UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA DE INGENIERÍA EN TELEINFORMÁTICA

TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TELEINFORMÁTICA

ÁREA
TECNOLOGÍA DE LAS TELECOMUNICACIONES

TEMA
"ANÁLISIS DE FACTIBILIDAD DEL USO DE AUTENTICACION RADIUS EN REDES WIRELESS MEDIANTE VALIDACIÓN DE USUARIO"

AUTOR
FRANCO SANCHEZ ENRIQUE WILLIAM

DIRECTOR DEL TRABAJO
ING. TELEC. VEINTIMILLA ANDRADE JAIRO GEOVANNY, MG.

GUAYAQUIL, ABRIL 2022

ANEXO XI.- FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	ANÁLISIS DE FACTIBILIDAD DEL USO DE AUTENTICACION RADIUS EN REDES WIRELESS MEDIANTE VALIDACIÓN DE USUARIO		
AUTOR(ES)	FRANCO SANCHEZ ENRIQUE WILLIAM		
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	ING. TRUJILLO BORJA XIMENA FABIOLA, MG / ING. VEINTIMILLA ANDRADE JAIRO GEOVANNY, MG.		
INSTITUCIÓN:	UNIVERSIDAD DE GUAYAQUIL		
UNIDAD/FACULTAD:	FACULTAD DE INGENIERÍA INDUSTRIAL		
MAESTRÍA/ESPECIALIDAD:			
GRADO OBTENIDO:	INGENIERO EN TELEINFORMÁTICA		
FECHA DE PUBLICACIÓN:	21 DE ABRIL DEL 2022	No. DE PÁGINAS:	90
ÁREAS TEMÁTICAS:	TECNOLOGÍA DE LAS TELECOMUNICACIONES		
PALABRAS CLAVES/ KEYWORDS:	Radius, autenticación, diseño, protocolo, seguridad Wireless / Radius, authentication, design, protocol, wireless security		

RESUMEN (150-200 palabras):

Las redes inalámbricas en la actualidad cuentan con un crecimiento exponencial debido a su forma de despliegue permitiendo mayor operatividad en redes PyMes como corporativas. Debido a su crecimiento existen diferentes factores o amenazas que afectan a la disponibilidad de la información por lo que el trabajo de investigación se realiza la autenticación en la red Wireless de la empresa SERVIORDER a través del protocolo RADIUS mediante validación de usuarios de dominio a fin de evitar el acceso no autorizado en la red corporativa logrando aplicar controles en gestión centralizada así como la autenticación, autorización y contabilización en los accesos de la red incrementando su nivel de seguridad y administración de SSID con autenticación en dominio. Por último, se presenta un diseño el cual demuestra el correcto funcionamiento del servicio NPS de Windows.

ABSTRACT (150-200 palabras):

Wireless networks currently have an exponential growth due to its deployment form allowing greater operability both home and corporate networks. Due to its growth there are different factors or threats that affect the availability of information so this research work is performed authentication in the wireless network of the company SERVIORDER through RADIUS protocol by validation of domain users in order to prevent unauthorized

access to the corporate network and achieving the implementation of controls and centralized management as authentication, authorization and accounting in network access increasing its level of security and administration of SSID with domain authentication. Finally, a design is presented which demonstrates the correct operation of the Windows NPS service.

Key words: Radius, authentication, design, protocol, wireless security

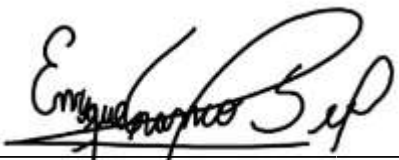
ADJUNTO PDF:	SI (X)	NO ( )
CONTACTO CON AUTOR/ES:	Teléfono: +593995362648	E-mail: enrique.francos@ug.edu.ec
CONTACTO CON LA INSTITUCIÓN:	Nombre: Ing. Ramón Maquilón Nicola	
	Teléfono: 593-2658128	
	E-mail: direccionTi@ug.edu.ec	

ANEXO XII.- DECLARACIÓN DE AUTORÍA Y DE AUTORIZACIÓN DE LICENCIA GRATUITA INTRANSFERIBLE Y NO EXCLUSIVA PARA EL USO NO COMERCIAL DE LA OBRA CON FINES NO ACADÉMICOS

FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

LICENCIA GRATUITA INTRANSFERIBLE Y NO COMERCIAL DE LA OBRA CON FINES NO ACADÉMICOS

Yo, **FRANCO SANCHEZ ENRIQUE WILLIAM**, con C.C. No. **095195347-0**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es "**ANÁLISIS DE FACTIBILIDAD DEL USO DE AUTENTICACION RADIUS EN REDES WIRELESS MEDIANTE VALIDACIÓN DE USUARIO**" son de mi absoluta propiedad y responsabilidad, en conformidad al Artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN*, autorizo la utilización de una licencia gratuita intransferible, para el uso no comercial de la presente obra a favor de la Universidad de Guayaquil.



FRANCO SANCHEZ ENRIQUE WILLIAM
C.C. No. 095195347-0

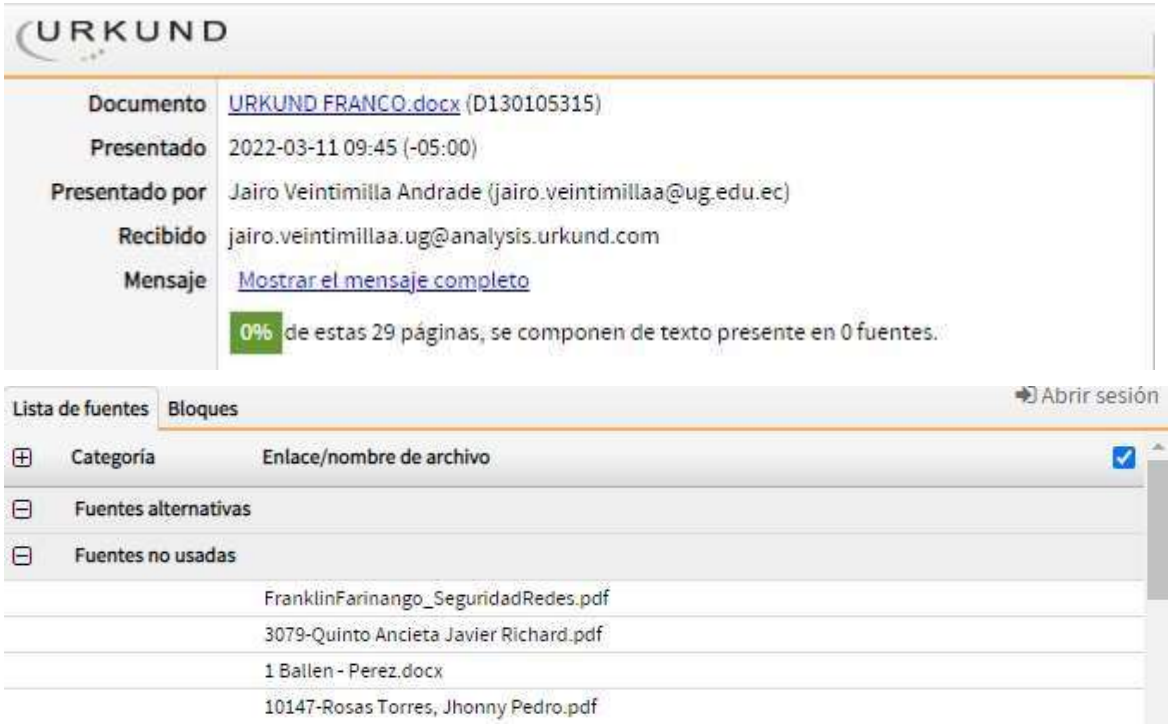
ANEXO VII.- CERTIFICADO PORCENTAJE DE SIMILITUD

FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

Habiendo sido nombrado ING. VEINTIMILLA ANDRADE JAIRO GEOVANNY, tutor del trabajo de titulación certifico que el presente trabajo de titulación ha sido elaborado por FRANCO SANCHEZ ENRIQUE WILLIAM, C.C.: 0951953470, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERO EN TELEINFORMÁTICA.

Se informa que el trabajo de titulación: **"ANÁLISIS DE FACTIBILIDAD DEL USO DE AUTENTICACION RADIUS EN REDES WIRELESS MEDIANTE VALIDACIÓN DE USUARIO"**, ha sido orientado durante todo el periodo de ejecución en el programa Antiplagio URKUND quedando el 0% de coincidencia.

https://secure.urkund.com/old/view/124265227-220752-616301#q1bKLVayio7VUSrOTM/LTMtMTsxLTlWyMqgFA==



JAIRO GEOVANNY VEINTIMILLA ANDRADE

ING. VEINTIMILLA ANDRADE JAIRO GEOVANNY, MG.
DOCENTE TUTOR
C.C. 0922668025
FECHA: 16/03/2020

ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR DEL TRABAJO DE TITULACIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

Guayaquil, 16 de marzo del 20222

Sr (a).
Ing. Annabelle Lizarzaburu Mora, MG.
Director (a) de Carrera Ingeniería en Teleinformática / Telemática
FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL
Ciudad. -

De mis consideraciones:

Envío a Ud. el Informe correspondiente a la tutoría realizada al Trabajo de Titulación **"ANÁLISIS DE FACTIBILIDAD DEL USO DE AUTENTICACION RADIUS EN REDES WIRELESS MEDIANTE VALIDACIÓN DE USUARIO"** del estudiante **FRANCO SANCHEZ ENRIQUE WILLIAM**, indicando que ha (cumplido con todos los parámetros establecidos en la normativa vigente:

- El trabajo es el resultado de una investigación.
- El estudiante demuestra conocimiento profesional integral.
- El trabajo presenta una propuesta en el área de conocimiento.
- El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se adjunta el certificado de porcentaje de similitud y la valoración del trabajo de titulación con la respectiva calificación.

Dando por concluida esta tutoría de trabajo de titulación, CERTIFICO, para los fines pertinentes, que el (los) estudiante (s) está (n) apto (s) para continuar con el proceso de revisión final.

Atentamente,

Firmado electrónicamente por:
JAIRO GEOVANNY VEINTIMILLA ANDRADE

ING. VEINTIMILLA ANDRADE JAIRO GEOVANNY, MG.
TUTOR DE TRABAJO DE TITULACIÓN
C.C. 0922668025
FECHA: 16 de marzo de 2022

ANEXO VIII.- INFORME DEL DOCENTE REVISOR
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

Guayaquil, 5 de abril de 2022

Sra.
Ing. Annabelle Lizarzaburu Mora, MG.
Directora de Carrera Ingeniería en Teleinformática / Telemática
FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL
Ciudad. -

De mis consideraciones:

Envío a Ud. el informe correspondiente a la REVISIÓN FINAL del Trabajo de Titulación ANÁLISIS DE FACTIBILIDAD DEL USO DE AUTENTICACIÓN RADIUS EN REDES WIRELESS MEDIANTE VALIDACIÓN DE USUARIO del estudiante FRANCO SANCHEZ ENRIQUE WILLIAM. Las gestiones realizadas me permiten indicar que el trabajo fue revisado considerando todos los parámetros establecidos en las normativas vigentes, en el cumplimento de los siguientes aspectos:

Cumplimiento de requisitos de forma:
El título tiene un máximo de 15 palabras.
La memoria escrita se ajusta a la estructura establecida.
El documento se ajusta a las normas de escritura científica seleccionadas por la Facultad.
La investigación es pertinente con la línea y sublíneas de investigación de la carrera.
Los soportes teóricos son de máximo 10 años. La propuesta presentada es pertinente.

Cumplimiento con el Reglamento de Régimen Académico:
El trabajo es el resultado de una investigación.
El estudiante demuestra conocimiento profesional integral.
El trabajo presenta una propuesta en el área de conocimiento.
El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se indica que fue revisado, el certificado de porcentaje de similitud, la valoración del tutor, así como de las páginas preliminares solicitadas, lo cual indica el que el trabajo de investigación cumple con los requisitos exigidos.

Una vez concluida esta revisión, considero que el estudiante está apto para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente,

Firmado electrónicamente por:
XIMENA FABIOLA TRUJILLO BORJA

Ing. Trujillo Borja Ximena, Mg.
DOCENTE TUTOR REVISOR
C.C: 0603375395 FECHA: 5 de abril del 2022

Dedicatoria

Dedico este proyecto de titulación a Dios y a la Virgen de Agua Santa por están conmigo siempre, brindarme fuerzas, salud y sabiduría para lograr una meta muy importante en mi vida.

También dedico este logro a mis padres el Sr. Enrique Franco y la Sra. Ana Sánchez quienes, con su amor incondicional, esfuerzo y valores me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades.

Mis hermanos David y Viviana por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias. A toda mi familia porque con sus oraciones, consejos y palabras de aliento simulando mi profesión hicieron de mí una mejor persona de una u otra forma me acompañan en todos mis sueños y metas.

Finalmente quiero dedicar esta tesis a cada uno de mis compañeros, por brindarme su ayuda cuando más las necesito, por extender su mano en todo momento y por la fidelidad brindada cada día, de verdad mil gracias.

Agradecimiento

Agradezco a Dios y a la Virgen de Agua Santa por brindarme salud y bendecirme con sabiduría para poder concluir con mi carrera universitaria.

A mi familia por la paciencia, el apoyo incondicional, y el amor que fue necesario para poder seguir en este largo camino.

A mis profesores de mi facultad, grandes maestros que fueron la guía necesaria para ir por el camino correcto de este proyecto, en especial un agradecimiento a mi tutor Ing. Veintimilla Andrade Jairo y a la mi directora de proyecto Ing. Trujillo Borja Ximena por su paciencia y guía para poder realizar este proyecto de titulación.

Gracias sinceras a mis amigos que me apoyaron cuando el recorrido se hizo empinado. Sin ustedes nada esto hubiese sido posible.

Declaración de autoría

"La responsabilidad del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y el patrimonio Intelectual del mismo a la Facultad de Ingeniería Industrial de la Universidad de Guayaquil"

Franco Sánchez Enrique William
C.C. 095195347-0

Índice General

Capítulo III

Metodología de la Investigación y Propuesta

Índice de Tablas

Índice de Figuras

ANEXO XIII.- RESUMEN DEL TRABAJO DE TITULACION (ESPAÑOL)

FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

"ANÁLISIS DE FACTIBILIDAD DEL USO DE AUTENTICACION RADIUS EN REDES WIRELESS MEDIANTE VALIDACIÓN DE USUARIO"

Autor: Franco Sanchez Enrique William

Tutor: Ing. Veintimilla Andrade Jairo, MG.

RESUMEN

Las redes inalámbricas en la actualidad cuentan con un crecimiento exponencial debido a su forma de despliegue permitiendo mayor operatividad en redes PyMes como corporativas. Debido a su crecimiento existen diferentes factores o amenazas que afectan a la disponibilidad de la información por lo que en el presente trabajo de investigación se realiza la autenticación en la red Wireless de la empresa SERVIORDER a través del protocolo RADIUS mediante validación de usuarios de dominio a fin de evitar el acceso no autorizado en la red corporativa logrando aplicar controles en gestión centralizada así como la autenticación, autorización y contabilización en los accesos de la red incrementando su nivel de seguridad y administración de SSID con autenticación en dominio. Por último, se presenta un diseño el cual demuestra el correcto funcionamiento del servicio NPS de Windows.

Palabras Claves: Radius, autenticación, diseño, protocolo, seguridad Wireless

ANEXO XIV.- RESUMEN DEL TRABAJO DE TITULACIÓN (INGLÉS)

FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA

"FEASIBILITY ANALYSIS OF THE USE OF RADIUS AUTHENTICATION IN WIRELESS NETWORKS THROUGH USER VALIDATION"."

Author: Franco Sanchez Enrique William

Advisor: TE. Veintimilla Andrade Jairo, MG

ABSTRACT

Wireless networks currently have an exponential growth due to the way they are deployed, allowing greater operability in SME and corporate networks. Due to its growth there are different factors or threats that affect the availability of information so in this research work is performed authentication in the wireless network of the company SERVIORDER through RADIUS protocol by validation of domain users in order to prevent unauthorized access to the corporate network, being able to implement controls in centralized management and authentication, authorization and accounting in network access increasing its level of security and administration of SSID with domain authentication. Finally, a design is presented which demonstrates the correct operation of the Windows NPS service.

Keywords Radius, authentication, design, protocol, wireless security

Introducción

En la actualidad se ha evidenciado un aumento constante en cuanto al uso de las redes inalámbricas debido a su facilidad de despliegue. Al mismo tiempo la velocidad en la que se gestionan los servicios en la red incluso puede llegar a ser igual o más rápidos que las redes cableadas.

El acceso a los diferentes servicios que posee una organización o entidad se realiza mediante la conexión de equipos que usen tecnología WI-FI que se conecta a uno o varios equipos de acceso (Access Point) facilitando la conexión en cualquier parte de la institución.

Las conexiones inalámbricas en los últimos años han tenido un gran avance, soportando cualquier tipo de servicio que se tenga en la organización e incluso desplazando a las redes cableadas debido a las limitaciones de crecimiento en cuanto esta última necesita, siendo el medio inalámbrico la primera opción de uso a nivel de crecimiento y uso en las redes empresariales.

Hoy en día se incluyen mecanismos de seguridad que permiten gestionar la entidad a fin de identificar los factores o riesgos de la red. Para ello se aplican ciertos niveles de control en el modelo OSI para controlar el acceso mediante la autenticación, el permiso a través de la autorización y el tiempo o la cantidad de registros mediante el conteo (AAA).

Los controles de acceso en la red se establecen ya sea mediante un medio guiado o no guiado en el que es necesaria la participación de un sistema de seguridad RADIUS que permita la autenticación a cualquier usuario que acceda a la red a través de todos los puntos de accesos distribuidos en la entidad.

Al realizar la autenticación se logra tener una gestión de datos debido a que permite llevar un registro de lo realizado llegando a ser interpretados de forma mucho más efectiva reduciendo el alto costo en tiempo para la gestión de información, de igual forma a la calidad de resultados.

Capítulo I
El Problema

1.1 Planteamiento del problema

Según estudios previos realizados afirman que, aproximadamente el 76,6% de las personas han sufrido problemas de conexión debido al acceso no autorizado de terceros sin debido consentimiento en las redes inalámbricas donde más del 40% de los encuestados mencionan que, el problema está dado credenciales conocidas, (welivesecurity, 2012).

Por otra parte, Cisco (2017) menciona que los adversarios han desarrollado nuevas amenazas utilizando herramientas que cuentan con complementos de ciber inteligencia siendo una amenaza hoy en día cada vez mayor donde a nivel de organizaciones aproximadamente más del 20% han sufrido el acceso no autorizado en sus redes generando pérdidas millonarias en sus ingresos.

Las redes LAN inalámbricas son una tecnología que mediante ondas electromagnéticas propagar señales a ciertas distancias en la que dispositivos finales obtienen acceso a la compartición de información usando altas tasas de transmisión de forma interna o incluso externa al navegar en internet, (Cevallos, 2017).

En la última década en el Ecuador se ha presentado un crecimiento de forma exponencial en el desarrollo tecnológico permitiendo ofertar servicios a través de los diferentes medios de comunicación (guiados y no guiados) donde hoy por hoy las empresas prefieren hacer uso de un despliegue de tecnología inalámbrica debido a su bajo costo de propiedad en las implementaciones en redes LAN, (Arévalo, 2018).

Las redes Wireless son una de las tecnologías con mayor uso en entornos corporativos debido a su fácil configuración y despliegue ofreciendo mayores beneficios en cuanto a conectividad a diferencia de las redes cableadas, permitiendo que un usuario pueda desplazarse de un sitio a otro a través de un dispositivo inteligente ya sea una laptop o un smartphone manteniendo la comunicación en todo momento, a tal punto de ser el medio preferido de conexión debido a sus altas velocidades propuestas a diferencia del medio cableado, (Sanchez, 2019).

Este tipo de conexión es cada día más frecuente lo que hace que varios usuarios de una organización hagan uso de este, para establecer la comunicación a través de diferentes nombres de red conocidos por sus siglas en inglés como SSID (Service Set Identifier) que son validados mediante un PSK (Pre-Share Key) que cuentan con niveles de encriptación

siendo el método de cifrado AES-WPA2 (Advanced Encryption Standard) el más utilizado debido a su robustez, que impide que sea vulnerado, (Dordoigne, 2015).

En muchas ocasiones existe un factor determinante a este tipo de autenticación wireless el cual está dado por la compartición de claves entre usuarios de la red o el no cambio de credenciales cada cierto tiempo ocasionando que cualquier usuario pueda conectarse a un SSID previamente definido y recibir los parámetros de red acorde a como estén configurados, esto ocasiona que se generen ataques previos basados en un modelo de pasos para el ataque el sistemas conocido como Kill Chain o cadena de la muerte aplicado por un tercero de forma no autorizada obteniendo acceso a los sistemas de seguridad a tal punto de afectar a la organización en cuanto a pérdidas monetarias, recuperación o filtración de datos se trata. Otro factor determinante es el nivel de robustez con el que la clave del SSID se crea usando contraseñas fáciles de adivinar y con ello obteniendo acceso a los datos de la organización, (Serrano, 2011).

Del mismo modo otra afectación que existe es que al crearse diferentes SSID se degrada el rendimiento en cada red anunciada para cada uno de sus canales por lo que se recomienda no exceder el máximo definido de cinco mejorando la transmisión.

Las organizaciones por lo general hacen caso omiso al proceso indicado afectando no solo al rendimiento o throughput de la red sino también aumentando el delay o incluso el jitter en las conexiones que existen a nivel de wireless, (IONOS, 2019).

1.2 Formulación del problema

Así ante lo expuesto se responderá la siguiente pregunta ¿Se puede diseñar una red wireless que permita realizar la autenticación a nivel de dominio mediante el protocolo Radius para mejora en seguridad de la Serviorder S.A.

1.3 Sistematización del problema

- ¿De qué manera se puede optimizar las redes wireless en las redes corporativas?
- ¿Qué criterios se deben de considerar a la hora de desplegar una red inalámbrica?
- ¿Cuáles son los niveles de seguridad aplicados actualmente en las redes inalámbricas?
- ¿Qué método de autenticación permite mejoras a nivel de red wireless?
- ¿Cuáles son los requerimientos necesarios para realizar una autenticación a nivel de Radius?

- ¿Qué tipo de escenario demuestra mejora en el rendimiento de la red corporativa?
- ¿De qué forma se mitiga las vulnerabilidades en las redes Wireless mediante el uso de directorio activo?

1.4 Alcance

Diseñar una red LAN que permita autenticar vía wireless mediante el protocolo Radius a través de usuarios creados a nivel de dominio.

1.5 Objetivos de la investigación

1.5.1 Objetivos General

Diseñar una red LAN que permita la autenticación de SSID mediante la validación de usuarios gestionados a nivel de directorio activo permitiendo el acceso a internet.

1.5.2 Objetivos específicos

- Analizar los diferentes métodos de autenticación que existen a nivel de redes wireless
- Identificar los niveles de seguridad apropiados para el uso de las redes wireless
- Diseñar una red LAN que permita la autenticación en redes wireless mediante el uso del protocolo Radius.

1.6 Justificación e importancia

Hoy en día gran parte de las organizaciones no cuentan con los debidos niveles de seguridad existiendo falencias en cuanto a conectividad siendo las soluciones empresariales mayormente afectadas debido a su forma tradicional de operación, por lo que, el presente trabajo de investigación se pretende analizar la correcta implementación con el fin de reducir el riesgo en la seguridad permitiendo mejoras en cuanto a la comunicación, así como la tolerancia a fallas.

Las empresas en la actualidad necesitan diferentes criterios de seguridad en los medios inalámbricos que permitan asegurar la confidencialidad – integridad y disponibilidad de la información donde en la actualidad no todos conocen debido al poco conocimiento sobre el tema o limitaciones en cuanto a despliegues de infraestructura.

Para ello el uso de estándares de seguridad en las redes Wireless permitirá tener un control y autorización a los diferentes accesos logrando así se ofrezcan servicios según este definido mejorando de gran manera la forma en la que actualmente las redes corporativas operan.

De este modo el presente trabajo de investigación pretende realizar la autenticación de usuarios a través de servicios de directorio activo en base a usuarios predefinidos de la organización.

1.7 Delimitación del Problema

El presente trabajo de investigación está limitado en el área de las tecnologías de los ordenadores el cual se diseña una red LAN inalámbrica que permita realizar la autenticación a nivel de dominio en la empresa Serviorder S.A. mediante el uso del protocolo Radius.

Capítulo II
Marco Teórico

2.1 Antecedentes de la investigación

Hoy en día, existe una gran cantidad de medios o dispositivos de intercomunicación los cuales según su funcionalidad permiten establecer el envío y recepción de datos siendo un requisito indispensable en las redes actuales. Por lo general este tipo de servicios se ofrece de diferentes formas donde las redes de área local inalámbricas por sus siglas en Ingles (Wireless Local Área Network) cada vez son más comunes en el sector corporativo.

Un punto importante por mencionar es que debido al exponencial crecimiento en estas redes han surgido problemas en cuanto a la disponibilidad del servicio por los ataques o factores que afectan a los usuarios de la red debido al acceso no autorizado a los dispositivos, siendo un factor determinante y en muchas ocasiones críticas. Por lo que (Yurema & Gerardo, 2016) menciona en su trabajo de investigación la elaboración de un modelo que permita el control en el acceso de los usuarios a la red a través de las redes wireless protegiendo al sistema así como a los diferentes activos de ataques o accesos no validados a través de un dispositivo autenticador evitando así movimientos laterales o verticales de equipos con un mejor control mediante logs de los inicios de sesión realizados por los usuarios.

Del mismo modo, es necesario mencionar que un eslabón débil a nivel de seguridad informática son las redes wireless debido a su nivel de encriptación de datos o claves utilizadas por los sysadmin (Administradores de sistema) siendo sencillas de romper mediante mecanismos de hash basados en ataques de fuerza bruta. En lo que (Pallo & Martínez, 2010) en su diseño de red wireless para Siderúrgica Tungurahua S.A establece los factores o medios que más daño hacen en la red a nivel de cifrados utilizados en el que propone los tipos de formatos a utilizar evitando los ataques de diccionario al igual que de fuerza bruta siendo más robustos y seguros.

Por otra parte Asadovay y Caiza (2013) indica que en la actualidad existen diferentes métodos de cifrado seguro que permiten ocultar contraseñas débiles creadas en las redes wireless con protocolos vulnerables como WEP (Wired Equivalent Privacy) o WPA (Wi-fi Protected Access) donde en su estudio de investigación relacionado a la autenticación de usuarios mediante protocolos de cifrado robusto para redes wireless con contraseñas débiles, define que métodos son los más seguros de utilizar cumpliendo con ciertos requisitos de operación siendo la interoperabilidad el mecanismo primordial logrando así una perspectiva de la forma de encriptación asegurando el canal al igual que la información.

Asimismo, Mendoza en al (2021) propuso una red wireless mediante un caso práctico realizando la autenticación de forma centralizada a través de protocolos basados en el estándar 802.1x demostrando una eficiencia en cuanto a establecimiento de comunicación utilizando uno de los tres métodos de autenticación en redes wireless más comunes.

Del mismo modo, Celestino (2009) en su diseño de red propuso un esquema basado en RIU el cual cumple controles de red en el que mediante nuevos protocolos de red hacen que el sistema sea funcional, operativo y escalable haciendo uso de diferentes equipos inalámbricos.

Un factor importante a la hora de manejar los entornos inalámbricos es la forma en la que pueden ser administrados mediante una sola controla de gestión en el que Tobar (2015) en su estudio de investigación para el Gobierno Autónomo Descentralizado de la Provincia del Guayas propone la creación de un NAC (Network Access Control) en el que los equipos inalámbricos puedan interactuar con dicho servidor a tal punto de poder monitorear, configurar y administrar los access point desde su controla de gestión reduciendo costos de operación al igual un mínimo cambio en la infraestructura de datos al mismo tiempo de promover una escalabilidad en cuanto a información a procesar o usuarios a conectar desde cualquier sitio de la prefectura.

Una forma muy común de asegurar las redes wireless es mediante contraseñas robustas donde el administrador de la red las define y en base a ello en cierto punto son complejas de descifrar, pero al ser compartidas con otros usuarios genera en la mayoría de los casos que personas no autorizadas tengan acceso a ellas logrando unirse a la red siendo esta última vulnerable.

2.2 Fundamentación teórica

2.2.1 Modelo OSI

Conocido comúnmente como el modelo de interconexión de sistemas abiertos es aquel modelo de referencia que es usado para permitir entender el funcionamiento de los protocolos de red y con ello saber cómo se comunican en una infraestructura o arquitectura de red. OSI fue creado en la década de los años 80 por la ISO el cual es la (Organización Internacional de Normalización) definiendo a el modelo OSI un modelo referenciar constituido por varias capas definiendo diferentes niveles de abstracción, (Cisco, 2020).

Cada una de las capas creadas en el modelo ya previamente definido ayudaron a entender las capacidades a la hora de transmitir datos por la red y con ello hacer posible una segregación efectiva en los diferentes niveles de comunicación. Cada una de las capas tienen un conjunto de niveles o formas de operación tal como en la figura 1.

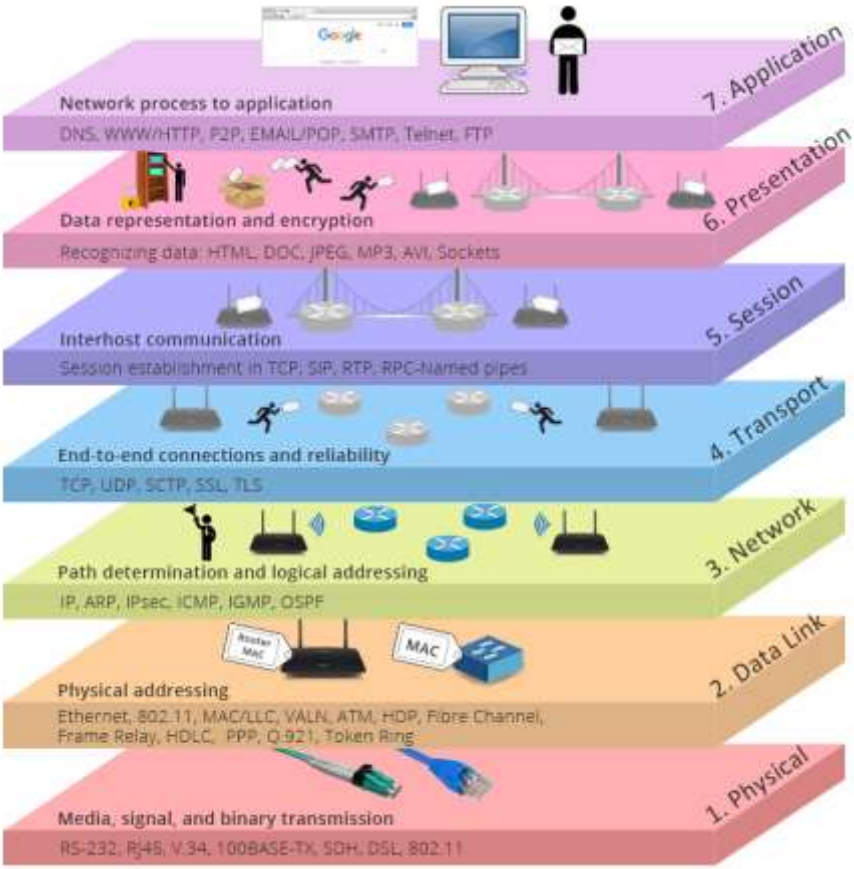


Figura 1.- Modelo OSI, tomada de sites.google.com, elaborado por Enrique Franco

Para mejor detalle se procede a explicar el funcionamiento de cada una de las capas del modelo OSI con el fin de entender el proceso que cada una de ellas realiza a la hora de llevar a cabo una comunicación entre capas.

2.2.1.1 Capa física

Es la capa más baja del modelo OSI, encargada de definir todo lo referente a especificaciones eléctricas a nivel de diferentes procedimientos y funcionalidades. Dentro de la capa física viajan todos los datos en formato de código binario que es entendible para un ordenador haciendo uso de un medio (Tolosa, 2014).

Como principales características de la capa física se puede indicar que:

- Permite transportar datos de un lado a otro usando un medio de comunicación ya sea guiado o no guiado previamente mencionados
- Cuenta con diferentes componentes eléctricos utilizados en los medios para hacer posible la transmisión e información
- Garantiza el envío de datos más no la confiabilidad o entrega en sus conexiones

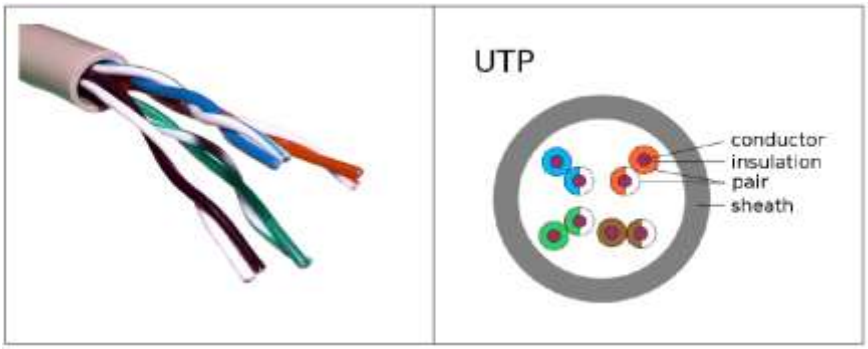


Figura 2.- Cable de red, tomada de sites.google.com, elaborado por Enrique Franco

2.2.1.2 Capa enlace

Es la encargada de usar un medio para que los datos procesados en la capa 1 puedan ser enviados, por lo general esta capa hace la entrega ordenada de la información a través de tramas de tipo Ethernet en el que se define algunas especificaciones dadas por la IEEE 802.3.

Un punto importante por mencionar es que dentro de esta capa se hace uso de dos protocolos esenciales para la comunicación entre equipos que comparten un mismo medio en la red como son la MAC (Media Access Control) encargada de validar que el equipo receptor sea ser quien reciba la trama al igual forma la validación de datos que sea correcta, y el protocolo LLC (Logical Link Control) encargado de establecer la comunicación con las capas superiores del modelo OSI, (Tolosa, 2014).

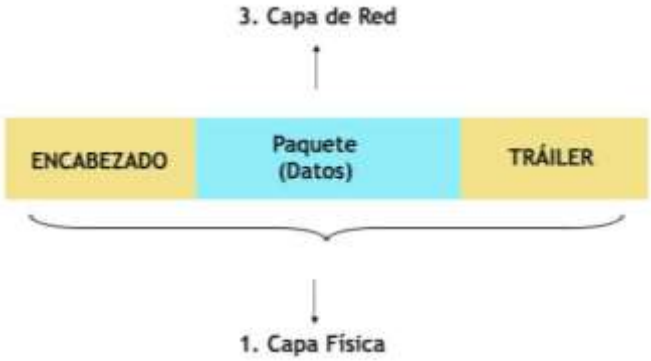


Figura 3.- Entramado 802.3, tomada de sites.google.com, elaborado por Enrique Franco

2.2.1.3 Capa de red

Es aquella capa que tiene como fin establecer la comunicación entre una o más redes existentes las cuales no necesariamente tienen que estar interconectadas de forma directa, sino que en base a ciertos procesos llamadas protocolos de enrutamiento se logra que los equipos compartan información en muchas veces de manera eficiente, (Aguirre, Calva, Guerrero , Hernández, & Hernández, 2017).

A la hora de establecer la comunicación en esta capa de red es necesario como se mencionó establecer algoritmos que permitan determinar de qué manera se hace la comunicación entre hosts u equipos que se encuentran en diferentes segmentos de red, para ello existen ciertos mecanismos definidos como protocolos enrutables y protocolos de enrutamiento.

- Enrutables: hace referencia en como viajan los paquetes a través de la capa de red, como puede ser (IP, IPX, AppleTalk)
- Enrutamiento: Permite hacer la selección de rutas óptimas para llegar al destino un punto a considerar es que es necesario previamente definir métricas que indiquen la forma de operación, así como la comunicación hacia los demás sitios ejemplo (RIP, EIGRP, OSPF, entre otros).

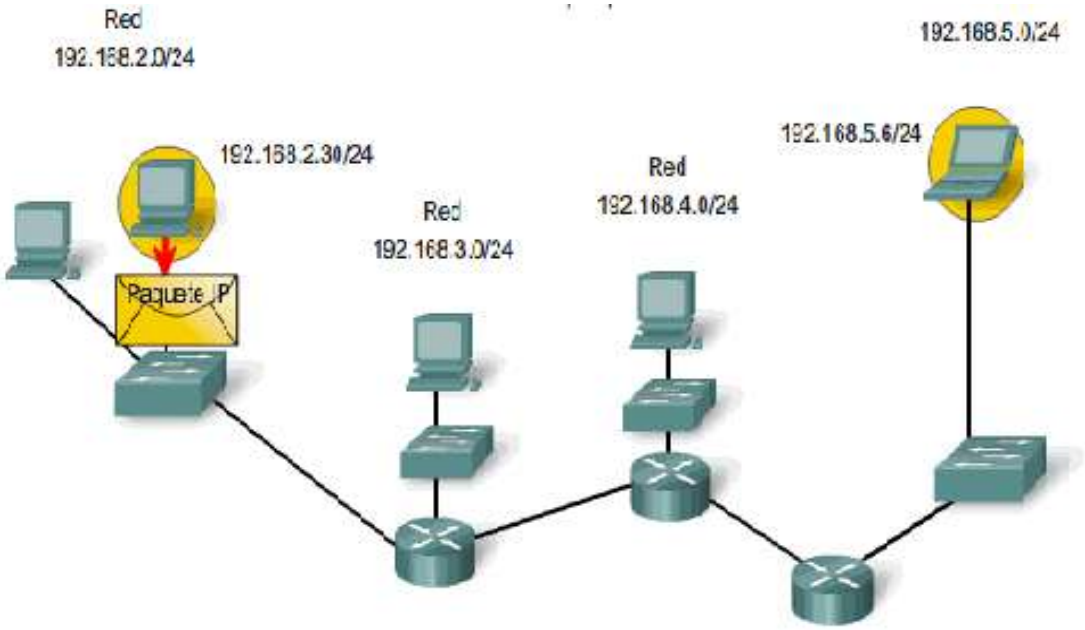


Figura 4.- Enrutamiento, tomada de sites.google.com, elaborado por Enrique Franco

2.2.1.4 Capa de transporte

Es la encargada de crear conexiones de red con el fin de establecer mecanismos de recuperación, así como acuses de recibo entre los equipos que se comunican a nivel de red con el fin de evitar la pérdida de paquetes haciendo uso de mecanismos avanzado que permitan tener una operatividad constante y la información no se pierda.

Al hablar de la capa de transporte se refiere a los datos que viajan libre de errores que se encuentran dentro de un paquete IP que previamente fue procesado por las capas inferiores llamando a ese proceso encapsulación. Otro factor para mencionar es que al hablar de capa 4 se utiliza el termino de segmento para hacer referencia a los datos como viajan en un medio (Aguirre, Calva, Guerrero , Hernández, & Hernández, 2017).

Figura 5.- Conexión TCP, tomada de sites.google.com, elaborado por Enrique Franco

2.2.1.5 Capa de sesión

Es la capa que se encarga de establecer todas las sesiones realizadas entre dos computadoras ya sea en topología peer to peer o cliente-servidor, en este proceso existe un intercambio de información ya sea entre capas adyacentes es decir a nivel de todo el stack de OSI o TCP/IP o de igual a igual, (Rodriguez, Ladino, Bejarano, & Quimbayo, 2018).

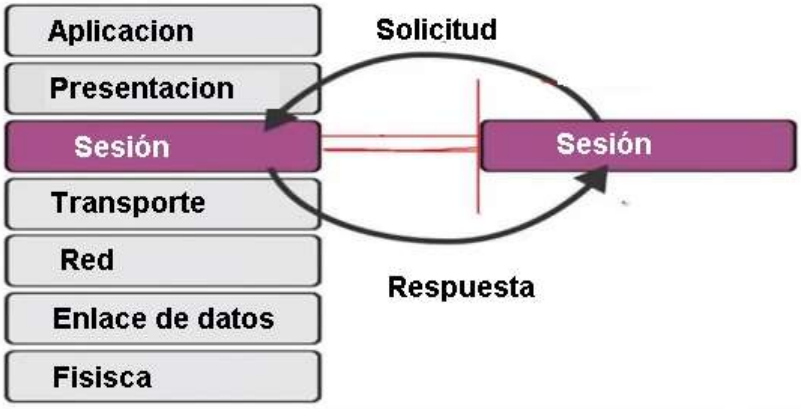


Figura 6.- Comunicación en misma capa, tomada de sites.google.com, elaborado por Enrique Franco

2.2.1.6 Capa de presentación

La capa de presentación se encarga de definir los diferentes formatos a utilizar a la hora de intercambiar información permitiendo ser legible para un equipo.

Figura 7.- Entrega de servicio, tomada de sites.google.com, elaborado por Enrique Franco

2.2.1.7 Capa de aplicación

Brinda los servicios necesarios a la aplicación en si para que pueda trabajar en otras palabras la capa de aplicación es aquella que permite acceder a diferentes servicios y así establecer un intercambio de datos permitiendo el funcionamiento de los servicios tales como correo electrónico, transferencia de archivos, gestores de bases de datos y muchas aplicaciones más.

Cabe recalcar que el usuario no interactúa directamente con la capa de aplicación, sino que en esta capa se hace uso de programas o componentes que permitan a la capa de aplicación brindarnos la información necesaria para establecer la comunicación, (Rodriguez, Ladino, Bejarano, & Quimbayo, 2018)..

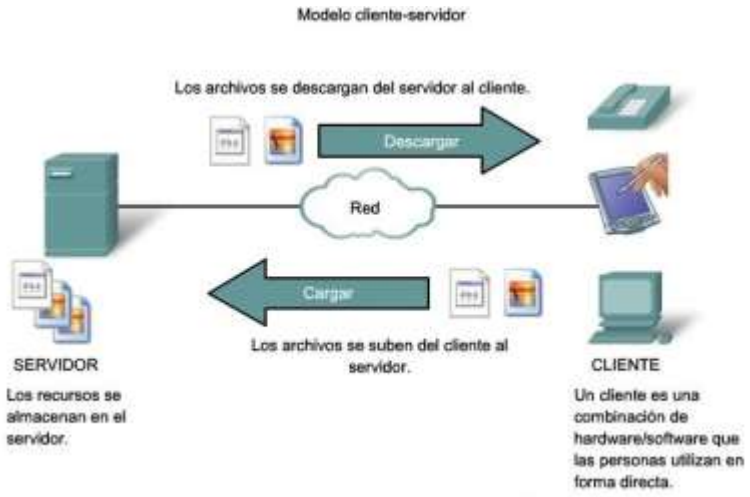


Figura 8.- Capa de nivel superior, tomada de sites.google.com, elaborado por Enrique Franco

2.2.2 Redes inalámbricas

Se conoce como redes inalámbricas aquellas que son usadas en informática para permitir una conexión entre distintos dispositivos sin necesidad de un medio guiado siendo las ondas electromagnéticas las pioneras en la comunicación, (Offensive Security, 2014).

La transmisión y recepción de los datos es realizado comúnmente por dispositivos conocidos como Access Point los que cuentan con diferentes antenas según el estándar definido por la IEEE 802.11 siendo actualmente una de las tecnologías más prometedoras.

Una de las ventajas que tienen las redes wireless a diferencia de las cableadas es que tienen mucho menos costo de operación debido a que no se necesita cables para conectar nodos, así como la facilidad en cuando a desplazamiento de un lugar a otro.

Asimismo, debido al gran impacto que generan se han creado diferentes estándares que ayuden a mejorar la calidad de la señal a sí mismo el aumento de su velocidad en tal punto que

en muchas ocasiones pueden llegar a tener las mismas velocidades que un medio cableado, (Offensive Security, 2014).

De igual forma una desventaja a este tipo de escenarios es que la seguridad debe ser mucho más exigente y son más propenso a ataques debido al medio siendo visible por un atacante según la potencia que el equipo irradie.

Figura 9.- Comunicación en 802.11, tomada de sites.google.com, elaborado por Enrique Franco

2.2.3 Estándares wireless

Como se mencionó las redes wireless son definidas en base al estándar del Instituto de Ingenieros Eléctricos y Electrónicos IEEE 802.11 siendo una institución encargada de indicar las normas o procedimientos que se deben aplicar a las redes tanto de forma inalámbrica como cableada sin importan el modelo de equipo o la frecuencia de operación es decir tengan operatividad multi fabricante

Los estándares IEEE definen la forma en la que se desarrolla una tecnología, así como su operatividad con los demás proveedores del mercado es decir el usuario final no debe sentir algún tipo de afectación al querer trabajar.

Actualmente existen diferentes estándares definidos en base al estándar 802.11 en el que según la velocidad de transmisión y la cantidad de bandas o canales tienen ciertas mejoras en relación a uno u otro tal como se menciona a continuación:

- **Estándar 802.11a. -** El estándar 802.11a es definido en las redes inalámbricas como aquel que cuenta con un mayor rendimiento a diferencia del 802.11b/g llegando a alcanzar en el envío y recepción de datos hasta 54 Mbps en la banda de 5GHz.

802.11a especifica 8 canales para el funcionamiento de sus bandas de frecuencia en el que puede llegar a operar y crear múltiples SSID, (Offensive Security, 2014).

- **Estándar 802.11b. -** Utiliza frecuencias basadas en señalización de 2.4 GHz de velocidad a su vez permite ampliar la tasa de transferencia de hasta 11 Mbps. Algo a tener en consideración es que el estándar puede llegar a tener hasta una gama de 300m en un área de entorno libre, (Offensive Security, 2014).
- **Estándar 802.11g. -** Desarrollado en 2003 como una mejora del 802.11b con la idea principal de aumentar la velocidad de transmisión de hasta 54 Mbps usando los 2,4 GHz de ancho de banda utilizados en su antecesor.

802.11g utiliza la transmisión mediante el protocolo basado en prevención de colisiones (CSMA/CA) (Carrier Sense Multiple Access with Collision Avoidance).

Por lo general las velocidades en las que opera el estándar varía en relación de la negociación con los activos o equipos finales en el que se puede trabajar con una tasa de 6 Mbps hasta una de 54 Mbps, (Offensive Security, 2014).

Una desventaja de este protocolo es que al igual que 802.11b tienen un alto nivel de interferencia afectando a los equipos teniendo problemas de red.

- **Estándar 802.11n. -** Desarrollado para ser implementado en redes inalámbricas de área amplia en el que se ofrece altos niveles de rendimiento a diferencia de los estándares Legacy donde a diferencia de los estándares anteriores mencionados el estándar 802.11n proporciona mejor conectividad en los equipos, así como un mayor ancho de banda donde al hacer uso de los cabezales de extensión se puede llegar a obtener hasta 300 Mbps en conectividad. (Offensive Security, 2014).
- **Estándar 802.11ac. -** Desarrollado entre los años 2011 y 2013 el protocolo 802.11ac consiste en mejorar la tasa de transferencia hasta de 433 Mbps consiguiendo velocidades teóricas de 1.3 Gbps en el que hace uso al igual que 802.11n de MIMO (Multiple In Multiple Out) estableciendo diferentes canales para poder pasar una gran cantidad de tráfico. De igual manera se logra hacer uso de la banda de 5 GHz ampliando su ancho de banda a 160 MHz., (CEH, EC-Council Certified Ethical).
- **Estándar 802.11ax. -** Conocido como el estándar Wifi 6 desarrollado por Wi-Fi Alliance es un tipo de red inalámbrica que puede operar en las redes ya existentes de 2.4 GHz y 5 GHz además de incluir OFDMA logrando una velocidad hasta de 37% mucho mayor a relación de 802.11ac. (Offensive Security, 2014).

2.2.4 Modo de operación de las WLAN

Al referirnos a las redes inalámbricas se debe considerar que existen 2 tipos de operaciones o funcionamiento con los siguientes detalles:

2.2.4.1 Modo de infraestructura (Red Centralizada)

Conocido como punto de acceso en el que se usa diferentes AP y en base a ello se tiene una mayor cobertura donde según como el o los equipos se configuren se pueden gestionar de forma centralizada o individual donde según la necesidad o forma de uso el escenario a implementar va a diferir de otro.

En este tipo de modo opera el equipo inalámbrico de forma centralizada respondiendo a cada una de las peticiones que desea el cliente, encargándose de transmitir el diseño planteado, , (Offensive Security, 2014).

Figura 10. - Red centralizada, tomada de sites.google.com, elaborado por Enrique Franco.

2.2.4.2 Modo Ad-Hoc (Red Descentralizada):

Es un tipo de conexión inalámbrica que es mucho más económica a la hora de diseñar redes wireless debido a que no es requerido un equipo centralizado a diferencia de la red centralizada un problema a este tipo de red es que no es tan escalable y produce fallas en cuanto a la transmisión de paquetes debido a que los equipos finales deben ser capaz de transmitir y procesar datos haciendo que se generen cuellos de botella. Una red Ad-Hoc también es conocida como un IBSS (Conjunto de servicios básicos independiente) el cual consiste en tener una comunicación de 2 STAs o equipos sin necesidad de un Access Point. Por lo general este modo de comunicación muchas veces toma el nombre de comunicación peer-to-peer ya que a la hora de operar existe solamente dos responsables en la comunicación a diferencia de un medio con APs, , (Offensive Security, 2014).

Figura 11.- Red AD-Hoc, tomada de sites.google.com, elaborado por Enrique Franco

2.2.4.3 Wireless Distribution System (WDS)

WDS es una tecnología inalámbrica que tiene como finalidad establecer una intercomunicación entre diferentes puntos de accesos en una red llegando a cubrir zonas muchos más amplias, en la actualidad según la marca del equipo algunos fabricantes conocen a esta tecnología con diferentes nombres, (CEH, EC-Council Certified Ethical).

Por lo general una WDS busca mediante múltiples puntos de acceso establecer diferentes vínculos o comunicación permitiendo ampliar el área de cobertura sus modos de operación pueden ser:

- Wireless Bridging: Permite que solamente los APs WDS puedan establecer comunicación con otros equipos
- Wireless Repeating: Permite una comunicación entre los diferentes equipos

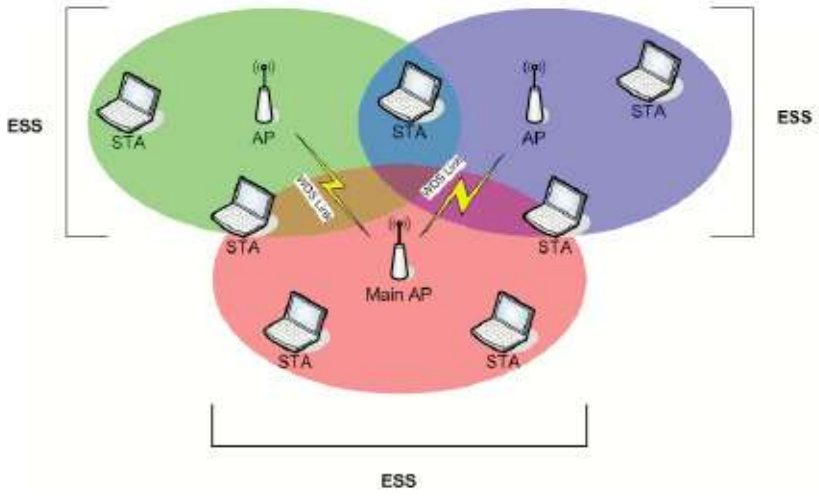


Figura 12.- Red WDSc, tomada de sites.google.com, elaborado por Enrique Franco

2.2.4.4 Modo Monitor

No es considerado un modo inalámbrico, pero se hace mucha referencia de este tipo de modo ya que es común usarlo en ataques a redes inalámbricas ya que a través de una tarjeta inalámbrica se puede lograr el monitoreo de los paquetes que se reciben sin realizar ningún tipo de filtrado por lo general el modo monitor tiene la misma funcionalidad a un modo promiscuo, (CEH, EC-Council Certified Ethical).

2.2.5 Roaming

Es una de las tecnologías en la actualidad muy utilizada debido a que permite realizar un desplazamiento en un sitio donde de existir diferentes puntos de accesos permitirá establecer una conexión con el que cuente mejor nivel de potencia logrando una mejor operabilidad y

evitando la desconexión y conexión a equipos inalámbricos de forma manual en tanto equipos móviles como teléfonos o laptops, (Offensive Security, 2014).

Para que el Roaming trabaje es necesario activar sus dos protocolos claves siendo el 802.11k el encargado de enviar notificaciones de tránsito a los diferentes APs conectados a la red en el que a medida surja el desplazamiento el AP con mejor cobertura pueda vincular el equipo, donde, el protocolo 802.11v será el encargado de realizar la desconexión del dispositivo forzando a la estación de trabajo se reubique al equipo más cercano.

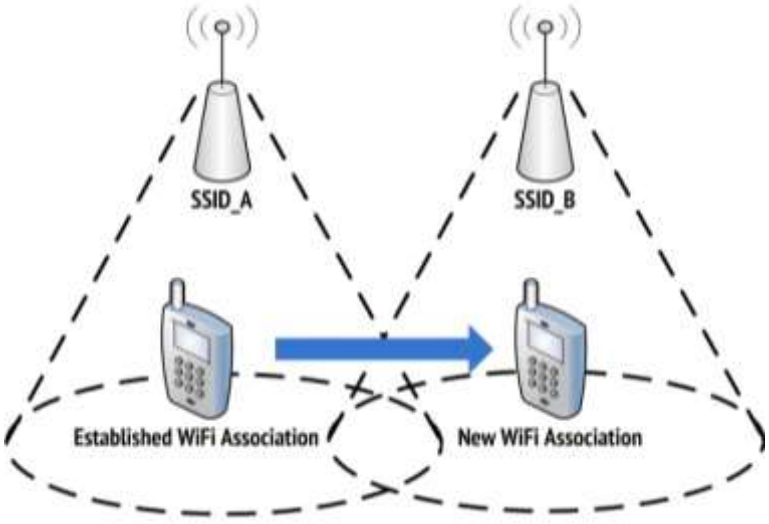


Figura 13.- Roaming en redes, tomada de sites.google.com, elaborado por Enrique Franco

2.2.6 Métodos de encriptación en redes wireless

Con el tiempo a medida que se las redes wireless han ido evolucionando se ha necesitado medidas de protección que eviten problemas en cuanto a la disponibilidad del servicio donde para ello se crearon mecanismos de cifrado que ayuden de una u otra a establecer seguridad en el medio inalámbrico. Una técnica muy común de hacerlo es a través de PSK (Pre Shared Key) donde un usuario para poder conectarse al SSID deberá proporcionar una contraseña para establecer la conexión logran brinda una seguridad en la red, (Arévalo, 2018).

El problema está en que la forma de operación en el que se requiere hacer uso de un PSK se ha realizado desde los primeros métodos de cifrado en el que hoy en día existen herramientas que pueden mediante ataques de diccionario o fuerza brutal obtener el hash de la clave siendo vulnerable en muchas situaciones a este tipo de amenazas.

Otro punto también a resaltar es que según el protocolo utilizado en las redes wireless mayor complejidad para ello a continuación se detalla los protocolos comúnmente usados en las redes inalámbricas y con ello la vulnerabilidad que representa de ser utilizados en la actualidad.

2.2.6.1 Protocolo WEP (Wired Equivalent Privacy)

Es un Sistema de cifrado definido para redes inalámbricas por la IEEE 802.11 que tiene como finalidad cifrar el medio por el cual se establece la conexión a la hora de querer conectarse a un SSID. El protocolo WEP está basado en el algoritmo RC4 en el que las longitudes o cadenas de bits para las claves no excedían los 64 bits siendo estos (40 utilizados para clave y los otros 24 para vectores de inicialización), el algoritmo WEP al usar este tipo de cifrado hace que sea susceptible en el que mediante ataques de MITM (Hombre en el medio) se puede llegar a capturar los hashes y con los respectivos ataques de fuerza bruta se puede obtener las credenciales, (Arévalo, 2018).

En la actualidad se recomienda que no se haga uso de este tipo de cifrado siendo este último utilizado en las redes inalámbricas hasta el 2004 en el que Wi-Fi Alliance dio por anunciado el nuevo protocolo para redes inalámbricas WPA.

2.2.6.2 Autenticación del protocolo WEP

El sistema de encriptación WEP es un método que tiene como finalidad realizar la autenticación en redes inalámbricas el cual diferentes métodos siendo el sistema abierto y la clave compartida, (Asadovay & Caiza, 2013).

En el que un usuario de querer acceder por medio de credenciales debería ingresarlas en algún SSID que este siendo irradiado por un AP y de ser válido automáticamente se establecerá una conexión permitiendo el acceso a Internet o recursos de una red LAN de equipos ubicados en el mismo segmento.

Autenticación de sistema abierto: Es aquel sistema que no requiere de ningún método de autenticación para permitir conexión en la red, donde por lo general este sistema es usado en la actualidad para las redes invitados de organizaciones en el que no se usa el protocolo WEP, pero si se establece este método para navegación.

Autenticación mediante PSK: Dentro del formato de autenticación del protocolo WEP existen 4 fases que permiten establecer conexión entre el AP y el End Point.

- El End Point envía una solicitud para ser autenticado en el AP
- El AP envía un reply con una cadena de caracteres en texto claro
- El End Point deberá cifrar la cadena de texto usando la clave del protocolo WEP.
- El AP procederá a descifrar el texto llegando hacer una comparación con el texto que fue enviado en el que valida si es idéntico donde de ser así se permitirá el acceso, así como la navegación.

2.2.6.3 WPA

Se conoce como WPA (Wi-fi Protected Access) al protocolo utilizado para ofrecer seguridad a las redes inalámbricas. A diferencia de WEP el protocolo WPA cuenta con un diseño más robusto a la hora de permitir una autenticación haciendo uso de protocolos avanzados como EAP (Extensible Authentication Protocol) el cual es aplicado a nivel de certificados digitales o autenticación en túneles el cual tiene como finalidad asegurar ofrecer mayor seguridad a la red LAN. WPA fue diseñado para operar mediante un servidor que permita la autenticación a nivel de 802.1x en el que mediante una comunicación dedicada se establecen diferentes claves de acceso para cada usuario, (CEH, EC-Council Certified Ethical).

Una desventaja de este protocolo es que se siguen usando cadenas de caracteres para establecer claves compartidas en el que la longitud del cifrado a aplicar no es tan robusta siendo efectivo para realizar ataques de fuerza o por diccionario llegando obtener las credenciales de acceso siendo un riesgo para la integridad de la información.

2.2.6.4 WAP2

A diferencia de sus antecesores WPA2 cuenta con una mayor robustez en su cadena de bloques al igual que combinaciones de cifrado como AES o TKIP permitiendo corregir o aplicar combinaciones más robustas utilizadas en redes wireless. WPA2 ha tenido en la actualidad una gran aceptación en el que debido a ello se han creado diferentes métodos de autenticación siendo WPA2-Personal el comúnmente utilizado en redes wireless y WPA2-Enterprise el cual permite realizar una autenticación 802.1x con el protocolo EAP llegando a fortalecer las formas de acceso a las redes wireless tradicionales en el que se elimina el uso de una sola credencial y aumentando los niveles en cuanto a seguridad de la red, (CEH, EC-Council Certified Ethical)..

Para mayor detalle en cuanto a las ventajas o desventajas de cada método o mecanismo de cifrado se presenta una comparativa de los puntos más importante:

Tabla 1.- Tipos de cifrados en redes Wireless

	WEP	**WPA**	**WPA2**
Año de publicación	1997	2003	2004
Cifrado	RC4	TKIP con RCA	AES-CCMP
Tamaño de clave	64 y 128 bits	128 bits	128

	WEP	WPA	WPA2
Tipo de cifrado	Flujo	Flujo	Bloque
Autenticación	Sistema abierto y clave compartida	Clave compartida y 802.1x con EAP	802.1x con EAP y sistema con PSK

Información tomada de la investigación directa. Elaborado por Enrique Franco

2.2.7 Seguridad en redes inalámbricas

Hoy en día una contraseña a nivel de red wireless no es suficiente por lo que cada día se busca aplicar diferentes métodos que permitan hardenizar los componentes inalámbricos como son los Access Point, siendo las vlan y el portal cautivo los más aceptados logrando no solo impedir el acceso no autorizado, sino que también un control o administración centralizada teniendo un mejor panorama de la red, (Chulli & Espinoza, 2019).

2.2.7.1 Vlans

Las Virtual LAN o Vlans son una tecnología que permiten lógicamente dividir un equipo físico de conmutación conocido como switches en múltiples dominios de broadcast a tal punto de segmentar las redes e impedir que usuarios de vlans diferentes se comuniquen a menos que exista un equipo capaz de realizar el enrutamiento. Por lo general las Vlans son aplicadas en las redes wirelesss con el fin de definir un segmento de red que gran parte del tiempo no puede acceder a los recursos de la red interna, (Netlearning, 2015).

Un punto muy importante por mencionar es que según el equipo inalámbrico la comunicación en las vlans puede darse de manera estática o de forma dinámica siendo el ultimo utilizado con protocolo de autenticación EAP el mismo que previamente fue definido.

Al usar las vlans en los medios wireless se logra mitigar en gran medida los ataques de red como smurfing o ARP Attack debido a que si se llega a comprometer una vlan las demás no serán afectadas.

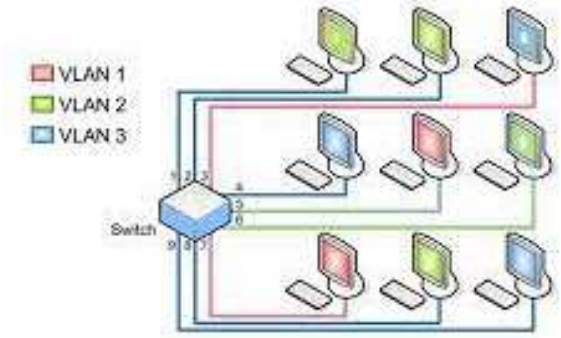


Figura 14.- Redes virtuales, tomada de sites.google.com, elaborado por Enrique Franco

2.2.7.2 Portal Cautivo

Aplicación utilizada comúnmente en los medios inalámbricos con el objetivo en muchas veces de recopilar información por lo general es una página que se despliega una vez que se establece comunicación con un SSID sin un método de cifrado, al desplegarse el portal se solicita que ingrese información o que utilice métodos para registro, si el registro es exitoso, se le otorga una dirección ip así como dns, gateway y máscara de red caso contrario no podrá autenticar y con ello acceder a Internet, (Purple AI, 2021).

Por lo general un hostpot o portal cautivo no tiene comunicación a otro segmento de red debido a que se busca proteger los recursos internos de una organización es decir que no habrá más allá de una conexión a Internet. En la actualidad los portales cautivos son vinculados con redes cableadas evitando algún tipo de acceso de usuarios no éticos.

Los hostpot pueden ser instalados en equipos con poca capacidad de procesamiento ya que solo permiten la validación con los usuarios cabe mencionar que existen portales cautivos tanto para sistemas opensource así como de código fuente privatizados, de igual forma en equipos de baja gama de enrutamiento como por ejemplo el WRT54-G Linksys o más avanzados como equipos Mikrotik o incluso Firewall de nueva generación.

Figura 15.- Portal cautivo Fortinet, tomada de sites.google.com, elaborado por Enrique Franco.

2.2.8 Control de acceso

Es el enfoque otorgado a las redes de computadoras que consisten en utilizar diferentes tecnologías de seguridad que puedan ser aplicadas a EndPoint teniendo entre ellos los más comunes como (Antivirus, sistema de prevención y detección de intrusos, Radius, entre otros) permitiendo reforzar el acceso tanto a nivel de red LAN como Wireless (Cevallos, 2017).

2.2.9 Radius

El protocolo Radius por sus siglas en inglés (Remote Authenticatin Dial In User Service) es un protocolo definido en los archivos de la IETF conocidos como RFC (Request for Comment), tiene como finalidad proporcionar servicios mediante la gestión centralizada es decir a través de la autenticación de usuarios en las redes se podrá distribuir acceso a recursos, (Cepeda & Proaño, 2007)

Radius es un modelo basado en cliente-servidor el que tiene un servidor NAC (Network Access Control) el cual cumple la función de un cliente para el servidor Radius. Para ello el cliente interactúa con el servicio mandando información hacia el servidor el cual según su configuración buscará permitir o denegar servicios. De no realizarse la autenticación de manera efectiva el servidor puede redireccionar las peticiones hacia servidores alternativos como pueden ser portal cautivo, o redes separadas de los servicios principales. Algo a tener en cuenta es que cuando el servidor recibe las peticiones este tiene la finalidad de validarlas mediante el descifrado del paquete obteniendo usuario y contraseña.

La información recopilada es pasada a un sistema de seguridad el que se encarga de validar que sea correcta para ello existen muchos tipos de sistemas de autenticación teniendo principalmente a NTLM (Network Technology Lan Magager) de Windows en su versión 1 y 2, asimismo, el protocolo basado en UNIX, NTLM, (CEH, EC-Council Certified Ethical). Una vez validada la información en los sistemas antes mencionados, la misma, es devuelta hacia el sistema y el usuario podrá utilizarla siempre y cuando esta sea correcta. Es necesario mencionar que todo proceso de validación que se realice será aumentado en los accounting en base a la IP que hizo la solicitud. Una de las ventajas más importante de RADIUS es la forma en la que puede procesar sus sesiones mediante los contadores con ello puede determinar a qué hora comienza y termina una conexión.

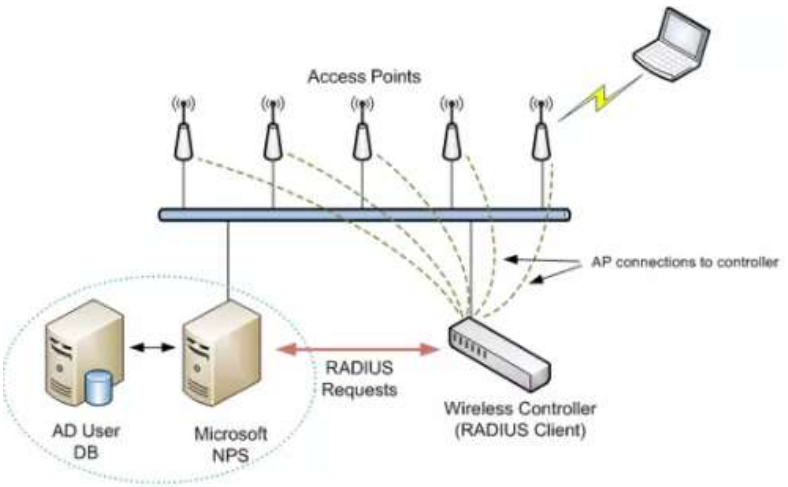


Figura 16.- Protocolo RADIUS, tomada de sites.google.com, elaborado por Enrique Franco

En la actualidad existen diferentes mecanismos de autenticación en el que se aplica el uso del protocolo Radius en el que se incluyen diferentes variantes según los requerimientos entre ellos la seguridad con la que se comparte la información a la hora de realizar la autenticación en las redes. Por lo general implementar un servidor Radius demandaba mucho tiempo ahora existen sistemas basados en software libre que permiten optimizar la carga operativa permitiendo tener servicios aplicados en redes de diferentes tamaños.

2.2.9.1 Funciones de un servidor RADIUS

Permite ofrecer diferentes mecanismos de autenticación en el que un usuario puede tener conectividad a un sistema para ello existen diferentes métodos siendo entre ellos 802.1x basado al medio cableado, así como EAP o EAP-TLS, entre otros.

Hoy en día el protocolo Radius es multi-fabricante es decir que puede funcionar con cualquier marca además de servicios de VPN como OpenVPN si este último es configurado correctamente, (Mendoza, Barraza, Estrada, Esquivel, & Calderón, 2016).

2.2.10 IEEE 802.1X

Definido por la IEEE es un protocolo que brinda seguridad en la capa de acceso en la red, el protocolo 802.1x está basado en la autenticación de puertos en el que los activos conectados en switches administrables pueden recibir configuración previa al igual que ajustes o datos personalizados como segmento de red según al grupo de puerto que pertenezca, (Mendoza, Barraza, Estrada, Esquivel, & Calderón, 2016)..

802.1x está disponible en la mayor parte de switches administrables que tengan la opción de configuración y permitan a los suplicantes validarse con el servidor centralizado y recibir sus parámetros previamente definidos, (Nuno & Barraca, 2019).

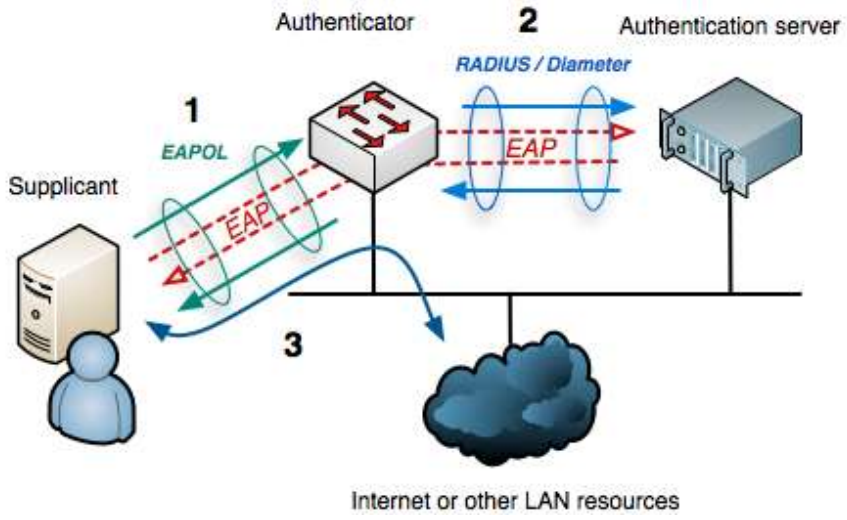


Figura 17.- Estándar 802.1x, tomada de sites.google.com, elaborado por Enrique Franco

Un factor por mencionar es que las redes wireless también pueden hacer uso de este mecanismo en el que un equipo configurable puede ofrecer este tipo de autenticación mejorando la forma de acceso a la red y descartando la clave compartida tradicional entre todos los equipos de red.

Existen diferentes métodos para brindar un control de acceso permitiendo brindar accesibilidad a la red los cuales son explicados a continuación.

2.2.10.1 EAP

Por sus siglas sen Ingles (Extensible Authentication Protocol) es un framework usado en las redes ethernet inalámbricas de tipo punto a punto esto no significa que haya limitación en la parte cableada. Nuno y Barraca (2019) en su estudio menciona que, EAP es el estándar oficial para las redes inalámbricas debido a que fueron adoptados para sus mecanismos oficiales de autenticación siendo entre ellos: EAP-MD5, EAP-TLS, EAP-AKA, PEAP, EAP-SIM.

En las redes inalámbricas cuando se desea establecer una comunicación el protocolo EAP ofrece mecanismo seguro para la autenticación a tal punto de establecer una contraseña única usando cifrado de tipo TKIP o AES.

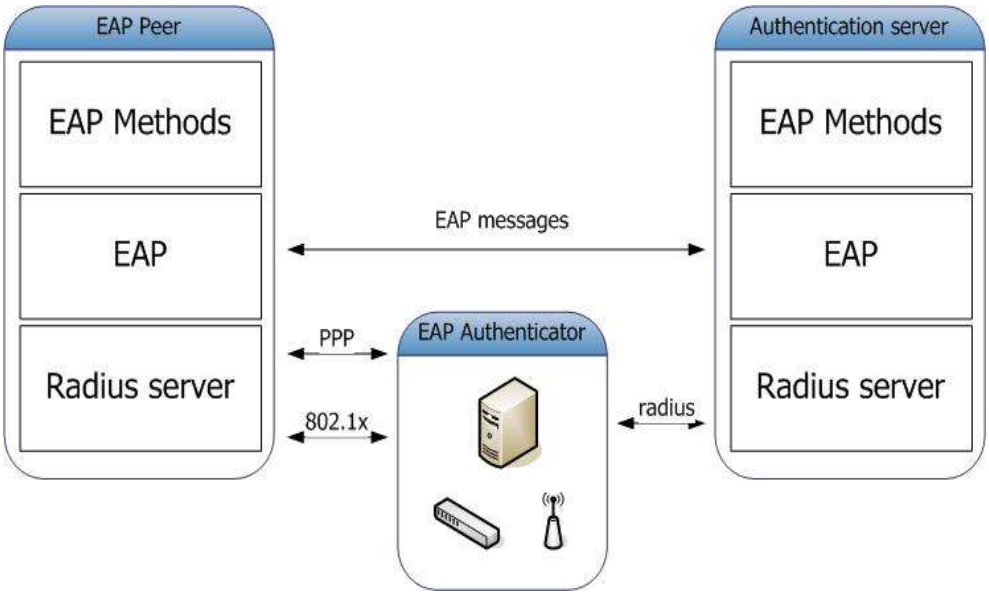


Figura 18.- Extensible authentication protocol, tomada de sites.google.com, elaborado por Enrique Franco

2.2.10.2 EAP-TLS

Es el tipo de autenticación con mayor uso debido a la facilitada con la que existe compatibilidad con el protocolo de trasporte seguro. La comunicación se establece en base a certificados emitidos para establecer la comunicación donde para ello es necesario utilizar el tipo de conexión cliente-servidor.

Un problema común de este protocolo es la administración de los certificados debido a que debe dar de ambos lados lo que podría ocasionar problemas de configuración debido a la tarea compleja que esto lleva en sí, (Nuno & Barraca, 2019).

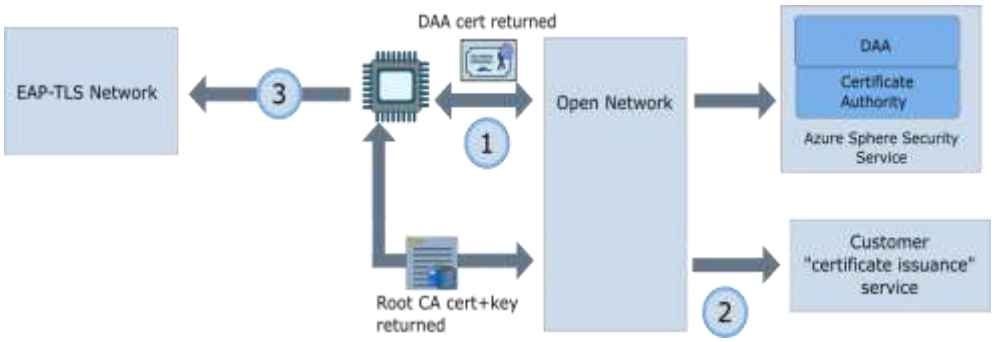


Figura 19.- Extensible Authentication Protocol con TLS, tomada de sites.google.com, elaborado por Enrique Franco

2.2.10.3 EAPoL

El Protocol Extensible Authenticación Protocolo ver Local Area Network (EAPoL) es utilizado en la comunicación del estándar 802.1x en las redes cableadas en los diseños basados en control de acceso por puerto en el que se logra interactuar con los recursos de la red si y solo sí la comunicación previamente es establecida, (Ramakrishanan & Veerakumar, 2019).

EAP tiene gran similitud con EAP debido a que usa una simple encapsulación en sus datos permitiendo ejecutar sobre la LAN este tipo de servicios, cabe mencionar que para el proceso mencionado solo 3 equipos participan del establecimiento de comunicación.

- El equipo suplicante es decir el EndPoint conectado a un puerto de acceso solicita ser autorizado por el servidor de autenticación
- El autenticador es decir el equipo de conmutación establece controles de red basados al protocolo EAP
- El servidor de autenticación el encargado de validar las solicitudes recibidas por el autenticador.

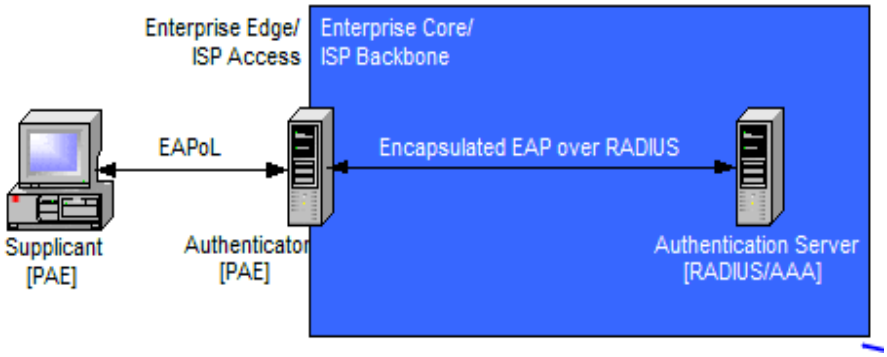


Figura 20.- Authentication con EAPoL, tomada de sites.google.com, elaborado por Enrique Franco

2.2.10.4 PEAP

Protocolo desarrollado por Cisco, Microsoft y RSA Security encargado de cifrar el protocolo EAP aplicando en sus cabeceras encriptación a través de TLS (Transport Layer Security) estableciendo un túnel seguro de comunicación, (Taufik & Imam, 2021).

El objetivo de PEAP es proporcionar protección en los canales de comunicación que EAP no ofrece.

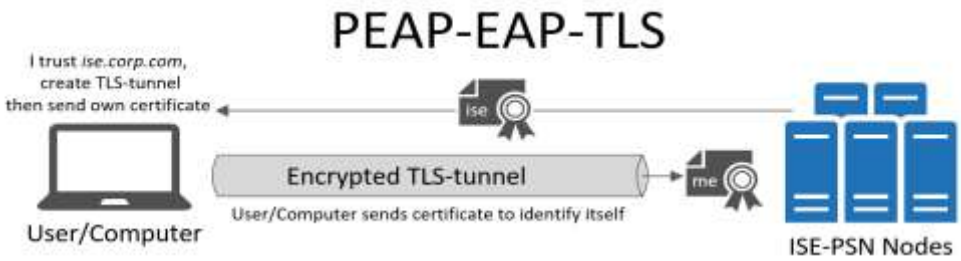


Figura 21.- PEAP con EAP-TLS, tomada de sites.google.com, elaborado por Enrique Franco

2.2.11 Vulnerabilidades en redes wireless

Como se mencionó previamente las redes inalámbricas cuentan con varios problemas en cuando a seguridad se trata siendo el PSK el mayor problema debido a que es una clave de autenticación a nivel de red en el que en muchos casos personas no atadas a la organización tiene acceso, (Offensive Security, 2014).

Por otro lado, otro error grave es la longevidad con el que las credenciales son creadas llegando muchas veces nunca ser cambiadas produciendo no solo acceso no autorizado sino también alteración a la confidencialidad de la información.

Existen otro tipo de vulnerabilidades o amenazas que afectan directamente a los SSID logrando mediante técnicas apropiarse de las credenciales de los equipos o de las redes inalámbricas a tal punto de desplegar una red idéntica y hacer que los usuarios naveguen sin que se den cuenta que todos sus datos son procesados por el atacante, este tipo de amenazas son:

- **Ataque de diccionario. -** Es un ataque empleado a las redes wireless que por lo general es dado por un atacante o actor malicioso con el fin de descubrir una contraseña y así acceder a los recursos de terceros. Para efectuarse este tipo de ataque se tiene un diccionario de claves comúnmente conocidos que pueden ser elaborado por el atacante o descargado de Internet el que con herramientas de hacking pueden llegar a vulnerar el sistema. Cabe destacar que contraseñas menores a 8 caracteres sin importar el protocolo con el que estén cifrado serán descubiertas siendo el primer factor de amenaza a proteger, (Offensive Security, 2014).

Es recomendable tener contraseñas mayores a 8 letras incluyendo números, símbolos y caracteres raros logrando que el proceso sea muy lento llegando a mitigar la amenaza.

- **Fuerza bruta**. - Ataque muy parecido al anterior, pero a diferencia del ataque de diccionario en este método se crean miles y miles de contraseñas las cuales son combinadas con el fin de tener éxito y descubrir las credenciales. Debido a que este ataque necesita combinar las contraseñas requiere de más tiempo y recursos, (Offensive Security, 2014).

2.2.12 Windows Server

Es una distribución de Windows usado para el ámbito empresarial a nivel de servidores cuenta con una alta gama de soluciones y complementos fáciles de administrar o configurar.

Según la distribución se requiere de diferentes características de hardware, un punto muy importante es que Windows Server cuenta con Active Directory y NPS los mismos que serán útiles a futuro para el presente trabajo de investigación, (Windows, 2022).

Del mismo modo, Windows Server puede ser instalado en versión de prueba de 90 días donde posterior a ello se requiere una licencia para funcionamiento.

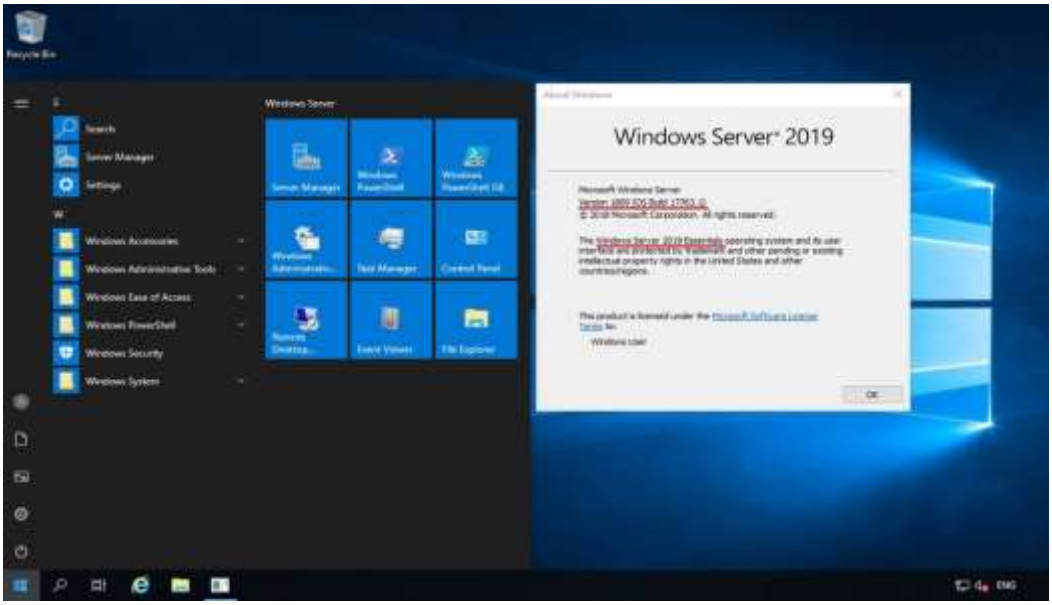


Figura 22.- Windows Server, tomada de sites.google.com, elaborado por Enrique Franco

2.2.13 Active directory

Active Directory es un servicio implementado por Microsoft que permite tener un control jerárquico a nivel de redes permitiendo gestionar, administrar o configurar equipos de forma mucho más sencilla y en el menor tiempo posible, (Díaz, 2021).

Active directory está basado en el estándar X.500 en el que se establece las funciones de un servicio de directorio al igual de cuáles son los distintos protocolos que utilizar.

Se maneja por objetos que están relacionados a los componentes de red, como usuarios así misma asignación de recursos o políticas de acceso al igual que los contenedores o los diferentes roles que existen dentro del servicio.

Active directory actualmente puede ser implementado en sitio o en la nube siendo este último el uso en pago por suscripción o pago por lo que usas.

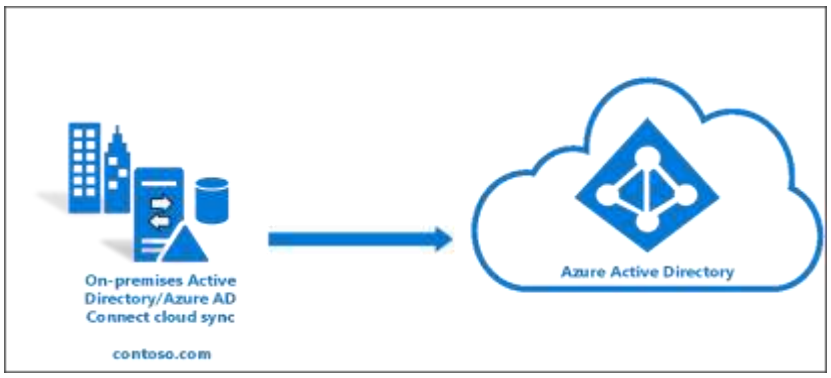


Figura 23.- Directorio activo, tomada de sites.google.com, elaborado por Enrique Franco

2.2.14 NPS de Windows

Network Policy Server permite crear políticas para hardenizar la organización a través de políticas de acceso utilizando Radius logrando centralizar las configuraciones y administración de la red a través de un dominio para autenticación y autorización, (Windows server, 2021).

NPS permite centralizar los ajustes de configuración mediante diferentes características como son la Autenticación, Autorización y los contadores o Accounting.

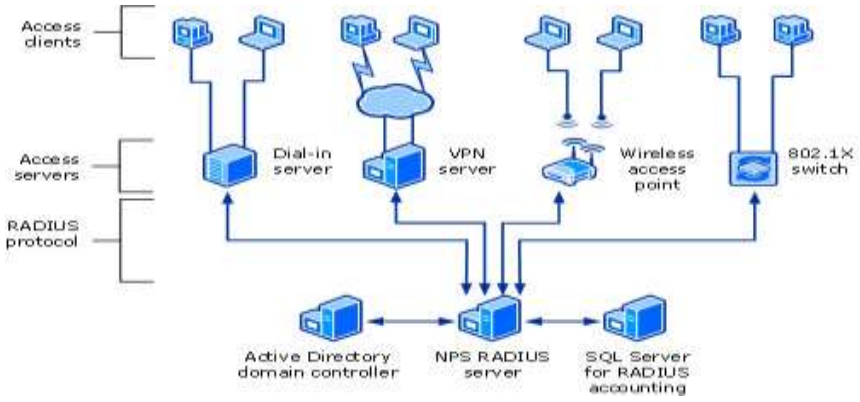


Figura 24.- Network Policy Server, tomada de sites.google.com, elaborado por Enrique Franco

2.3 Definiciones conceptuales

PSK. - Se conoce como clave compartida la misma que consiste en una llave que permite establecer un canal seguro antes de que este sea utilizado, el PSK se utiliza en cifrados como

WEP, WPA y WPA2 en el que un Access Point como el cliente a conectarse deben compartir la misma clave para que la comunicación sea efectiva.

Radius. - Protocolo encargado de brindar seguridad de forma gestionada a través de la autenticación en el que los usuarios para acceder a un recurso de red deberán primero ser validados con el servidor y de coincidir los parámetros acordes a las políticas definidas se le otorgará parámetros de red.

802.11. - Estándar inalámbrico que permite comunicar a diferentes dispositivos móviles a la red mediante un medio no guiado el cual según al tipo de estándar a utilizar puede llegar alcanzar velocidades desde 1Mbps hasta 1.2Gbps.

Ethernet. - Tecnología enfocada en el uso de cable y la concatenación de hardware y software entre sí, al hablar de ethernet se hace referencia a la capa 2 del modelo OSI es la capa encargada de validar como se realiza la comunicación a través de un medio ya sea guiado o no guiado.

AES. - Cifrado por bloques de uso público que consiste en un cifrado de tipo simétrico capaz de soportar claves de cifrado de 128, 192 y 256 bits logrando mayor complejidad en las redes inalámbricas, el protocolo AES puede ser implementado tanto en hardware como en software.

Kerberos. - Protocolo de autenticación en redes que funciona en modalidad cliente-servidor, tiene como finalidad demostrar la identidad de manera segura en la red. Creado por el Instituto de Massachusetts. Un punto por mencionar de Kerberos es el tipo de autenticación debido a la protección que existe para evitar ataques de tipo relay o incluso eavesdropping. Asimismo, kerberos utiliza un tipo de criptografía simétrica.

Eavesdropping. - Conocida como la técnica de escuchar de manera secreta es decir se puede obtener información de una comunicación existente sin ser detectado.

NTLM. - Es un protocolo de autenticación utilizado en Windows a la hora de registrar sus usuarios de dominio, actualmente NTLM está en la versión 2 contando con mejoras de seguridad que la versión 1 no brindaba

TLS. - Protocolo encargado de cifra los datos en un sistema con el fin de mantener los sitios web seguros a los ataques de MITM. El protocolo TLS es una versión mejorada y más segura del famoso protocolo SSL.

2.4 Marco Legal

A través de la Ley Orgánica de Telecomunicaciones, se establece el conjunto de leyes que permitan brindar competencias en cuanto a la regulación, control, y administración a nivel

nacional, de acuerdo con lo establecido en los principios y derechos constitucionales, (Ley Organica de las Telecomunicaciones, 2015)

Según lo dispuesto en el artículo 3 de la Ley de Telecomunicaciones se establece que:

- Es necesario definir el desarrollo, así como el fortalecimiento en el área de las telecomunicaciones
- Incentivar el despliegue en cuanto a nivel de redes e infraestructura se requiere permitiendo mantener comunicación con sectores cercanos y aledaños.
- Impulsar al país para contar con servicios de alta velocidad y capacidad permitiendo obtener un crecimiento en cuando a operabilidad e Internet de banda ancha

De igual forma el Art 12 de la Ley Orgánica de Comunicación estipula que es necesario crear medios de comunicación que permitan generar participación, así como el acceso de frecuencias para estipulación de servicios de radio y televisión abierta, así como de suscripción.

El artículo 6 menciona que todo medio que sea capaz de brindar capacidad en cuanto a comunicación entre los diferentes usuarios es considerado como dispositivos de servicio final de red. En cuanto al funcionamiento de las redes el artículo 9 indica que las redes son clasificadas en base a dos grupos siendo ellos:

a) Redes privadas para comunicación de servicios internos
b) Redes públicas permitiendo el anuncio de sus servicios en Internet

Donde el articulo 13 menciona que se conocen como redes privadas aquellas que compartan una comunicación en políticas de ruteo internas es decir que no son anunciadas o procesadas en Internet y pueden usarse para desarrollos o pruebas de concepto.

El articulo 15 en cambio indica que las redes privadas son servicios que pueden ser distribuidos en sistemas privados para organizaciones o redes SOHO en el que no puede existir comunicación de forma directa a menos que existan políticas de ruteo previas.

Por otro lado, el Artículo 24 inciso 15 busca adaptar las medidas necesarias para procesar la seguridad en las redes a tal punto de resguardar la confiabilidad, disponibilidad e integridad de la información.

Por lo que el inciso 17 busca limitar, interferir, así como priorizar el derecho a los usuarios y con ello evitar, recibir u ofrecer contenido, aplicaciones o servicios de forma legal a través de Internet.

Asimismo, el articulo 29 referente a la regulación técnica menciona que es necesario establecer y supervisar con el fin de establecer la compatibilidad al igual que la calidad de los servicios ofrecidos con el fin de solucionar problemas relacionados con la seguridad.

En cuanto el Articulo 76 indica que todos los prestadores de servicios deberán poseer medidas de seguridad que garanticen la seguridad de sus servicios y no vean afectadas las vulnerabilidades de la red.

Capítulo III

Metodología de la Investigación y Propuesta

El presente capítulo de investigación tiene como finalidad definir las diferentes metodologías que serán empleadas para contribuir al trabajo de titulación.

Para ello es necesario definir las funciones de cada una de ellas y de qué manera serán empleadas en el estudio de factibilidad que permiten alcanzar objetivos y metas que se encuentran dentro de un sistema.

3.1 Tipo de investigación

Se hará uso del enfoque cualitativo debido a la profundidad con la que se podrá definir ideas permitiendo establecer características o elementos necesarios para el correcto entendimiento del proceso de autenticación mediante protocolo Radius y con ello definir la factibilidad de su uso.

Del mismo modo a través del enfoque cualitativo se busca interpretar los resultados generados con el fin de tener mayor conocimiento de la solución mediante una validación de datos.

3.2 Modalidad de la investigación

3.2.1 Bibliográfica

Utilizado en el presente trabajo con el fin de realizar un proceso investigativo en fuentes ya sea revistas, periódicos, libros, entre otros en el que se busca profundizar acerca del problema, permitiendo resolver en muchos casos la hipótesis planteada.

3.2.2 Descriptiva

Se busca explicar una situación actual a través de eventos, personas o grupos con el fin de validar un suceso en concreto. El método descriptivo lo que busca es conceptualizar los procedimientos a través de un análisis que incluya una participación del investigador llegando a comprobar un suceso.

- Se busca determinar el suceso de un problema
- Conceptualizarlo y definir una hipótesis

3.2.3 Exploratoria

Utilizado en el presente trabajo de investigación para el desarrollo de la autenticación en redes wireless mediante protocolo Radius obteniendo resultados concisos en cuanto a la operatividad del sistema.

3.2.4 Deductiva

Busca llegar a una conclusión general de los procesos analizados y con ello determinar el funcionamiento de un sistema o diseño donde en este caso se hace referencia a la autenticación Radius realizada en redes inalámbricas.

3.3 Técnicas de la investigación

Se conoce como técnicas de investigación al método u opiniones que se obtienen de diferentes usuarios sobre un estudio puntual con el fin de estratificar resultados y lograr reforzar el trabajo de investigación.

Por lo general se hace uso de diferentes aspectos que permitan definir el tipo de sondeo o verificación realizado sobre un tema, teniendo:

- Entrevista
- Encuesta
- Observación

3.3.1 Población y muestra

La empresa Serviorder S.A, actualmente no cuenta con suficiente personal operativo para desarrollar las actividades referentes a redes en la organización debido a la reducida cantidad de colaboradores pertenecientes a la empresa.

Por lo que la población a escoger es mínima (1 persona) que posee los conocimientos necesarios en cuanto a conectividad; proporcionando información relacionada con las preguntas a realizarse.

3.3.2 Entrevista

Se conoce como entrevista a la técnica que se utiliza para realizar la recopilación de datos sobre una información específica de un tema planteado dentro del proceso de la investigación. Por lo general el proceso de la entrevista se divide en: entrevista estructurada, semiestructurada o no estructurada.

Para el estudio el tipo de entrevista que mejor se adapta es la de tipo semiestructurada debido a que permite obtener opiniones de manera abierta siguiendo un cuestionario definido.

La entrevista será realizada a un especialista en el área de las redes y telecomunicaciones con el fin de obtener conocimientos sobre el tema y permitir así tener una mejor gestión en cuanto al análisis de factibilidad en la autenticación de usuarios mediante el protocolo Radius en el sistema de dominio.

3.3.3 Entrevista semiestructurada

Se define el modelo de entrevista semiestructurada que permitirá tener una cantidad de preguntas referentes al tema permitiendo la recopilación de los datos de manera abierta por parte del especialista en redes y telecomunicaciones lo que permitirá tener una explicación más amplia en cuanto al tema a tratar.

3.3.4 Entrevista a especialista en redes y conectividad

Cómo se mencionó previamente se realizará la recolección de información a través de la entrevista la misma que está dirigida a un personal especializado en el área de redes y conectividad con el fin de obtener una perspectiva al uso de autenticación Radius en redes wireless mediante validación de usuario, para ello a continuación se detalla las preguntas realizadas con su respectivo análisis.

Serviorder S.A es una entidad que brinda servicios de configuración y soporte de Internet a través de un pequeño grupo de colaboradores las 24 horas del día, en el sitio como tal solo existe una persona encargada de la parte de infraestructura.

Debido a que es una empresa pequeña SERVIORDER S.A no tiene mucho nivel de complejidad cuando en redes se trata siendo incluso un diseño plano que en muchas veces de no estar bien gestionado podría generar conflictos a nivel de rendimiento.

Dicho esto, se procede a realizar las siguientes preguntas de investigación con el fin de obtener una perspectiva más amplia de cómo opera la red y si el uso de RADIUS puede llegar a beneficiar a los servicios con lo que cuenta la empresa.

1.- ¿Cuál es el problema que constantemente tienen la red wireless?

Respuesta: Qué existe un SSID el cual permite conectar a los usuarios de la red mediante el uso de credenciales no tan seguras, equipos con poca irradiación de señal, diferentes proveedores.

Análisis: Se puede apreciar que un problema común es el tipo de autenticación utilizado y con ello la robustez de la clave que existe esto es debido a que los usuarios muchas veces van en contra de políticas del área de tecnología como por ejemplo contraseñas con más de 8 caracteres que incluyan símbolos y números.

2.- ¿Qué método de autenticación actualmente considera más seguro?

Respuesta: Creo que el protocolo WPA3 actualmente ofrece mayor robustez en cuanto a cifrado mediante uso de claves con más de 128 bits de longitud, aunque no es compatible para todos los equipos lo que podría ser una desventaja.

Análisis: El especialista indica que el protocolo WPA3 es más seguro, pero así mismo cuenta con más incompatibilidad con los equipos por lo que no puede ser utilizado del todo a la hora de establecer contraseñas de tipo Pre-Shared Key.

3.- ¿Qué problema presenta al hacer uso de claves pre compartidas en las redes wireless?

Respuesta: Muchas veces existe personal que sabe cómo obtener la clave desde el ordenador y pueden llegar a distribuirlas por todo el lugar, volviendo la red de datos lenta e insegura debido a la gran cantidad de peticiones que se realizan a Internet por los diferentes usuarios.

Análisis: No existe una confidencialidad en el acceso de los usuarios a la red Wireless permitiendo conexión a cualquier persona que forme o no parte de la organización.

4.- ¿De qué manera se podría impedir el acceso no autorizado en las redes wireless?

Respuesta: Ocultar la red inalámbrica

Análisis: Se menciona que para evitar el problema se puede ocultar la red, aunque pueda llegar a ser una buena práctica no es recomendado ya que no brinda seguridad alguna y puede ser la red igual descubierta.

5.- ¿Considera necesario el uso de protocolos de autenticación externos a la hora de establecer la autenticación en redes inalámbricas?

Respuesta: Mantener el uso de credenciales mediante servidores centralizados sería muy buena práctica impidiendo el acceso no autorizado en la red.

Análisis: Se puede notar que el especialista en redes menciona que el uso de un protocolo externo que permita la validación de usuarios sería un método idóneo para la red que actualmente ellos manejan.

6.- ¿Conoce usted sobre la autenticación WPA2-Enterprise?

Respuesta: Si, si conozco

Análisis: el especialista menciona que, si conoce el protocolo como tal, así como su operación.

7.- ¿Qué ventajas considera que se obtienen de este tipo de autenticación WPA2-Enterprise frente a las autenticaciones mediante PSK (Pre-Share Key) tradicional?

Resultados: Control en cuanto a la gestión de acceso a la red wireless

Análisis: Tal como mencionan al hacer uso de un protocolo centralizado se logra tener mayor control de inicios mediante registros.

8.- ¿Considera necesario la autenticación de las redes wireless según el perfil de usuarios en el directorio activo?

Respuesta: Si, aunque desconozco su forma de operación, considero que sería muy efectivo en la red actual.

Análisis: El cliente no tiene noción al uso de Radius con directorio activo por lo que no conoce todas las ventajas que incluye este servicio.

9.- ¿A través de este tipo de autenticación considera que se mitiga en gran medida algún tipo de vulnerabilidad?

Respuesta: El acceso no autorizado en la red wireless

Análisis: Cómo menciona el cliente al hacer uso de Radius se mitiga en gran medida el acceso no autorizado teniendo un control de este

10.- ¿A nivel de autenticación Radius que tipo de comunicación considera necesaria establecer a la hora de realizar la autenticación en la red?

Respuesta: Una que incluya certificados o contraseñas robustas

Análisis: Es necesario hacer uso de mecanismos de autenticación robustos para hacer que la red pueda operar de forma correcta mediante una autenticación de dominio.

3.4 Análisis de la situación actual

Serviorder es una empresa encargada de brindar soporte a problemas de conectividad a usuarios finales que adquieren planes de Internet para hogar o corporativos, en sus oficinas actualmente se cuenta con un pequeño número de empleados que trabajan en diferentes horarios a fin de brindar soporte las 24 horas de día.

Algo muy importante a mencionar es que a nivel de redes la empresa cuenta solo con un switch de 48 puertos el cual interconecta a todos los demás usuarios en topología estrella en el que la conexión puede llegar a ser dedicada es decir un puerto para el usuario en específico o muchas veces realizar una expansión con switches no administrables para conectar más de un usuario o equipos finales.

El problema de esto es que al hacerlo el rendimiento del puerto y la velocidad de conexión se degrada llegando haber muchos problemas a veces, del mismo modo en la red Wireless existen dos puntos de acceso que están distribuidos en el lugar para conectar a los trabajadores de forma inalámbrica y poder realizar funciones adicionales.
La red utilizada es una red totalmente plana con un pool de direcciones de 254 debido a la máscara /24 utilizada para distribuir el servicio a todos los usuarios de la red.

Actualmente Serviorder S.A cuenta con diferentes componentes que se explican a mejor detalle a continuación:

- Se tiene un controlador de dominio el que permite tener una gestión centralizada del usuario mediante controles o GPO aplicados, el controlador de dominio que posee la organización no tiene mayores niveles de control por lo que puede ser adecuado para la autenticación de Radius.
- Switch administrable en el que se conectan los diferentes usuarios y tienen conexión hacia Internet e incluso a la red interna
- Un servidor DHCP encargado de asignar de forma dinámica direcciones IP y permitir que cualquier usuario que se conecte pueda obtener una dirección que le permita navegar y hacer funciones incluso la resolución de problemas
- Un servidor DNS encargado de realizar la resolución de nombres de Internet
- Access Point distribuidos en el lugar a fin de permitir conexión inalámbrica a los diferentes usuarios de la empresa.

Toda la red está conectada de forma centralizada es decir hacia el Switch administrable este último siendo altamente crítico debido a que si llegase a fallar toda la organización se quedaría sin servicio.

La empresa posee un total de 2 equipos inalámbricos que se encargan de proveer acceso a los colaboradores de SERVIORDER S.A., los equipos adicionales están conectado a un switch de distribución encargado de comunicar los usuarios. Otro punto por destacar es que existe un promedio de llamadas de 850 a 1250 que son diariamente atendidas por los colaboradores.

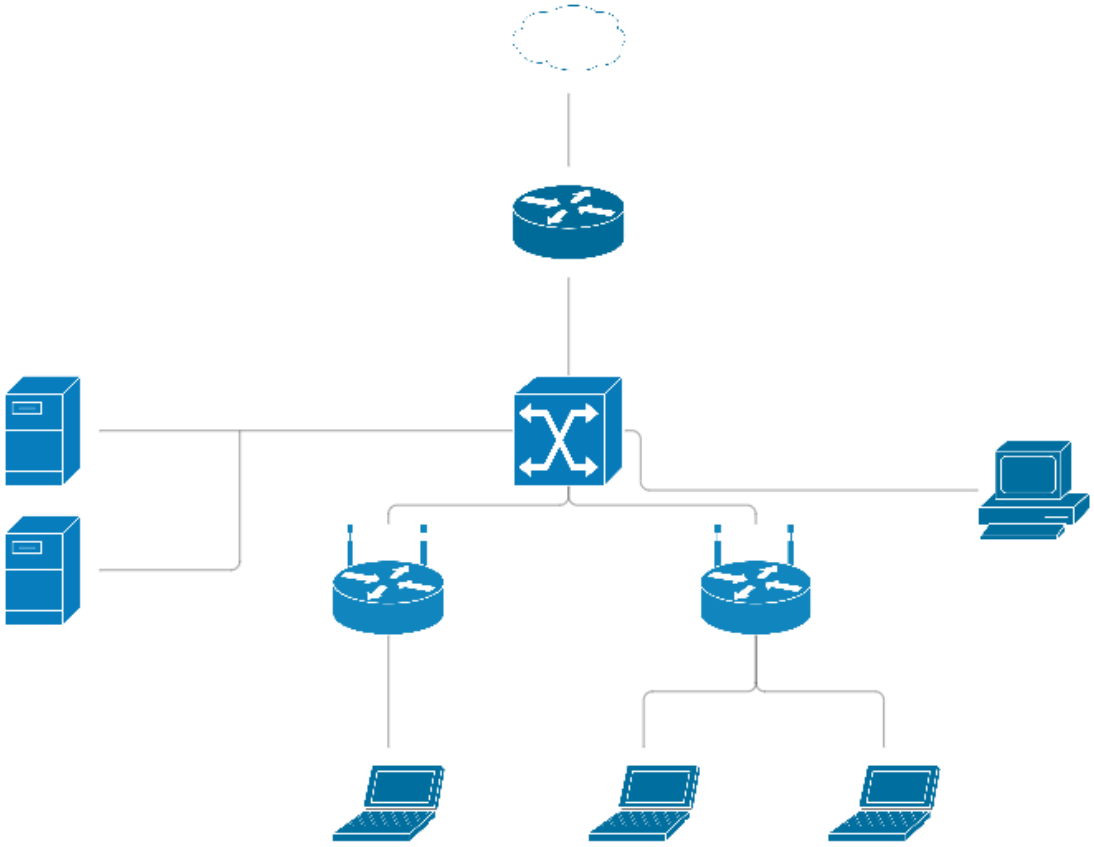


Figura 25.- Esquema actual SERVIORDER S.A, tomada de sites.google.com elaborado por Enrique Franco

3.5 Requerimientos de red

Tabla 2.- *Detalles técnicos para operatividad*

Requerimiento	Descripción
CPU	Equipo con al menos procesador de 1.7GHz de velocidad
Memoria	Al menos contar con 6Gb de memoria RAM
Router	Capaz de proveer salida a Internet
AP	Permita tener una amplia cobertura

Elaborado por Enrique Franco

3.6 Comparativas de cifrado

Para el trabajo de investigación es necesario determinar el tipo de protocolo a utilizar en las redes inalámbricas con el fin de poder establecer una comunicación más robusta y segura con otros servicios que permitan la validación del usuario.

De este modo se compara los mecanismos comunes y mayormente utilizados en cuanto a cifrado y se determina el que mejor se adapte, tal y como se menciona a continuación:

Tabla 3.- Tipos de cifrados

Característica	**WPA**	**WPA2**	**WPA3**
Cifrado	TKIP con RC4	AES con CCMP	AES-GCMP
Característica	**WPA**	**WPA2**	**WPA3**
Tamaño de clave	64 y 128 bits	128 bits	128 y 256
Cifrado	Flujo	Bloque	Bloque
Autenticación	PSK	PSK	SAE

Información tomada de la investigación directa. Elaborado por Enrique Franco

Como se puede observar existen diferentes protocolos de cifrado para las redes inalámbricas pero un factor a considerar es que WPA2 es el que comúnmente se utiliza y esto es debido a sus funciones y operatividad con todos los equipos actuales a diferencia de WPA3 que no está al 100% funcional en todos los diseños de red actuales.

3.7 Comparativas de Access Point

Para el diseño propuesto es necesario establecer el tipo de equipo Wireless a utilizar el cual podrá conectarse con el protocolo Radius a través de PEAP haciendo una validación con el dominio registrado.

Para la elección del equipo se consideró más que una marca un equipo que pueda cubrir el área de cobertura donde los colaboradores se ubican además del costo siendo un punto muy relevante.

Cabe mencionar que cualquier equipo Wireless que funcione con el tipo de cifrado WPA2-Enterprise será capaz de establecer comunicación con el protocolo Radius a utilizarse por lo que a continuación se detalla los diferentes modelos a ser empleados y por último elegir el más idóneo para la propuesta.

Para la elección del equipo a utilizarse se establece una ponderación acorde a lo determinado por expertos, foros e incluso el cuadrante de Gartner en el que la evaluación es hecha por 3 puntos (Alto, Medio y Bajo), permitiendo determinar la elección del equipo de forma más sencilla.

Hoy en día existen muchos equipos inalámbricos que operan en el mercado, pero debido a la cantidad que existen la comparativa se hace con los equipos más comunes desplegados en entornos de infraestructura.

Tabla 4. Comparativas de Access Point

Características	Modelos					
	Mikrotik	**TP-Link**	**Ubiquiti**	**Aruba**	**Cisco**	**D-Link**
Cobertura	Baja	Alta	Alta	Alta	Alta	Baja
Precio	Bajo	Bajo	Medio	Alto	Alto	Bajo
Velocidad	Media	Alta	Alta	Alta	Alta	Media
Mesh	Fácil	Fácil	Fácil	Fácil	Complejo	N/A
Administración	Media	Fácil	Media	Fácil	Media	Fácil
Configuración	Media	Fácil	Media	Fácil	Media	Fácil

Información tomada de la investigación directa. Elaborado por Enrique Franco

Como se observa en la tabla 4 que antecede todos los equipos cumplen con la función WPA-2 Enterprise en el que debido a los altos precios o problemas de interoperabilidad y configuración que existen en algunas marcas se eligió trabajar con el AP TP-Link el cual es simple de configurar y factible de adquirir y ser desplegado en la entidad sin necesidad de comprar nuevo equipamiento al que posee la empresa SERVIORDER S.A.

3.8 Comparativa de los métodos de autenticación 802.1x

Debido a que Radius maneja diferentes formas de autenticación a la hora de validar sus usuarios es necesario determinar cuáles son el mecanismo para utilizar esto con el fin de poder identificar de qué manera se adapta y funciona el protocolo en los escenarios planteados.

Para ello a continuación se hace una comparativa de los diferentes métodos de autenticación y con ello elegir el más idóneo para la implementación a realizarse.

Tabla 5.- Métodos de autenticación

Característica	**EAP-TLS**	**PEAP**	**EAP-FAST**
Autenticación de usuarios	OTP LDAP	Windows NT Dominio y AD	Windows NT AD y LDAP
Certificado del lado servidor requerido	Si	Si	No
Certificados del lado cliente	No	No	No

Sistema operativo en el que opera	Windows XP/2000	Windows / MAC / Linux	Windows
Credenciales de usuario	Certificado digital	Certificado digital	Password LDAP
Autenticación de doble factor	No	No	Si
Expiración de credenciales	No	No	Si
WPA compatible	Si	Si	Si

Información tomada de la investigación directa. Elaborado por Enrique Franco

Como se observa existen varios métodos que pueden ser utilizados a la hora de desplegar una red con Radius en el que por lo general según el tipo de autenticación a utilizar tendrá ciertos parámetros que completar. Un punto importante para notar es que el protocolo PEAP cuenta con ciertas funciones más sencillas de realizar como la creación de certificados auto-firmados u otorgados por una entidad certificadora permitiendo un despliegue mucho más rápido que a diferencia de EAP-TLS y EAP-FAST.

PEAP es un protocolo que en la actualidad convive en todos los mecanismos de seguridad avanzados en las redes wireless siendo su despliegue mucho más simple de implementar a diferencia de otros protocolos de autenticación.

Debido a ello se tiene pensado hacer realizar un escenario que demuestre la factibilidad de usar el protocolo Radius en redes inalámbricas en la empresa SERVIORDER S.A.

3.9 La Propuesta

Como se mencionó previamente a través del presente trabajo de investigación se busca indicar la factibilidad que existe a la hora de usar Radius en lugar de las autenticaciones típicas realizadas por usuario y contraseña a fin de tener un mejor control en cuanto acceso así mismo monitoreo de forma más detallada de que ocurre en la entidad.

Un punto para mencionar es que la red al estar trabajando mediante el controlador de dominio el cual generará mayor nivel de seguridad debido a que cualquier usuario que se quiera

conectar y navegar deberá hacerlo con sus respectivas claves de acceso al dominio evitando se realice la propagación de las credenciales.

Para el diseño actual el esquema a realizarse es el siguiente:

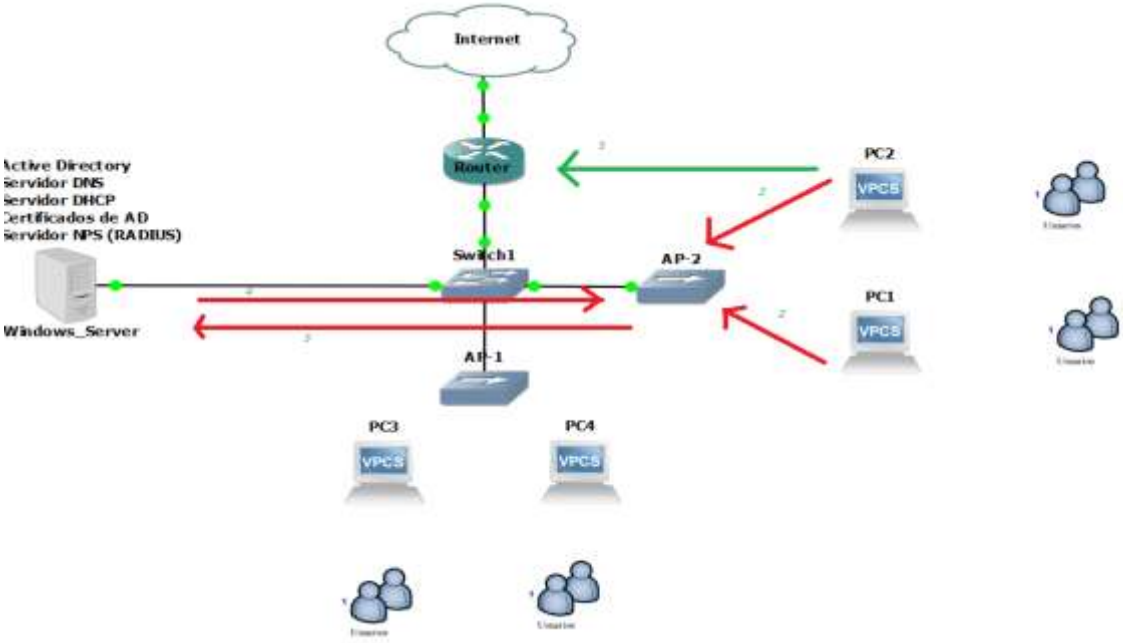


Figura 26.- Esquema de autenticación aplicado, tomada de sites.google.com, elaborado por Enrique Franco

1.- El usuario se conecta al AP en el que para poder tener acceso deberá ingresar su user y password del dominio

2.- El AP está conectado a la red mediante un switch de capa 2 el cual no tiene muchas características en densidad de puertos y velocidad además de ser un equipo no administrable

3- El AP al tener una configuración de tipo PEAP deberá preguntar al servidor Radius y validar la autenticación del usuario con el servidor de dominio.

4.- El servidor NPS buscará en su registro de Active Directory si el usuario se encuentra creado y este habilitado.

4.1 Si el usuario no existe o esta deshabilitado el NPS enviará un error de autenticación al AP indicándole que no se permite la conexión al usuario que se registró vía Wireless.

4.2- Si el usuario existe el servidor le notificará al servidor DHCP que se asigne direccionamiento IP.

5.- El servidor DHCP realizará el proceso conocido como DORA (Discover, Offert, Request, Acklowngment) con la dirección MAC del equipo que se registro

Una vez completado el proceso del DHCP y el Radius validado se enviará al AP permisos para el usuario que se validó así mismo se le otorgará los parámetros de red dados por el DHCP.

6.- El usuario tendrá conectividad y podrá navegar hacia Internet como acceder a los recursos que existan en Serviorder S.A.

El esquema propuesto busca que cuando un usuario quiera validarse o conectarse a la red deberá en primer lugar conectarse al AP y colocar credenciales de dominio. Una vez ingresadas y busque conectar con el AP, este último enviará esa información hacia el servidor Radius en este caso el NPS que a su vez revisará las políticas internas creadas en él y de ser posible validará con el controlador de dominio verificando si los datos ingresados se encuentran en el directorio activo es decir el usuario y la contraseña.

De haber sido fallida la comunicación el servidor Radius enviará un error de autenticación y conexión hacia el equipo que ingreso las credenciales dando una idea del problema. Ahora si la autenticación realizada fue exitosa el AD envía al NPS un Ok que le permite al NPS saber que el usuario existe y posteriormente aplicar políticas o ajustes avanzados que se hayan configurado a nivel del servidor Radius. Una vez aplicado el servidor envía al equipo final el permiso, pero con debidos criterios de seguridad que permitirán no solo acceso al servidor sino a tener una visibilidad completa de toda la red de forma más segura debido a que todos los registros o datos por el usuario generado son almacenados según su usuario y contraseña de dominio que realiza la validación.

Para mejor detalle se presenta la fase de peticiones realizadas entre el access point y el servidor NPS.

Figura 27.- Autenticador g suplicante, tomada de sites.google.com. elaborado por Enrique Franco

Como se observa en la figura 27 se realizan cuatro pasos para tratar de obtener la autenticación a nivel de Radius siendo estas:

- Solicitud de descubrimiento: En este punto el AP ha recibido una petición de conexión por parte de un usuario vía inalámbricamente por lo que envía esa petición al servidor Radius

- El servidor Radius observa que llega un mensaje de descubrimiento por parte del AP y le envía una respuesta con el fin de que el AP establezca la comunicación y proporcione mayores detalles de la conexión
- El AP al ver que ha sido aceptada su petición envía una solicitud de registro que incluye la información del usuario y contraseña ingresados a través de WPA2-Enterprise
- El servidor Radius revisa de manera interna si la validación es aprobada o no donde ambas respuestas llegan en la respuesta de registro que van dirigidas hacia el AP

Para mayor detalle a continuación se pretende probar el servidor NPS de Windows con el objetivo de proponer a la empresa SERVIORDER S.A mejoras en cuanto a conexión mediante autenticación de dominios y no por claves pre compartidas.

Como primer punto los materiales utilizados para el desarrollo de la solución son:

- Windows server cualquier versión preferible 2016 en adelante
- Un switch para permitir comunicación
- Un punto de acceso
- Un servidor DNS, DHCP y de certificado
- Un servidor Radius
- Una máquina que pueda conectarse vía wireless

3.9.1 Características del switch de capa 2 a utilizar

El equipo utilizado para la propuesta es un modelo basado en capa 2 de marca Cisco no administrable capaz de ofrecer velocidades a 10/100/1000 Mbps con una baja densidad de puertos para pruebas respectivas y solo establecer la comunicación entre los equipos de la red.

Figura 28. Switch capa 2. tomada de sites.google.com. elaborado por Enrique Franco

3.9.2 Configuración de Active directory

Para el escenario actual es necesario que el servidor funcione como controlador de dominio esto con el objetivo de tener un control o gestión centralizada en los equipos que forman parte de la red.

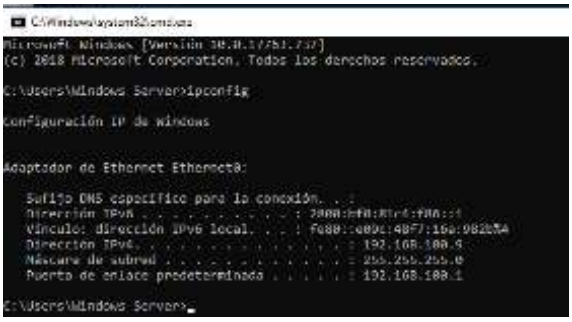


Figura 29.- Configuración de direccionamiento IP, tomada investigación directa, elaborado por Enrique Franco

Para que el servidor de AD funcione sin ningún problema se deberá hacer que uno de sus DNS sea la misma dirección IP que el equipo con el fin de poder anunciarlo a controlador de dominio encargado de hacer las peticiones referentes a sitios web o nombres de equipos que estén atados a la organización.

Cabe recalcar que cualquier equipo que se conecte al dominio deberá poseer el DNS del equipo que va a hacer controlador de dominio esto para que se pueda tener una mejor gestión de los activos.

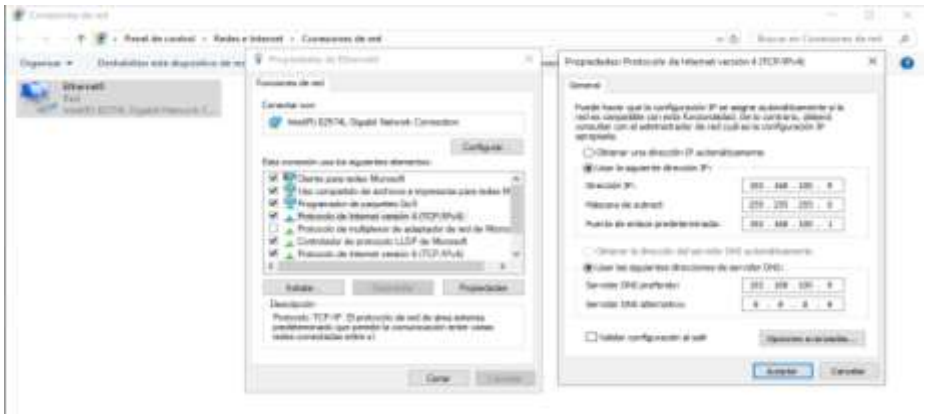


Figura 30.- Asignación de IP de forma estática, tomada investigación directa, elaborado por Enrique Franco

Una vez configurado el siguiente paso a realizar será instalar todas las características necesarias siendo estas:

- Servidor de AD
- Servidor DHCP
- Servidor de políticas de red
- Servidor de certificados raíz

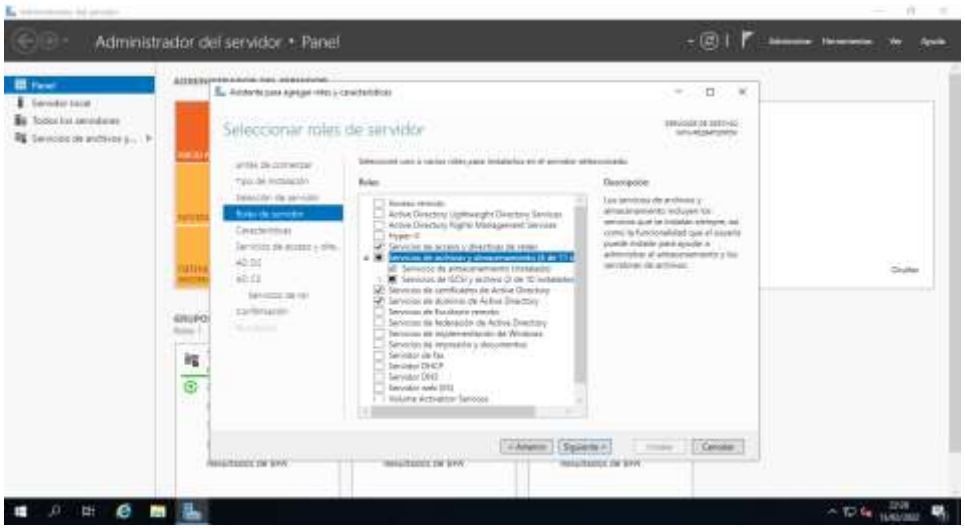


Figura 31.- Asignación de roles de servidor, tomada investigación directa, elaborado por Enrique Franco

Una vez instalados es necesario configurar cada uno de ellos siendo el controlador de dominio el primero debido a que es el componente principal para la solución

3.9.3 Configuración de servidor a controlador de dominio

El primer paso para considerar es que al ser el único controlador de dominio a utilizar será necesario que se promueva como el equipo principal de la red.

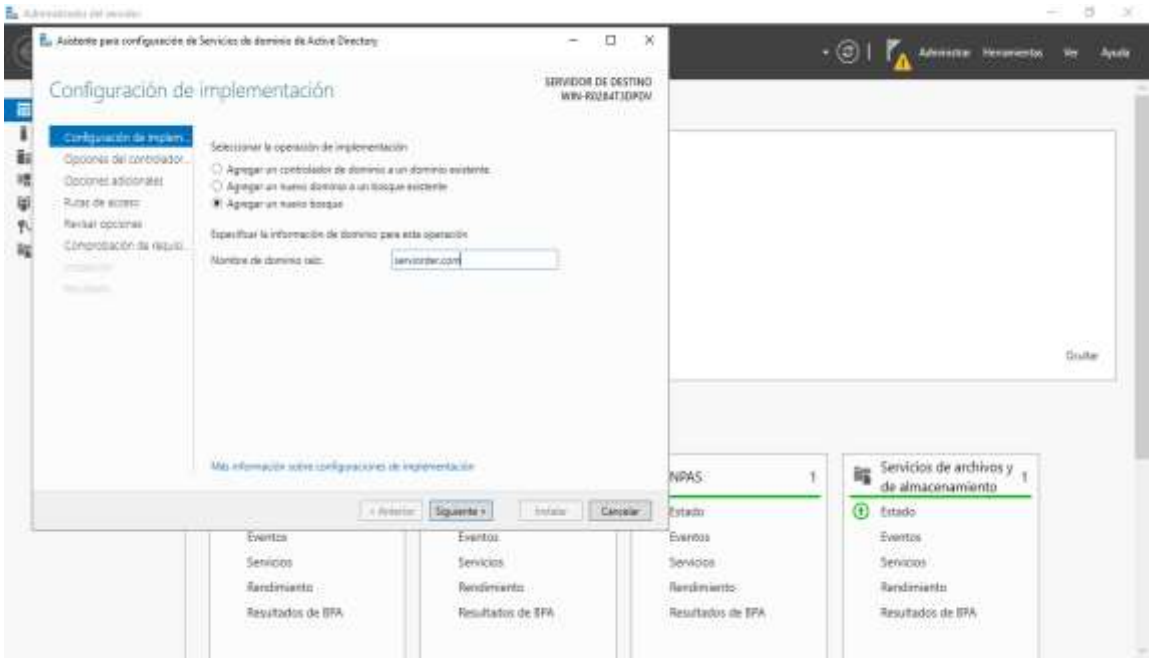


Figura 32.- Creación de dominio, tomada investigación directa, elaborado por Enrique Franco

Se establece mecanismos de seguridad mediante el uso de usuarios y contraseñas

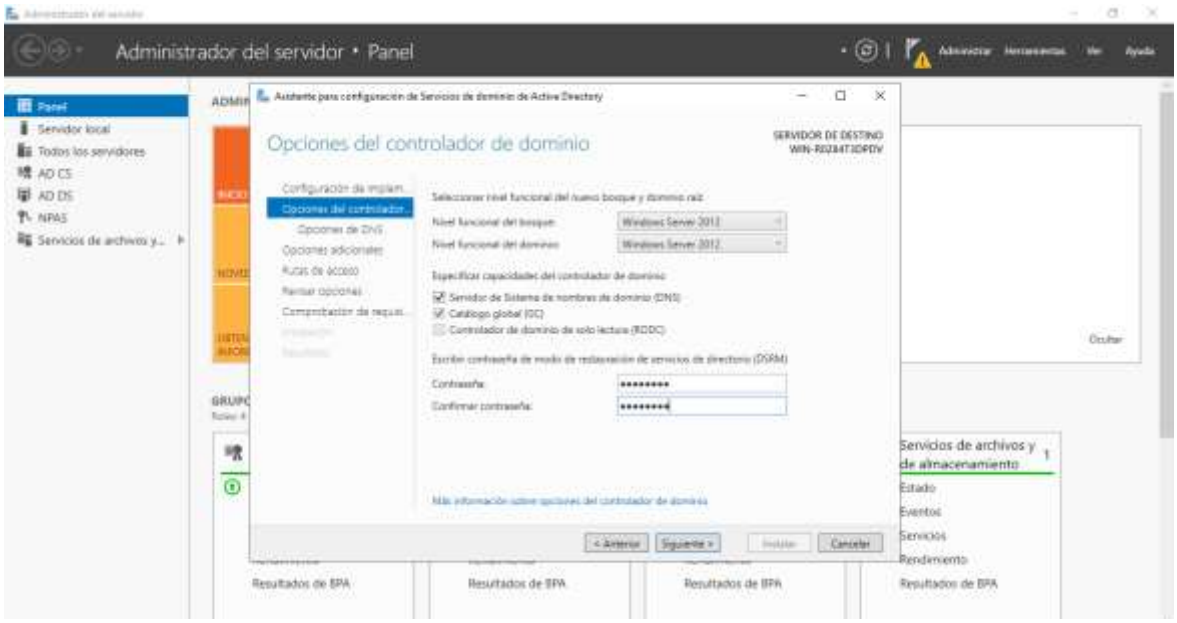


Figura 33.- Asignación de contraseña al dominio, tomada investigación directa, elaborado por Enrique Franco

De igual manera se tiene que comprobar por parte de Windows el nombre que va a recibir la NetBIOS de ahora en adelante.

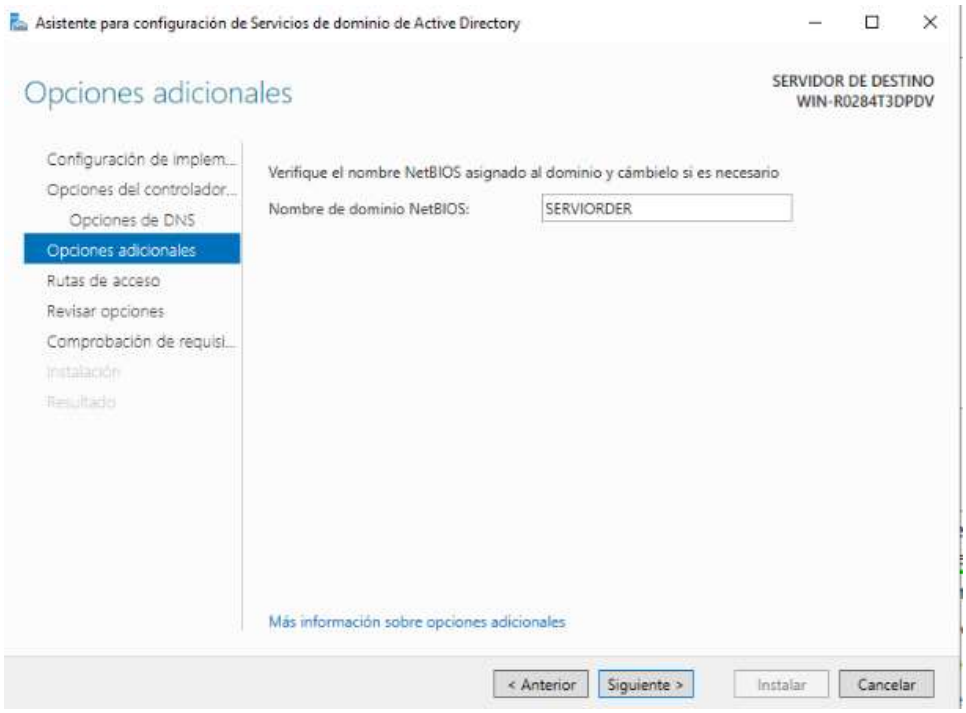


Figura 34.- Se delegó el NETBIOS, tomada investigación directa, elaborado por Enrique Franco

Una vez realizado el paso anterior se deberá esperar hasta que el controlador de dominio se reinicie. Donde se podrá observar que junto al nombre del equipo aparecerá el nombre de dominio creado.

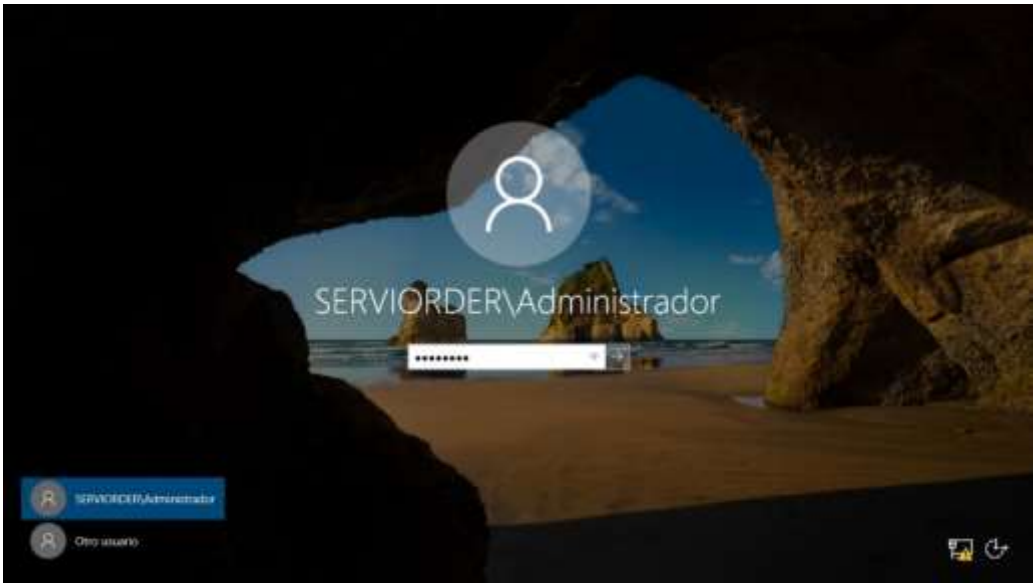


Figura 35.- Servidor promovido a controlador de dominio, tomada de investigación directa, elaborado por Enrique Franco

3.9.4 Configuración de certificados digitales en controlador de dominio

Es necesario que luego de activar el equipo como controlador de dominio ahora instalar los certificados digitales ya que permitirá más adelante hacer la validación en paso al tipo de encriptación segura que se realice cuando un equipo quiera conectarse vía wireless. Los certificados gestionados por AD son auto firmados por lo que solo tendrán uso en la red interna ya que no están certificados por una entidad legítima esto no quiere decir que se vaya a ver afectado el proceso de validación de usuarios con Radius.

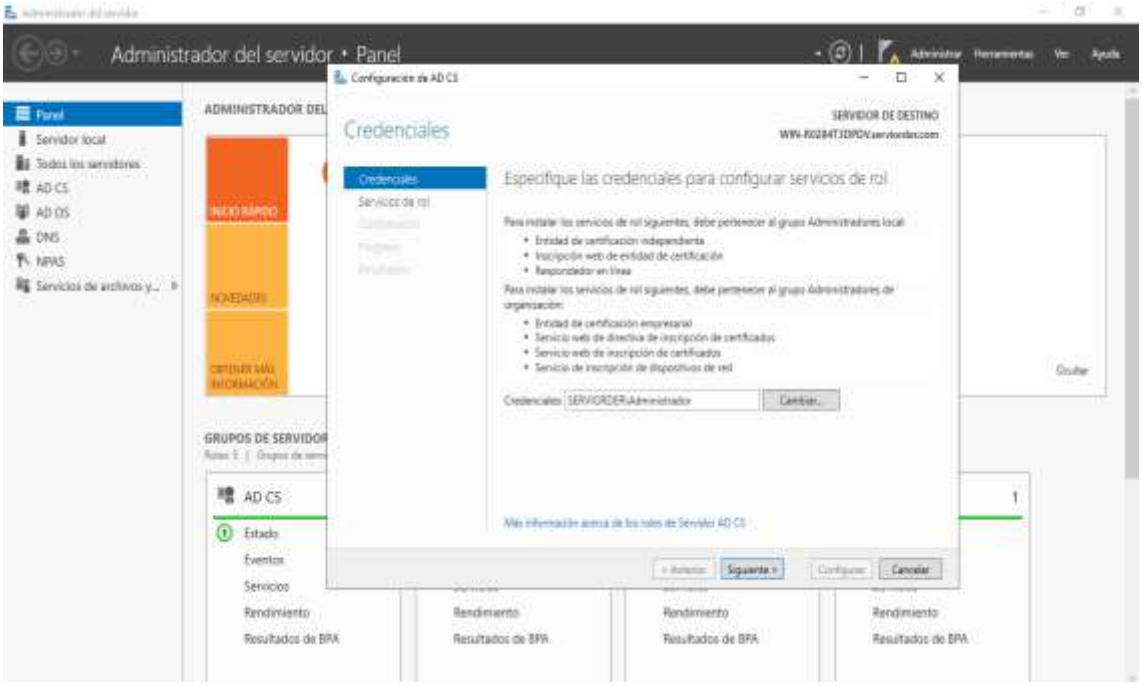


Figura 36.- Configuración de certificados, tomada investigación directa, elaborado por Enrique Franco

Se debe elegir el tipo de instalación en este caso es de tipo CA Empresarial por que estará dentro de una organización.

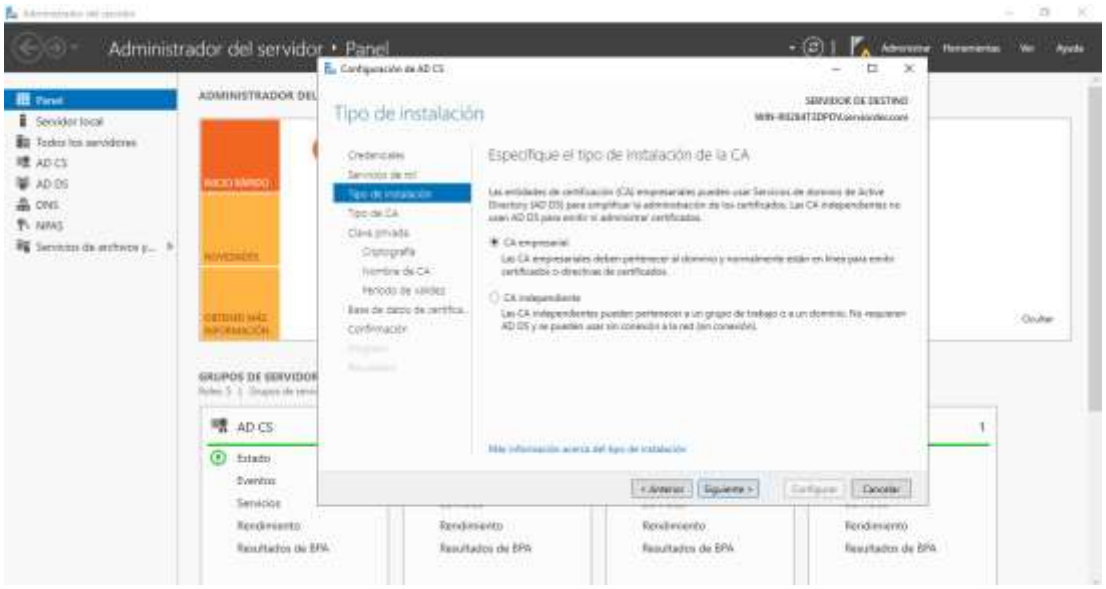


Figura 37.- Elección del tipo de certificado, tomada investigación directa, elaborado por Enrique Franco

El tipo de servidor a elegir es el de raíz para que permita todos los equipos certificarlos

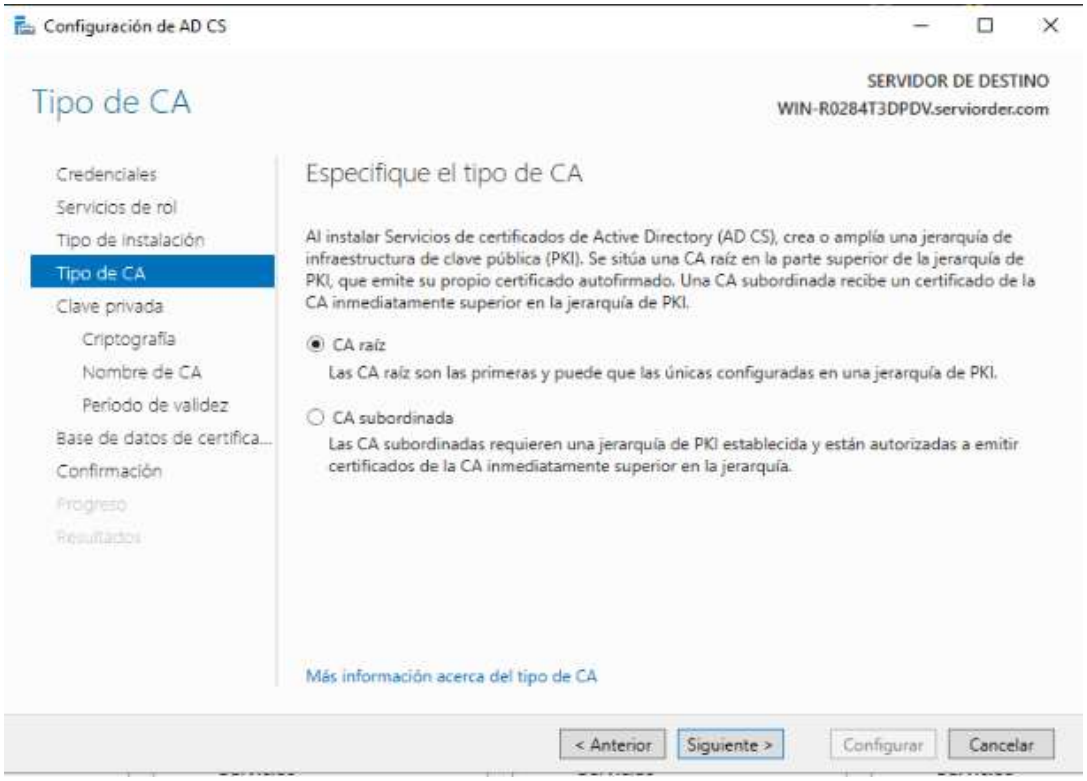


Figura 38.- Delegación de certificado raíz, tomada investigación directa, elaborado por Enrique Franco

Además, se debe establecer la clave pública que será utilizada fuera de la entidad de ser necesario y tipo de cifrado con el que es firmado.

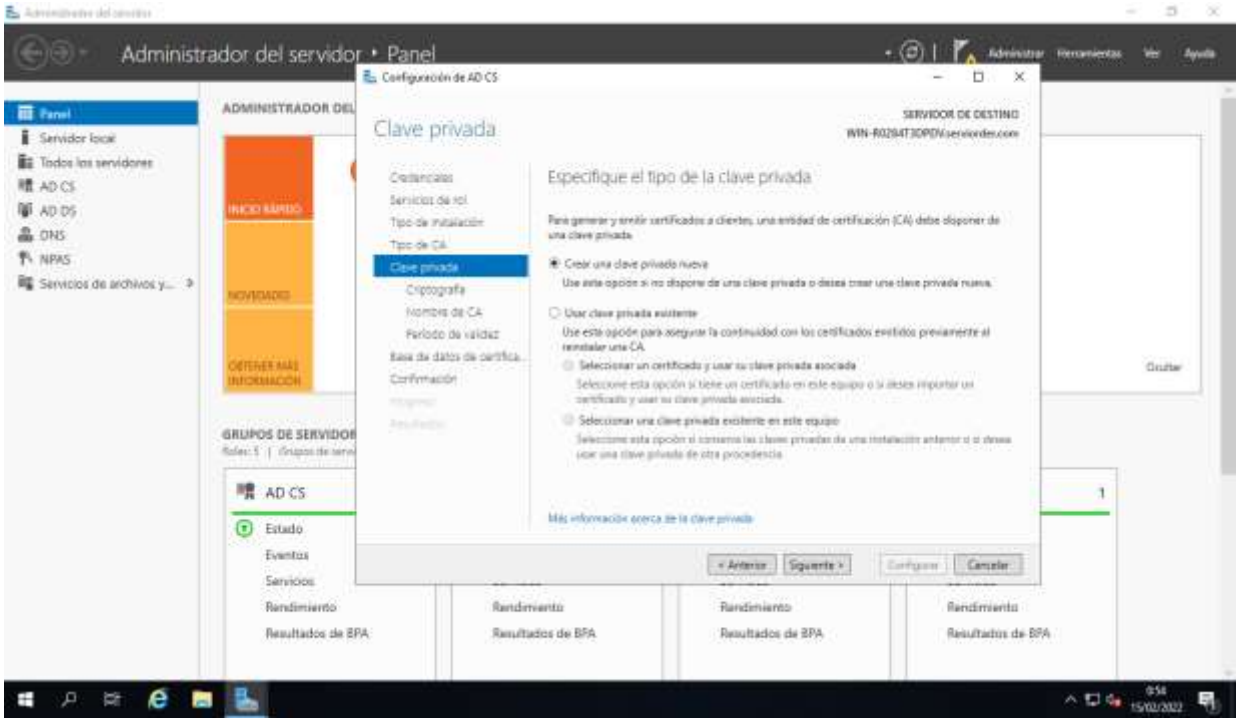


Figura 39.- *Asignación de clave privada, tomada investigación directa, elaborado por Enrique Franco*

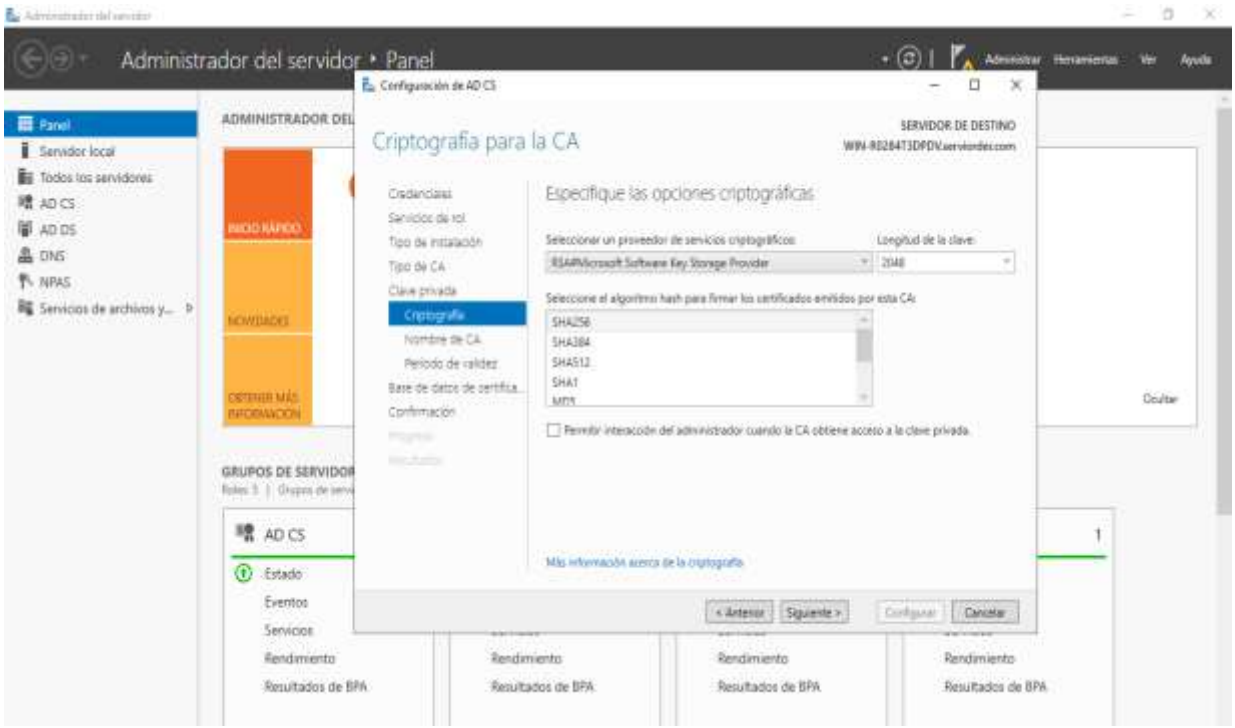


Figura 40.- Tipo de cifrado para certificado, tomada investigación directa, elaborado por Enrique Franco

Es necesario que el servidor raíz tenga un identificador único a la hora de ser utilizado limitando las configuraciones por error

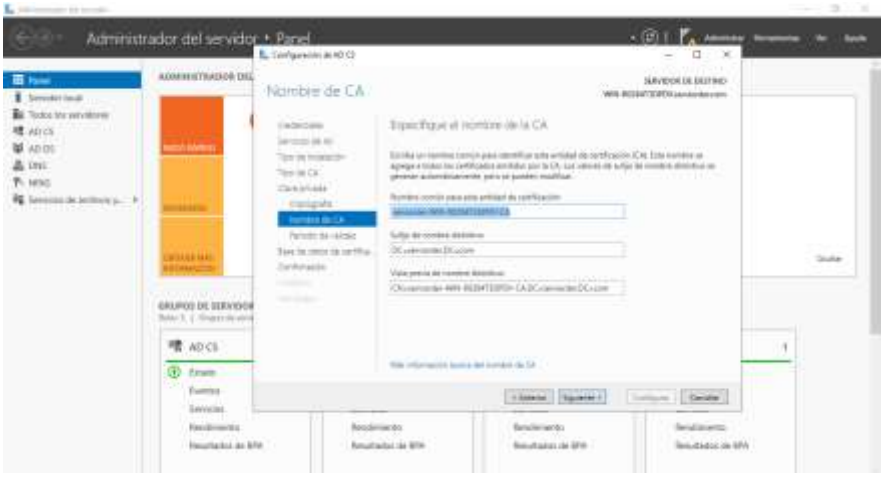


Figura 41.- Elección del dominio para firma de certificado, tomada investigación directa, elaborado por Enrique Franco

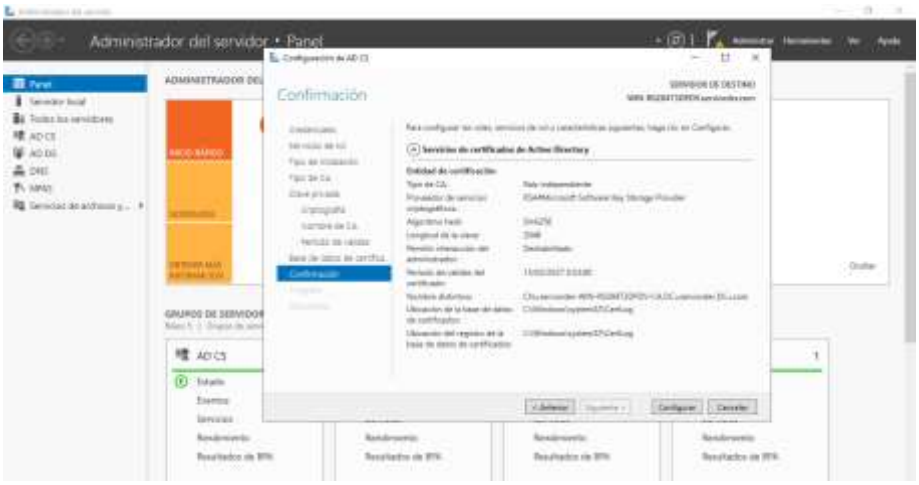


Figura 42.- Resumen de lo configurado, tomada investigación directa, elaborado por Enrique Franco

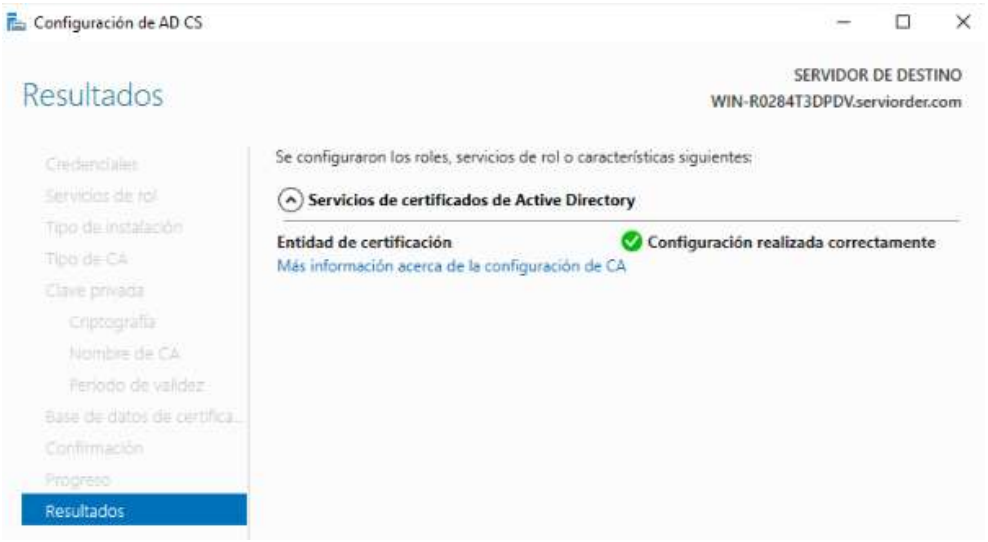


Figura 43.- Validación de configuración, tomada investigación directa, elaborado por Enrique Franco

Es necesario comprobar que los certificados se han creado de forma correcta y estén instalados a nivel de dominio para evitar posibles fallas más adelante en cuanto a la autenticación con el servidor Radius

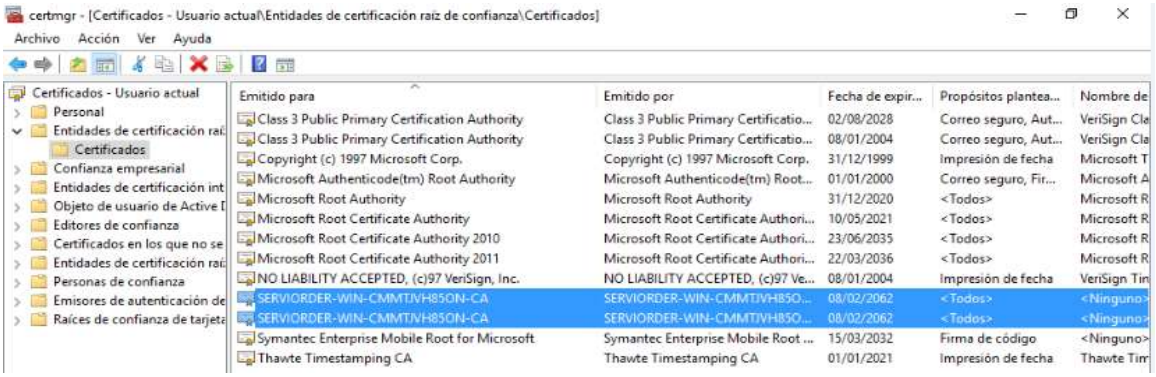


Figura 44.- Validación de certificado registrado, tomada investigación directa, elaborado por Enrique Franco

3.10 Creación del servidor DHCP

Como se detalló con anterioridad el servidor DHCP será el encargado de asignar los parámetros de red necesarios a los equipos que se conecten siempre y cuando sean autenticados por el servidor Radius.

En este caso la red de Serviorder está compuesta por la red 192.168.100.0/24 por lo que a través de Windows Server se agrega la característica de servidor DHCP el cual sea capaz de asignar direccionamiento de forma automática.

Para ello se creó el respectivo ámbito dentro del controlador de dominio de Seerviorder a fin de proporcionar conectividad y permitir recibir parámetros de red.

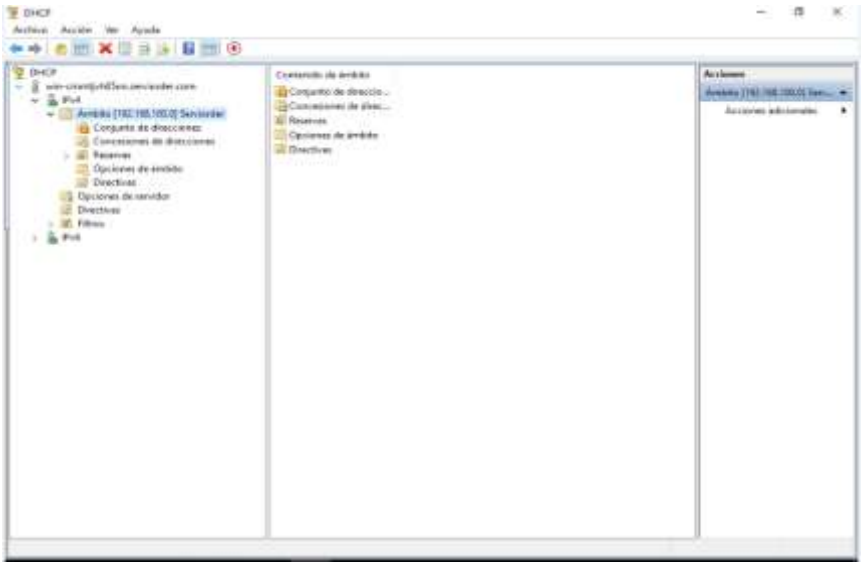


Figura 45.- Creación de ámbito para DHCP, tomada investigación directa, elaborado por Enrique Franco

3.11 Configuración del servidor Radius NPS de Windows

Una vez realizada la instalación de certificados así mismo el controlador de dominio es necesario habilitar los servicios de directivas de redes con el fin de hacer uso del protocolo Radius en Windows Server para ello se debe considerar que la directiva a activar debe tener comunicación directa con el equipo wireless que este en la red con el fin de enviar paquetes ICMP y validar posteriormente los usuarios registrados.

Teniendo en cuenta el proceso a realizarse se debe habilitar el cliente Radius en el que se debe establecer la dirección IP del AP así mismo una clave Pre-Compartida que permitirá la comunicación entre el AP y el servidor Radius tal como se presenta en la imagen que antecede.

Figura 46.- Creación de cliente Radius, tomada investigación directa, elaborado por Enrique Franco

Es necesario de igual forma establecer un método de autenticación a nivel de 802.1x con PEAP para validar la comunicación entre el AP y el Servidor a la hora de realizarse peticiones de usuarios que deseen acceder a la red.

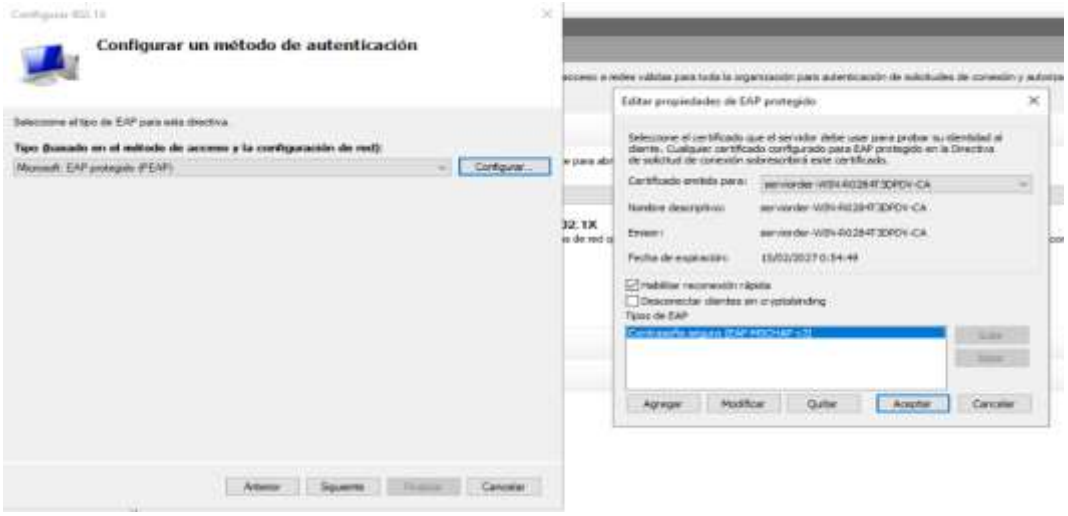


Figura 47.- Configuración de políticas NPS, tomada investigación directa, elaborado por Enrique Franco

Para que el servicio funcione sin ningún problema es necesario especificar los grupos de usuarios que van a pertenecer a la configuración de 802.1x en el que para su funcionamiento se deberá en primer lugar crear los usuarios y grupos para luego ser incluidos a la configuración.

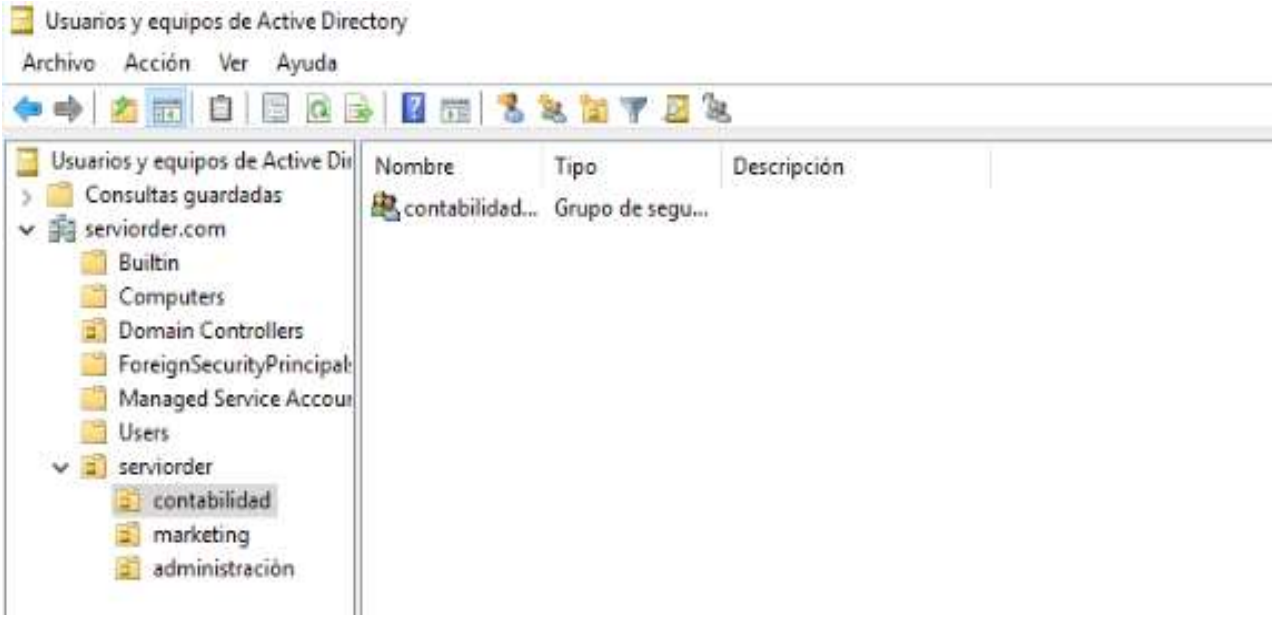


Figura 48.- Creación de grupos en OU, tomada investigación directa, elaborado por Enrique Franco

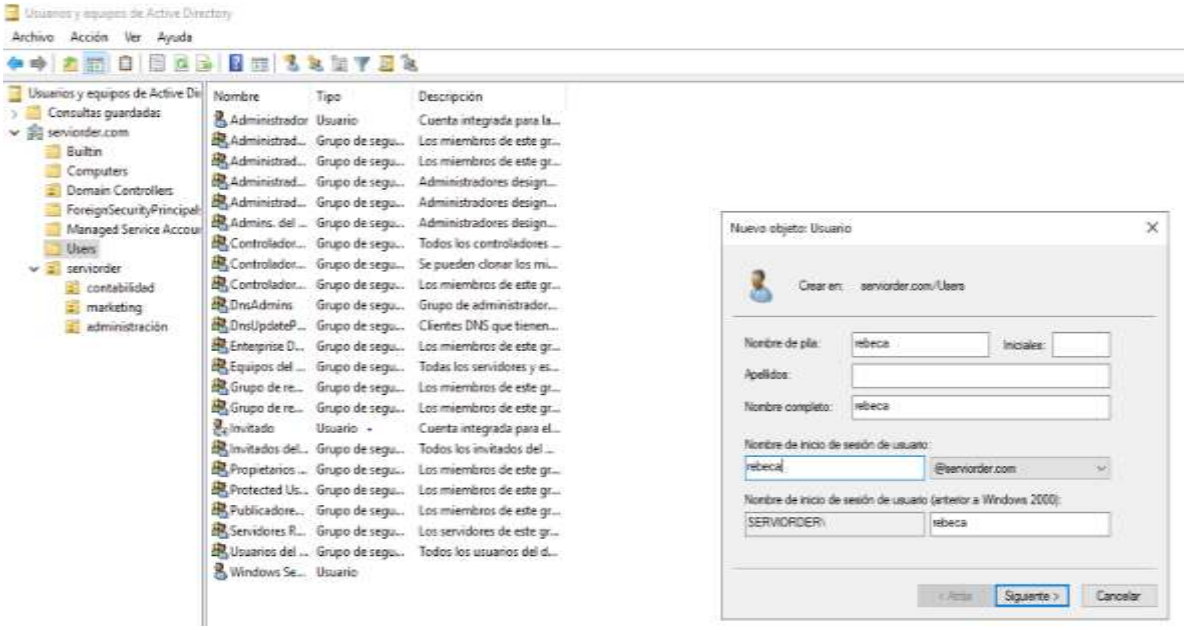


Figura 49.- Creación de usuarios, tomada investigación directa, elaborado por Enrique Franco

Una vez creado los usuarios se deberá incluirlos al grupo que forman parte a fin de tener un mejor control y que cuando se realice la validación con el NPS de Windows se pueda identificar su rol de forma mucho más fácil.

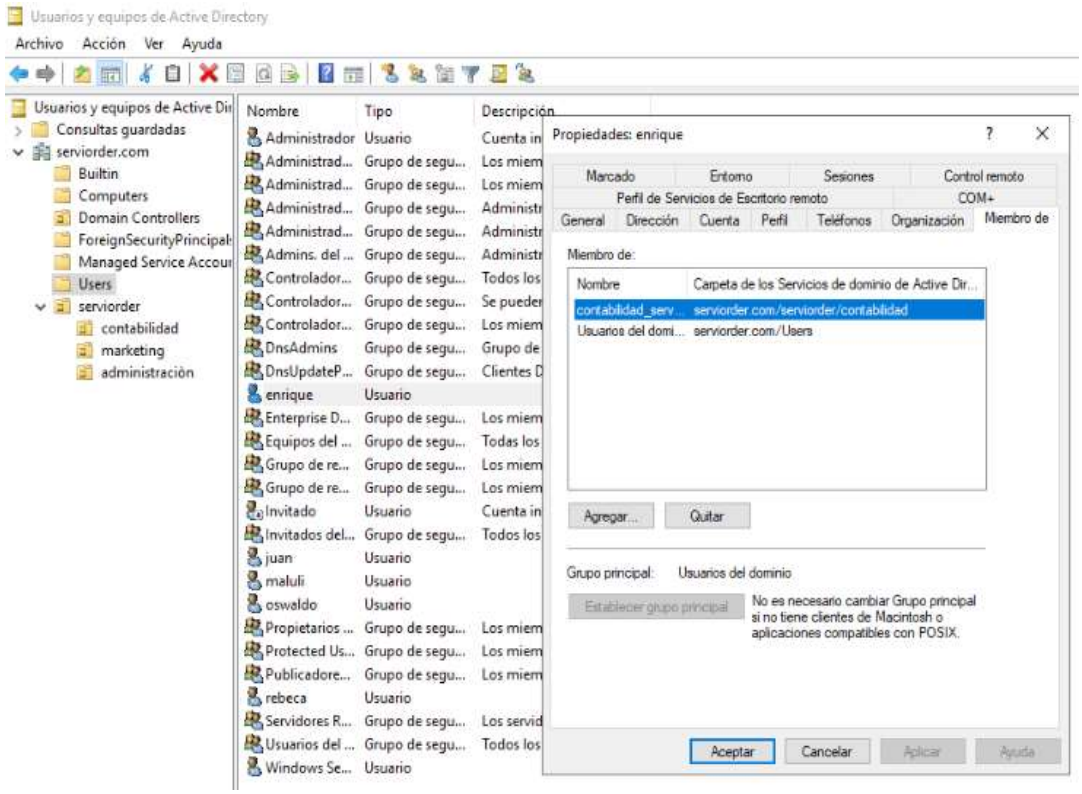


Figura 50.- Asignación de usuarios en grupos, tomada investigación directa, elaborado por Enrique Franco

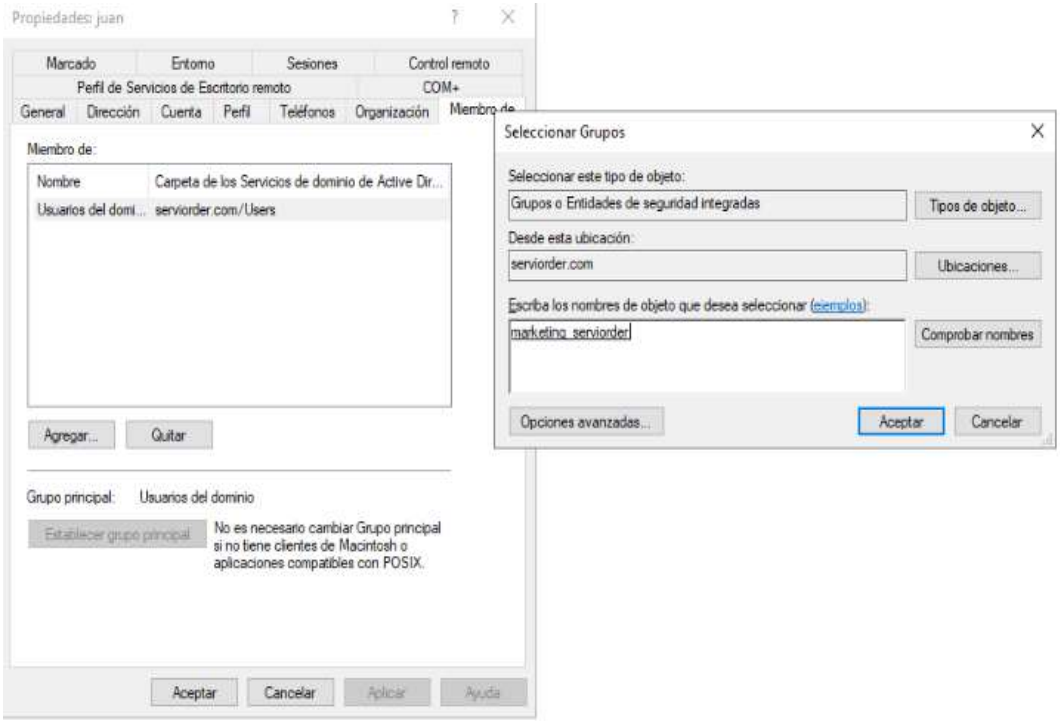


Figura 51.- Búsqueda de usuarios en dominio, tomada investigación directa, elaborado por Enrique Franco

Una vez configurado los usuarios serán agregados a las políticas de NPS y con ello tener los permisos de acceso según como este configurada la directiva de red.

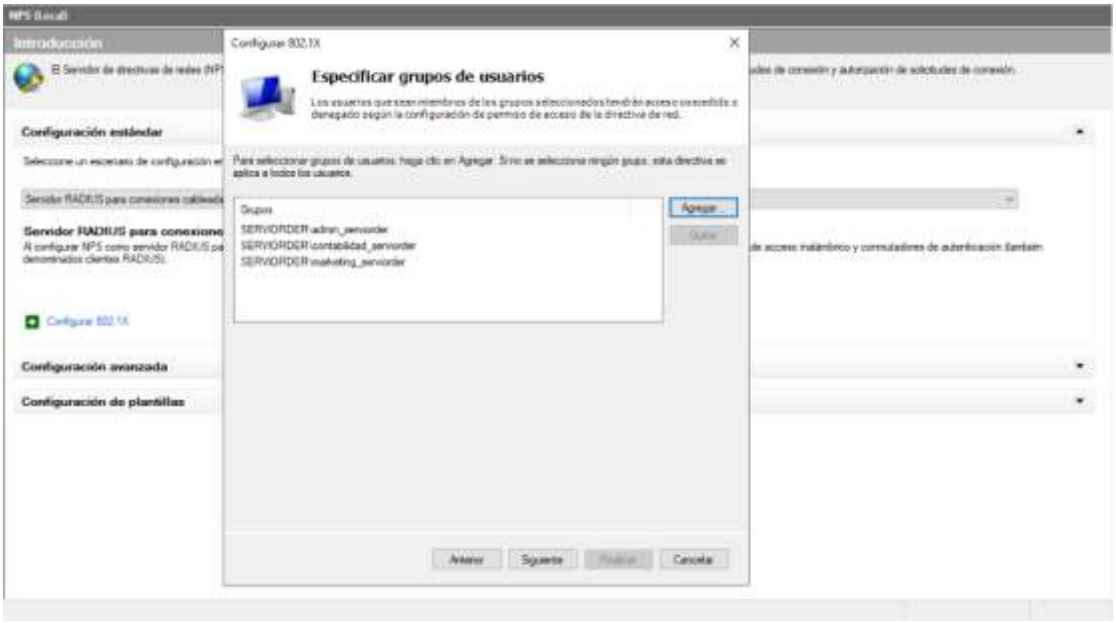


Figura 52.- Validación de NPS de grupos de usuarios, tomada investigación directa, elaborado por Enrique Franco

A las políticas implementadas es necesario establecerle los diferentes controles de tráfico a ser utilizados con el fin de asignar controles de acceso a través de Radius tal como se presenta a continuación

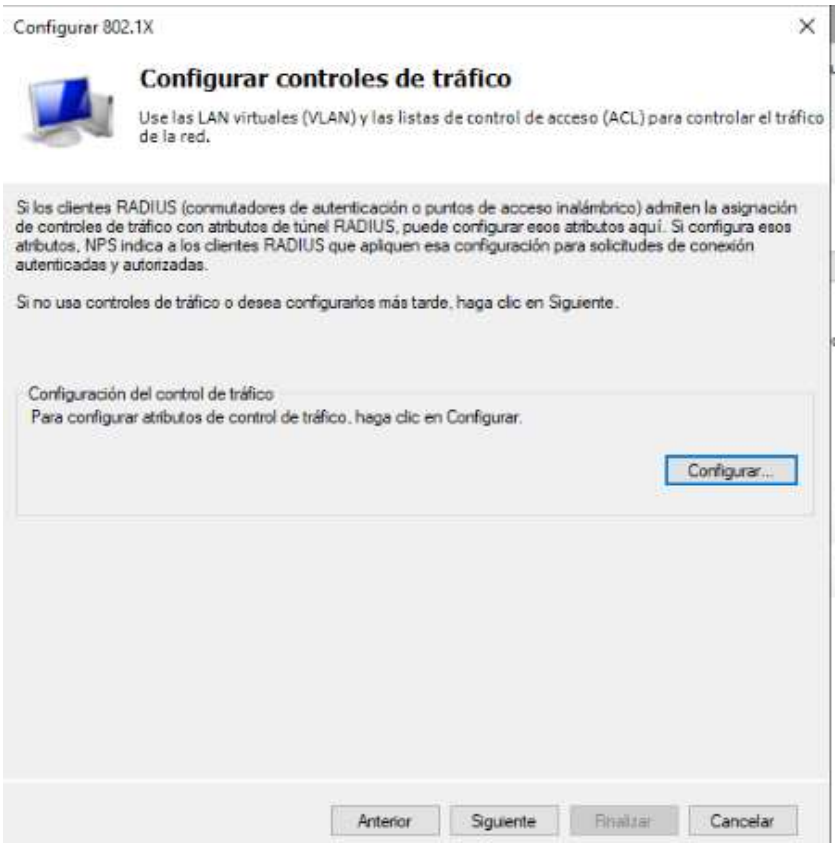


Figura 53.- Configuración de controles de tráfico, tomada investigación directa, elaborado por Enrique Franco

Por último, se comprueba que el cliente configurado, así como las directivas de red a nivel de comunicación con el AP estén creadas de forma correcta.

Figura 54.- Validación de política de usuarios creadas, tomada investigación directa, elaborado por Enrique Franco

Un punto importante para mencionar es que a la hora de definir las policitas de red es necesario que el medio de acceso sea seleccionado acorde a como operará la red para el presente trabajo de investigación se hizo uso de la red inalámbrica permitiendo la autenticación de los usuarios hacia el servidor.

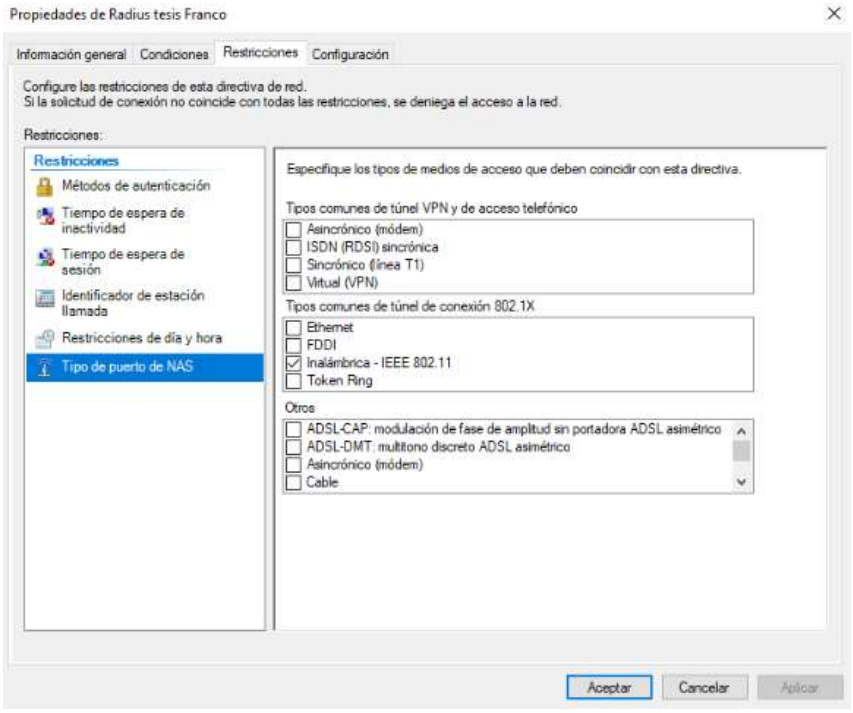


Figura 55.- Elección de configuración basada en wireless, tomada investigación directa, elaborado por Enrique Franco

3.12 Configuración de AP para autenticación con Radius

Hasta ahora se ha desarrollado la autenticación del lado del servidor, pero para que el escenario funcione es necesario habilitar todas las funciones en el AP que será encargado de recibir las solicitudes de los suplicantes y pasarlas al servidor NPS de validación.

Cabe recalcar que cualquier AP puede ser utilizado evitando grandes costos de implementación. El trabajo de investigación hace uso de un AP de tipo TP-Link para comprobar que la autenticación es factible reduciendo los gastos de operación.

Figura 56.- Acceso router TP-Link, tomada investigación directa, elaborado por Enrique Franco

Una vez que se ingresa al TP-Link lo primero a realizarse es el modo de operación con el que va a trabajar donde para este caso será necesario que el AP cumpla funciones de solo Wireless y no de router con el fin de conectar redes ya sean cableadas o inalámbricas y que no cumplan funciones de NAT ni reciban direccionamiento IP del AP sino que todo sea otorgado por el servidor DHCP creado configurado en el Windows Server donde se tiene de igual manera el AD el protocolo Radius y los servicios de certificados.

Figura 57.- Configuración en modo AP, tomada investigación directa, elaborado por Enrique Franco

Así mismo se le asigna un direccionamiento al equipo mencionado para poder ser administrado y que forme parte de la red del servidor Radius con la finalidad de compartir mensajes y así poder realizar las solicitudes

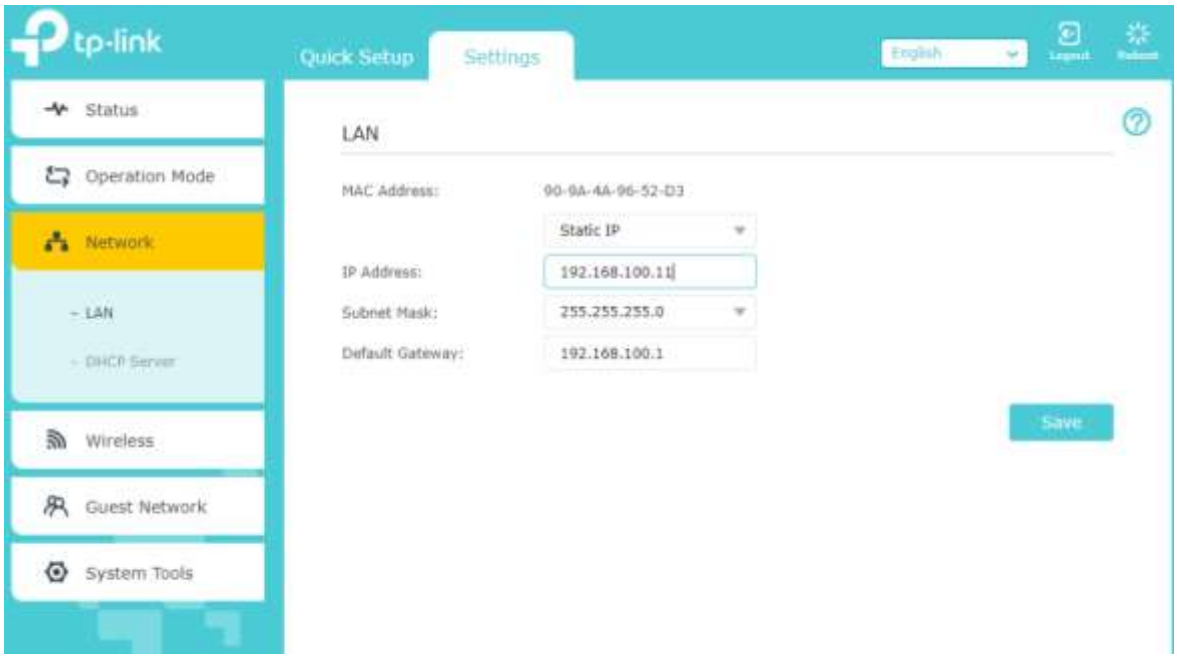


Figura 58.- Asignación de direccionamiento IP, tomada investigación directa, elaborado por Enrique Franco

Se comprueba una vez asignada la IP que se tenga comunicación desde cualquier equipo a fin de validar el funcionamiento correcto del AP

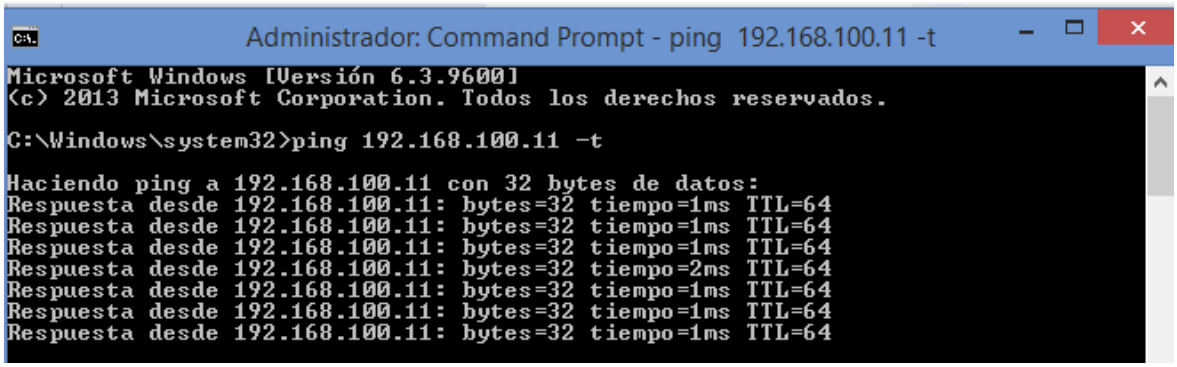


Figura 59.- Prueba de conectividad con equipo, tomada investigación directa, elaborado por Enrique Franco

Para que el AP funcione y realice las peticiones al servidor Radius es necesario hacer uso de la seguridad WPA/WPA2-Enterprise en el que se puede definir diferentes puntos como son:

- La versión de la seguridad a utilizar en este caso establecida en automática
- El tipo de encriptación realizado ya sea TKIP o AES
- La dirección IP del servidor Radius al cual se va a validar los usuarios
- El puerto utilizado por Radius en el que escucha todas las peticiones

- El Radius password definido tanto en el lado servidor como cliente
- El modo de operación según las bandas que soporte el AP
- El ancho del canal definido en automático
- El canal de comunicación de igual forma establecido en automático
- La potencia para transmitir que sea alta para llegar a tener mejor cobertura

Figura 60.- Configuración WPA-2 Enterprise, tomada investigación directa, elaborado por Enrique Franco

Una vez realizado el proceso de configuración en el AP se deberá validar desde una máquina cliente a fin de ingresas parámetros de dominio que permitan validar que la red se encuentre funcionando.

Figura 61.- Verificación de SSID creado, tomada investigación directa, elaborado por Enrique Franco

Como se observa en la figura 61, la red Radius tesis se encuentra activa por lo que si se procede a conectar deberá pedir usuario y contraseña del dominio para ello se ingresó las credenciales del Ingeniero en redes de la empresa Serviorder S.A.

Figura 62.- Ingreso de credenciales de dominio, elaborado por Enrique Franco tomada investigación directa, elaborado por Enrique Franco

Una vez se haya dado clic en aceptar el Wireless le menciona que se va a hacer una búsqueda del servidor Radius por lo que si desea continuar dando conectar para validar que todo opere con normalidad.

Figura 63.- Aceptación de certificados, tomada investigación directa, elaborado por Enrique Franco

Figura 64.- Conexión con la red wifi creada, tomada investigación directa, elaborado por Enrique Franco

Si todo funciona de forma correcta y se establece la comunicación el servidor Radius le proporcionará direccionamiento dado por el DHCP presentando como validación el nombre del DNS que será el de la empresa SERVIORDER S.A

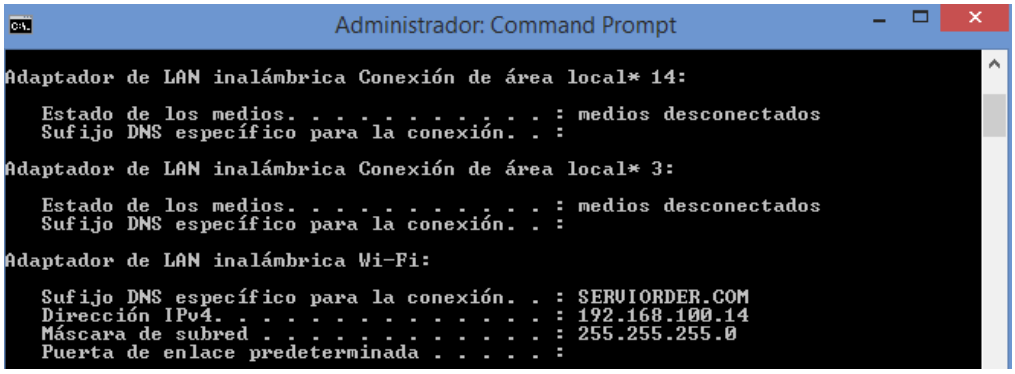


Figura 65.- Verificación de asignación IP por DHCP, tomada investigación directa, elaborado por Enrique Franco

Del mismo modo en el servidor DHCP se observa que la IP 192.168.100.14 fue asignada de forma dinámica por el servidor a la PC que hizo la petición.

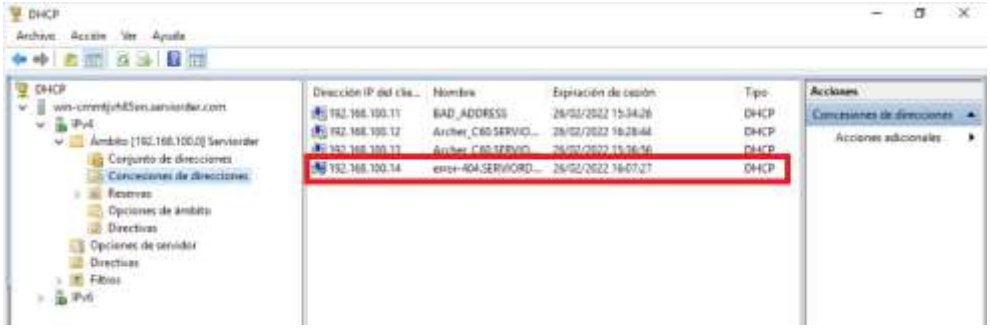


Figura 66.- Verificación de asignación de IP en el DHCP, tomada investigación directa, elaborado por Enrique Franco

Por último, cada vez que exista una nueva petición a través de la red wireless y sea fallida o exitosa el servidor guardará los registros esto a fin de tener mejores niveles de seguridad en la red actual y en caso de vulnerabilidades o amenazas vía wireless se tenga una mejor perspectiva del atacante.

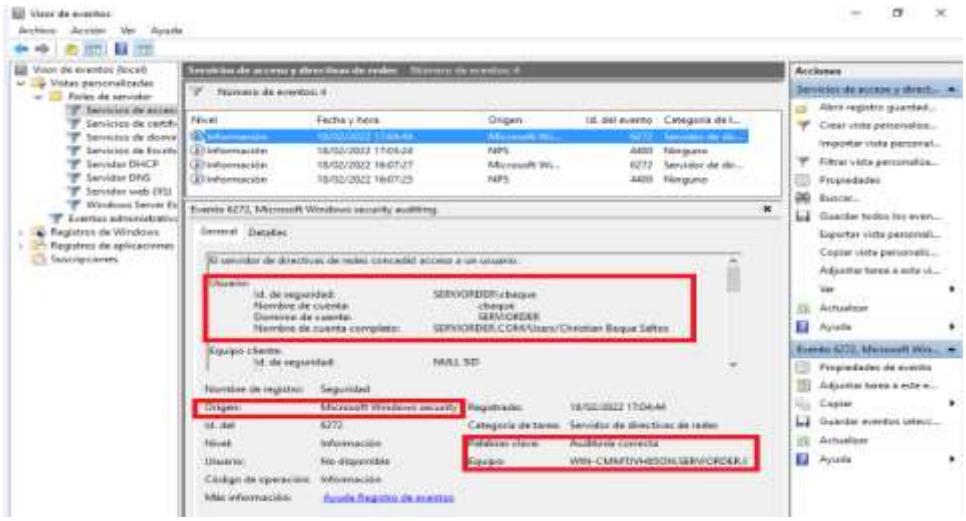


Figura 67.- Revisión de registros en el servidor, tomada investigación directa, elaborado por Enrique Franco

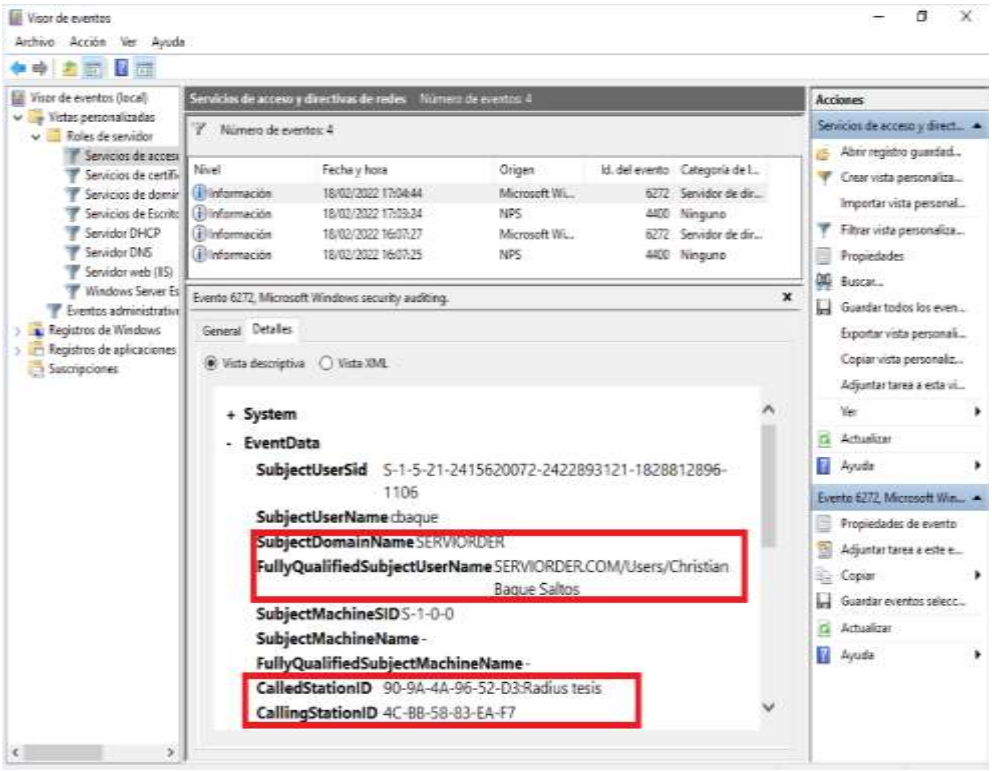


Figura 68.- Detalles de la conexión, tomada investigación directa, elaborado por Enrique Franco

Por último, se presenta el diseño de la propuesta creado y operativo para la empresa Serviorder S.A

Figura 69.- Equipos configurados, tomada investigación directa, elaborado por Enrique Franco

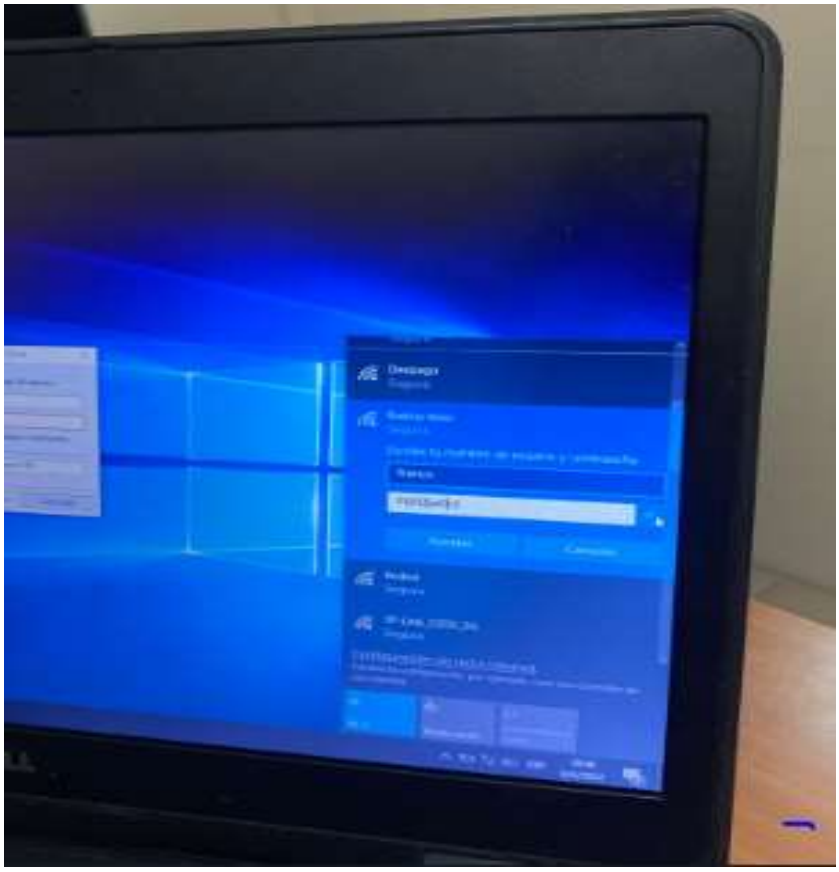


Figura 70.- Prueba de conectividad PC

Figura 71.- Especialista en sistema probando funcionalidad

Figura 72.- Colaboradores de Serviorder

Figura 73.- Colaboradores de Serviorder

Figura 74.- Foto con el especialista del área

3.13 Costo de implementación

Para el presente trabajo se establece el costo total del diseño propuesto para la empresa Serviorder o cualquier otra institución o persona que desee desarrollar la propuesta los que son detallados a continuación.

Tabla 6.- *Costo de la solución*

Detalle	Cantidad	Precio	Total
Access Point (TP-Link)	1	$25.00	$25.00
Cables de red	4	$0.75	$3.00
Switch de capa 2	1	$10.00	$10.00
PC para servidor	1	$400.00	$400.00
Total			$433.00

Información tomada de la investigación directa. Elaborado por Enrique Franco

Cabe recalcar que de contar con un equipo en el que se pueda instalar el servidor el costo total del proyecto disminuye de manera considerable siendo muy factible de operar e implementar.

3.14 Análisis de la solución

Una vez desplegada la solución en la empresa SERVIORDER S.A. se puede constatar que es necesario el uso de credenciales a nivel de dominio por los usuarios para poder acceder al sistema

El ingreso a través de credenciales de cuentas de dominio por parte de los colaboradores de la empresa limita a la entrega de credenciales a otros empleados debido a que se puede validar la contabilización en los accesos e incluso las direcciones MAC de equipo permitiendo tener un control en cuanto a conectividad.

Otro punto para mencionarse es que el ingeniero especialista en redes y conectividad tendrá un mejor control en cuanto a los usuarios conectados es decir de haber alguna afectación o ataque generado por algún usuario vía wireless podrá identificar en el servidor la MAC, así como el nombre del usuario en el dominio permitiendo una mejor gestión y control de la red.

La solución puede ser integrada con diferentes equipos wireless por lo que si a futuro se requiere de algún dispositivo que tenga mayor cantidad de usuarios y desee ser integrado a la solución propuesta será factible.

A diferencia de la solución anterior planteada las políticas de seguridad de Active Directory en cuanto a credenciales le obliga a un usuario a tener al menos 8 caracteres que incluyan (Números, símbolos y letras mayúsculas y minúsculas) a diferencia de la clave pre-compartida (PSK) en el que en muchas ocasiones no existe un control en cuanto a la robustez de las credenciales wireless.

3.15 Conclusiones

- El protocolo PEAP permitió establecer una comunicación con el servicio NPS de Windows permitiendo la autenticación de forma centralizada en la red
- La autenticación realizada por los usuarios es capaz de ser registrada y revisada para la solución de problema e incluso mejoras de seguridad
- Al hacer uso de la autenticación de Radius cada usuario tiene la gestión de sus credenciales dando un mayor criterio de seguridad a la institución
- Se redujo de forma considerable los dominios de broadcast además de mitigar cualquier tipo de vulnerabilidad existente vía Wireless

3.16 Recomendaciones

- Se recomienda realizar la autenticación 802.1x mediante la asignación vlans dinámicas a la hora de proporcionar los parámetros de red en entorno inalámbrico
- Realizar la integración de la solución con servicios de directorio opensource como LDAP en distribuciones de Linux Server
- Proporcionar la autenticación a nivel de puertos otorgando robustez a nivel físico de la red
- Integrar la solución con herramientas como NetFlow para la recolección de datos y observar en tiempo real los problemas que existen en la red
- Ocultar el SSID a fin de evitar ataque en las redes wireless
- Segmentar el ancho de banda acorde a las vlans que pertenezca un usuario teniendo una mejor gestión en cuanto a rendimiento.

Bibliografía

Aguirre, E., Calva, J., Guerrero , A., Hernández, A., & Hernández, S. (2017). Comparación de los modelos OSI y TCP/IP. *UAEH*.

Álava, J. C., & Arcia, A. P. (2021). Análisis de tráfico de datos en la capa de enlace de redes LAN, para la detección de posibles ataques o intrucciones sobre tecnologías ethernet y wifi 802.11 en la carrera de ingeniería en sistemas computacionales de la Uni. de Manabí. *Universidad Estatal del Sur de Manabí*.

Altamirano, D. O., & Álvarez, D. C. (2016). Estudio de la probabilidad de pérdida de carga y pérdida de carga horaria para sistemas autónomos y/o conectados a la red en Ecuador. *Universidad de Cuenca*.

Alvarado, R. C. (2010). Documentación, implementación y elaboración de guías de laboratorio sobre protocolos de enrutamiento en la red: RIP, IS-IS, OSPF y BGP; basados en un software de simulación. *Universidad Pontifica Bolivariana*.

Arévalo, G. T. (2018). Propuesta del diseño de red para la distribuición de los dispositivos de conexión onalámbrica en la cuidad universitaria de la Universidad Nacional de San Martin. *Universidad Nacional de San Martín*.

Asadovay, G. L., & Caiza, L. O. (2013). Análisis comparativo de servidores de autenticación RADIUS y LDAP con el uso de certificados digitales para mejorar la seguridad en el control de acceso a redes wifi. *Escuela Superior Politécnica de Chimborazo*.

Barbecho, P. B. (2016). Diseño y simulación de una topología y gestión de red basadas en túneles GRE y enrutamiento dinámica OSPF y EIGRP, caso de estudio grupo automotriz EIJURI. *Pontifica Universidad Católica Ecuador*.

CEH. (EC-Council Certified Ethical). *Certified Ethical Hacking*.

Celestino, A. M. (2009). Implementación de seguridad en redes inalámbricas. CASO PRÁCTICO: RIU. *Universidad Nacional Autónoma de México*.

Cepeda, C. C., & Proaño, P. S. (2007). Diseño e implementación de un cliente radius en linux. *Red de repositorios latinoamericanos*.

Cevallos, J. L. (2017). Estudio de factibilidad para la aplicación de estándares de seguridad en redes locales inalámbricas de la carrera de Ingeniería en sistemas computacionales de la Universidad Estatal del Sur de Manabí. *Universidad Estatal del Sur de Manabi*.

Chulli , J. V., & Espinoza, B. P. (2019). Análisis de vulnerabilidad de redes inalámbricas con herramientas MITM. *Universidad Estatal de Milagro*.

Cisco. (Octubre de 2017). *Cisco.com*. Obtenido de www.cisco.com

Cisco. (2020). *CCNA 200-301*. Estados Unidos.

Cisco. (2020). CCNA 200-301. *Cisco.com*.

Cordova, C. R. (2010). Implementación de protocolos de comunicación para mejorar la disponibilidad de una red informática. *Universidad Señor de Spain*.

Díaz, M. R. (2021). Implementación de un prototipo virtualizado de integración de servicios de intranet sobre plataforma Linux y Windows. *Escuela Politécnica Nacional*.

Dordoigne, J. (2015). *Redes informáticas . Nociones fundamentales (5° edicion).* Ediciones ENI, 2015.

Espinosa, E. C., & Moncayo, J. V. (2010). Análisis de los protocolos VRRP y CAP aplicado a la redundancia de gateway usando GNU/Linux para la empresa INFOQUALITY S.A. *Escuela Superior Politécnica de Chimborazo*.

Espinoza, E. (2018). Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante Radius. *Universidad Nacional Mayor de San Marcos*.

Figueroa, D., Díaz, F., & Gramajo, M. (2017). Estudio de la influencia de un entorno de simulación en la enseñanza de redes de computadoras en el nivel universitario. *Universidad de la Pata*.

IONOS. (14 de Agosto de 2019). *ionos.es*. Obtenido de https://www.ionos.es/digitalguide/servidores/seguridad/seguridad-wlan-la-mejor-proteccion-para-tu-red/

Jimenez, C. R. (2012). Implementación de un servidor radius para apoyar la seguridad en una red de telecomunicaciones. *Universidad Santo Toma*.

Ley Organica de las Telecomunicaciones. (18 de Febrero de 2015). *Arcotel*. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Luje, L. Z., & Mosquera, H. G. (2011). Análisis de la metodología de integración de modelos de madurez de capacidades (CMMI) para el desarrollo de software. Caso prácticio: Diseño e implementación de un sistema de fuerza de ventas de la empresa GATO SPORT importaciones de la cuidad de Quito. *Universidad Técnica de Cotopaxi*.

Mendoza, A. C., Barraza, A. H., Estrada, F. S., Esquivel, C. R., & Calderón, D. N. (2016). Análisis del desempeño del protocolo RADIUS en redes inalámbricas. *Revista de investigación en ingeniería e innovación tecnológica*.

Mendoza, M. N., Zambrano, M. Z., Sanchéz , L. P., Linares, M. A., & Hung, D. L. (2021). Manejo de servicio de autenticación de usuarios con servidores RADIUS. *Revista Sinapsis*.

Miranda, C. F., Villatoro, K. A., & Hernández, R. H. (2012). Implementación de un prototipo de red inalámbrica que permita elevar los niveles de seguridd a través de la autenticación de un servidor Radius para los usuarios que acceden a internet en el edificio Franciso Morazán de la UTEC. *Universidad Tecnológica de el Salvador*.

Netlearning. (2015). *netlearning*. Obtenido de www.netlearning.cl

Nuno, A., & Barraca, J. (2019). Integration of the Captive Portal paradigm with the 802.1x architecture. *arXiv*.

Offensive Security. (2014). Wireless Attacks - WiFu. *Offensive Security*.

Pallo, J. N., & Martínez, J. U. (2010). Diseño de una Red Inalámbrica con Tecnología Wi-fi para Siderúrgica Tungurahua S.A. *Universidad Técnica de Ambato*.

Patiño, E. C. (2015). Reingeniería de la infraestructura de datos de la cooperativa de ahorro y crédito "San Antonio LTDA" y diseño de los enlaces inalámbricos a sus sucursales. *Universidad Técnica del Norte*.

Pérez, C. S. (2017). Diseño e implementación de un enrutamiento redundante usando el protocolo Border Gateway Protocol (BGP) para la red de un proveedor de servicios de Internet en Bogotá. *Universidad Santo Tomás*.

Purple AI. (13 de Octubre de 2021). *purple*. Obtenido de https://purple.ai/es/blogs/portales-cautivos-para-que-sirven-y-como-funcionan/

Quiroz, R. V., Ramírez, F. M., & Rivera, Y. G. (2013). Propuesta de prácticas de laboratorios de switching y routing para la carrera de ingeniería en telemática de UNAN - LEÓN. *Universdad Nacional Autónoma de Nicaragua UNAN - León*.

Ramakrishanan, K., & Veerakumar, U. (2019). Interoperability Solution for Ieee 802.1x Based Authentication Unsupported Customer Premises Equipment. *IEEE Xplore*.

Riffo, M. (2009). Vulnerabilidades de las redes TCP/IP y principales mecanismos de seguridad. *Universidad Austral de Chile*.

Rodriguez, J., Ladino, E., Bejarano, J., & Quimbayo, L. (2018). Modelo OSI y direccionamiento IP. *Universidad Nacional Abierta y a Distancia*.

Sanchez, B. R. (2019). Trabajo de suficiencia profesional redes wireless. *Universidad José Carlos Mariátegui*.

Serrano, A. F. (2011). *Análisis de vulnerabilidades de seguridades en redes inalámbricas dentro de un entorno empresarial que utilizan cifrado AES y TKIP, WPA persona y WPA2 personal del DMQ.* Quito.

Taufik, H., & Imam, R. (2021). Optimation Wireless Security IEEE 802.1X using the Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP). *International Journal of Computer Applications*.

Telecapp. (2022). *telecapp*.

Tolosa, G. (2014). Protocolos y modelo OSI. *Labiratorio de redes* .

Torres, P. R. (2016). Diseño de una red privada virtual para la optimización de las comunicaciones en la empresa comunicaciones e informática SAC caso: redes de datos. *Universidad Inca Garcilaso de la Vega*.

Vasquez, A. R. (2021). Diseño de una red de alto rendimiento aplicando el protocolo BGP o GLP con la funcionalidad de balanceo de carga transparente. *Universidad de Guayaquil*.

welivesecurity. (6 de Agosto de 2012). *Wilivesecurity*.

Windows. (2022). *Windows server*. Obtenido de https://www.microsoft.com/es-es/windows-server?SilentAuth=1

Windows server. (29 de Julio de 2021). *Network Policy Server*. Obtenido de https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top

Yerovi, N. L., & Flores, J. O. (2010). Análisis de los protocolos de la alta disponibilidad de gateways en la interconectividad LAN/WAN aplicadas al diseño de redes de campus. *Escuela Superior Politécnica de Chimborazo*.

Yurema, T., & Gerardo, M. (2016). Implementación de un servidor RADIUS en Windows Server para centralizar la administración de nuevos Access Points en las oficinas remotas de Galpones y Huertos del Gobierno Autónomo Descentralizado del Guayas. *Universidad Politécnica Salesiana Sede Guayaquil*.

Zambrano, J. G. (2015). Estudio de una conexión de Internet aplicando un protocolo de alta disponibilidad para empresa grupo AGRIPRODUCT S.A. en la cuidad de Guayaquil. *Universidad de Guayaquil*.