQUE
Daniel, TORRES LANDEO

A fin de proceder con la evaluación y calificación de la sustentación del proyecto de investigación, antes citado. Se dio inicio a la sustentación del proyecto de investigación en mención, a horas 16 con 08 minutos, concluyendo a horas 17 con 20 minutos.

Finalizado la sustentación; se invitó al público presente y a los sustentantes a abandonar la sala de actos; y, luego de una amplia deliberación y calificación por parte del jurado, se llegó al siguiente resultado:

APROBADO POR: MAYORÍA

.....
Dr. John Fredy, ROJAS BUJAICO
Presidente

.....
Dr. Rafael Wilfredo, ROJAS BUJAICO
Secretario

.....
Mg. Roly Alcides, CRISTOBAL LARA
Vocal

Título:

"SERVIDOR RADIUS EN EL CONTROL DE ACCESO A LA RED INALÁMBRICA DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA"

Autores:

Bach. RAMOS AYUQUE, Luis Ángel

Bach. TORRES LANDEO, Daniel

Asesor:

Mg. ALMIDÓN ORTÍZ, Carlos Alcides

Dedicatoria

A mi persona por desarrollar este trabajo de investigación.

Agradecimiento

A Dios por habernos guiado durante toda mi vida, por ser un soporte esencial en mi vida y por brindarme fortaleza en los momentos más difíciles.

A nuestros padres por sus buenos consejos, valores que siempre nos han inculcado.

Al Mg. Carlos Alcides Almidón Ortiz por su asesoramiento.

A mis docentes en la Escuela Profesional de Ingeniería de sistemas por habernos brindado sus sabidurías.

Tabla de contenido

Tabla de contenido de Tablas

Tabla de contenido de Figuras

Resumen

La investigación “Servidor Radius en el control de acceso a la red inalámbrica de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica”, se desarrolló con la finalidad de proteger la información como activo primordial de la organización, fundamentándose en el problema de investigación sobre el control del acceso a la red inalámbrica de la Escuela, la comunidad universitaria de la Escuela Profesional de Ingeniería de Sistemas (EPIS) ingresa de forma libre a la red de datos, por lo que la información administrativa se vuelve vulnerable debido a la falta de niveles de seguridad que salvaguarden ésta, por lo que la investigación desarrollada tiene por objetivo determinar la influencia que tiene un Servidor Radius en el control del acceso a la red inalámbrica, para esto se planteó una infraestructura de red de datos en donde se implementó la seguridad inalámbrica el cual permitirá un mayor control en las actividades de los usuarios, el trabajo del Servidor Radius permitió que los usuarios puedan conectarse de manera inalámbrica de forma segura y confiable, concluyéndose que hubo mejoras tanto en los niveles WAN y WLAN.

Palabras clave: Servidor Radius, control de acceso, WLAN, WAN, disponibilidad.

Abstract

The research "Radius Server in the Access Control to the Wireless Network of the Professional School of Systems Engineering of the National University of Huancavelica", is given by the need to protect the information as a primary asset of the organization, having as a research problem: How does the Radius server influences the access control to the wireless network in the Professional School of Systems Engineering of the National University of Huancavelica, Currently, the entire university community that makes up the Professional School of Systems Engineering (EPIS), freely accesses the data network, all the information of the administrative part is exposed to vulnerability, even students access the network wirelessly because they have access points and there are no security controls to safeguard the information. The objective of the research is: To determine the influence of the Radius server in the control of access to the wireless network in the Professional School of Systems Engineering of the National University of Huancavelica. A data network infrastructure, where wireless security was implemented, this will allow greater control over the activities of all users who make use of the network in the EPIS, thus will be in safeguarding all information and resources of the EPIS, a model of network managed through a radius server is proposed, this platform allows users to connect wirelessly securely and reliably. Concluding that the radius server will improve the access control to the wireless network in the Professional School of Systems Engineering of the National University of Huancavelica.

Keywords: Radius server, access control, subnet, vlan, availability.

Introducción

Es indiscutible que estamos inmersos en un mundo dominado por las tecnologías que día a día se van desarrollando se vuelve indispensable la implementación de una infraestructura tecnológica empresarial basado en redes convencionales o inalámbricas. La mayoría de organizaciones no toman en cuenta los niveles de seguridad que estas infraestructuras tecnológicas tienen para salvaguardar la información. La tesis busca diseñar una red inalámbrica que cuente con los protocolos de comunicación para poder administrarlo a través de un servidor Raduis, el cual proporcionará la autenticación centralizada, autorización y contabilidad de usuarios registrados, esto con el propósito de implantar un sistema de control de acceso que permita proteger la información, frente a usuarios mal intencionados y convirtiéndose en una ventaja competitiva ya que suple todas la deficiencias que presenta la plataforma de red de la EPIS. La tesis comprende los siguientes capítulos: En el **capítulo I** se describe el planteamiento del problema, antecedentes, objetivos y hipótesis, el cual constituye el marco referencial para el desarrollo de la tesis, así como se identificó los problemas que involucra la falta de conocimiento acerca de la seguridad informática, enfocándonos en los objetivos tal como implementar un servidor Radius. En el **capítulo II** se presentan trabajos relacionados los cuales se toman como muestra para esta tesis y la base teórica necesaria para la misma. En el **capítulo III** abarca el marco metodológico y los lineamientos generales. En el **capítulo IV** se establece los resultados obtenidos, teniendo en cuenta las diferencias que existen en comparación a otros proyectos y la eficacia del servidor Radius frente a situaciones adversas, brindando así, diferentes recomendaciones para su uso efectivo.

Los tesistas

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del problema

En la actualidad en el mundo globalizado en que vivimos y con el desarrollo tecnológico, se presenta nuevos inconvenientes para poder resguardar uno de los elementos más importantes de la época, la información, activo necesario que tiene que ser resguardado, para que no pueda ser sustraída de la organización, por esta razón es preciso determinar cuáles son las alternativas que ofrece la seguridad de datos.

El tener acceso a una red de área local, es una forma de comunicación para facilitar los recursos al usuario de la red LAN; contar con acceso a información, es correr riego que se filtren intrusos, por este motivo la implantación de un sistema de control de acceso a la rede de datos es muy importante, de esta manera, podemos establecer diferentes estrategias para alcanzar el objetivo, que es resguardar la información, para esto se debe de contar con el uso de esquemas de seguridad que garanticen la confidencialidad de la información solicitada.

La Escuela Profesional de Ingeniería de Sistemas (EPIS) de la Universidad Nacional de Huancavelica, prepara profesionales de manera íntegra y de

calidad a través del fortalecimiento de habilidades y capacidades para dominar las tecnologías de la información y comunicación con principios éticos, profesionales y competitivos para el mundo, que implanta soluciones de tecnologías de la información integrada, basada en la investigación científica y tecnológica, para contribuir al desarrollo sostenible de la sociedad, aplicando el pensamiento sistémico, para este proceso de formación profesional la Escuela Profesional de Ingeniería de Sistemas, cuenta con un campus universitario propio, ubicado frente a la plaza principal del distrito de Daniel Hernández, provincia de Tayacaja – Huancavelica, que cuenta con una infraestructura de dos pisos, en el primer piso tiene cinco aulas de clases con una cámara IP en cada aula, un tópico con un equipo de cómputo, un aula magna con 3 cámaras IP y en el segundo piso se tiene cinco laboratorios (laboratorio de tecnología de información con 23 equipos de cómputo, laboratorio de ingeniería de software con 24 equipos de cómputo, laboratorio de simulación con 20 equipos de cómputo, laboratorio de redes y teleprocesos con 18 equipos de cómputo, laboratorio de internet sin quipos de cómputo, una cámara en cada laboratorio; una sala de servidores con 5 servidores, equipos de comunicación con 02 router y 04 switch CISCO; una sala de docentes, ambientes administrativos de dirección de la escuela con 2 equipos de cómputo, dirección de departamento con un equipo de cómputo, un equipo de control de personal, área de calidad con 2 equipos de cómputo, área académica con un equipo de cómputo, área de proyección social con un equipo de cómputo, área de investigación, área de prácticas pre profesionales, área de bienestar, área de tutoría, área de producción, una biblioteca con 2 equipos de

cómputo y un cafetín, en los pasadizos se tienen 05 cámaras IP. Se cuenta con un total de 7 docentes ordinarios, 3 docentes contratados a tiempo completo, 4 docentes CAS, 4 docentes a tiempo parcial, cada docente con su propia laptop. También se tiene 210 estudiantes de los cuales un promedio de 120 estudiantes tiene su propia laptop. Haciendo un total de 258 host los cuales tienen necesidad de estar conectados a la red, para el uso de aplicaciones LAN y WAN.

El servicio de internet con que cuenta la Escuela Profesional de Ingeniería de Sistemas es de 6 Mbps, el cual está distribuido mediante los puntos de red interconectados con un cableado estructurado solo para algunos ambientes específicos, quedando excluida la mayoría de los docentes y estudiantes.

Esto genera una molestia de parte de los docentes, estudiantes, y personal administrativo, porque la mayoría de procesos que realizan es mediante el internet, los cuales son interrumpidos por la saturación de datos que se genera en la EPI Sistemas, la saturación de datos constante genera malestar entre todos los usuarios, porque no pueden realizar sus objetivos mediante el internet, esto genera pérdida de tiempo y mucha incomodidad entre todo el personal administrativo, docentes y los estudiantes.

El servicio de internet que se tiene en la EPIS es un servicio inestable, debido a equipos básicos implantados en la comunicación, también se observó que no se tiene administrada la red de datos, esto influye directamente en el consumo de ancho de banda, porque cualquier usuario conectado a la red está libre de usar cualquier aplicación de red, consumiendo el ancho de banda existente y mucho más si sé apertura la red Wifi.

Haciendo la evaluación se observó que la saturación del ancho de banda es más frecuente entre las 9:30 hasta las 13:00 pm, debido a que todos están conectados al internet, haciendo descargas, viendo videos o en otros casos jugando en línea.

Teniendo en cuenta que la disponibilidad de la red no es constante durante la permanencia de la comunidad universitaria, tanto docentes, estudiantes y personal administrativo, esto lo podemos constatar en la medición que se realizó a un host de laboratorio de informática, donde nos da como resultado cortes y tiempos de respuesta exagerada, la medición se hizo usando el comando ping del host de laboratorio a un toma data de un salón de clase, de igual manera se hizo similares medidas de disponibilidad en diferentes horas durante los días laborales, pudiéndose evidenciar el mismo problema.

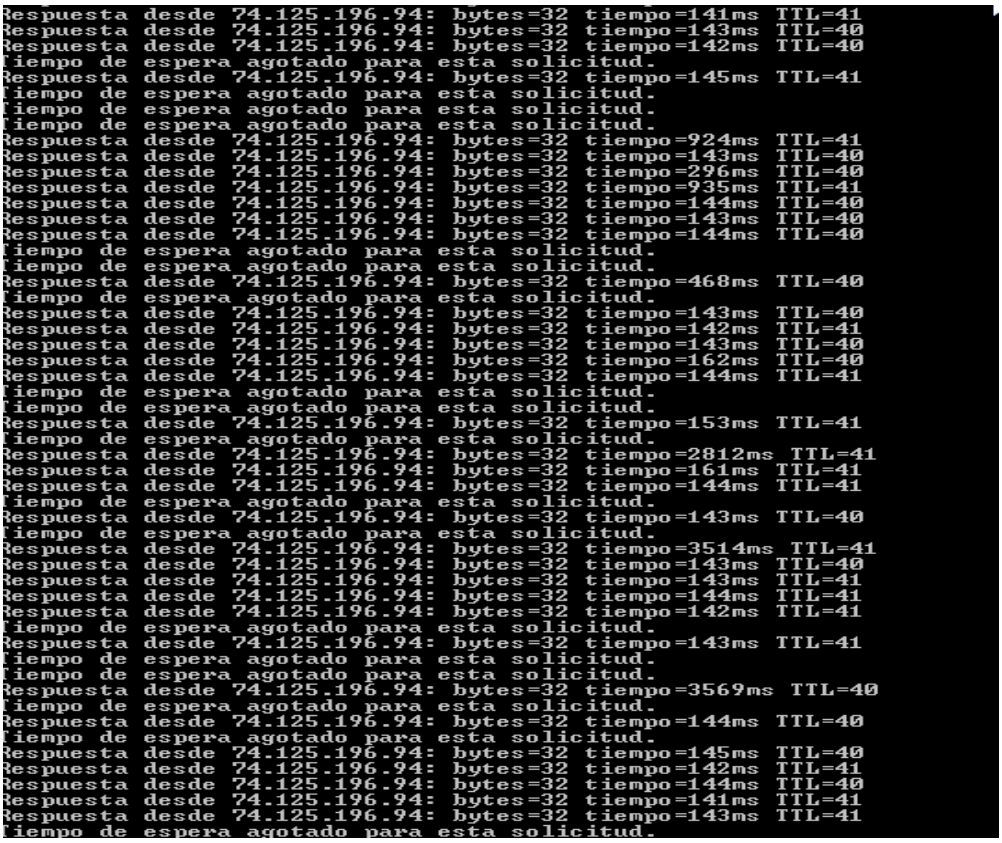

Figura 1: Latencia obtenido en una máquina de laboratorio de redes

Tabla 1: Distribución de ambientes en la EPIS

Escuela Profesional de Ingeniería de Sistemas						
Primer Nivel	Aulas de I-II	Aulas del III - IV	Aulas Del V- VI	Aulas del VII - VII	Aulas del IX- X	Sala de Reuniones
Segundo Nivel	Área administrativa	Sala de docentes	Aula de redes	Aula de Software	Aula de Ensamblaje	Sala de Servidores

Teniendo en cuenta que es un problema que aqueja a la Escuela Profesional de Ingeniería de Sistemas (EPIS), se realizó la medición de velocidad del internet y también la medición de carga y descarga de archivos en un periodo determinado.

Tabla 2: Medición de velocidad (test de velocidad primer Nivel EPIS)

Medición de velocidad (test de velocidad primer Nivel EPIS)								
N°	**Hora**	**Retardo Ms**	**Bajada (Mbps)**	**Subida (Mbps)**	**Retardo**	**FTP(Put) Kbps**	**FTP(Get) Kbps**	**Intentos realizados**
1	9:00	1200	0.92	0.30	1600	11.20	20.53	2
2	9:30	1300	0.83	0.28	1750	8.30	17.85	3
3	10:00	1550	0.75	0.23	1953	6.35	13.65	2
4	10:30	1723	0.60	0.20	2125	4.50	9.54	5
5	11:00	1883	0.58	0.17	2254	3.90	8.42	6
6	11:30	1760	0.60	0.19	2156	4.30	8.69	4
8	12:00	1700	0.68	0.20	2130	4.80	8.89	5
9	12:30	1754	0.75	0.22	2101	5.20	9.02	3

Tabla 3: Medición de velocidad (test de velocidad Segundo Nivel EPIS)

Medición de velocidad (test de velocidad Segundo Nivel EPIS)								
N°	**Hora**	**Retardo Ms**	**Bajada (Mbps)**	**Subida (Mbps)**	**Retardo**	**FTP(Put) Kbps**	**FTP(Get) Kbps**	**Intentos realizados**
1	14:00	1430	0.81	0.27	1802	9.02	15.25	2
2	14.30	1565	0.78	0.24	1952	5.15	12.63	2
3	15:00	1758	0.72	0.19	2108	3.23	8.40	3
4	15:30	1943	0.58	0.17	2312	2.25	5.26	4
5	16:00	2078	0.52	0.15	2525	2.60	4.26	5
6	16:30	1949	0.57	0.17	2326	3.15	4.45	3
8	17:00	1974	0.61	0.18	2320	3.12	3.63	4
9	17:30	1957	0.69	0.17	2300	4.10	3.88	2

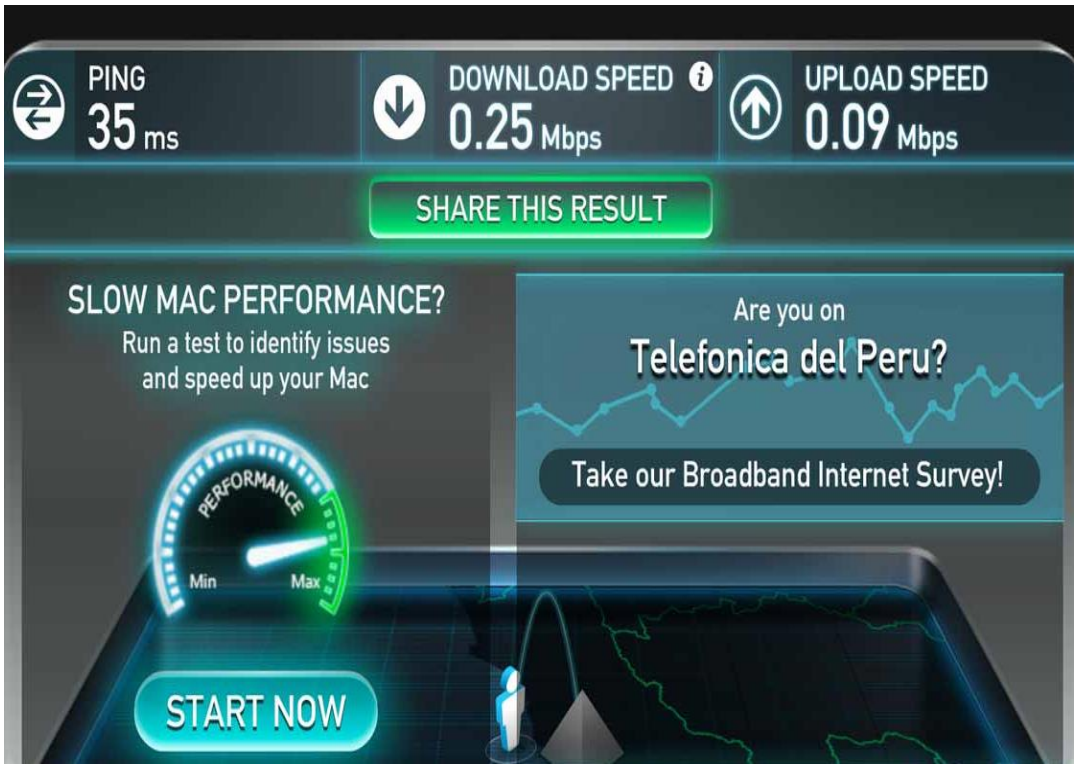

Figura 2: Test de velocidad de internet

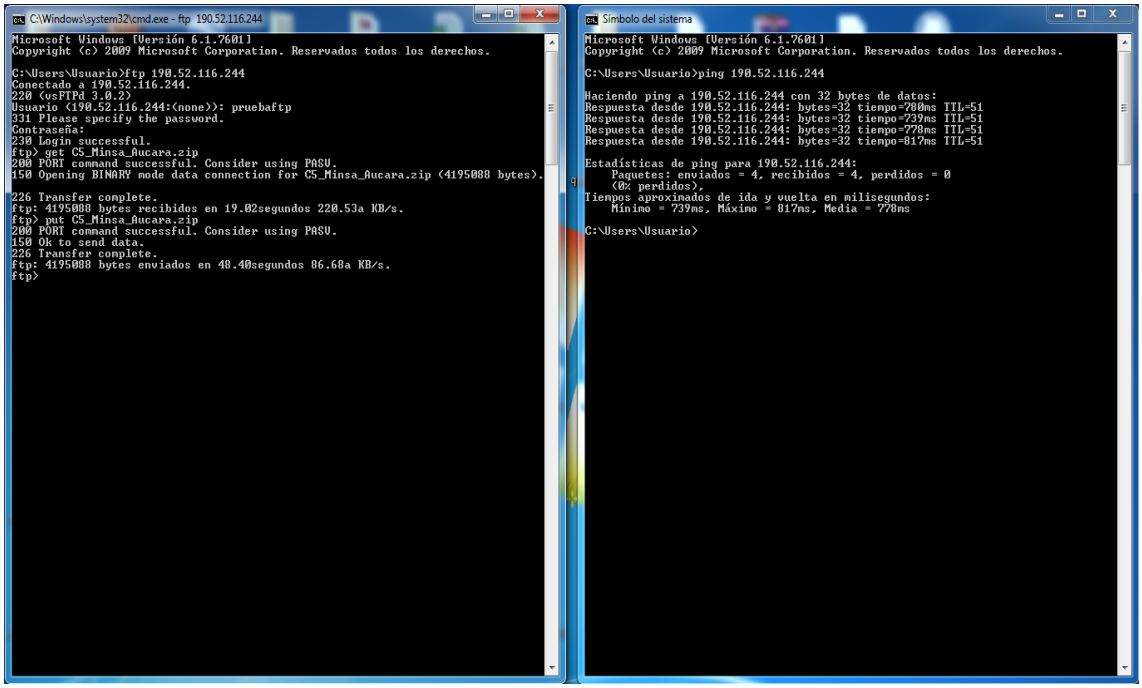

Figura 3: Medición de velocidad nivel de la EPIS
Fuente: elaboración propia

- **La autentificación en la EPIS**

Es el acto o proceso en la cual no permite confirmar que algo o alguien es quien dice ser. A la parte que se identifica se le llama probador y a la parte que verifica se le llama verificador.

Es habitual que el probador sea un usuario que quiera acceder a ciertos recursos y el verificador sea un sistema que pueda proteger el acceso a dichos recursos y tiene que verificar que el que acceda sea un usuario que tenga los permisos para que pueda acceder a dicha información.

La autentificación en la seguridad de información, es el proceso de intento de comprobar la identidad digital del remitente en una comunicación como una petición para que se pueda conectarse. El remitente siendo autentificado puede ser una persona que está utilizando un ordenador o un programa de

ordenadores. En una web de confianza, la autentificación es una manera de asegurar que los usuarios son quienes ellos dicen ser.

En la EPIS no tenemos un control para poder restringir el acceso a la red, esto implica que cualquier persona con un ordenador puede ingresar a la red, se tiene el riesgo de apropiarse de información y también de hacer uso el internet, esto pude ocasionar una lentitud perjudicando al personal que tiene que mandar información requerida o solicitada a la sede central, teniendo una demora considerable y ocasionando muchos problemas dentro de la EPIS, los docentes también se perjudican, puesto que no podrían preparar bien sus clases o más grave al momento de usar el sistema "SISACAD" al momento de subir las notas de todos los estudiantes y en algunos otros sistemas administrativos que cuenta la Universidad Nacional de Huancavelica.

Tabla 4: Ordenadores conectados a la red (Nivel EPIS)

Ordenadores conectados a la red (Nivel EPIS)		
N°	Hora	Cantidad Ordenadores
1	9:00	12
2	9:30	15
3	10:00	14
4	10:30	15
5	11:00	17
6	11:30	19
8	12:00	18
9	12:30	16

- **Otros problemas secundarios**

Saturación de los servidores al cual queremos conectarnos en la EPIS:

La velocidad de internet no solo depende de nuestro equipo en la EPIS. Si tratamos de conectar con un servidor, el cual tiene muy poco ancho de banda o está saturado, la velocidad se reducirá notablemente.

En estos casos no podemos hacer nada, ya que no depende de nosotros solamente, pero si hay algunos factores en la que podemos intervenir.

Adecuación del ancho de banda según el número de equipos conectados:

El ancho de banda que cuenta la EPIS es de 6 MB, quiere decir que si conectamos varios equipos a este ancho de banda se va a repartir según sea el requerimiento de cada máquina conectada. Este reparto no se hace de forma equitativa (es decir, si tenemos 6 MB contratados y tres equipos conectados no significa que cada equipo tendrá 6 MB), pero lo que no podemos conseguir es tener la misma velocidad con un único equipo conectado, sé que tiene varios equipos. Teniendo en cuanta esto, la velocidad de internet no abastecerá para los 258 hosts que tiene el campus universitario de la EPIS.

Actualización de programas:

Las actualizaciones de programas (sobre todo de los antivirus y Windows Update) cuando estos programas se están ejecutándose podrá notar una pérdida de velocidad en nuestra conexión.

Si necesitamos que no se actualicen los programas podemos deshabilitar, pero siempre teniendo en cuenta que por lo menos una vez al día se tendrá que actualizar algunos programas importantes para el correcto funcionamiento de los equipos, tal es el caso de los antivirus.

- **Estados de los equipos de la EPIS:**

  El estado de nuestro equipo influye también en la velocidad de nuestra conexión.

  No es tanto en la velocidad, si no en el consumo de memoria del disco duro y también una cantidad considerada de archivos en el historial de internet que se guardan, en páginas sin conexión e incluso en las Cookies.

1.2. Formulación del problema

1.2.1. Problema general

¿De qué manera influye el servidor Radius en el control del acceso a la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica?

1.2.2. Problema especifico

- ¿Cómo influye el servidor Radius en la disponibilidad de la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica?
- ¿Cómo influye el servidor Radius en la autentificación de la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica?

1.3. Objetivos

1.3.1. Objetivo general

Determinar la influencia del servidor Radius en el control del acceso a la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.

1.3.2. Objetivo específico

- Determinar la influencia del servidor Radius en la disponibilidad de la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica
- Determinar la influencia del Servidor Radius en la autentificación en la red de datos de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.

1.4. Justificación

1.4.1. Justificación teórica

La investigación tiene como objetivo optimizar los recursos de la información debido al acceso a las aplicaciones LAN y WAN de parte de la comunidad universitaria, este trabajo de investigación puede ser de gran utilidad para la entidad beneficiada y también se puede implantar en otras universidades.

En los últimos años, se ha incrementado considerablemente el uso de internet a nivel nacional, las universidades, empresas, instituciones públicas y privadas. Se ha observado que los usuarios no están haciendo el uso adecuado

del internet, la cual genera perdida de dinero en lo que concierne a las distintas instituciones a nivel nacional como internacional.

El control de acceso a la red inalámbrica mejorará la disponibilidad de la información en la red, lo cual es un factor que no se tiene en cuenta en la escuela de sistemas, hacerlas más eficientes, productivas y económicas. En un mundo tan desarrollado como el actual, la comunicación entre los miembros de la organización en tiempo real es de suma importancia. Por lo tanto, el objetivo de esta tesis, es presentar una solución óptima, que es diseñar un modelo para el control de acceso a la red inalámbrica.

Es imprescindible mencionar el uso de la metodología de James McCabe. La metodología de James McCabe consiste en la gestión de redes, también es determinado como la suma total de todas las políticas, procedimientos que interceden en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá manifestado en la calidad de los servicios ofrecidos.

1.4.2. Justificación metodológica

La mayoría o todos los trabajadores que laboran en la escuela de sistemas, usan las tecnologías de información y comunicación, es de vital importancia que los sistemas de información y específicamente la red que los conecta y comunica con internet funcionen correctamente, sin fallas, sin retrasos y garantizando la seguridad de la información que por ella fluye. Más aún, para lograr la eficiencia en la gestión pública, es necesario que los equipos, medios, y software de comunicaciones estén correctamente configurados respecto a la

necesidad de la entidad, para que los funcionarios puedan laborar de la mejor manera, siendo respaldados por una red de datos confiable y rápida. El trabajo se justifica por la importancia de contar con una red que garantice el intercambio de información sin retraso alguno y de forma segura, de manera que coadyuve al logro de objetivos institucionales.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes nacionales

(Fernández Rivera, 2016) en su investigación titulada “Metodología para el diseño de una red LAN inalámbrica 802.11 n/ac con servidor radius para la Gerencia Regional de Salud – Arequipa” menciona entre las diversas causas de los problemas encontrados la falta de control de manera correcta en el uso de la infraestructura de red de datos, dando como resultado el inconveniente en cuanto a la seguridad de los recursos de información, en la investigación se diseña una red inalámbrica que tenga los protocolos respectivos para una red inalámbrica recurriendo al protocolo radius y con ello conseguir la autenticación y autorización en la red inalámbrica.

(Avalos Reyes & Romero Palacios, 2018) en su investigación titulada “Rediseño de la Interconexión de Datos de la Red de Área Local Inalámbrica (WLAN) del Campus – Los Pinos, la Facultad de Educación y Humanidades y la Facultad De Medicina Humana de la Universidad San Pedro”, tiene como propósito el rediseño de la infraestructura Wlan del campus – los pinos, con esto solucionar ciertos inconvenientes de la red, contribuyendo que la red sea lo más rápido y eficiente en cuanto a la conexión y seguridad a los datos

utilizando tecnología raduis restringiendo de esta manera el acceso a terceras personas, con ello mantener seguros los recursos de la organización.

(Blas Rinza, 2017) en su investigación titulada “Seguridad y control del acceso a las redes inalámbricas en la UNSM-T mediante servidores de autenticación radius con el uso de certificados digitales” hace mención que existe una necesidad de perfeccionar la seguridad en el acceso a la infraestructura de red inalámbrica de la organización, para lograr la necesidad en mención hace uso de los protocolos de seguridad de un servidor radius con certificados digitales ello va a permitir que estén encriptados los mensajes que son enviados entre un servidor y cliente, ello va a garantizar la seguridad en la transmisión de la información a través de internet.

2.1.2. Antecedentes internacionales

Según (Mena Molina, 2019) en su investigación titulada “Implementación de servidores Radius para controlar los accesos no autorizados a redes inalámbricas, caso OSFL”. Menciona la importancia de perfeccionar la seguridad y el acceso no autorizado a una infraestructura inalámbrica de la organización OSFL, implementando un servidor Radius, teniendo como resultado después de la implementación, logrando un control mayor a los accesos de los clientes que acceden inalámbricamente, de esa manera minimizar el acceso y robo de información por personas no autorizadas, de igual manera el ataque a los recursos de la red de la empresa.

(Loor Anchundia, 2019) en su investigación titulada “Acceso a redes inalámbricas de la ESPAM MFL mediante un servidor Radius”, trata sobre la implementación de un servidor Radius en la organización, frente al no

cumplimiento de los procesos adecuados para el control de acceso a la infraestructura de red de datos, llegándose a implementar ciertos mecanismos para su posterior y mejor administración.

(Espinoza Alarcón & Tejena Vergara, 2019) en su investigación titulada "Análisis e implementación de servicios de seguridad, autenticación y optimización para la red LAN y WLAN del Instituto Tecnológico Superior Guayaquil". Hace un análisis e implementa servicios que involucran seguridad, autenticación y optimización para la infraestructura LAN y WLAN de la organización, donde llegan a implementar tecnologías como proxy, radius, segmentos de red como VLAN, también toma en consideración puntos de acceso en ciertas áreas para aumentar el rendimiento de la red inalámbrica, esto con el fin de tener un mayor control en el uso de internet de los laboratorios, de esa manera disminuir las amenazas a los recursos de red de terceras personas que no tengan nada que ver con la organización.

2.2. Bases teóricas

Generalmente, para la implementación correcta de este proyecto se requería acumular ciertos conceptos e información que representen una fuente importante de datos de las que se pueda extraer requisitos fundamentales de los procesos de autenticación Radius, considerando principalmente que los conceptos que vimos en el transcurso de esta investigación fueron documentos relacionados con la implementación de mecanismos de seguridad para el control de acceso en redes inalámbricas.

2.2.1. Servidor radius

Radius se le conoce como un protocolo que trabaja como cliente/servidor. En una implementación Radius el cliente se le conoce como NAS y al servidor podemos decir que es un proceso de Daemon que podría ser corrido en Unix o en Windows. El cliente transporta la información usuaria a los servidores Radius que fueron designados. Los servidores Radius son los que recogen las peticiones de una conexión usuaria, esto pasan por un proceso de autenticación para luego devolver la información de una configuración óptima donde el cliente pueda devolver el servicio al usuario. Los servidores Radius funcionan como un cliente proxy para otros servidores Radius, incluso para servidor de autenticación. En la figura siguiente se puede mostrar la interacción que existe entre un usuario que marca entrada, un servidor y cliente Radius. (Cisco, 2006)

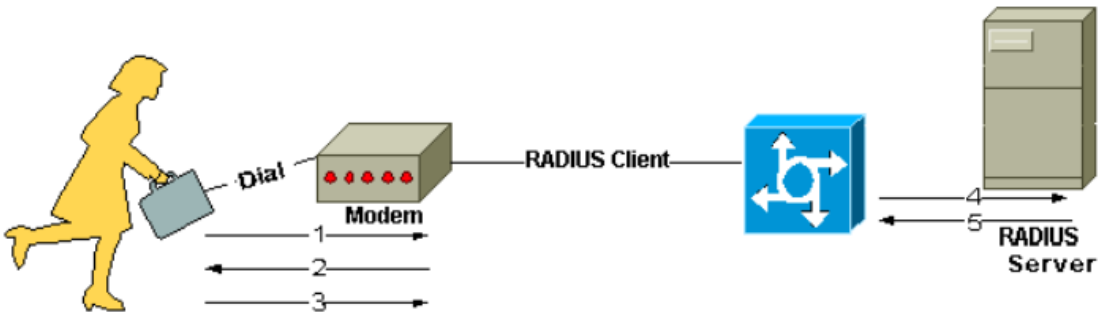

Figura 4: Interacción entre el usuario, cliente y servidor Radius

1. El proceso se inicia cuando el usuario pide autenticación PPP al NAS.
2. NAS solicitará el ingreso de usuario y contraseña (PAP) o la integración (CHAP).
3. Se produce respuestas de parte del usuario.
4. Acto seguido, el cliente Radius envía el nombre de usuario y contraseña en condición de encriptado al servidor Radius.

5. Las opciones de respuesta que adopta el servidor Radius es que puede aceptar, rechazar o impugnar.
6. Finalmente, el cliente Radius procede su actuación en función de los servicios y parámetros de ciertos servicios agrupados con aceptar o rechazar.

a) Componentes del servidor Radius

Protocolo: Actúa sobre UDP, RFC 2865 y 2866 que precisa la estructura de la trama Radius y nos provee una forma de transmisión de mensajes y utiliza la 1812 como el puerto de autenticación y la 1813 como el puerto de auditoria. (TeleInfo, 2008)

Servidor: Un servidor Radius corre en un ordenador llamado también estación de trabajo, y conserva la información que es usada para la autenticación de usuarios y servicio para que puedan ingresar a la red. (TeleInfo, 2008)

Cliente: En cuanto al cliente Radius, podemos decir que se ejecuta en el NASS que se encuentra en toda la red. (TeleInfo, 2008)

b) Base de datos que trabaja el servidor Radius

Usuarios*:* Son los encargados de almacenar la información de parte del usuario, que pueden ser el nombre de usuario, la contraseña, protocolos y dirección IP. (TeleInfo, 2008)

Clientes: Son los encargados de acumular la información de todos los clientes Radius, así como la clave compartida. (TeleInfo, 2008)

Diccionario: Guarda la información para que pueda ser interpretada por parte de las propiedades del protocolo Radius. (TeleInfo, 2008)

2.2.2. Disponibilidad de red

Se define como el porcentaje de tiempo que un sistema de red, un componente o una aplicación están disponibles para un usuario Se basa en la fiabilidad de los componentes individuales de la red Depende de la disponibilidad de los componentes, y de su organización (componentes redundantes, arquitectura robusta). (Sosa, 2011)

2.2.3. Métodos de seguridad y control de acceso a las redes

a) Autenticación

En su mayoría de protocolos sustentados en contraseñas o passwords, en la actualidad depende de lo difícil que pueda ser la contraseña que esté utilizando el usuario, el servidor proporciona los intentos de confirmación al usuario pidiendo una contraseña que el cliente solicita al servidor, siendo confirmada esta respuesta por el usuario contra la contraseña que está registrada en un repositorio o base de datos. A modo general, este acercamiento lo podemos ver en CHAP, MS- CHAP, MS-CHAP-V2, entre otros. (Olivares Montes, 2017)

Lo dificultoso de este acercamiento consiste en que si un usuario no autorizado tiene conocimiento del proceso de envío y respuesta, puede inicializar lo que se llama un diccionario de ataque, donde las contraseñas de forma aleatoria se prueban con las validaciones que son solicitadas por parte de los usuarios a los servidores, en conocer cuál de esas respuestas enviadas son las correctas. De forma estándar las contraseñas podríamos decir que tiene reducida entropía, con esta forma de ataque podría ser fácil de encontrar varias contraseñas. (Olivares Montes, 2017)

b) Privacidad de datos

Otro punto importante es la seguridad de la interconexión de datos que se da entre un cliente y un punto de acceso después que se haya dado la autenticación. Incluso si los clientes pudiesen realizar negociaciones principales después de la autenticación, en caso de que esas contraseñas no estén encriptadas cuando se produce una autenticación, la secuencia de envío de datos podría estar vulnerable a espías. Por lo tanto, este índice a que en un proceso de autenticación el tener contraseñas que puedan ser distribuidos entre los clientes y los puntos de acceso al momento de ejecutar la conexión de datos puedan ser encriptados. (Olivares Montes, 2017)

c) Puntos de acceso no permitidos

Otro punto importante en cuanto a seguridad nace de la posibilidad de que a un usuario tenga la necesidad de colocar un punto de acceso que no esté permitido en una infraestructura inalámbrica. Este tipo de situaciones son poco probables porque las formas de autenticación que se da en ambas partes lo impiden, aquí el usuario inalámbrico valido la red al cual quiere tener acceso. (Olivares Montes, 2017)

2.2.4. Confiabilidad de la red

Es la probabilidad que se presente una falla en un intervalo de tiempo definido, excluyendo las interrupciones producto de intervenciones programadas. La relación con el intervalo de tiempo que el elemento o sistema está libre de falla. Se dice, también, de la probabilidad de sobrevivir correctamente en funciones una vez que comienza a operar. Se propone como

índice de confiabilidad a definir por año, dependiendo de la topología y tecnología de la red, correspondiendo a una estimación teórica que se convierte en la referencia objetiva. Típicamente, se ha descrito, para equipos y sistemas, que la confiabilidad esperada, obedece a una tendencia de fallas que sigue un comportamiento en el tiempo, en una función que se le denomina la curva de la bañera, la cual es una gráfica que representa los incidentes de falla durante el período de vida útil. Se llama así porque tiene la forma de una bañera. En ella se pueden apreciar tres etapas: (Apablaza, 2012)

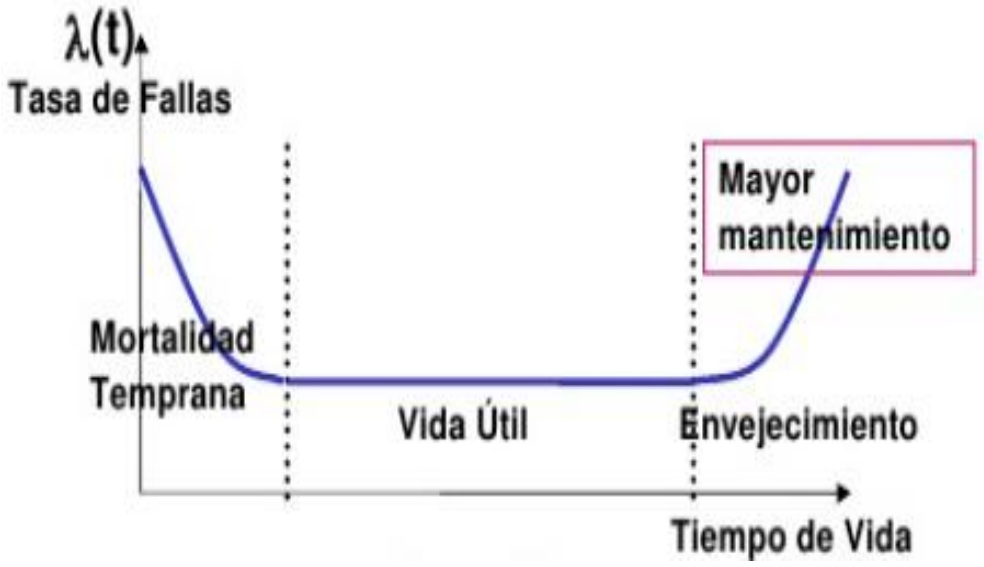

Figura 5: Confiabilidad de la red

2.2.5. Seguridad de datos

En cuanto a la seguridad de datos, que también se conoce como seguridad de la información o seguridad informática, es un recurso importante que está relacionado con la seguridad de los datos, en protección al ingreso de terceras personas ajenas a la organización, para salvaguardar de una posible vulneración de la misma. (Perez Garay, 2019)

Seguridad de datos es el cifrado de los datos, buenas prácticas en la administración de contraseñas que fortalezcan la protección de los datos en las diferentes aplicaciones y plataformas de una entidad. (Perez Garay, 2019)

2.2.6. Seguridad de redes inalámbricas

Las redes inalámbricas forman parte de una infraestructura inalámbrica, de forma particular, de qué manera está protegida de información de quienes están ingresando a la red inalámbrica, viendo las redes wifi en este tipo de red, su funcionamiento está en base, ha cifrado de datos, y para poder ser cifrado se tendrá que tener conocimiento de algún usuario y contraseña para de esa manera tomar en forma correcta los paquetes enviados. Es en esta parte, donde se encaminan las vulneraciones a las señales inalámbricas de lograr y tener conocimiento de algún modo, el usuario y contraseña para poder conocer sus paquetes. Para imposibilitar que usuarios no autorizados tengan información confidencial, es que se debe implementar variados sistemas de seguridad, como el que citamos: WEP, WPA, WPA2, que se rigen bajo las normas IEEE, organización que se encarga de formar estos protocolos de seguridad, todo ello establecido en sistema de usuario y contraseña. Una vez ingresado en la red inalámbrica, la probabilidad es alta en tener conocimiento de lo que están descargando los usuarios pertenecientes a la red, de esa manera saber información confidencial de la organización, estando dentro de la red es posible conocer contraseñas, información de cada uno de los usuarios entre otros, entonces es necesario que las señales inalámbricas estén protegidas. (Gonzales J, 2014)

WEP: Este protocolo tiene un proceso de cifrado elemental determinado en el estándar IEEE 802.11, hace uso del algoritmo de cifrado RC4 (Rivest Cipher 4), para codificar los datos que se envían entre el cliente y los puntos de acceso. La función de RC4 es crear una contraseña de forma pseudoaleatoria con una longitud igual que el texto original. En esta contraseña y el texto original se empleó de la operación lógica XOR, llamado también O exclusiva, teniendo como resultado un texto cifrado. La contraseña pseudoaleatoria es generada utilizando la clave secreta que es definida por el usuario que tiene una longitud de 40 o 104 bits con un vector de inicialización de 24 bits que el mismo sistema de manera aleatorio lo genera. (Gonzales J, 2014)

WPA: La Alianza Wi-Fi lanza el protocolo de seguridad WPA con el fin de solucionar los problemas generados por el protocolo WEP. Con este protocolo se implementa las mejoras como: Autenticación del usuario usando el estándar IEEE 802.1x que consisten en tener un control al acceso de la red establecido en los puertos. En cuanto a la debilidad del vector de inicialización, este protocolo brinda solución empleando la inclusión de vectores de longitud doble usando 48 bits. Hace uso del protocolo TKIP (Temporal Key IntegrityProtocol) para un intercambio automático de contraseñas. Este protocolo sigue haciendo uso el RC4 como algoritmo de cifrado, la diferencia está en la comprobación de la integridad de los mensajes, utiliza un nuevo código llamado MIC (MessageIntegrityCode). (Gonzales J, 2014)

WPA2: Este protocolo nos brinda una ventaja de tener mucha más seguridad, integra un cambio dinámico de las contraseñas, brinda un cifrado mucho más estable, de igual forma la autenticación de usuario con algunas

mejoras como: provee un algoritmo cifrado nuevo llamado AES (AdvancedEncryption Standard) que es un algoritmo de codificación de bloque simétrico. Hace uso del protocolo CCMP (CounterModewithCipher Block ChainingMessage Authentication CodeProtocol) para tener más Seguro en cuanto a la integridad y autenticidad de la información. (Gonzales J, 2014)

2.2.7. Control de datos

El control de datos consiste en identificar evasiones de información de forma ocasional, que son producidos por descuido de los propios usuarios en la manipulación de los datos, como por ejemplo cuando mandamos un archivo que contiene datos relevantes por medio del correo electrónico haciendo uso del internet. El control de datos nos facilita tener un control al momento de transferir archivos a dispositivos de almacenamiento o a través de aplicaciones que estén conectadas a internet. (Gaya Fuertes, 2019)

2.2.8. Autentificación del usuario

La autenticación del usuario son los procesos que brindan dar garantía en cuanto a la seguridad de las infraestructuras de redes de datos, pero estos difieren según el sistema y la calidad de los datos que deberán ser protegidos, a continuación de forma resumida definimos: (Perez Porto & Gardey, 2016),

a) Autenticación, Consiste en validar la identidad de los usuarios que están intentando realizar una conexión con una base de datos.

b) Autorización: Establecido la identificación del usuario de forma correcta, se le permite hacer uso o que puede acceder a los recursos de la red.

c) Auditoría: Es cuando se tiene registrado todos los accesos de un usuario que ha tenido autorización durante su sesión en la red.

2.2.9. Control de acceso

Una persona no autorizada puede tener acceso libre a los dispositivos de comunicación de la red y a los servicios sensibles. Para poder limitar los accesos no deseados, tener un control al acceso de manera necesaria. Tener el control de acceso activado es poner límite de quienes pueden tener acceso a la infraestructura de red o que usuarios pueden hacer uso de los recursos específicos, así como servicios que se tenga disponible una vez permitido el ingreso. En una infraestructura de red, se pueden utilizar muchas formas de autenticación, donde cada método predispone mucha formas o niveles de seguridad. (Cisco N. A., 2009)

Una de las maneras más simples que se puede tener en cuanto a autenticación son las contraseñas que podamos utilizar. Este método se puede programar haciendo uso de la combinación de login y contraseñas, para los equipos de comunicación podrían ser para las líneas de consola y las líneas virtuales, como también los puertos auxiliares, esto es una de las maneras más fáciles de implementar, en contraposición es la más débil y menos seguro. (Cisco N. A., 2009)

a. Características de AAA

- **Autenticación AAA**

  Se puede hacer uso de AAA para autenticar usuarios que van a tener un acceso administrativo o que van a tener un acceso remoto a una

infraestructura de red. Estas dos formas de acceso usan maneras diferentes para pedir servicios AAA: (Cisco N. A., 2009)

Modo carácter. En este modo, el usuario manda una solicitud para crear un proceso en modo exe con el router con propósitos administrativos. (Cisco N. A., 2009)

Modo paquete. En este modo es el usuario quien envía una petición para que pueda establecerse una conectividad con un dispositivo en la plataforma de red por medio del enrutador. (Cisco N. A., 2009)

- **Registro de auditora AAA**

  El registro de auditoría es el que recolecta y reporta datos que pueden ser utilizados para auditorías. La información recolectada puede contener el principio y a terminación de conexiones, comandos que se han ejecutado, número de paquetes, así como número de bytes. (Cisco N. A., 2009)

  El registro de auditoría se puede implementar haciendo uso de AAA basado en un servidor. Este hace un reporte estadístico de uso al servidor ACS. Estos datos estadísticos se pueden hacer uso para crear reportes con bastante detalle sobre la configuración de la infraestructura de red. (Cisco N. A., 2009)

2.3. Organigrama de la EPIS

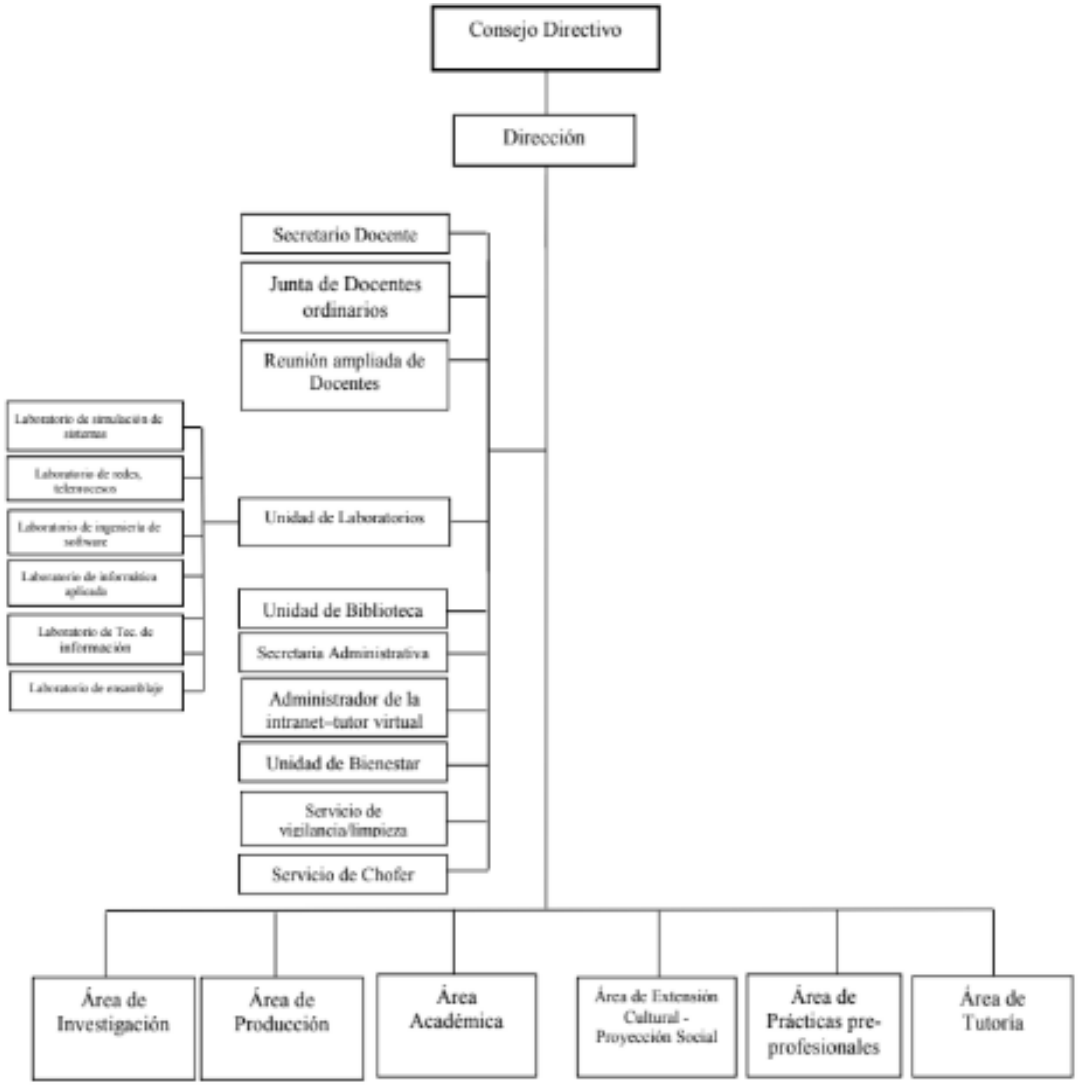

Figura 6: Organigrama de la EPIS

2.4. Bases conceptuales

2.4.1. Servidor Radius

Es un protocolo que nos permite controlar la autenticación, autorización y registro de un usuario que necesita conectarse a una red. (Tamayo, 2013)

2.4.2. Red de datos

Una red es una infraestructura que tiene un patrón que lo caracteriza. Donde existe computadoras y diferentes dispositivos que están conectadas a la red que intercambian recursos. (Pérez & Merino, 2011).

Dato es una terminología inmersa en información, documento o testimonio que nos induce a tener un conocimiento o deducción en las consecuencias de un hecho. (Pérez & Merino, 2011).

Una red de datos es una plataforma cuya estructura nos da la posibilidad de transmitir información como un intercambio de datos. Esta plataforma se diseña teniendo ciertas especificaciones para satisfacer objetivos y por ende el intercambio de datos. (Pérez & Merino, 2011).

2.4.3. Redes inalámbricas

Una red es un conjunto de dispositivos conectados de manera individual, eso nos quiere decir que es un sistema de comunicaciones donde se unen diferentes unidades que les facilita intercambiar datos, una red de datos brinda la facilidad de comunicar con otros usuarios, así como compartir archivos y periféricos. Un dispositivo para estar conectado a la red no es necesario que la red sea alámbrica, puede hacerse usando la tecnología inalámbrica como uso de láser, microondas, satélites. Una infraestructura inalámbrica no hace uso de cables para mantener comunicado sus dispositivos como computadoras u otros dispositivos. Una red de área local, más conocido como red LAN, son las redes que van a permitir que un grupo de usuarios estén conectados para poder compartir archivos y recursos como impresoras, almacenamiento, entre otros. Las redes WAN son infraestructuras que permiten la comunicación a usuarios

que se encuentran en lugares distantes y con ello se traspasa espacios geográficos. Wi-Fi forma un conjunto de normas o estándares para infraestructuras inalámbricas teniendo como norma el IEEE 802.11, este sistema de comunicaciones tiene una velocidad máxima de 11 Mbps, pudiéndose alcanzar distancias mayores de varios metros, existen tecnologías que alcanzan los 22, 54, hasta 100 Mbps. (Velazquez, 2007)

2.5. Definición de términos

- **Radius,** "Desarrollado por Livingston Enterprises, es un protocolo AAA abierto de estándar IETF con aplicaciones en acceso a las redes y movilidad IP. RADIUS trabaja tanto en situaciones locales y de roaming, y generalmente se usa para los registros de auditoría." (Cisco N. A., 2009)
- **DHCP,** "Permite a los dispositivos de una red obtener direcciones IP y demás información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, gateways y otros parámetros de redes IP." (Cisco Networking Academy, 2009)
- **Protocolo AAA,** "El AAA es un protocolo, especificado en RFC 2903 y varias otras RFC, para especificar quién puede acceder a un sistema o a una red, cómo puede acceder a estos y qué hizo mientras estuvo conectado." (Cisco Networking Academy, Acceso a la WAN, 2009)
- **Wlan,** "La LAN es la red inalámbrica de área local que permite una conexión a la red entre dos o más computadoras sin utilizar cables. Usa una comunicación radial para realizar la misma funcionalidad que la de una LAN cableada." (Cisco Networking Academy, Conmutación y conexión inalámbrica de LAN, 2009)

- **TACACS,** “Protocolo de autenticación, desarrollado por la comunidad DDN, que suministra autenticación de acceso remoto y servicios relacionados, por ejemplo, registro de eventos. Las contraseñas de usuarios se administran en una base de datos central en lugar de routers individuales.” (Cisco Networking Academy, Conmutación y conexión inalámbrica de LAN, 2009)
- **Tasa de transferencia,** “En informática y telecomunicaciones, el término tasa de bits, a menudo tasa de transferencia, define el número de bits que se transmiten por unidad de tiempo a través de un sistema de transmisión digital o entre dos dispositivos digitales.” (Cisco Networking Academy, Aspectos básicos de redes, 2009)
- **Latencia de red,** “Latencia de red es la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red. ” (Cisco Networking Academy, Conmutación y conexión inalámbrica de LAN, 2009)
- **Paquete,** “Agrupación lógica de información que incluye un encabezado que contiene información del control y (generalmente) datos del usuario. Los paquetes a menudo se usan para referirse a las unidades de datos de la capa de red.” (Cisco Networking Academy, Aspectos básicos de redes, 2009)
- **QoS,** “Calidad de Servicio, medida de rendimiento de un sistema de transmisión que refleja la calidad de transmisión y la disponibilidad de servicio.” (Cisco Networking Academy, Conmutación y conexión inalámbrica de LAN, 2009)

2.6. Hipótesis

2.6.1. Hipótesis general

El servidor Radius influye positivamente en el control de acceso a la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.

2.6.2. Hipótesis especifico

- El servidor Radius influye positivamente en la autentificación al momento de ingresar a la red inalámbrica la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.
- El servidor Radius influye positivamente en la disponibilidad de la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.

2.7. Definición de términos

2.7.1. Variable independiente

X: Servidor Radius

2.7.2. Variable dependiente

Y: Control de acceso a la red inalámbrica

2.8. Operacionalización de la variable

Tabla 5: Operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
Variable Independiente (X) Servidor Radius	Radius es un protocolo cliente / servidor que es ejecutado en la capa aplicación del modelo OSI, y se puede utilizar en TCP o UDP. Son servidores de acceso a la red, por lo general se ejecuta en un servidor Unix o Windows.	Red de datos	✓ N° de subredes ✓ N° de host conectados.
Variable Dependiente (Y) Control de Acceso a la Red Inalámbrica	Son mecanismos de seguridad establecidos en una red de inalámbrica de área local, los cuales tendrán la función principal de garantizar la integridad, confidencialidad y disponibilidad de la información, mediante la autenticación de los que ingresan a la red.	1) Autenticación 2) Disponibilidad	1) % de usuarios conectados de manera inalámbrica con acceso permitidos. 1) Latencia de red

CAPITULO III

MATERIALES Y MÉTODOS

3.1. Ámbito temporal y espacial

3.1.1. Delimitación temporal

El periodo que comprende la investigación, corresponde al periodo 2019

3.1.2. Delimitación espacial

Esta investigación está comprendida dentro de la Región de Huancavelica, Provincia de Tayacaja, del Distrito de Daniel Hernández, en el campus universitario de la Escuela Profesional de Ingeniería de Sistemas.

3.2. Tipo de investigación

Según (Bunge, 1969) con la investigación de tipo aplicada lo que se busca es resolver problemas, este tipo de investigación hace uso de los conocimientos teóricos, que más adelante son transformados en conocimientos prácticos y con ello resolver problemas.

Nuestra investigación es de tipo aplicada porque evidencia la problemática de la red wifi en la EPIS y propone una solución a través de diseñar un modelo de servicio de red basado en servidores radius para mejorar el tipo de seguridad y tráfico de esta red.

3.3. Nivel de investigación.

(Bunge, 1969), divide a la investigación en pura y aplicada. En términos sencillos, la finalidad de la investigación pura es “conocer”, mientras que la finalidad de la investigación aplicada es “mejorar”, por tanto, la investigación pura abarca los cinco primeros niveles de la investigación y la investigación aplicada se corresponde con el nivel aplicativo.

La investigación aplicada cuenta claramente con intervención, pero no se trata de una intervención delibera, como ocurre en los experimentos, a lo cual se le denomina manipulación, sino de una intervención a propósito de las necesidades de la población objetiva.

Tanto es así que la investigación aplicada plantea resolver problemas o intervenir en la historia natural de la enfermedad, es por esto que algunos investigadores la denominan investigación acción.

Nuestra investigación es de nivel aplicativo porque va a permitir controlar el acceso a la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica, además, las técnicas estadísticas apuntan. a evaluar el éxito de la intervención en cuando a proceso, resultados e impacto, para lograr esto se debe identificar los indicadores apropiados.

3.4. Diseño de investigación

Según (Sampieri, 2012) la investigación es Pre-Experimental: cuando manipulan deliberadamente una o más variables independientes para observar su efecto y relación con una o varias dependientes, únicamente que trabajan

con “grupos intactos”, formados por motivos ajenos al experimento, en los diseños pre experimentales los participantes no se asignan al azar a los grupos ni se emparejan, sino que dichos grupos ya están integrados previamente al experimento.

Además, es un Diseño de pre-prueba – pos-prueba con un solo grupo, pues a un grupo se le aplica una prueba previa al estímulo o tratamiento experimental, después se le administra el tratamiento y finalmente se le aplica una prueba posterior al estímulo, esto permite mostrar un punto de referencia inicial para ver qué nivel tenía el grupo en las variables dependientes antes del estímulo (variable dependiente).

Diseño de investigación con pre y post prueba en los hosts conectados en la red propuesta por el Diseño del Modelo de gestión y los hosts conectados en la red de datos actual.

El diagrama del diseño es el siguiente:

RGE: O_1 X 0_2

Donde:

RGE: Grupo experimental (hosts conectados en la red de wifi EPIS)

O_1: Resultado de los valores de los indicadores de la red wifi actual

X: Tratamiento (servidor radius)

O_2: Resultado de los valores de los indicadores de la red wifi luego de la intervención del servidor radius.

3.5. Población, muestra y muestreo

3.5.1. Población

(Arias, 2006) Define que la población está conformada como un conjunto de elementos que tienen peculiaridades comunes que tienen un carácter válido en una investigación. La población para el trabajo de investigación está compuesta por cada uno del host, haciendo un total 120 que están conectados a la red actual híbrida (wifi y estructurado).

3.5.2. Muestra

(Arias, 2006) Define a la muestra como una parte o fracción, que es una parte representativa de la población, también menciona que la muestra puede tomarse la totalidad de la población, para el caso de estudio se tomó la totalidad, que es 120 hosts.

3.6. Técnicas e instrumentos de recolección de datos

3.6.1. Técnicas de recolección de datos

En un análisis documental, en cualquier investigación, al momento se recolecta los datos, se tiene que usar un grupo de técnicas e instrumentos que a través de ello podemos obtener y medir la información recolectada sobre un grupo de parámetros que queremos determinar, teniendo en cuenta el diseño de la investigación, la muestra con el problema científico a resolver y la hipótesis, teniendo en cuenta las variables utilizadas.

(Arias, 2006) Define los instrumentos como: “Los medios materiales que se emplean para recoger y almacenar la información.” Según Arias, los

instrumentos de recolección son: “las distintas forman o maneras de obtener la información.”

Las técnicas que utilizaremos en nuestra investigación son:

- El Análisis de Contenido.
- La Observación.

3.6.2. Instrumentos de recolección de datos

Hoy en día existen varias técnicas e instrumentos de colección de datos que se pueden utilizar en la investigación científica.

Los instrumentos que se utilizara son las siguientes:

- Fichas de observación.
- Listas de comparaciones

3.6.3. Fuentes de recolección de datos.

La recolección de datos se realizará mediante las fichas de observación, teniendo como fuente cada uno de los equipos de la red de datos que tiene la Escuela Profesional de Ingeniería de Sistemas y cada uno de los hosts propuestos para el diseño del servicio de la red inalámbrica.

3.6.4. Técnicas y procesamiento y análisis de datos

Toda la información se recolectará en las fichas de observación, y en las listas de cotejo, las cuales se analizarán a través de tablas de resultado, las pruebas obtenidas de cada host del pre test y post test con las que se tendrá resultados, las cuales se procesaran.

Así también se tendrán en cuenta los gráficos obtenidos de dichas fichas, la cual nos servirá para poder visualizar e interpretar los resultados.

CAPITULO IV

DISCUSIÓN DE RESULTADOS

4.1. Diseño del modelo de red con servidor radius

Se diseñó el modelo de red aplicando Servidor Radius para el control de acceso a la red inalámbrica utilizando la metodología propuesta por James Mcabe, lo cual desarrollaremos a continuación:

4.1.1. Fase de diagnóstico

En esta fase se realiza el esquema de la solución presentada, utilizando los resúmenes elegidos en los puntos anteriores.

Inicialmente, se ejecuta el diagnóstico de la red de datos estructurada e inalámbrica, esta fase nos permite evaluar cuantos hosts se están conectando a través de la red estructurada y cuantos hosts a través de la red inalámbrica, finalmente se explica el funcionamiento de la red actual.

La Escuela Profesional de Ingeniería de Sistemas, tiene dos pisos, en la primera planta están los salones del I ciclo hasta el X ciclo, y la segunda planta alberga los laboratorios, sala de docente y personal administrativo, cuenta con una infraestructura de red de datos ya instalada con equipos administrables.

- **Descripción de la situación actual de la red, tal y como se encuentra**

La situación actual de la infraestructura de red de datos de la Escuela Profesional de Ingeniería de Sistemas se encuentra implementada de manera correcta, pero no cuenta con una información disponible para la autenticidad de la red de acceso, para la protección de los datos de los usuarios.

- **Verificación de la documentación de la infraestructura física de la red.**

  Se solicitó la documentación de la infraestructura física de la red de datos, la respuesta fue un no, se nos entregó un informe de certificación del cableado estructurado del año 2014.

- **Verificación de la documentación de la infraestructura lógica de la red.**

  Se solicitó la documentación de la infraestructura lógica de la Red de Datos, la respuesta fue no, por lo cual se infiere que no cuenta ningún documento del funcionamiento lógico de la red de datos.

- **Verificación de la infraestructura física y lógica, si cumple con los estándares internacionales.**

  Al finalizar la evaluación de la instalación física, la distribución física de la red de datos, se puede determinar que la red de datos tiene una certificación del cableado estructurado del año 2014.

  Al finalizar la evaluación de la configuración lógica se determinó que no existe ningún tipo de configuración, por lo tanto, no existe ningún tipo de seguridad, así mismo no cumple con ningún tipo de estándar de calidad de servicio y autenticidad.

4.1.2. Fase de análisis

Listado de cada área con su respectiva cantidad de host que funcionan en EPIS y sus respectivas computadoras en que cuenta cada área, las cuales han sido considerados como objeto de estudio para la presente investigación.

Tabla 5: Número de hosts por áreas

ÁREAS escuela académico profesional de ingeniería de sistemas	Nº Host
Laboratorio de Tecnologías de la Información	23
Laboratorio de Ingeniería de Software	24
Laboratorio de Simulación	20
Laboratorio de Redes y Teleproceso	18
Sala de docentes	16
Área Administrativa	19
TOTAL	**120**

ESTRUCTURA LÓGICA ACTUAL DE LA RED DE DATOS DE LA EPIS

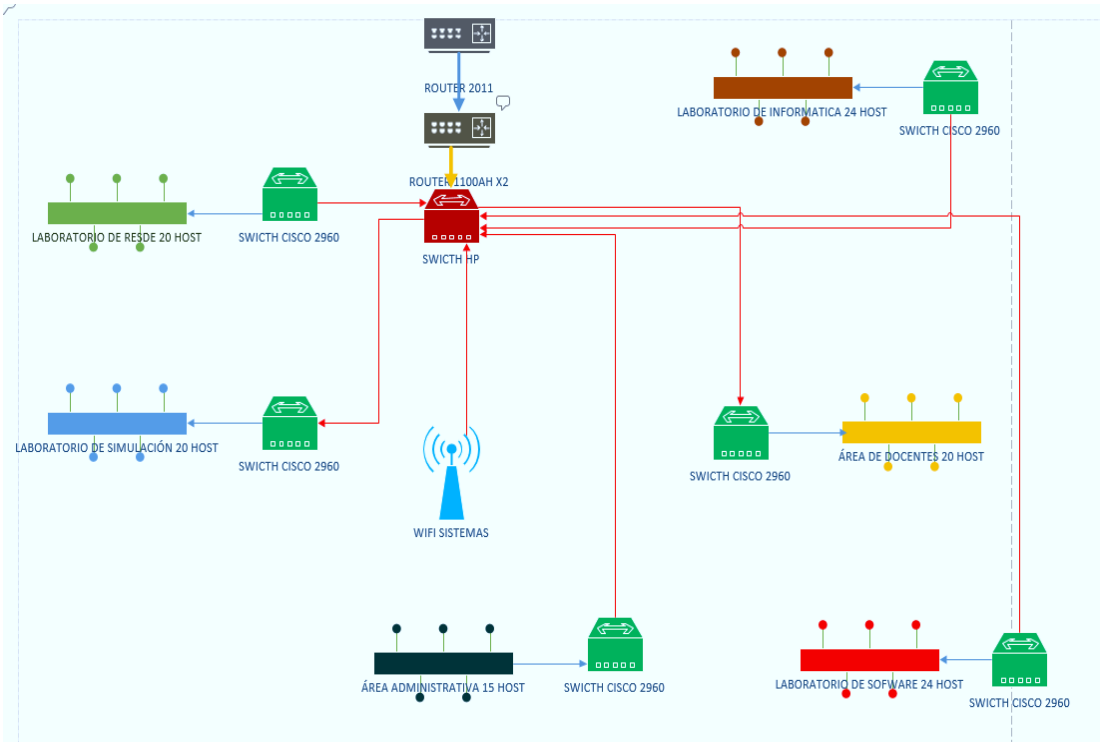

Figura 7: Estructura lógica de la RED de datos de la EPIS

❖ **Definiciones de Requerimientos**

- Diagnóstico de la infraestructura de red
- Diseño físico de la red WLAN
- Instalar Servidor Radius.
- Diseño Lógico de la Red WLAN
- Realizar el control de datos
- Autenticidad de datos de los usuarios
- Configuración de equipos.
- Pruebas

❖ **Descripciones de Flujos de datos, Simples y Compuestos.**

En la figura visualizamos los megabits que consumen los equipos de la EPIS, que en su totalidad son 120 computadoras. Este cálculo se realiza mediante el mismo dispositivo que utilizaremos, en este caso saldrá todo por la Ethernet 3 y nos indicará el consumo total de los megabits asignados.

En la actualidad la EPIS cuenta con 8 Megabits de velocidad que ofrece la empresa Cable Red.

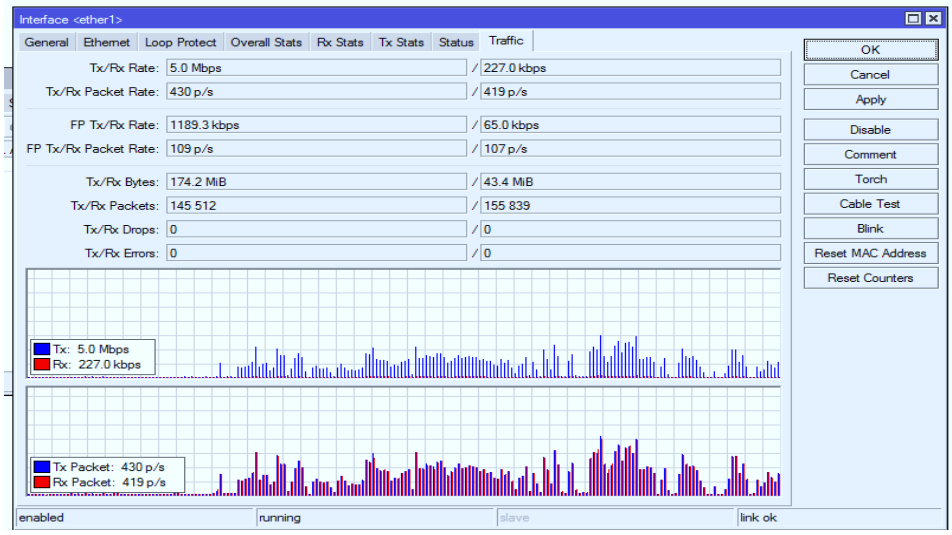

Figura 8: Consumo de la RED de datos de la EPIS

4.1.3. Definición de ubicación de host.

Para realizar este proceso logramos obtener la información actual de la EPIS, haciendo este funcionamiento tal y como está en los planos de ubicación de cada host, debemos prevalecer que en un inicio la EPIS instalo las computadoras según necesidad, se compró máquinas nuevas, tampoco existe una política del proceso de asignación de IP, de cada uno del host.

Como parte de este trabajo se elaboró los planos de ubicación de los hosts piso por piso, para obtener una muestra real de cómo se encuentra la infraestructura de red, como se muestra a continuación.

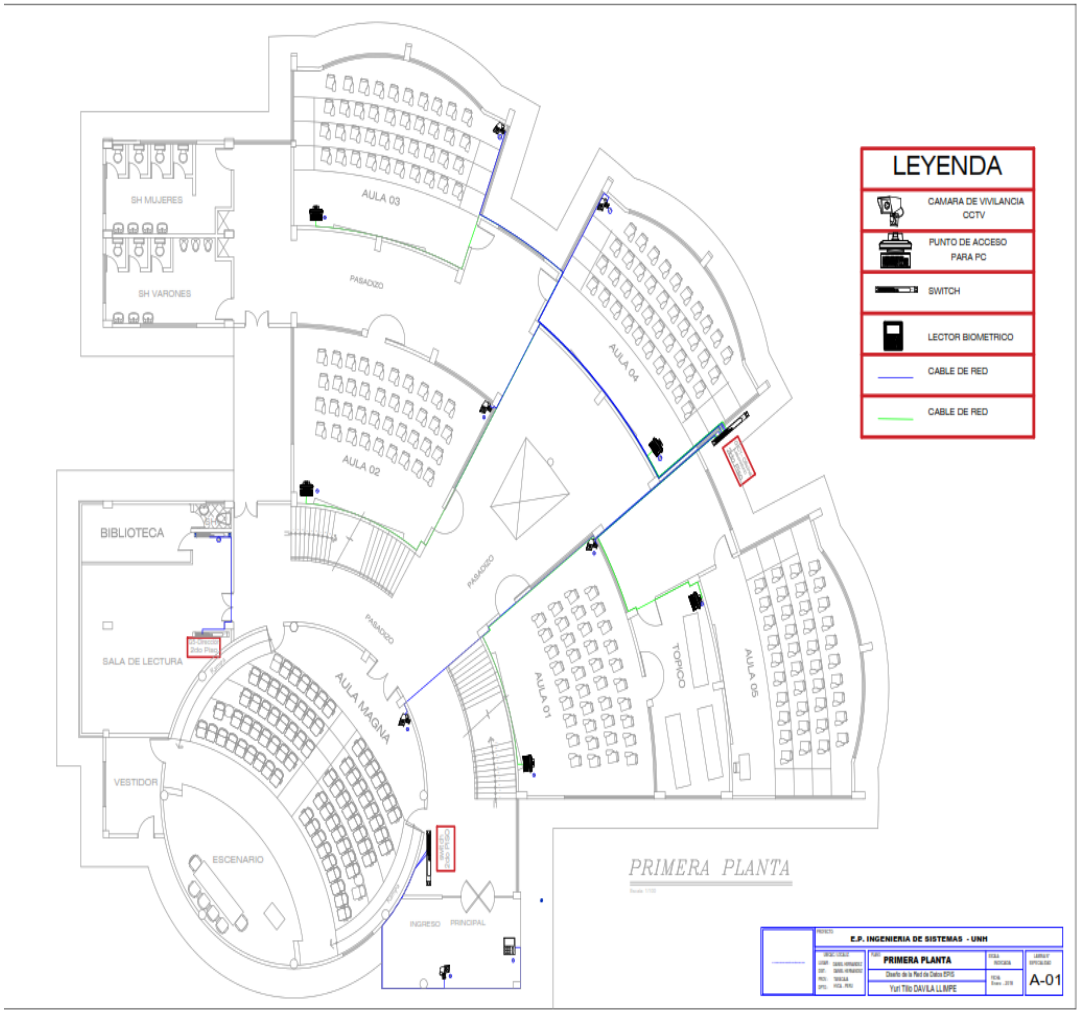

Figura 9: Diseño físico de la red, primera planta EPIS

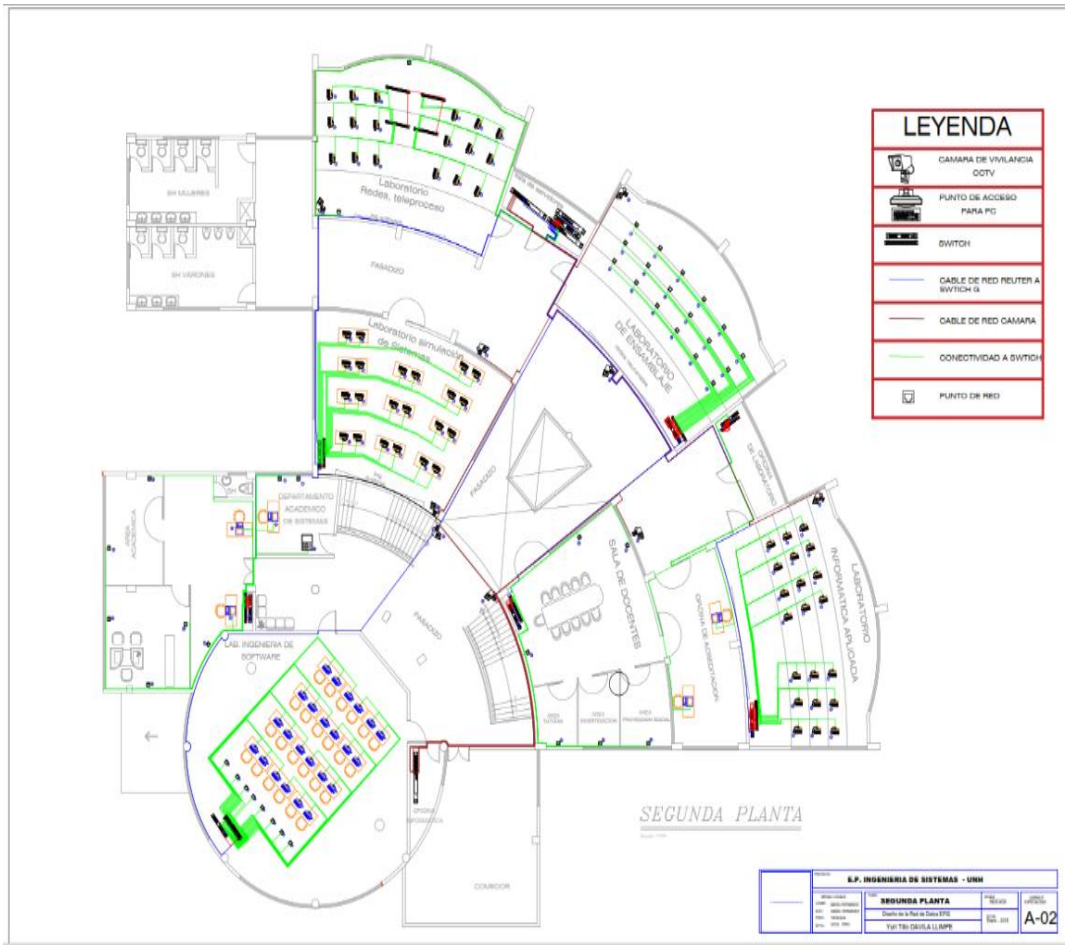

Figura 10: Diseño físico de la red, Segunda planta de la EPIS.

4.1.4. Fase de diseño

- **Diseño Físico de la red propuesta**

Tabla 6: Distribución de áreas de la EPIS

Áreas de la Escuela Profesional de Ingeniería de Sistemas	Nº de Host
Laboratorio de Tecnologías de la Información	23
Laboratorio de Ingeniería de Software	24
Laboratorio de Simulación	20
Laboratorio de Redes y Teleproceso	18
Sala de docentes	16
Área Administrativa	19
Red Inalámbrica	60
TOTAL	**180**

❖ **Diseño de red inalámbrico.**

Considerando que el acceso a la red inalámbrica es utilizado por los estudiantes que tienen sus laptops y hacen uso de ellas durante las labores académicas, y de acuerdo al último registro de los estudiantes que ingresan sus equipos al campus universitario son en promedio 50, se consideró habilitar una red inalámbrica para 60 hosts.

El total de host conectado a la red de acuerdo a los requerimientos de la EPIS es de 120 hosts estructurados más 60 hosts inalámbricos, todo ellos estarán conectados a la red de datos de la EPIS, que se tendrá una administración a través del Router y el Servidor Radius. Todos los hosts que se conectan de manera inalámbrica serán administrados bajo las reglas asignadas en el Servidor Radius.

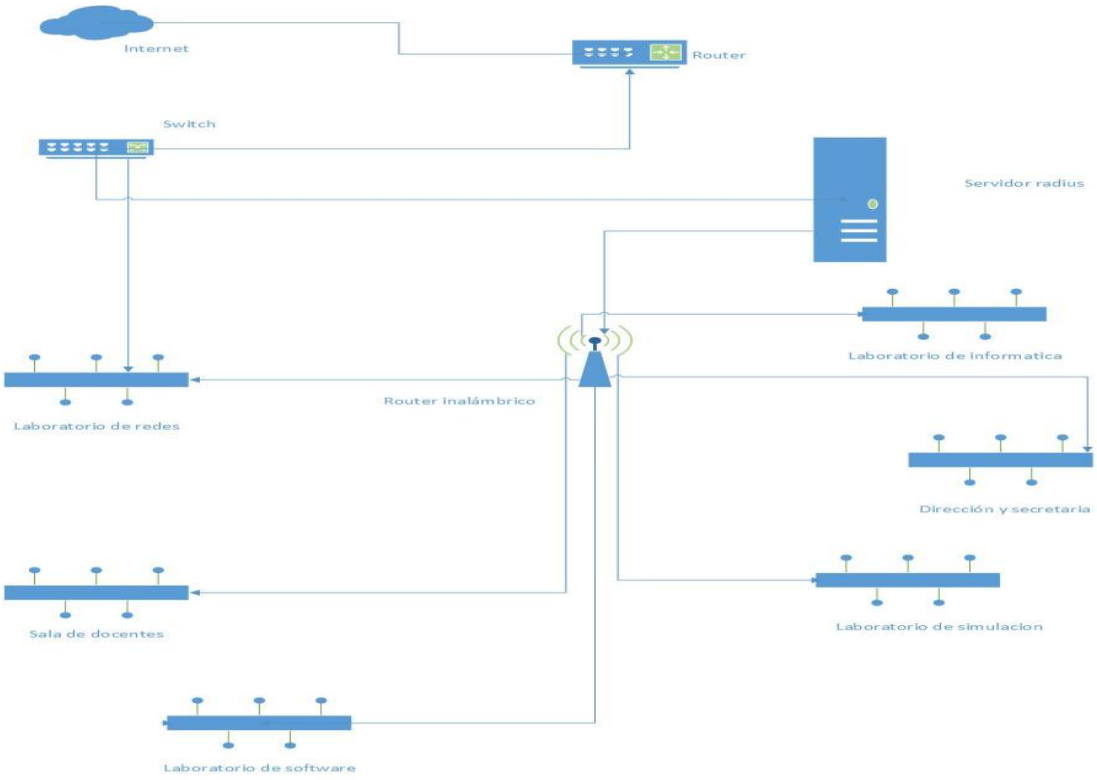

Figura 11: Diseño de red Wlan propuesto con Radius Server

4.1.5. Diseño lógico de la red propuesta

En la siguiente figura visualizamos claramente el diseño que ya está en funcionamiento en el programa Cisco Packet Tracer.

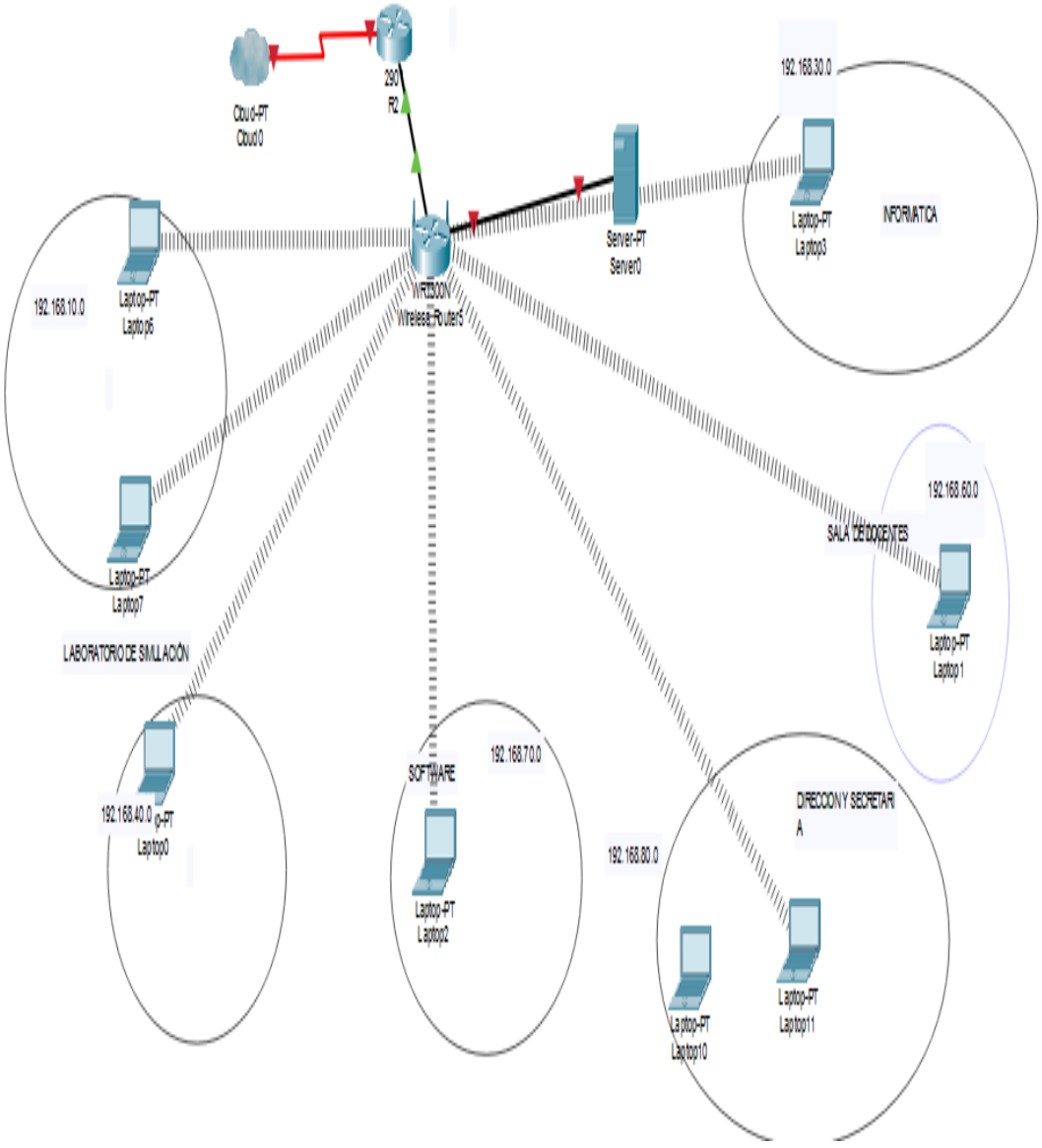

Figura 12: Diseño lógico de la red WLAN propuesta con Radius Server

- **Elección del equipo para poder realizar la administración con el Servidor Radius**

  Existen alternativas para poder utilizar servidores como Linux como sistema operativo, pero para la investigación se propone utilizar Windows

server 2016 Datacenter, y que nos provee las características para poder configurar clientes Radius, permitiendo agregar un gran número de clientes como puntos de acceso inalámbrico. Sin embargo, para poder instalar y usarlo es necesario contar con los requisitos mínimos de hardware.

- Procesador: 1.4Ghz de 64 bits
- RAM: 512 MB
- Espacio del disco: 32 GB
- Network: Gigabit (10/100/1000baseT) Ethernet adapter
- Optical Storage: DVD drive (if installing the OS from DVD media)

Este equipo es el más óptimo que se tiene y adecuado para poder administrar todos los Hosts de la EPIS.

- **Identificar y determinar el control de acceso de datos a la red de la EPIS y su implantación del Servidor Radius**

Se evaluó y se determinó que los servicios a implementar para el control de datos, se tuvo en cuenta ciertas reglas de restricción a los usuarios conectados de manera inalámbrica, considerando los siguientes ítems

- Privacidad al acceso a la red de datos de la EPIS
- Restricción a las páginas con el contenido no educativo
- Servidor de video vigilancia IP
- Control de acceso de datos al software académico autorizados por los docentes.
- Protección de datos de los usuarios.

4.1.6. Asignación de direcciones IP

De la misma manera para las demás WLAN

Tabla 7: Cuadro de asignación de Vlans

Nombre de la Red	ID VLAN	Área	Direcciones de Host disponibles	Dirección de Red	Mascara de Sub Red	Número de Host Posibles	Gateway	Rango de Ips
Redes	10	Lab. de Redes y Teleproceso	253	192.168.10 .0/24	255.255. 255.0	254	192.168. 10.1	(2-254)
Lab Informatica	30	Lab. de Tec. Informacion	253	192.168.30 .0/24	255.255. 255.0	254	192.168. 30.1	(2-254)
Lab Simulacion	40	Laboratorio de Simulación	253	192.168.40 .0/24	255.255. 255.0	254	192.168. 40.1	(2-254)
Wi Fi Sistemas	50	Campus Universitario Epis	253	192.168.50 .0/24	255.255. 255.0	254	192.168. 50.1	(2-254)
Docentes	60	Sala de Docentes	253	192.168.60 .0/24	255.255. 255.0	254	192.168. 60.1	(2-254)
Lab De Software	70	Laboratorio de Software	253	192.168.70 .0/24	255.255. 255.0	254	192168.7 0.1	(2-254)
Administrativo	80	Secretaria y Dirección	253	192.168.80 .0/24	255.255. 255.0	254	192.168. 80.1	(2-254)

Tabla 8: Cuadro de asignación para la Vlan 10

Nombre de la Red	ID VLAN	Área	Direcciones de Host disponibles	Nº de Maquina	Dirección de Red	Mascara de Sub Red	Gateway	IP/HOST
REDES	10	LAB. DE REDES Y TELEPROCESO	253	Maquina 01	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.2
				Maquina 02	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.3
				Maquina 03	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.4
				Maquina 04	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.5
				Maquina 05	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.6
				Maquina 06	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.7
				Maquina 07	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.8
				Maquina 08	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.9
				Maquina 09	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.10
				Maquina 10	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.11
				Maquina 11	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.12
				Maquina 12	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.13
				Maquina 13	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.14
				Maquina 14	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.15

				Maquina 15	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.16
				Maquina 16	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.17
				Maquina 17	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.18
				Maquina 18	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.19

Tabla 9: Cuadro de asignación para la WLAN 30 Redes Informática

Nombre de la Red	ID VLAN	Área	Direcciones de Host disponibles	Nº de Maquina	Dirección de Red	Mascara de Sub Red	Gateway	IP/HOST
INFORMATICA	30	LAB. TEC. INFORMACION	253	Maquina 01	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.2
				Maquina 02	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.3
				Maquina 03	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.4
				Maquina 04	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.5
				Maquina 05	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.6
				Maquina 06	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.7
				Maquina 07	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.8
				Maquina 08	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.9
				Maquina 09	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.10
				Maquina 10	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.11
				Maquina 11	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.12
				Maquina 12	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.13
				Maquina 13	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.14
				Maquina 14	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.15
				Maquina 15	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.16
				Maquina 16	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.17
				Maquina 17	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.18
				Maquina 18	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.19
				Maquina 19	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.20
				Maquina 20	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.21

				Maquina 21	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.22
				Maquina 22	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.23

Tabla 10: Cuadro de asignación para la WLAN 50 WI FI Sistemas

Nombre de la Red	ID VLAN	Área	Direcciones de Host disponibles	Nº de Maquina	Dirección de Red	Mascara de Sub Red	Gateway	IP/HOST
WIFI SISTEMAS	50	CAMPUS UNIVERSITARIO	253	WIFI-EPIS 01	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.2
				WIFI-EPIS 02	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.3
				WIFI-EPIS 03	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.4
				WIFI-EPIS 04	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.5
				WIFI-EPIS 05	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.6
				WIFI-EPIS 06	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.7
				WIFI-EPIS 07	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.8
				WIFI-EPIS 08	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.9
				WIFI-EPIS 09	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.10
				WIFI-EPIS 10	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.11
				…	…	…	…	…
				WIFI-EPIS 54	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.55
				WIFI-EPIS 55	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.56
				WIFI-EPIS 56	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.57
				WIFI-EPIS 57	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.58
				WIFI-EPIS 58	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.59
				WIFI-EPIS 59	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.60
				WIFI-EPIS 60	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.61

4.1.7. Asignación y configuración de los equipos de comunicación

Asignar un nombre a cada equipo a emplear (Router, switch, servidor radius.) dependiendo del servicio que brindará y al piso al cual estará asignado.

Tabla 10: Equipos de comunicación

Nº	ROUTER	NOMBRE
01	ROUTER GENERAL	ROUTER GENERICO
02	SERVIDOR RADIUS	RADIUS-EPIS

- **Asignación de switch**

Tabla 11: Designación de nombres a Switch

SWITCH	NOMBRE
SWITCH 1	switch_nucleo

Tabla 12: Designación de nombre al servidor

SERVIDOR	NOMBRE
SWITCH 1	Servidor radius

La configuración de los equipos de comunicación, tomando en cuenta los puntos anteriores se empezará con la creación de las WLANS. Primero en el router genérico, luego en el router wifi donde daremos el permiso para el servidor radius, luego en el servidor radius donde permitiremos la conexión de los equipos de cada área.

Creación y asignación de ID y nombre de la WLAN.

Configurando el router general, en la siguiente imagen se visualiza los códigos de configuración

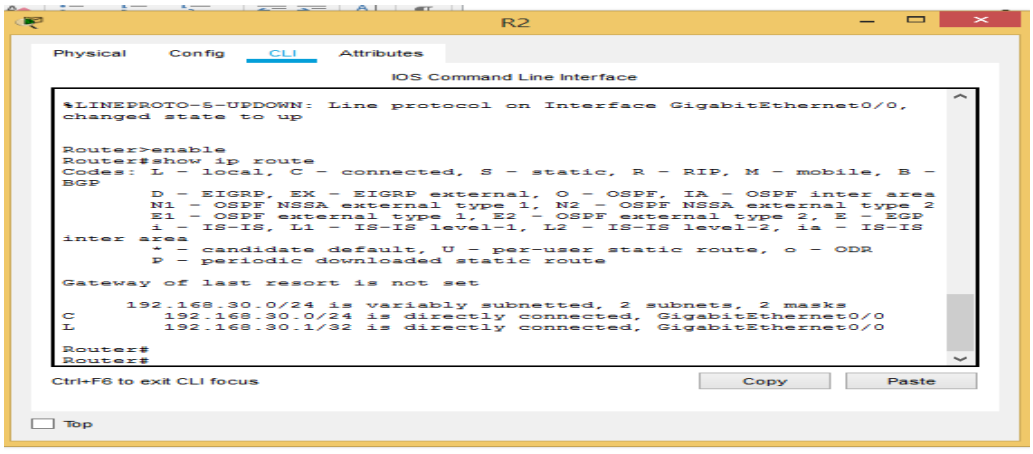

Figura 13: Configuración de router general

❖ **Configuración de servidor Radius**

Esta imagen muestra el número IP del servidor radius y la cantidad de host que van a acceder.

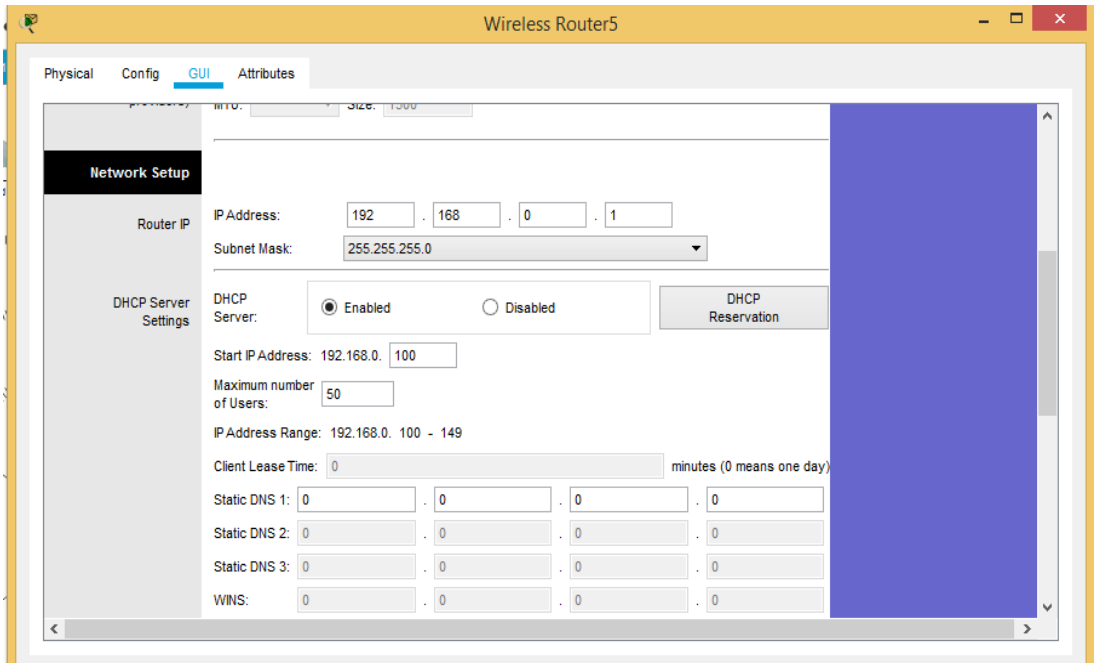

Figura 14: Configuración de router inalámbrico

En esta imagen visualizamos la dirección IP del servidor radius y la contraseña por la cual accederá los hosts.

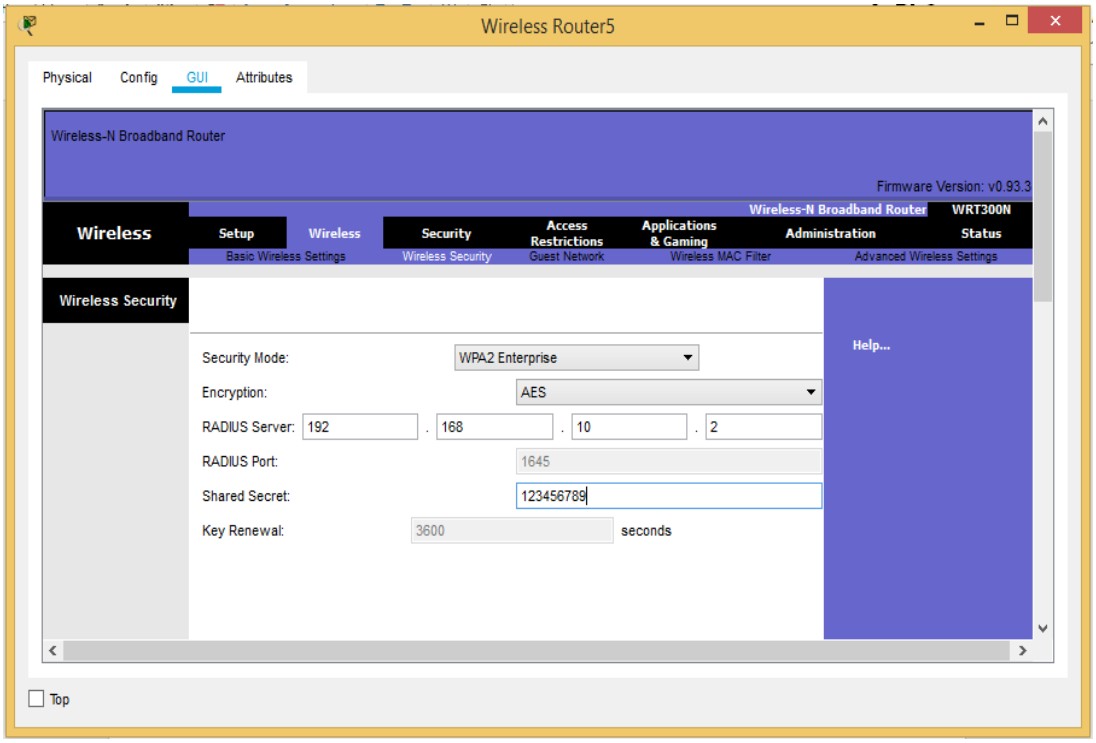

Figura 15: Asignación IP al router inalámbrico

❖ **Configuración del servidor radius**

En la siguiente imagen se visualiza la configuración del servidor radius, donde se asigna la dirección IP y los respectivos usuarios y contraseñas a las áreas.

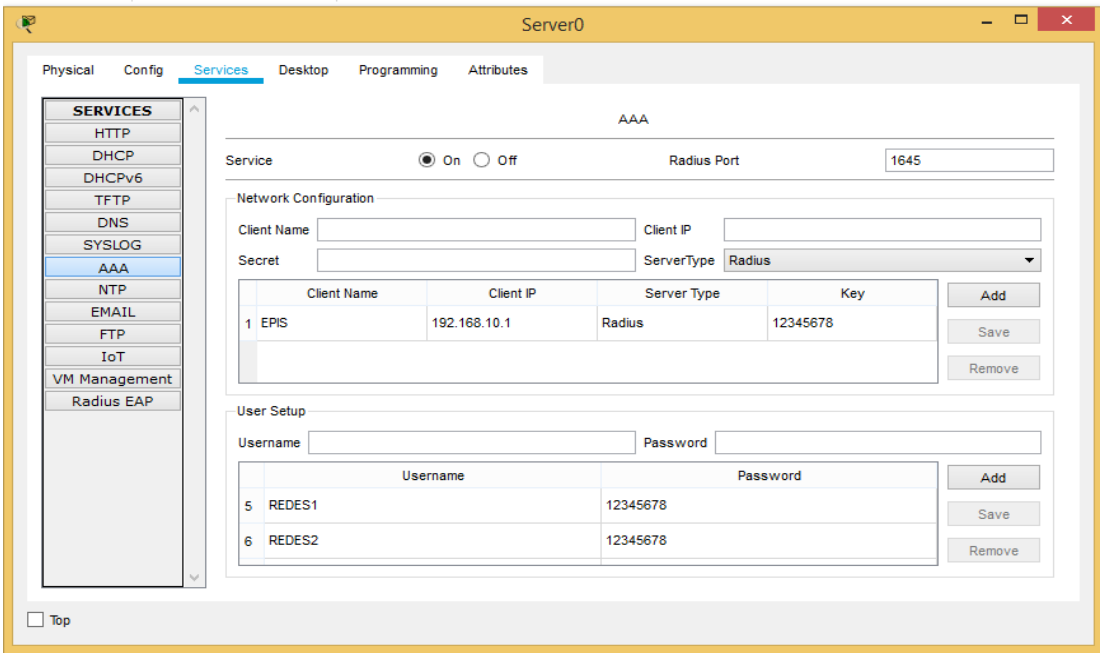

Figura 16: Configuración del servidor Radius

En esta imagen se visualiza la conexión de los equipos.

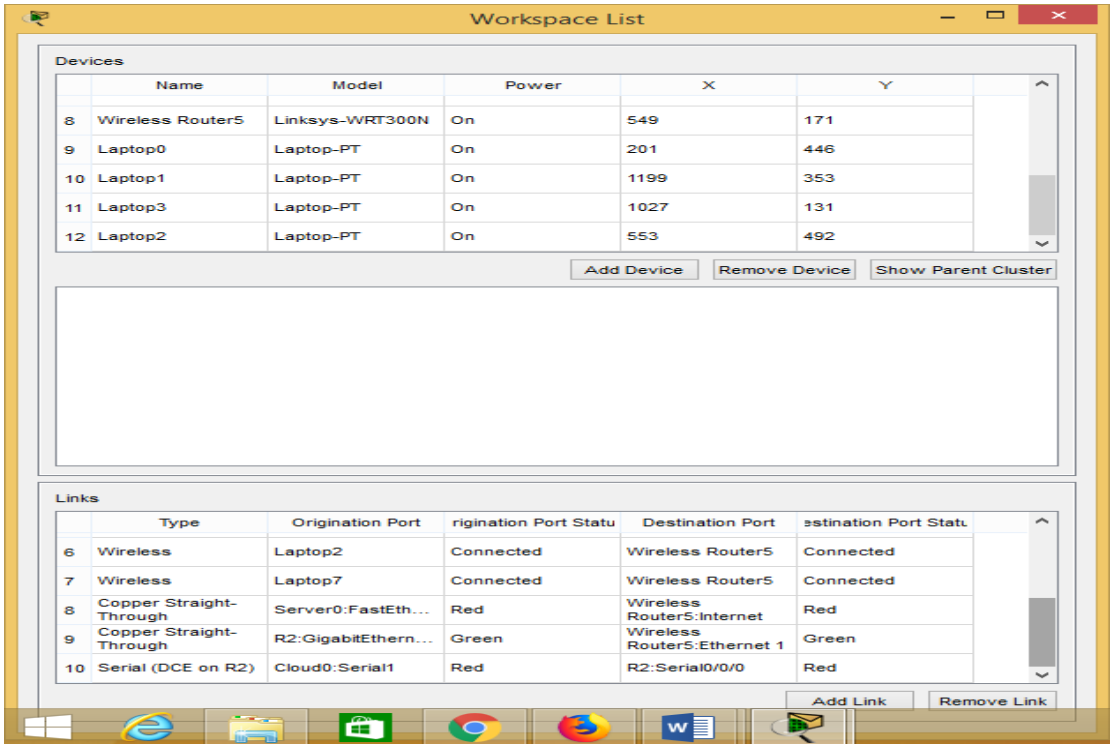

Figura 17: Visualización de los IPS conectados

Propuesta de diseño

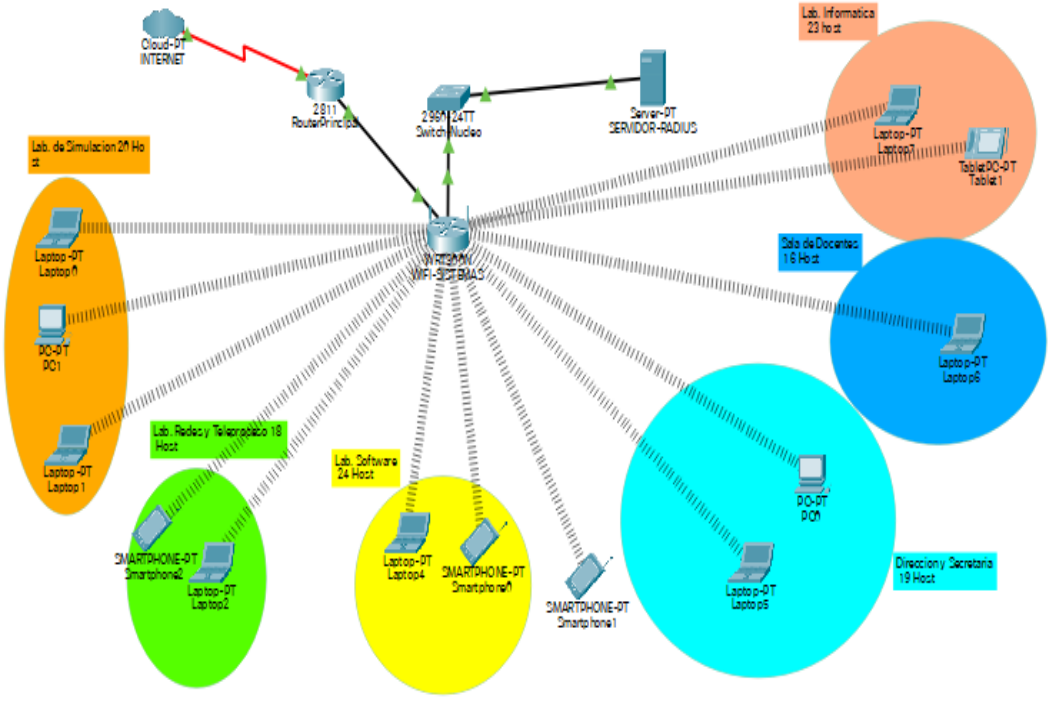

Figura 18: Propuesta del diseño

4.2. Presentación de resultados

En esta parte se muestran los resultados obtenidos según las fichas de observación, realizadas al host de la red de datos actual y al host propuestos con los servidores radius en el control de acceso de datos de la Escuela Profesional de Ingeniería de Sistemas.

4.2.1. Dimensión 1: Autentificación

- **Indicador 1.1: N°** hosts conectados a la red identificados**.**

➢ **Red sin servidor radius**

Tabla 13: N° hosts conectados a la red identificados- red sin servidor radius.

RED EVALUADA		Red sin servidor radius	
DIMENSION 1		Autenticación	
INDICADOR 1.1		N° hosts conectados a la red de identificados	
TIPO DE RED	N° host identificados red estructurada	N° Host inalambricos identificados	N° hosts conectados a la red de identificados
Red sin servidor radius	120	0	120

➢ **Red con servidor radius**

Tabla 14: N° hosts conectados a la red identificados - red con servidor radius

RED EVALUADA		Red con Servidor Radius	
DIMENSION 1		Autenticación	
INDICADOR 1.1		N° hosts conectados a la red de identificados	
TIPO DE RED	N° hosts identificados red estructurada	N° Host inalambricos identificados	N° hosts conectados a la red de identificados
Red con Servidor Radius	120	60	180

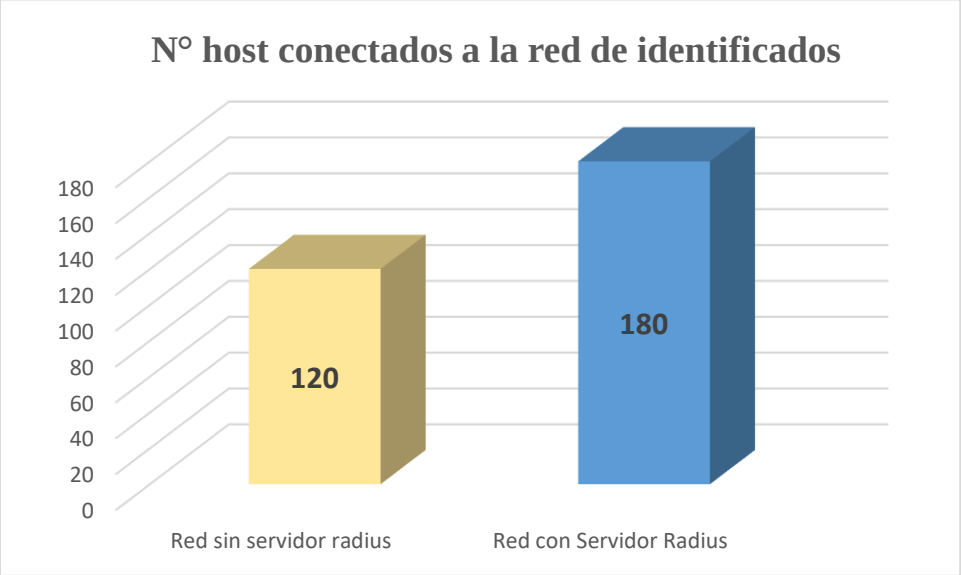

Figura 19: Número de host conectados a la red identificados

Interpretación

De acuerdo a las tablas 14 y 15, podemos observar que el número de hosts identificados en la red sin servidor radius, es 120 hosts, que son las que pertenecen a la red cableada, el número de host identificados en la red con servidor radius, es de 180 hosts que incluye a la red inalámbrica, por lo que podemos inferir que la red con servidor radius identifica todos los hosts conectados a la red, sea estructurada y/o inalámbrica, representando en este caso un 33.33% más de host identificados en la red.

4.2.2. Dimensión 2: Disponibilidad

- **Indicador 2.1:** Latencia de red.

  - **Red sin servidor radius**

Tabla 15: Evaluación de la red sin Servidor Radius –Indicador Latencia de red

Item	**RED EVALUADA**	**Red sin servidor radius**
	DIMENSION 2	**Disponibilidad**
	INDICADOR 2.1	**Latencia de Red**
	Nombre del host	Latencia de red promedio en milisegundos

1	R- Máquina 01	1200
2	R- Máquina 02	1300
3	R- Máquina 03	1550
4	R- Máquina 04	1723
5	R- Máquina 05	1883
6	R- Máquina 06	1760
7	R- Máquina 07	1700
8	R- Máquina 08	1754
9	R- Máquina 09	1600
10	R- Máquina 10	1750
11	R- Máquina 11	1953
12	R- Máquina 12	2125
13	R- Máquina 13	2254
14	R- Máquina 14	2156
15	R- Máquina 15	2130
16	R- Máquina 16	2101
17	R- Máquina 17	1430
18	R- Máquina 18	1565
19	TI- Máquina 01	1758
20	TI- Máquina 02	1943
21	TI- Máquina 03	2078
22	TI- Máquina 04	1949
23	TI- Máquina 05	1974
24	TI- Máquina 06	1957
25	TI- Máquina 07	1802
26	TI- Máquina 08	1952
27	TI- Máquina 09	2108
28	TI- Máquina 10	2312
29	TI- Máquina 11	2525
30	TI- Máquina 12	2326
31	TI- Máquina 13	2320
32	TI- Máquina 14	2300
33	TI- Máquina 15	1723
34	TI- Máquina 16	1883
35	TI- Máquina 17	1760
36	TI- Máquina 18	1700
37	TI- Máquina 19	1754
38	TI- Máquina 20	1600
39	TI- Máquina 21	1750
40	TI- Máquina 22	1953

41	TI- Máquina 23	2125
42	IS- Máquina 01	2254
43	IS- Máquina 02	2156
44	IS- Máquina 03	2130
45	IS- Máquina 04	2101
46	IS- Máquina 05	1430
47	IS- Máquina 06	1565
48	IS- Máquina 07	1758
49	IS- Máquina 08	1943
50	IS- Máquina 09	2078
51	IS- Máquina 10	1949
52	IS- Máquina 11	1974
53	IS- Máquina 12	1957
54	IS- Máquina 13	1802
55	IS- Máquina 14	1952
56	IS- Máquina 15	2108
57	IS- Máquina 16	2312
58	IS- Máquina 17	2525
59	IS- Máquina 18	2326
60	IS- Máquina 19	1723
61	IS- Máquina 20	1883
62	IS- Máquina 21	1760
63	IS- Máquina 22	1700
64	IS- Máquina 23	1754
65	IS- Máquina 24	1600
66	SIM- Máquina 01	1750
67	SIM- Máquina 02	1953
68	SIM- Máquina 03	2125
69	SIM- Máquina 04	2254
70	SIM- Máquina 05	2156
71	SIM- Máquina 06	2130
72	SIM- Máquina 07	2101
73	SIM- Máquina 08	1430
74	SIM- Máquina 09	1565
75	SIM- Máquina 10	1758
76	SIM- Máquina 11	1943
77	SIM- Máquina 12	2078
78	SIM- Máquina 13	1949
79	SIM- Máquina 14	1974
80	SIM- Máquina 15	1957

81	SIM- Máquina 16	1802
82	SIM- Máquina 17	1952
83	SIM- Máquina 18	2108
84	SIM- Máquina 19	2312
85	SIM- Máquina 20	2525
86	D- Máquina 01	2326
87	D- Máquina 02	1565
88	D- Máquina 03	1758
89	D- Máquina 04	1943
90	D- Máquina 05	2078
91	D- Máquina 06	1949
92	D- Máquina 07	1974
93	D- Máquina 08	1957
94	D- Máquina 09	1802
95	D- Máquina 10	1952
96	D- Máquina 11	2108
97	D- Máquina 12	2312
98	D- Máquina 13	2525
99	D- Máquina 14	2326
100	D- Máquina 15	2320
101	D- Máquina 16	2300
102	Adm- Máquina 01	1723
103	Adm- Máquina 02	1883
104	Adm- Máquina 03	1760
105	Adm- Máquina 04	1700
106	Adm- Máquina 05	1754
107	Adm- Máquina 06	1600
108	Adm- Máquina 07	1750
109	Adm- Máquina 08	1953
110	Adm- Máquina 09	2125
111	Adm- Máquina 10	2254
112	Adm- Máquina 11	2156
113	Adm- Máquina 12	2130
114	Adm- Máquina 13	2101
115	Adm- Máquina 14	1430
116	Adm- Máquina 15	1565
117	Adm- Máquina 16	1758
118	Adm- Máquina 17	1943
119	Adm- Máquina 18	2078
120	Adm- Máquina 19	1949

Promedio	**1940.46**

- **Red con servidor radius**

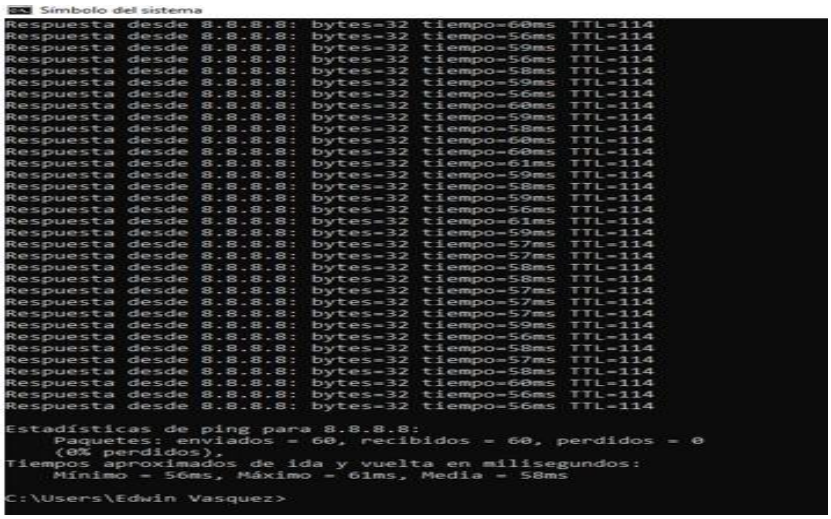

Figura 20: Tiempos de respuesta del servidor radius

Tabla 16: Red con servidor radius – indicador latencia de red

Item	**RED EVALUADA**	**Red con Servidor Radius**
	DIMENSION 1	**Disponibilidad**
	INDICADOR 1.1	**Latencia de Red**
	Nombre del host	latencia de red promedio en milisegundos
1	R- Máquina 01	520
2	R- Máquina 02	620
3	R- Máquina 03	870
4	R- Máquina 04	1043
5	R- Máquina 05	1203
6	R- Máquina 06	1080
7	R- Máquina 07	1020
8	R- Máquina 08	1074
9	R- Máquina 09	920
10	R- Máquina 10	1070
11	R- Máquina 11	1273
12	R- Máquina 12	1445
13	R- Máquina 13	1574
14	R- Máquina 14	1476
15	R- Máquina 15	1450
16	R- Máquina 16	1421
17	R- Máquina 17	750
18	R- Máquina 18	885

19	TI- Máquina 01	1078
20	TI- Máquina 02	1263
21	TI- Máquina 03	1398
22	TI- Máquina 04	1269
23	TI- Máquina 05	1294
24	TI- Máquina 06	1277
25	TI- Máquina 07	1122
26	TI- Máquina 08	1272
27	TI- Máquina 09	1428
28	TI- Máquina 10	1632
29	TI- Máquina 11	1845
30	TI- Máquina 12	1646
31	TI- Máquina 13	1640
32	TI- Máquina 14	1620
33	TI- Máquina 15	1043
34	TI- Máquina 16	1203
35	TI- Máquina 17	1080
36	TI- Máquina 18	1020
37	TI- Máquina 19	1074
38	TI- Máquina 20	920
39	TI- Máquina 21	1070
40	TI- Máquina 22	1273
41	TI- Máquina 23	1445
42	IS- Máquina 01	1574
43	IS- Máquina 02	1476
44	IS- Máquina 03	1450
45	IS- Máquina 04	1421
46	IS- Máquina 05	750
47	IS- Máquina 06	885
48	IS- Máquina 07	1078
49	IS- Máquina 08	1263
50	IS- Máquina 09	1398
51	IS- Máquina 10	1269
52	IS- Máquina 11	1294
53	IS- Máquina 12	1277
54	IS- Máquina 13	1122
55	IS- Máquina 14	1272
56	IS- Máquina 15	1428
57	IS- Máquina 16	1632
58	IS- Máquina 17	1845

59	IS- Máquina 18	1646
60	IS- Máquina 19	1043
61	IS- Máquina 20	1203
62	IS- Máquina 21	1080
63	IS- Máquina 22	1020
64	IS- Máquina 23	1074
65	IS- Máquina 24	920
66	SIM- Máquina 01	1070
67	SIM- Máquina 02	1273
68	SIM- Máquina 03	1445
69	SIM- Máquina 04	1574
70	SIM- Máquina 05	1476
71	SIM- Máquina 06	1450
72	SIM- Máquina 07	1421
73	SIM- Máquina 08	750
74	SIM- Máquina 09	885
75	SIM- Máquina 10	1078
76	SIM- Máquina 11	1263
77	SIM- Máquina 12	1398
78	SIM- Máquina 13	1269
79	SIM- Máquina 14	1294
80	SIM- Máquina 15	1277
81	SIM- Máquina 16	1122
82	SIM- Máquina 17	1272
83	SIM- Máquina 18	1428
84	SIM- Máquina 19	1632
85	SIM- Máquina 20	1845
86	D- Máquina 01	1646
87	D- Máquina 02	885
88	D- Máquina 03	1078
89	D- Máquina 04	1263
90	D- Máquina 05	1398
91	D- Máquina 06	1269
92	D- Máquina 07	1294
93	D- Máquina 08	1277
94	D- Máquina 09	1122
95	D- Máquina 10	1272
96	D- Máquina 11	1428
97	D- Máquina 12	1632
98	D- Máquina 13	1845

99	D- Máquina 14	1646
100	D- Máquina 15	1640
101	D- Máquina 16	1620
102	Adm- Máquina 01	1043
103	Adm- Máquina 02	1203
104	Adm- Máquina 03	1080
105	Adm- Máquina 04	1020
106	Adm- Máquina 05	1074
107	Adm- Máquina 06	920
108	Adm- Máquina 07	1070
109	Adm- Máquina 08	1273
110	Adm- Máquina 09	1445
111	Adm- Máquina 10	1574
112	Adm- Máquina 11	1476
113	Adm- Máquina 12	1450
114	Adm- Máquina 13	1421
115	Adm- Máquina 14	750
116	Adm- Máquina 15	885
117	Adm- Máquina 16	1078
118	Adm- Máquina 17	1263
119	Adm- Máquina 18	1398
120	Adm- Máquina 19	1580
121	WIFI-EPIS 01	1592
122	WIFI-EPIS 02	1748
123	WIFI-EPIS 03	1952
124	WIFI-EPIS 04	2165
125	WIFI-EPIS 05	1966
126	WIFI-EPIS 06	1363
127	WIFI-EPIS 07	1523
128	WIFI-EPIS 08	1400
129	WIFI-EPIS 09	1340
130	WIFI-EPIS 10	1394
131	WIFI-EPIS 11	1240
132	WIFI-EPIS 12	1390
133	WIFI-EPIS 13	1593
134	WIFI-EPIS 14	1765
135	WIFI-EPIS 15	1894
136	WIFI-EPIS 16	1796
137	WIFI-EPIS 17	1770
138	WIFI-EPIS 18	1741

139	WIFI-EPIS 19	1070
140	WIFI-EPIS 20	1205
141	WIFI-EPIS 21	1398
142	WIFI-EPIS 22	1583
143	WIFI-EPIS 23	1718
144	WIFI-EPIS 24	1589
145	WIFI-EPIS 25	1614
146	WIFI-EPIS 26	1597
147	WIFI-EPIS 27	1442
148	WIFI-EPIS 28	1592
149	WIFI-EPIS 29	1748
150	WIFI-EPIS 30	1952
151	WIFI-EPIS 31	2165
152	WIFI-EPIS 32	1966
153	WIFI-EPIS 33	1205
154	WIFI-EPIS 34	1398
155	WIFI-EPIS 35	1583
156	WIFI-EPIS 36	1718
157	WIFI-EPIS 37	1589
158	WIFI-EPIS 38	1614
159	WIFI-EPIS 39	1597
160	WIFI-EPIS 40	1442
161	WIFI-EPIS 41	1597
162	WIFI-EPIS 42	1442
163	WIFI-EPIS 43	1592
164	WIFI-EPIS 44	1748
165	WIFI-EPIS 45	1952
166	WIFI-EPIS 46	2165
167	WIFI-EPIS 47	1966
168	WIFI-EPIS 48	1205
169	WIFI-EPIS 49	1398
170	WIFI-EPIS 50	1583
171	WIFI-EPIS 51	1718
172	WIFI-EPIS 52	1589
173	WIFI-EPIS 53	1614
174	WIFI-EPIS 54	1597
175	WIFI-EPIS 55	1442
176	WIFI-EPIS 56	1614
177	WIFI-EPIS 57	1597
178	WIFI-EPIS 58	1442

179	WIFI-EPIS 59	1614
180	WIFI-EPIS 60	1786
Promedio		**1381.36**

- **Resumen**

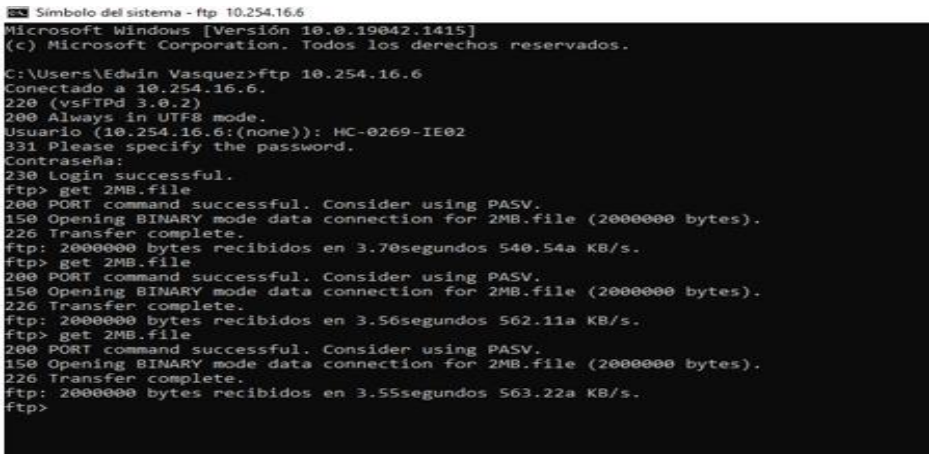

Figura 21: Información resumen del servidor radius

Tabla 17: Comparación de latencia de red en milisegundos

Descripción	latencia de red promedio en milisegundos
Red sin servidor radius	1940.46
Red con Servidor Radius	1381.36

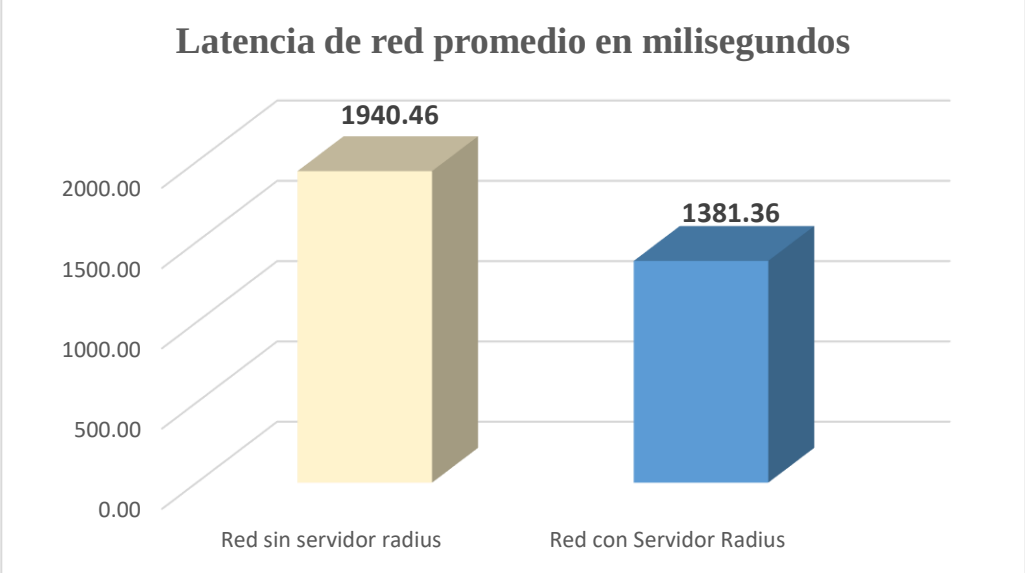

Figura 22: Comparación latencia de red promedio en milisegundos

Interpretación

De acuerdo a la figura mostrada en la parte superior, podemos observar que la latencia promedio de red disminuyó de 1940.46 milisegundos con la red sin servidor radius, a 1381.36 milisegundos con la red con servidor radius, disminuyendo el tiempo de latencia de red (retardo) de 559.10 milisegundos, considerando que la red con servidor tiene 60 hosts más de la red wifi implementada.

4.3. Prueba de hipótesis

4.3.2. Hipótesis General

a= N° hosts conectados a la red identificados en la red sin servidor radius

b = N° hosts conectados a la red identificados en la red con servidor radius

4.3.3. Hipótesis Nula:

El N° hosts conectados a la red identificados en la red sin servidor radius es mayor o igual que el N° hosts conectados a la red identificados en la red con servidor radius.

Ho = a>= **b**

Hipótesis Alterna:

El N° hosts conectados a la red identificados en la red sin servidor radius es menor que el N° hosts conectados a la red identificados en la red con servidor radius.

H1 = a<b

- **Definir el valor de alfa (α)**

  Alfa =α= 0.05 = 5%

- **Elección de la prueba estadística**

Se elige la prueba de **T Student,** para muestras relacionadas, por ser un estudio dimensional con medidas del antes y después, además de trabajar con variables numéricas.

- **Calcular el P – Valor = Prueba de Normalidad.**

NORMALIDAD:

KOLMOGOROV-SMIRNOV (>100 Host)

Criterios para determinar la Normalidad:

P valor => **α** Aceptar Ho = Los datos son de una distribución **normal**

P valor < **α** Aceptar H1 = Los datos NO provienen de una distribución **normal.**

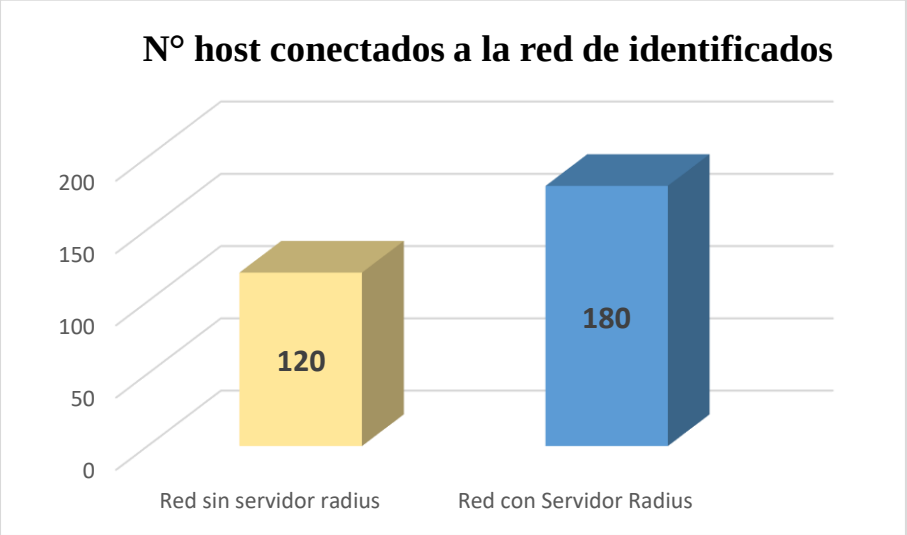

Figura 23: Número de host conectados a la red identificados

Tabla 18: Prueba de normalidad – Número de host conectados

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
N° hosts conectados a la red identificados en la red sin servidor radius	,188	20	,054	,916	20	,062

N° hosts conectados a la red identificados en la red con servidor radius	,128	20	,186*	,952	20	,091
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Como podemos observar el Pvalor:

Tabla 19: Analizando P valor

NORMALIDAD		
P valor (a)=0,062	>	**α** =0.05
P-valor (b)=0,091	>	**α** =0.05
Conclusión: Los datos provienen de una distribución normal		

De acuerdo a los datos obtenidos, se puede evidenciar que el número de hosts conectados a la red identificados sin servidor radius, es menor que número de hosts conectados a la red identificados con servidor radius, por lo que descartamos la Hipótesis Nula y Aceptamos la Hipótesis alterna.

4.3.4. Dimensión 1: Autentificación

a) Indicador 1.1: % de usuarios conectados de manera inalámbrica con acceso permitidos

Hipótesis

a= % de usuarios conectados de manera inalámbrica con acceso permitidos en la red sin servidor radius

b = % de usuarios conectados de manera inalámbrica con acceso permitidos en la red con servidor radius

Hipótesis Nula:

% de usuarios conectados de manera inalámbrica con acceso permitidos en la red sin servidor radius es mayor al % de usuarios

conectados de manera inalámbrica con acceso permitidos en la red con servidor radius.

Ho = a> **b**

Hipótesis Alterna:

% de usuarios conectados de manera inalámbrica con acceso permitidos en la red sin servidor radius, es menor al % de usuarios conectados de manera inalámbrica con acceso permitidos en la red con servidor radius.

H1 = a<b

Como se muestra en la Tabla 14 y Tabla 15, al utilizar el Servidor Radius, se logra identificar a todos los hosts que están conectados en la red, ya sea a través de cable o con conexión inalámbrica, es decir de 120 hosts que se reconocían inicialmente, con el uso del servidor radius pasó a reconocer 180 hosts, incrementándose en un 33.3% la detección de los hosts inalámbricos conectados a la red, por lo que se acepta la hipótesis alterna.

4.3.5. Dimensión 2: Disponibilidad

4.3.2.1. Indicador 2.1: Latencia de red

- **Redacción de Hipótesis.**

Ulrssr= Promedio de latencia de red, en la red sin servidor radius

Ulrcsr= Promedio de latencia de red, en la red con servidor radius

Hipótesis Nula:

El Promedio de latencia de red, en la red sin servidor, es menor o igual que el Promedio de latencia de red, en la red con servidor radius.

Ho = Ulrssr <= Ulrcsr

Hipótesis Alterna:

El Promedio de latencia de red, en la red sin servidor, es mayor que el Promedio de latencia de red en la red con servidor radius.

Ho = Ulrssr > Ulrcsr

Tabla 20: Pruebas de normalidad – Latencia de red

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Promedio de latencia de red en la red sin servidor radius	,196	20	,042	,906	20	,054
Promedio de latencia de red en la red con servidor radius.	,146	20	,200*	,931	20	,163
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Como podemos observar el Pvalor:

Tabla 21: P valor - Latencia de red

NORMALIDAD		
P valor (**Ulrssr**)=0,054	>	**α** =0.05
P-valor (**Ulrcsr**)=0,163	>	**α** =0.05
Conclusión: Los datos provienen de una distribución normal		

Paso N° 05: Decisión Estadística

Tabla 22: Estadísticas de muestras emparejadas – Latencia de red

Estadísticas de muestras emparejadas					
		Media	N	Desviación estándar	Media de error estándar
Par 1	Promedio de latencia de red en la red sin servidor radius	80,45	20	6,353	1,421

	Promedio de latencia de red en la red con servidor radius..	87,05	20	5,689	1,272

Tabla 23: Correlación de muestras emparejadas – Latencia de red

Correlaciones de muestras emparejadas				
		N	Correlación	Sig.
Par 1	Promedio de latencia de red en la red con servidor radius	120	,117	,622

Tabla 24: Prueba de muestras emparejadas – Latencia de red

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Promedio de latencia de red en la red sin servidor radius Promedio de latencia de red en la red con servidor radius.	-6,600	8,016	1,792	-10,351	-2,849	-3,682	19	,002

- Pvalor=0.002
- Pvalor<0.05 se rechaza la hipótesis nula.
- Rechazamos la hipótesis nula Ho y aceptamos la hipótesis alterna H1

El Promedio de latencia de red sin servidor, es mayor que el Promedio de latencia de red con servidor radius.

4.4. Discusión de resultados

De los resultados obtenidos, concluimos que los Servidores Radius en el control de Acceso a la Red Inalámbrica:

- ✓ Respecto a la dimensión, Accesibilidad de la red de datos se tiene el siguiente resultado:
  - Tiempos de respuesta de control de accesibilidad de los usuarios en el nivel WAN de la red, se mejoró de 78 milisegundos de la red actual a 40 milisegundos con los Servidores Radius en el control de Acceso a la red de datos.
  - Tiempo de respuesta de control de accesibilidad de los usuarios en el nivel WLAN de la red, se mejoró de 78 milisegundos de la red actual, a 17 milisegundos con los Servidores Radius en el control de Acceso a la Red de datos.
- ✓ Respecto a la dimensión, Autentificación en la red de datos, en los indicadores se tiene el resultado siguiente:
  - El % de éxito de autenticación de los usuarios de WLAN a WAN, a servicios autorizados, mejoro de 80% de la red actual a 87% con los Servidores Radius en el control de Acceso a la red inalámbrica.
  - Petición de autenticación de los usuarios WLAN a WAN a servicios no autorizados, disminuyo de 88% de la red actual a 9% con los Servidores Radius en el control de Acceso a la red inalámbrica.
  - Petición de autenticación de los usuarios de WAN a WLAN a servicios autorizados, mejoro de 87% de la red actual a 95% con los Servidores Radius en el control de Acceso a la red inalámbrica.

- Petición de autenticación de los usuarios de WAN a WLAN a servicios no autorizados, disminuyo de 89% de la red actual a 2% con los Servidores Radius en el control de Acceso a la red inalámbrica.

Entonces, de acuerdo a la prueba de hipótesis 1, podemos decir con los Servidores Radius en el control de Acceso a la Red Inalámbrica, mejora la autenticación de la información en la red de datos de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.

De acuerdo a la prueba de hipótesis 2, podemos decir que los Servidores Radius en el control de Acceso a la red inalámbrica, mejora la Prevención de ataques y denegación de servicios en la red de datos de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica. Por ende, por ser estas dos dimensiones de la Variable Disponibilidad de información, podemos decir que los Servidores Radius en el control de Acceso a la red inalámbrica, mejora la autenticación, control y confidencialidad de la información en la red Inalámbrica de La Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.

CONCLUSIONES

1) Hecho el análisis de la infraestructura de red de datos de la EPIS, se detectaron ingresos no autorizados, para cubrir estas necesidades se propone implementar mecanismos de seguridad como la autorización, autenticación de la red, los cuales favorecerán para que los recursos de la red sean utilizados de una forma correcta.
2) Para una mejor seguridad de los activos de la EPIS, se sugiere implementar mecanismos de autenticación, esto permitirá que los usuarios ingresen con usuario y contraseña a la red.
3) Finalizando este proyecto de investigación, llegamos a implementar el Servidor Radius para el control de acceso a la red inalámbrica en el campus universitario de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.

RECOMENDACIONES

1) Implementar controles de seguridad, involucra que los dispositivos de comunicación tengan que soportar o tengan esas características en la implementación de la misma para un mejor uso de los usuarios.
2) Implementar subredes ha permitido contar con una mejor administración de las direcciones IP y su posterior configuración, se podría considerar otras técnicas para tener una mejor administración en las direcciones IP.
3) Implementar políticas de seguridad, y que en ella estipule que la red sea monitoreada de manera constante, y que todo el personal de la EPIS tenga conocimiento sobre la importancia de los procesos que se llevan a cabo para tenerlo segura.

REFERENCIAS BIBLIOGRÁFICAS

aceproject.org. (2014). Recuperado el 23 de 08 de 2017, de http://aceproject.org: http://aceproject.org/main/espanol/et/ete03.htm

Alexandra, C. V. (2015). *Desarrollo de procedimientos para un modelo de gestion de fallas de la red para la plataforma isp de la cnt ep.* ecuador.

Anrango, R. (2014). Recuperado el 24 de 08 de 2017, de Definicion de terminos Mikrotik: http://configurarmikrotikwireless.com/blog/conceptos-winbox-routeros-mikrotik.html

Apablaza, F. (2012). *Calidad de servicio de telecomunicaciones.*

Arias, F. G. (2006). *El Proyecto de investigación.* Venezuela: Episteme.

Asadovay Lema, G. S., & Caiza Ortiz, L. M. (2013). *"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".* Ecuador.

Avalos Reyes, Y. G., & Romero Palacios, R. J. (2018). *Rediseño de la Interconexión de Datos de la Red de Área Local Inalámbrica (WLAN) del Campus – Los Pinos, la Facultad de Educación y Humanidades y la Facultad De Medicina Humana de la Universidad San Pedro.* Universidad San Pedro, Chimbote.

Blas Rinza, J. F. (2017). *Seguridad y control del acceso a las redes inalámbricas en la UNSM-T mediante servidores de autenticación radius con el uso de certificados digitales (Pregrado).* Universidad nacional de San Martín - T, Tarapoto.

Castrejon . (2013). *"Analisis, diseño e implementacion de tecnologias firewall para mejoera la gestion y administracion de la red de datos en la empresa s&b servicios generales".* Cajamarca.

CASTREJÓN, R. V. (2013). *Analisis, diseño e implementación de tecnología firewall para mejorar la gestión y administración de la red de datos de la empresa s&b servicios generales".* Cajamarca.

Cisco. (19 de Enero de 2006). *¿Cómo funciona RADIUS?* Obtenido de ¿Cómo funciona RADIUS?: https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Cisco Networking Academy, C. E. (2009). *Acceso a la WAN.*

Cisco Networking Academy, C. E. (2009). *Aspectos básicos de redes.*

Cisco Networking Academy, C. E. (2009). *Conmutación y conexión inalámbrica de LAN.*

Cisco, N. A. (2009). *CCNA Security 1.0.*

DUARTE, E. (2014). Recuperado el 24 de 08 de 2017, de CAPACITY : http://blog.capacityacademy.com/2014/04/09/que-es-mikrotik-routeros/

Enrique, R. G. (2005). *Edgar Enrique* . BOGOTA.

Espinoza Alarcón, M. M., & Tejena Vergara, M. I. (2019). *Análisis e implementación de servicios de seguridad, autenticación y optimización para la red LAN y WLAN del Instituto Tecnológico Superior Guayaquil (Pregrado).* Universidad de Guayaquil, Guayaquil.

Fernández Rivera, M. (2016). *Metodología para el diseño de una red LAN inalámbrica 802.11 n/ac con servidor radius para la Gerencia Regional de Salud - Arequipa.* Universidad Catolica de Santa Maria, Arequipa.

Figueroa, V. J. (2015). *Modelo de gestión para optimizar el servicio al cliente de.* LIMA.

Gaya Fuertes, G. (09 de marzo de 2019). *Sophos Enterprise console*. Obtenido de https://docs.sophos.com/esg/enterprise-console/5-5/help/es-es/esg/Enterprise-Console/concepts/data_21_howitworks.html

Gòmez Vergara , P. F. (2007). *"arquitectura unificada para control de acceso en redes inalambricas seguras".* Argentina-mendoza.

Gonzales J, A. (2014). *Seguridad inalàmbrica.*

Guillermo. (2010). *"Diseño y administracion centralizda de red vlan centrum catolica" universidad pontificia del Perú.* Lima -peru.

Guillermo, M. H. (2010). *Diseño y Administración centralizada de Redes Wlan centrun Catolica.* Lima.

Hernández Sampieri, R. (2014). *Fundamentos de metodología de la investigación.* México: Mc Graw-Hill.

hola. (2015). *que.* chile: chirre.

JOSITO. (08 de 23 de 2017). *Configurar equipos*. Obtenido de http://www.configurarequipos.com/doc711.html

Loor Anchundia, J. R. (2019). *Acceso a redes inalámbricas de la ESPAM MFL mediante un servidor Radius (Posgrado).* Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, Calceta.

Mena Molina, J. C. (2019). *Implementación de servidores radius para controlar los accesos no autorizados a redes inalámbricas, caso OSFL. (Pregrado).* Universidad Tecnológica Empresarial de Guayaquil, Guayaquil.

Mendoza Navarrete, M. L., Zambrano Zambrano, M. T., Sánchez Parrales, L. V., Linares Alvaro, M. J., & Hung León, D. (2021). Gestión del servicio de autenticación de usuarios a través de un servidor radius en la Universidad de Granma. *Revista Sinapsis. Vol 1*, 18.

Molina. (2012). *"Propuesta de segmentacion con redes virtuales y priorizacion del ancho de banda con qos para la mejora del rendimiento y segurida de la red lan en la empresa editora el comercio planta norte"*. Chiclayo.

Muñoz, M. (2010). *"Diseño e implementacion de arquitectura de conectividad y seguridad aaa en udnet (authentication authorization and accounting) "*. Bogota.

Nicolas Botero, A. (2005). *"Modelo de gestion de seguridad con soporte a snmp " en lapontificia Universidad Javeriana*. Bogota.

Nuttsy , A., & Lazo , G. (2012). *DIseño e implementación de una red lan y wlan con sistema de control de acceso mediante servidores AAA.* Lima.

Olivares Montes, B. (2017). Autenticación segura, control de acceso y privacidad de datos en redes inlámbrics. *Caverin Solutions*.

Paredes Calero, B. (2010). *"Implementación de un hotspot con servidor radius en la biblioteca de la ciudad y la provincia, ubicada en Ambato-Tungurahua.* Ecuador.

Perez Garay, j. (09 de marzo de 2019). *Power Data*. Obtenido de https://www.powerdata.es/seguridad-de-datos

Perez Porto, J., & Gardey, A. (2016). *Copyright © 2008-2019 - Definicion.de* . Obtenido de https://definicion.de/autenticacion/

Pérez, J., & Merino, M. (2011). Definición de red de datos. *Definicion.de*.

Sampieri. (2012).

SISTEMAS, E. P. (22 de 09 de 2017). *PRESENTACIÓN*. Obtenido de INICIO: http://www.sistemasunh.net/pagina/PRESENTACION

Sosa, V. (2011). *Gestion de redes* .

Suárez Sardón, D. A. (2014). *Propuesta de un modelo de gestión estratégica de pedido.* LIMA.

Tamayo, M. (2013). *Servidor remoto de autenticación de usuarios (RADIUS) PARA LA.* Ecuador.

TeleInfo. (22 de Noviembre de 2008). *Servidores Radius*. Obtenido de Servidores Radius: http://trabajotele08.blogspot.com/

Universia. (15 de 09 de 2018). Obtenido de http://noticias.universia.cl/educacion/noticia/2017/11/27/1156634/uso-redes-sociales-organizar-tiempo-universidad.html

Velazquez, O. (2007). Redes inalámbricas. *Gestiopolis*.

Wikipedia. (18:45 8 nov 2010). Recuperado el 23 de 08 de 2017, de Servicio de red: https://es.wikipedia.org/wiki/Servicio_de_red

Wikipedia. (2017). Recuperado el 23 de 08 de 2017, de Denegacion de servicio: https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

Wikipedia. (6 de septiembre del 2017). Recuperado el 23 de 08 de 2017, de Accesibilida de la Informacion : https://es.wikipedia.org/wiki/Accesibilidad

Yovanna, S. C. (2009). Diseño e implementacion de un modelo de gestion documental para la serie historias laborales del area de talento humano para la empresa colgrabar. Bogota.

GLOSARIO DE TERMINOS

Radius: Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

DHCP: Llamada protocolo de configuración dinámica de host, es un protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conformes estas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así, los clientes de una red IP pueden obtener sus parámetros de configuración automáticamente.

Protocolo AAA: En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

Wlan: Una red de área local inalámbrica, también conocida como WLAN (del inglés wireless local área network), es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

TACACS: Es un protocolo de autenticación remota, propietario de cisco, que se utiliza para comunicarse con un servidor de autenticación comúnmente utilizado en redes Unix. TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red.

Tasa de transferencia: En informática y telecomunicaciones, el término tasa de transferencia, define el número de bits que se transmiten por unidad de tiempo a través de un sistema de transmisión digital o entre dos dispositivos digitales.

Paquetes de datos: Paquete de red o paquete de datos, es cada uno de los bloques en que se divide la información para enviar, en el nivel de red.

QoS: Es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Cuantitativamente, mide la calidad de los servicios.

APÉNDICE

Anexo 1. Matriz de Consistencia

Título: SERVIDOR RADIUS EN EL CONTROL DE ACCESO A LA RED INALAMBRICA DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS DE LA UNIVERSIDAD NACIONAL DE HUANCAVELICA

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
Problema general: **¿**De qué manera influye el servidor Radius en el control del acceso a la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica?	**Objetivo general:** ¿Determinar la influencia del servidor Radius para mejorar el control del acceso a la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica?	**General:** El servidor Radius influye positivamente en el control de acceso a la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.	**Variable independiente (X)** el servidor radios	**Tipo:** aplicada **Nivel:** Aplicativa **Diseño:** pre experimental. **Problema y muestra:** **Población:** Total de HOST inalámbrico de la Epis. **Muestra:** Total, de HOST inalámbrico de la Epis
Problemas específicos a) **¿**Cómo influye el servidor Radius en la **disponibilidad** de la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica**?** b) **¿**Cómo influye el servidor Radius en la **autentificación** de usuarios en la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica?	**Objetivo especifico** a) Determinar la influencia del servidor Radius en la **disponibilidad** de la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica b) Determinar la influencia del servidor Radius en la **autentificación** de usuarios en la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.	**Hipótesis especifico** a) El servidor Radius influye positivamente en la **disponibilidad** de la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de b) el servidor Radius influye positivamente en la **autentificación** de usuarios en la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica.	**Variable dependiente (y)** control de acceso a la red inalámbrica	**Técnicas e instrumentos:** **Observación:** parte estadística del mismo software. Ficha de observación. **Encuesta:** cuestionario de encuesta. **Técnicas de procesamiento de datos:** Medidas de tendencial central **Medidas de dispersión** **Medida de regresión y correlación.**

Anexo 2. Desarrollo

2.1. Configuración de la red inalámbrica Wi-Fi para el acceso de los usuarios

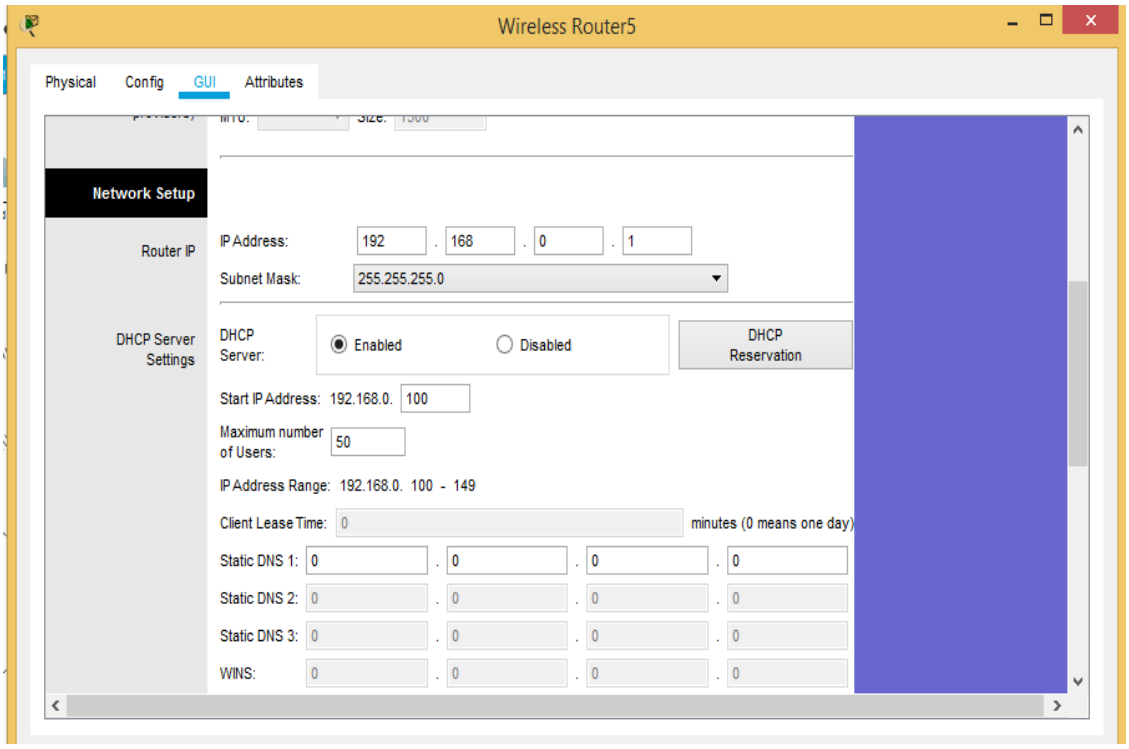

Figura 24: Configuración de router Wi-Fi para el acceso del Servidor Radius

2.2. Configuración de seguridad con el Servidor Radius de la red WLAN.

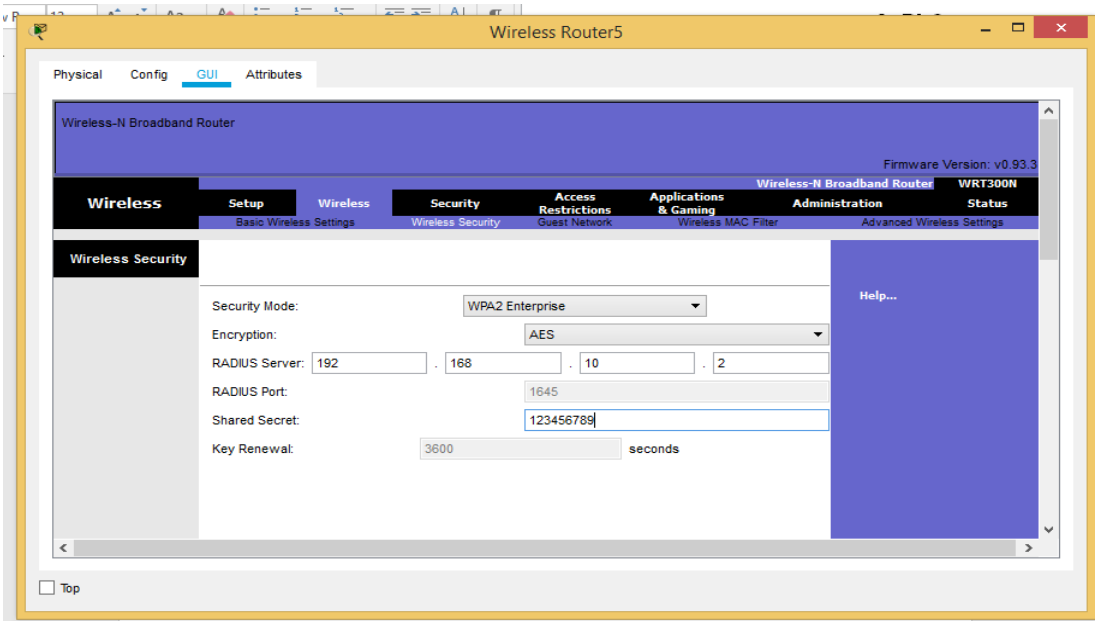

Figura 25: Asignación de IP del Servidor Radius

2.3. Configuración del Servidor Radius para la mejora en la política de seguridad en la EPIS.

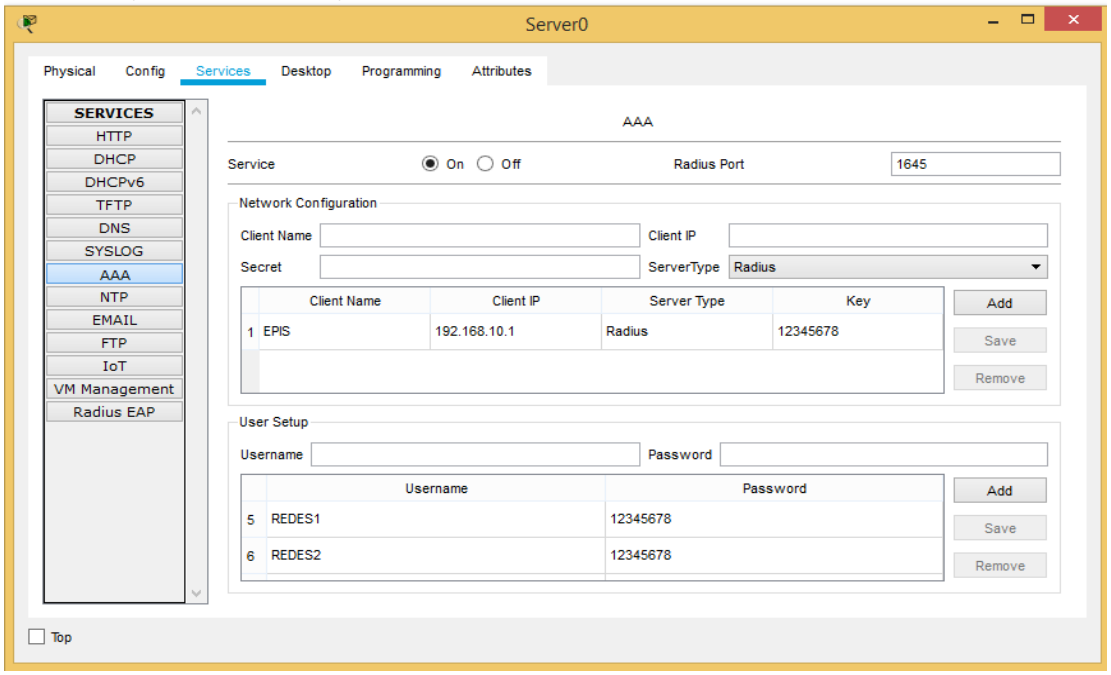

Figura 26: Configuración de Servidor radius