UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERIA

CARRERA DE TELECOMUNICACIONES

Análisis comparativo y evaluación de las principales tecnologías de Autenticación, Autorización y Auditoría (AAA) para proponer una solución de mejora a la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo.

Trabajo de Titulación para optar al título de

Ingeniero en Telecomunicaciones

Autor:

Solís Aguirre, Cristian Javier

Tutor:

Mgs. Alejandra del Pilar Pozo Jara

Riobamba, Ecuador. 2024

DERECHOS DE AUTORÍA

Yo, **Cristian Javier Solis Aguirre**, con cédula de ciudadanía 0604573956, autor del trabajo de investigación titulado: **Análisis comparativo y evaluación de las principales tecnologías de Autenticación, Autorización y Auditoría (AAA) para proponer una solución de mejora a la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, el 7 de agosto del 2024.

Cristian Javier Solís Aguirre

C.I: 0604573956

ACTA FAVORABLE - INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN

En la Ciudad de Riobamba, a los 8 días del mes de AGOSTO de 2024, luego de haber revisado el Informe Final del Trabajo de Investigación presentado por el estudiante **SOLÍS AGUIRRE CRISTIAN JAVIER** con CC: **060457395-6**, de la carrera de **INGENIERÍA EN TELECOMUNICACIONES** y dando cumplimiento a los criterios metodológicos exigidos, se emite el **ACTA FAVORABLE DEL INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN** titulado **"ANÁLISIS COMPARATIVO Y EVALUACIÓN DE LAS PRINCIPALES TECNOLOGÍAS DE AUTENTICACIÓN, AUTORIZACIÓN Y AUDITORÍA (AAA) PARA PROPONER UNA SOLUCIÓN DE MEJORA A LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO"**, por lo tanto se autoriza la presentación del mismo para los trámites pertinentes.

Firmado electrónicamente por:
ALEJANDRA DEL PILAR POZO JARA

Msc. Alejandra Pozo
TUTOR(A)

DICTAMEN FAVORABLE DEL TUTOR Y MIEMBROS DE TRIBUNAL

Quienes suscribimos, catedráticos designados Tutor y Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **"ANÁLISIS COMPARATIVO Y EVALUACIÓN DE LAS PRINCIPALES TECNOLOGÍAS DE AUTENTICACIÓN, AUTORIZACIÓN Y AUDITORÍA (AAA) PARA PROPONER UNA SOLUCIÓN DE MEJORA A LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO."**, presentado por **CRISTIAN JAVIER SOLIS AGUIRRE**, con cédula de identidad número **060457395-6**, bajo la tutoría de **Mgs. Alejandra del Pilar Pozo Jara**, recomendamos la **APROBACIÓN** de este con fines de titulación. Previamente se ha asesorado durante el desarrollo, revisado y evaluado el trabajo de investigación escrito y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 18 de octubre de 2024.

Dr. Antonio Meneses.
PRESIDENTE DEL TRIBUNAL DE GRADO

Mgs. José Jínez Tapia
MIEMBRO DEL TRIBUNAL DE GRADO

Mgs. Eduardo Daniel Haro Mendoza
MIEMBRO DEL TRIBUNAL DE GRADO

Mgs. Alejandra del Pilar Pozo Jara
TUTORA

CERTIFICACIÓN

Que, **SOLIS AGUIRRE CRISTIAN JAVIER** con CC: **060457395-6**, estudiante de la Carrera de **TELECOMUNICACIONES** , Facultad de **INGENIERÍA**; ha trabajado bajo mi tutoría el trabajo de investigación titulado **"ANÁLISIS COMPARATIVO Y EVALUACIÓN DE LAS PRINCIPALES TECNOLOGÍAS DE AUTENTICACIÓN, AUTORIZACIÓN Y AUDITORÍA (AAA) PARA PROPONER UNA SOLUCIÓN DE MEJORA A LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO",** cumple con el **5%**, de acuerdo al reporte del sistema Anti plagio **TURNITIN**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 25 de septiembre de 2024

Firmado electrónicamente por:
ALEJANDRA DEL PILAR POZO JARA

Ing. Alejandra del Pilar Pozo Jara Mgs.
TUTOR

DEDICATORIA

Quiero dedicar este trabajo a mis padres, con quienes he tenido la fortuna de contar con su apoyo incondicional en este arduo camino. A mi madre, Aracely Aguirre, por su amor inquebrantable e inagotable paciencia que me han acompañado en los peores momentos. Sus palabras de aliento y constante presencia me han brindado fuerza en cada obstáculo de la vida. A mi padre, Javier Solis, cuya sabiduría y consejos han sido pilares fundamentales en mi vida. Su incansable esfuerzo y dedicación han sido una fuente de inspiración para mí. Eres mi modelo a seguir y mi héroe. A ustedes les dedico este triunfo, con la esperanza de que se sientan tan orgullosos de mí como yo lo estoy de ser su hijo. Los amo y les agradezco por todo lo que han hecho por mí. Este logro es mío, pero el triunfo se los debo a ustedes.

Con todo mi amor y eterna gratitud,

Cristian Javier Solis Aguirre.

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a todas las personas e instituciones que han sido fundamentales para la realización de esta tesis.

En primer lugar, agradezco a Dios por otorgarme la salud, la sabiduría y la fortaleza necesarias para culminar esta etapa académica con éxito. A mis padres, Aracely Aguirre y Javier Solis, por su amor incondicional y su apoyo constante. Su consejos y fortaleza han sido mi fuente de motivación y han guiado cada paso de este viaje. Sus enseñanzas y valores han sido pilares fundamentales en mi vida. A mis queridas hermanas, Daniela, Evelyn y Sofía, y a toda mi familia, por su apoyo incondicional, cariño y comprensión durante este proceso. Su presencia y apoyo han sido una parte esencial en cada logro alcanzado. A mi novia, Sophia, por su amor y apoyo día a día. Sus palabras y constante motivación han sido incalculables para superar cada desafío que se presentó en este camino. A mi directora de tesis, Mgs. Alejandra Pozo, por su guía, paciencia y valiosos consejos. Su experiencia y conocimientos han sido cruciales para el desarrollo y éxito de este trabajo. A la Universidad Nacional de Chimborazo y a la Dirección de Tecnologías de la Información, por proporcionar los recursos académicos y tecnológicos necesarios para la realización de esta tesis en especial a los ingenieros Diego Romero, Javier Haro y Diego Caiza por su invaluable ayuda y colaboración durante todo el proceso.

Finalmente, agradezco a todos aquellos que, de alguna manera, han contribuido a mi formación académica y personal. Este logro es el resultado del esfuerzo y dedicación conjunta, y a todos ustedes les dedico este triunfo con profunda gratitud.

Con aprecio y agradecimiento,

Cristian Solis Aguirre

ÍNDICE GENERAL

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS

RESUMEN

Las tecnologías de autenticación, autorización y auditoría (AAA) se refieren a sistemas que controlan el acceso a la red, gestionan los permisos de usuario y monitorizan las actividades realizadas durante el uso de la red. La presente investigación se desarrolla con el objetivo de mejorar la seguridad y el control de la red inalámbrica del bloque “U” del campus "Dolorosa" de la Universidad Nacional de Chimborazo (UNACH). La metodología es de tipo aplicada y descriptiva y de enfoque mixto. La población está conformada por un conjunto de herramientas AAA y la muestra dependerá de la adaptabilidad con el hardware CISCO existente en el bloque “U” de la UNACH. Por ello, se realizó pruebas comparativas basadas en criterios como facilidad de uso, eficiencia, seguridad, escalabilidad e interoperabilidad. Los resultados del estudio comparativo entre el servidor de autenticación RADIUS implementado en Cisco ISE vs FreeRADIUS mostraron que Cisco ISE sobresale por sus características avanzadas, soporte técnico y facilidad de implementación, ofreciendo una visibilidad completa de la red, una interfaz gráfica intuitiva y una integración sin problemas con otros productos de Cisco. Sin embargo, estas ventajas vienen con costos elevados y una dependencia de productos específicos de Cisco, lo que puede reducir la flexibilidad y aumentar los gastos. En contraste, FreeRADIUS es una solución flexible y económica en términos de costos iniciales, adecuada para diversas infraestructuras, aunque ofrece menor visibilidad y es más compleja de gestionar. En conclusión, Cisco ISE utilizando el método de autenticación RADIUS demostró ser una herramienta efectiva en un entorno de prueba controlado, superando a FreeRADIUS en cuanto a características avanzadas, soporte técnico y facilidad de implementación, aunque es importante tener en cuenta sus altos costos. Este estudio recomienda considerar Cisco ISE para mejorar la seguridad AAA en el bloque “U” de la UNACH, ya que ofrece una solución robusta y eficiente, a pesar de su mayor inversión inicial en comparación con FreeRADIUS.

Palabras claves: AAA, Cisco ISE, Radius, TACACS+, 802.1x, WLC, FreeRADIUS.

ABSTRACT

Authentication, authorization, and auditing (AAA) technologies are critical systems that control network access, manage user permissions, and monitor activities performed on the network. This research was conducted to enhance the security and control of the wireless network in the "U" block of the Dolorosa campus at the National University of Chimborazo (UNACH). The study follows an applied and descriptive methodology with a mixed approach. The research population consisted of various AAA tools, while the sample was determined based on compatibility with the existing CISCO hardware in the "U" block at UNACH. Comparative tests were conducted using criteria such as ease of use, efficiency, security, scalability, and interoperability. The results from the comparative study between the RADIUS authentication server implemented in Cisco ISE and FreeRADIUS highlighted several key differences. Cisco ISE excels in advanced features, technical support, and ease of implementation, offering comprehensive network visibility, an intuitive graphical interface, and seamless integration with other Cisco products. However, these benefits come at a high cost and require a dependency on Cisco-specific products, which may reduce flexibility and increase expenses. On the other hand, FreeRADIUS is a more flexible and cost-effective solution in terms of upfront costs, suitable for a variety of infrastructures. However, it offers less visibility and is more complex to manage. In conclusion, Cisco ISE, utilizing the RADIUS authentication method, proved to be an effective tool in a controlled test environment, outperforming FreeRADIUS in terms of advanced features, technical support, and ease of implementation. However, its high cost is an important consideration. This study recommends Cisco ISE for improving AAA security in the "U" block of UNACH, as it offers a robust and efficient solution despite its higher initial investment compared to FreeRADIUS.

Keywords: AAA, Cisco ISE, Radius, TACACS+, 802.1x, WLC, FreeRADIUS.

Reviewed and improved by: Armijos Jacqueline

Firmado electrónicamente por:
JACQUELINE GUADALUPE ARMIJOS MONAR

CAPÍTULO I. INTRODUCCION.

El presente trabajo de investigación de tesis previo a la obtención del título de Ingeniero en Telecomunicaciones trata acerca del análisis comparativo de las diferentes soluciones AAA y la selección de una de ellas como propuesta para mejorar la seguridad en el control de acceso a la red inalámbrica del bloque U campus "Dolorosa" de la Universidad Nacional de Chimborazo. De esta forma garantizaremos la seguridad de los datos, proporcionando servicios que forman una arquitectura de sistema que se utiliza para la configuración de tres funciones de seguridad conocidas como Autenticación (Authentication), Autorización (Authorization) y Contabilidad (Accounting). [1]

Mediante el estudio comparativo y la evaluación de las principales tecnologías de Autenticación, Autorización y Auditoría (AAA), se propone una solución de mejora a la seguridad de la red inalámbrica del bloque "U" campus "Dolorosa" de la Universidad Nacional de Chimborazo.

Las instituciones públicas o privadas necesitan incorporar una solución que se adapte tanto a la cantidad de usuarios registrados en sus bases de datos y la seguridad en sus redes. Es por esto por lo que la UNACH tiene como propósito brindar acceso a internet de manera segura a sus estudiantes, profesores y personal administrativo.

Para el desarrollo de este tema de investigación se requiere un alto nivel de análisis y comprensión de las tecnologías de software y hardware de redes inalámbricas, así como conocimientos de las diferentes herramientas de seguridad de redes como: Cisco Identity Services Engine (ISE), TACACS+ y Radius. Estas herramientas pueden ser tanto de software abierto como de pago y enfocan su compatibilidad en diversos equipos de red. Actualmente, el backbone y la red inalámbrica de la universidad cuentan con equipos de la marca JUNIPER, mientras que la controladora Cisco está trabajando con un número reducido de Access Points en el campus "Dolorosa".

La elaboración de este proyecto de investigación es relevante puesto que proporciona datos e información acerca de las principales tecnologías de Autenticación, Autorización y Auditoría (AAA) y a su vez propone una solución de mejora a la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo, está investigación tiene mucha importancia porque existen pocos estudios a nivel nacional relacionados con estas dos variables de estudio.

Los beneficiarios serán los miembros de la comunidad Universitaria de la UNACH, se logrará obtener un estudio adecuado sobre las tecnologías de Autenticación, Autorización y Auditoría (AAA), para posteriormente proponer un plan de mejora de la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo, además, que esta tecnología sea tomada como una ayuda la cual no solo sirva a la comunidad universitaria, sino a las personas que se encuentren interesados en el tema como investigadores, estudiantes de pregrado y estudiantes de posgrado interesados en el tema.

Es factible la realización de este proyecto investigativo porque cuenta con todos los recursos académicos, investigativos, bibliográficos, además con el permiso pertinente por parte de las autoridades institucionales, así como el acceso a herramientas de software y hardware que se encuentran en la Dirección de Tecnologías de la Información y Comunicación de la UNACH.

1.1 Planteamiento del problema

Actualmente, la UNACH utiliza FreeRadius que es una implementación caduca y sin soporte del protocolo RADIUS, el cual permite la autenticación centralizada, autorización y contabilidad (AAA) para los usuarios que se conectan y utilizan servicios de red. Sin embargo, se han identificado ciertos problemas en el sistema de autenticación y seguridad cuando los usuarios intentan acceder a la red inalámbrica. Adicionalmente, esta herramienta no cumple con los requisitos de escalabilidad necesarios, carece de soporte de los desarrolladores del protocolo y, por lo tanto, no satisface las necesidades futuras de accesibilidad a la red inalámbrica en cuanto al incremento de usuarios y dispositivos. [2]

Usar contraseñas como único medio de acceso a aplicaciones específicas no suele ser suficiente para prevenir que hackers accedan a los recursos de forma no autorizada y en algunas ocasiones pueden causar problemas graves. Entonces para garantizar una protección adecuada de la red, es necesario contar con mecanismos de seguridad que utilicen métodos probados para controlar el acceso a la red. [3]

El presente trabajo evalúa diferentes soluciones de seguridad existentes y se analizan los diferentes requisitos de seguridad y escalabilidad planteados por la UNACH. Tomando en cuenta todos estos requerimientos, se propone una herramienta para garantizar un acceso seguro, confiable y amigable a la red inalámbrica de la UNACH.

1.2 Justificación

La Universidad Nacional de Chimborazo (UNACH) enfrenta desafíos significativos en la seguridad de su red inalámbrica debido a la dependencia de la herramienta FreeRadius para la autenticación, autorización y contabilidad (AAA). A pesar de proporcionar una autenticación centralizada, este protocolo presenta limitaciones en términos de escalabilidad y soporte técnico, lo cual impide satisfacer las crecientes demandas de accesibilidad y seguridad de la red.

Además, el uso de contraseñas como único medio de acceso a aplicaciones específicas resulta insuficiente para prevenir accesos no autorizados, exponiendo la red a potenciales intrusiones y ataques cibernéticos. Esto subraya la necesidad de adoptar mecanismos de seguridad más robustos que no solo controlen el acceso, sino que también ofrezcan una protección continua y adaptable a las futuras necesidades de la red.

El presente estudio tiene como objetivo evaluar y comparar dos tecnologías de AAA para identificar una solución que mejore la seguridad de la red inalámbrica de la UNACH. La implementación de una tecnología avanzada que combine autenticación y auditorías continuas podría proporcionar una defensa más eficaz contra accesos no autorizados, asegurando la integridad y confidencialidad de los datos. Este enfoque no solo mitigará los riesgos actuales, sino que también ofrecerá una solución escalable y sostenible para el crecimiento futuro de la red.

1.3 OBJETIVOS

1.3.1 Objetivo General

- Analizar y evaluar las principales tecnologías de autenticación, autorización y auditoría (AAA) para generar una propuesta que permita mejorar la seguridad y el control de la red inalámbrica del bloque U campus “Dolorosa” de la Universidad Nacional de Chimborazo.

1.3.2 Objetivos Específicos

- Estudiar las tecnologías de Autenticación, Autorización y Contabilidad (AAA) disponibles actualmente que permitan el acceso de usuarios a una red inalámbrica.
- Realizar un estudio comparativo de las principales tecnologías AAA, para determinar cuál de ellas se adapta de manera más efectiva a los requerimientos de la red inalámbrica del bloque “U” campus “Dolorosa” de la Universidad Nacional de Chimborazo.
- Implementar la tecnología AAA mediante un entorno de prueba controlado, utilizando condiciones reales de uso el bloque “U” campus “Dolorosa” de la Universidad Nacional de Chimborazo.
- Realizar una evaluación sistemática de la herramienta seleccionada frente a la actualmente usada, considerando parámetros fundamentales como: características, soporte, recursos necesarios, implementación y costos.

CAPÍTULO II. MARCO TEORICO.

Estado del Arte

La investigación con el título " Advanced AAA System for interoperable distributed architectures" aborda el diseño de sistemas seguros de Autenticación, Autorización y Registro (AAA) para entornos heterogéneos. Se enfoca en la autenticación y autorización de dispositivos portátiles, proponiendo un protocolo de autenticación y autorización, así como una arquitectura de control de acceso completa utilizando XACML. Además, se propone mejorar las limitaciones de rendimiento del protocolo XACML mediante el uso de bases de datos gráficas. Se presentan dos soluciones: un modelo puro de bases de datos gráficas y una aproximación híbrida. Además, se propone una solución para el registro de logs en entornos distribuidos de manera flexible y segura utilizando Blockchain. Todas las propuestas son prototipadas e integradas en el demostrador de la estación de control de tierra o Ground Control Station (GCS), o simuladas en la integración de bases de datos gráficas y la red de logs basada en Blockchain. Los resultados se evidenciaron un notable incremento en el rendimiento al adoptar el enfoque de la base de datos gráfica híbrida en comparación con la implementación estándar del PDP XACML, como WSO2 Balana, especialmente en situaciones donde el sistema enfrenta múltiples políticas o solicitudes de acceso simultáneas. [4]

El artículo "Diseño e Implementación de una Red LAN y WLAN con Sistema de Control de Acceso Mediante Servidores AAA" detalla la implementación de una red LAN y WLAN con control de acceso AAA, utilizando tecnologías como EtherChannel, GLBP, ACS con TACACS+, y servidor IAS con IEEE 802.1x. Se destaca la coexistencia de los protocolos AAA RADIUS y TACACS+ para garantizar un robusto control de acceso. Se demuestra la optimización de recursos mediante técnicas como EtherChannel y GLBP, y se consideran las preferencias de los usuarios finales, enfocándose en la continuidad del servicio, la velocidad de intercambio de datos y la seguridad de la información. Finalmente, el análisis económico muestra la rentabilidad del proyecto con una recuperación de la inversión en el primer año. [5]

El artículo de investigación "Desarrollo de un mecanismo ágil de auditoría a la seguridad informática de la red inalámbrica 802.11 con arquitectura AAA; caso de estudio: instituto ITSJOL" revela que la aplicación del mecanismo ágil de auditoría mediante la

norma ISO 27002 junto con la metodología OSSTMM (metodología estándar, usada para realizar pruebas de seguridad) y las mejores prácticas de seguridad en redes inalámbricas resultó en ajustes significativos y mejoras en la eficiencia del proceso de verificación, identificando controles duplicados y adaptando los niveles de aceptabilidad. Sin embargo, a pesar de los esfuerzos realizados, se evidenciaron deficiencias importantes, con aproximadamente el 49% de los controles evaluados no implementados o implementados de manera informal, destacando la necesidad de una mejora continua en la seguridad. Además, se enfatizó la importancia de acciones complementarias como auditorías regulares, monitoreo constante de controles y capacitación periódica de usuarios para fortalecer la seguridad de la red. [6]

2.1 Fundamentación teórica

2.1.1 AAA

AAA es un acrónimo sobre Autenticación, autorización y contabilidad, estas son las 3 funciones principales de realiza las herramientas que llevan su nombre. La autenticación determina quien puede ingresar a la red, la autorización especifica que acciones pueden llevar a cabo los usuarios una vez dentro y la contabilidad registrara y monitoriza las actividades realizadas durante el acceso a la red. [7]

Estas herramientas no solo facilitaran el acceso a la red además gestiona permisos de acceso a recursos específicos según los niveles de seguridad que proponga el administrador de la red.

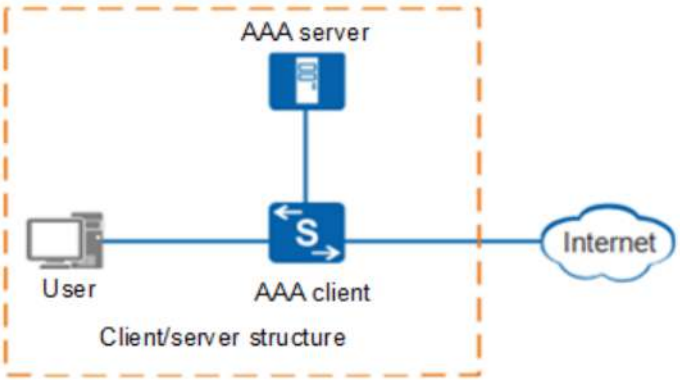

Figura 1. Arquitectura básica de AAA [8]

2.1.2 Beneficios

Entre tantos beneficios que maneja las herramientas AAA entre los más destacados están la mayor flexibilidad y control de la configuración de acceso se refiere a la capacidad de tener un amplio margen de maniobra y supervisión sobre cómo se establecen los permisos de acceso en un sistema. La escalabilidad implica la capacidad de expandir el sistema de autenticación, autorización y contabilidad de manera eficiente para adaptarse al crecimiento y a las necesidades cambiantes de la red. Por otro lado, los métodos estandarizados de autenticación son protocolos reconocidos y aceptados universalmente para verificar la identidad de los usuarios que intenten acceder a la red, garantizando así una mayor interoperabilidad y seguridad [9].

2.1.3 Importancia de las tecnologías AAA

Se resaltará la importancia de garantizar la seguridad de una red, destacando los riesgos asociados con el acceso no controlado de los usuarios que puede resultar en la perdida de datos y otros problemas de seguridad, la importancia de la implementación de medidas de seguridad basados en los protocolos 802.1x garantizan la integridad y seguridad de redes en entornos empresarial o institucional basándose así en la minimización de posibles ataques o accesos indebidos.

2.1.4 Riesgos

La falta de una herramienta adecuada de autenticación, autorización y contabilidad (AAA) en una red institucional conlleva varios riesgos significativos para la seguridad e integridad de los datos. En primer lugar, la ausencia de autenticación efectiva permite la entrada de usuarios no autorizados a la red, lo que resultaría en accesos no deseados a información sensible y un potencial robo de datos. La falta de autorización adecuada significa que los usuarios legítimos podrían obtener acceso no restringido a recurso críticos o confidenciales, lo que aumenta el riesgo de violaciones de seguridad y abusos internos, además la falta de una auditoria adecuada dificulta la capacidad de rastrear y restringir las actividades de los usuarios, lo que hace más difícil detectar y responder a amenazas o violaciones de seguridad. En conjuntos, estos riesgos pueden dar lugar a pérdidas financieras, daños a la reputación, violaciones regulatorias, afectando negativamente tanto a la organización como a sus usuarios. Por lo que es crucial implementar medidas solidas

de AAA para mitigar estos riegos y proteger la integridad y confidencialidad de la red y sus datos.

2.1.5 Evolución

A lo largo del tiempo, las tecnologías de Autenticación, Autorización y Contabilidad (AAA) han experimentado una evolución significativa para adaptarse a las crecientes demandas de seguridad en las redes. Inicialmente, las soluciones AAA se centraban en la autenticación, utilizando métodos como contraseñas y tokens. Con el aumento de las amenazas cibernéticas y la necesidad de un control más granular sobre el acceso a los recursos, se desarrollaron sistemas más avanzados que integran la autorización y la contabilidad. [10]

La evolución de las tecnologías AAA ha sido impulsada por estándares y protocolos emergentes, como el Protocolo de Acceso a la Red (RADIUS) y el Protocolo de Control de Acceso a la Red (802.1x), que han permitido una autenticación más robusta y centralizada, junto con una mejor gestión de autorización y registro de actividades. Además, el surgimiento de tecnologías como la biometría y la autenticación multifactorial ha añadido capas adicionales de seguridad para mitigar los riesgos de acceso no autorizado. [10]

Esta evolución ha permitido a las organizaciones implementar soluciones AAA más sofisticadas y adaptables, proporcionando un nivel más alto de seguridad y control sobre sus redes inalámbricas y sistemas de información.

2.2 Seguridad en redes inalámbricas

En la actualidad, las redes inalámbricas se han convertido en una parte fundamental de las instituciones educativas, incluyendo las universidades. Estas redes permiten a estudiantes, profesores y personal acceder de manera ágil y conveniente a recursos digitales, colaborar en proyectos y compartir información de forma inalámbrica. Sin embargo, el crecimiento exponencial de las redes inalámbricas ha traído consigo una serie de riesgos y desafíos relacionados con la seguridad de estos entornos educativos.

Las redes inalámbricas universitarias albergan una gran cantidad de datos sensibles, como información personal de estudiantes y profesores, datos de investigación y propiedad intelectual. La falta de seguridad adecuada puede conducir a amenazas y vulnerabilidades que podrían poner en riesgo la confidencialidad, integridad y

disponibilidad de estos datos, así como afectar la reputación y el buen funcionamiento de la institución. Por ello el estándar 802.11 establece ciertos elementos cruciales que deben considerarse en los protocolos de seguridad para redes inalámbricas locales. El cifrado implica procesar un conjunto de datos dentro de un paquete con el propósito de prevenir que cualquier persona, excepto el destinatario, pueda leerlos. Por lo general, se utiliza un algoritmo y una clave de cifrado para lograr esto. La autenticación es un mecanismo que verifica y garantiza la identidad del usuario y el servidor, evitando comprometer la privacidad y la integridad de los datos. En las redes WLAN, se utiliza para verificar la validez de una transmisión entre los puntos de acceso (AP) y las estaciones de trabajo. [11]

Los riesgos y desafíos asociados con la seguridad de las redes inalámbricas en entornos educativos son diversos. Los ataques de interceptación de datos, la suplantación de identidad y las denegaciones de servicio son solo algunos ejemplos de amenazas a los que están expuestas las redes inalámbricas universitarias.

2.3 Fundamentos de las redes inalámbricas

Para comprender la importancia de garantizar un acceso seguro a la red inalámbrica en una universidad, es fundamental tener claridad sobre los conceptos clave relacionados con las redes inalámbricas, así como los estándares y protocolos comúnmente utilizados. Además, es importante destacar las características y limitaciones de las redes inalámbricas que pueden afectar su seguridad.

En primer lugar, es necesario comprender algunos conceptos fundamentales relacionados con las redes inalámbricas. La frecuencia es uno de los aspectos clave, y se refiere a la tasa de oscilación de una señal electromagnética. En las redes inalámbricas de la UNACH, se utilizan diferentes bandas de frecuencia, como 2.4 GHz y 5 GHz, para la transmisión de datos. Estas bandas ofrecen diferentes capacidades y alcances de hasta 250 metros, los canales otro elemento importante permiten la separación de las señales y la transmisión simultánea de datos en diferentes frecuencias dentro de una banda determinada. [12]

2.4 Seguridad en las redes inalámbricas: Amenazas, mecanismos y limitaciones

En el contexto de garantizar un acceso seguro a la red inalámbrica en una universidad, es esencial comprender las amenazas y vulnerabilidades asociadas con las redes inalámbricas, así como los mecanismos de seguridad utilizados para mitigar estos riesgos. En este marco referencial, se explorarán las principales amenazas, los mecanismos de seguridad y se realizará una evaluación crítica de su efectividad y limitaciones. Algunas de las principales amenazas a las redes inalámbricas incluyen:

2.4.1 Ataques de interceptación

Estos ataques se producen cuando un atacante captura y analiza el tráfico de red para obtener información confidencial, como contraseñas o datos personales su interceptación puede llevarse a cabo con programas de software especiales llamados sniffers. Los datos transmitidos a través de una red inalámbrica sin cifrado son especialmente vulnerables a este tipo de ataques. [13]

2.4.2 Suplantación de identidad

También llamado suplantación de personalidad y en este tipo de ataque, un atacante se hace pasar por un usuario legítimo para obtener acceso no autorizado a la red y realizar actividades ilícitas. [12]

2.4.3 Denegación de servicio (DoS)

En un ataque de denegación de servicio, un atacante intenta inhabilitar la red o el punto de acceso inalámbrico con una gran cantidad de tráfico malicioso, lo que resulta en la interrupción de los servicios normales, la denegación de acceso a los usuarios legítimos afectando no solo el ancho de banda, sino también la latencia y las tablas conmutadas de flujo de datos. [14]

Para abordar estas amenazas, se utilizan diversos mecanismos y herramientas de seguridad en las redes inalámbricas. Algunos de los mecanismos más comunes incluyen:

2.4.3.1 Encriptación

La encriptación se utiliza para proteger la confidencialidad de los datos transmitidos a través de la red. Los protocolos de encriptación, como WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 todos estos usan un cifrado y encriptación mediante AES (Advanced Encryption Standard), el cual usa claves con una longitud de 128 bits. [12]

2.4.3.2 Autenticación

Esta se refiere al proceso de verificar que un usuario que solicita servicios de red es válido y legítimo, y se logra al presentar una identidad y credenciales para su verificación. El estándar WPA-Enterprise utiliza el protocolo de autenticación Extensible Authentication Protocol (EAP) para proporcionar un nivel más sólido de autenticación mediante el uso de certificados digitales. [15]

2.4.3.3 Control de Acceso

Implica otorgar permisos a usuarios o grupos y determinar quiénes están autorizados para acceder a los sistemas de información y recursos. Un mecanismo es el filtrado de direcciones MAC este establece una lista de direcciones físicas únicas que limita el acceso a la red solo a dispositivos y usuarios autorizados. [16]

2.5 Soluciones de acceso seguro a la red inalámbrica.

Se busca analizar y comparar diferentes tecnologías de acceso seguro a la red inalámbrica. En particular, se realizará un análisis comparativo dentro la tecnología Cisco Identity Services Engine (ISE) usando servidores de autenticación TACACS+ y Radius.

2.5.1 Cisco Identify Services Engine (ISE):

Es una herramienta de gestión de identidad y control de acceso que puede aportar importantes beneficios en la mejora de la seguridad de la red inalámbrica. ISE permite la autenticación centralizada de usuarios y dispositivos, garantizando políticas de acceso sólidas y consistentes. Además, ofrece un control de acceso granular basado en roles y políticas, lo que evita accesos no autorizados. Una de las características destacadas de

Cisco Identity Services Engine (ISE) es su capacidad para centralizar y unificar el control de acceso seguro basado en el rol de cada usuario. Esto significa que se puede establecer una política de acceso a la red coherente, independientemente de si los usuarios se conectan a través de cable o de forma inalámbrica.

La seguridad basada en contexto permite tomar decisiones de seguridad considerando requisitos y factores relevantes. ISE también permite autenticar dispositivos, reduciendo riesgos de intrusiones. La herramienta facilita el cumplimiento normativo y auditoría, y se integra con otras soluciones de seguridad de Cisco, ofreciendo una solución integral para proteger la red inalámbrica de la universidad. [17]

2.5.1.1 Definición:

El Cisco Identity Services Engine (ISE) representa un componente fundamental dentro de la infraestructura de seguridad de próxima generación, siendo presentado inicialmente en 2011. Concebido por Cisco, su propósito se centra en proporcionar a las empresas, universidades y organizaciones un enfoque integrado para gestionar sus necesidades de acceso y políticas de red. La solución ofrecida por CISCO se distingue por su capacidad para brindar una visibilidad exhaustiva y unificada de la red, aprovechando tanto la identidad como la comprensión del entorno de como los usuarios ingresan a la red. Esta compresión abarca aspectos tales como: [18]

- ¿Quién está accediendo?
- ¿Qué recursos están siendo solicitados?
- ¿Desde dónde se está realizando el acceso?
- ¿Cuándo se lleva a cabo y de qué manera se realiza la conexión a la red?

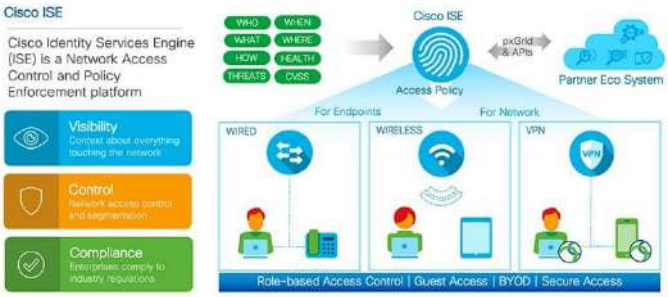

Figura 2. Políticas de ISE [19]

2.5.1.2 Tipos de autenticación en ISE

Ya definidos los parámetros que se incluirá en las políticas del Cisco Identity

Services Engine (ISE), es fundamental determinar los procedimientos para reunir dicha información. Se abordará cada uno de estos aspectos con un nivel de detalle apropiado, comenzando por la identificación del usuario. La obtención de la identidad puede llevarse a cabo mediante diversos métodos mediante la solución proporcionada por el ISE usando además servidores de autenticación como lo son RADIOS Y TACACS+, otros ejemplos: [18]

2.5.1.2.1 Acceso de invitado no autenticado/autenticado

El Cisco Identity Service Engine (ISE) incorpora una característica esencial denominada servidor de invitados, la cual despliega una página de bienvenida personalizada para los usuarios visitantes. Esta página puede incluir: [18]

- Un acuerdo de usuario y/o solicitar información adicional
- Como la dirección de correo electrónico
- Afiliación corporativa del usuario.

En el contexto de esta funcionalidad, se distingue entre dos modalidades de acceso para los huéspedes: acceso no autenticado y acceso autenticado.

- **Acceso de invitado no autentificado**

Frecuente se observará en lugares como laboratorios universitarios o cafés internet que ofrecen conectividad gratuita, permite a los usuarios ingresar a la red sin la necesidad de proporcionar información de identificación. En estos casos, el acceso se restringe típicamente a servicios básicos de Internet y se excluyen otros privilegios dentro del entorno gestionado por ISE. [18]

- **Acceso de invitado autenticado**

Este es más común en entornos corporativos que requieren una mayor protección de los datos y recursos de la red, implica que los usuarios visitantes deben autenticarse mediante credenciales proporcionadas por la organización. A pesar de esta autenticación, el acceso otorgado a los huéspedes suele ser significativamente limitado en comparación con el que se otorga a los empleados autenticados, generalmente restringiéndose al uso de servicios de Internet. Esta medida de seguridad se implementa para salvaguardar la integridad de los datos, archivos y demás información confidencial de la organización frente a posibles amenazas. [18]

2.5.1.2.2 Bypass de Autenticación MAC (MAB)

El método de "Bypass de Autenticación MAC (MAB)" se basa en la utilización de la dirección MAC para llevar a cabo la autenticación. La dirección MAC constituye un identificador único a nivel mundial asignado a todos los dispositivos conectados a una red, algunos lo llaman dirección física o de software. No obstante, aunque la dirección MAC sea un identificador globalmente único, es posible que cada usuario pueda asignar manualmente su propia MAC a un dispositivo implica que, por sí sola, dicha dirección no representa un método confiable para autenticar su entrada. [18]

2.5.1.2.3 Autenticación Web

La autenticación web se caracteriza por ofrecer un proceso de autenticación a través de una página web, generalmente mediante una dirección URL accesible desde el navegador del usuario. Esta capacidad se encuentra integrada en el servidor de invitados de Cisco Identity Services Engine (ISE), que actúa como un portal web para dicho propósito. Por ejemplo, cuando un usuario se conecta a una red inalámbrica que opera en modo abierto, es decir, sin autenticación previa, el navegador del usuario es automáticamente redirigido hacia la página de inicio de sesión hospedada por el ISE. En este punto, el ISE recopila las credenciales proporcionadas por el usuario y procede con el proceso de autenticación correspondiente. [18]

2.5.1.2.4 Firewall de identidad de ASA

El Cisco ASA (Adaptive Security Appliance) este cortafuegos incluye la funcionalidad de Firewall de Identidad (IDFW), una característica que permite al ASA utilizar el Cisco Identity Services Engine (ISE) como servidor de autenticación. De esta manera, el ISE será capaz de identificar y registrar la información de identidad de todos los usuarios que atraviesen el dispositivo ASA habilitado para IDFW. [18]

2.5.1.2.5 Autenticación VPN / RADIUS

Mediante el empleo del Cisco Identity Services Engine (ISE) para autenticar los clientes de VPN, se logra que el ISE disponga de la información relativa a la identidad de los usuarios de la VPN. A modo de ilustración, el Cisco ASA transmite las credenciales del cliente de VPN a través del protocolo RADIUS al ISE, que se encarga de llevar a cabo el

proceso de autenticación correspondiente. [18]

2.5.1.2.6 IEEE 802.1.X

El protocolo IEEE 802.1x se basa en la certificación de puertos, donde la autenticación implica identificar a una persona o un dispositivo mediante credenciales, permitiendo o denegando el acceso a ciertos recursos o áreas. En redes, este proceso se lleva a cabo a través de switches en redes cableadas o puntos de acceso en redes inalámbricas. IEEE 802.1x ofrece visibilidad, seguridad y control de acceso basados en la identidad, respondiendo a las necesidades actuales en las que contratistas, invitados, consultores, y empleados que solicitan acceso a los recursos de la red, creando una gestión compleja de los dispositivos conectados. [20]

Operando en la capa dos del modelo OSI, 802.1x es un estándar implementado para el control de acceso a la red, permitiendo o denegando la conectividad en función de la identidad del usuario o del dispositivo. Este protocolo habilita o cierra los puertos basándose en la autenticación validada por el servidor, lo que permite una gestión dinámica o estática de los elementos involucrados en el proceso de autenticación.

IEEE 802.1x consta de varios componentes esenciales: [20]

- **Suplicante:** El punto final, ya sea un usuario o un dispositivo, que solicita acceso a la red y presenta las credenciales necesarias para iniciar el proceso de autenticación.
- **Autenticador:** El dispositivo de red que facilita el proceso de autenticación mediante la comunicación entre el suplicante y el servidor. En este dispositivo, que puede ser un punto de acceso o una WLC, se aplican las políticas correspondientes a cada usuario.
- **Servidor de autenticación (Radius/TACACS+):** Encargado de validar las credenciales presentadas por el suplicante y determinar las políticas a aplicar.

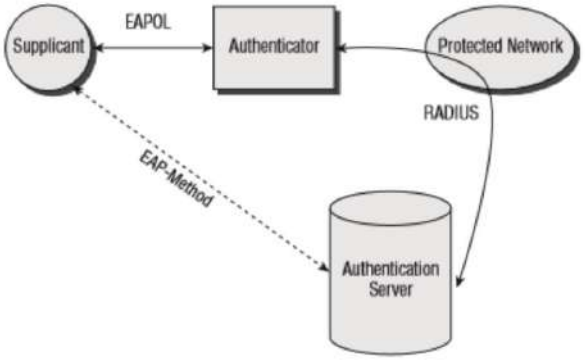

Figura 3. Elementos que componen el sistema de autenticación 802.1x [20]

En el proceso de autenticación mediante 802.1x, se emplean diversos protocolos para garantizar una comunicación segura y eficiente entre los diferentes componentes involucrados. A continuación, se detallan los principales protocolos utilizados: [20]

- **Protocolo de Autenticación Extensible (EAP):** Este protocolo establece un formato de mensaje que permite al autenticador y al suplicante negociar el método de autenticación a utilizar. EAP define cómo se deben enviar las credenciales del suplicante al servidor de autenticación a través de su estructura específica.
- **EAP sobre LAN (EAPoL):** Es una encapsulación especificada por 802.1x que se utiliza para transmitir información entre el suplicante y el autenticador. EAPoL opera en la capa dos del modelo OSI, facilitando una comunicación directa y segura en la red local.
- **RADIUS:** Este es el protocolo estándar para la comunicación entre el switch (o punto de acceso) y el servidor de autenticación. El switch encapsula los mensajes enviados por el suplicante y los transmite a la capa siete del modelo OSI, donde el servidor RADIUS procesa las solicitudes de autenticación.

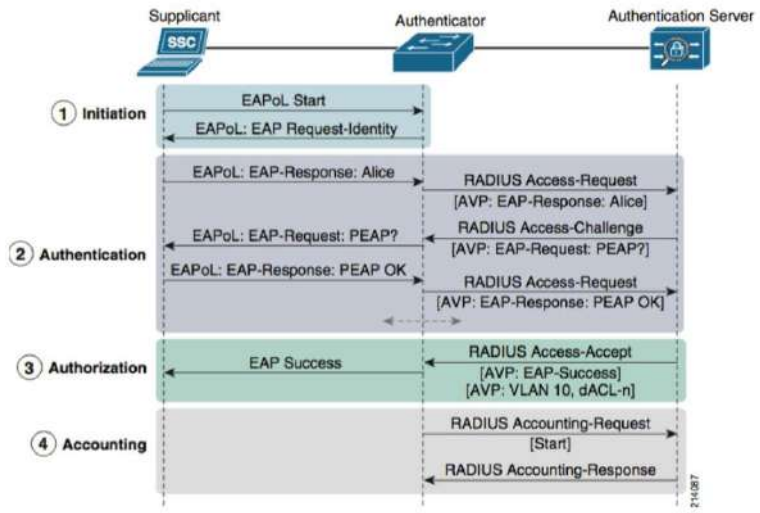

Figura 4. Cinco etapas en el proceso AAA de 802.1x [20]

El proceso de autenticación, autorización y contabilidad (AAA) mediante el protocolo 802.1x se puede dividir en cinco etapas principales:

- **Iniciación:** Este proceso puede ser iniciado por el switch o el suplicante. Desde la perspectiva del autenticador, el proceso comienza cuando se detecta una conexión al puerto, momento en el cual se envía un mensaje de solicitud de identidad, retransmitido periódicamente hasta obtener una respuesta. Alternativamente, el suplicante puede iniciar la sesión enviando una trama de comienzo, lo que acelera el proceso al eliminar la necesidad de transmisiones iniciales por parte del switch.
- **Autenticación:** En esta etapa, el autenticador inicia una comunicación con el servidor de autenticación, copiando la información recibida de los mensajes EAP en paquetes RADIUS. Durante la comunicación entre el suplicante y el switch, se define el tipo de credenciales necesarias para la validación de identidad, tales como contraseñas, tokens o credenciales específicas.
- **Autorización:** Si el suplicante presenta credenciales válidas, el servidor de autenticación envía un mensaje de aceptación en formato RADIUS, que el switch encapsula en un mensaje EAP. Esto habilita el puerto y aplica las políticas correspondientes, como listas de acceso o asignación a una VLAN específica. Si la respuesta es negativa, se sigue el mismo proceso de encapsulación para denegar el acceso, pudiendo reintentar la autenticación o negarla según la configuración del switch.
- **Contabilidad:** Una vez autorizado y aplicadas las políticas, el switch envía mensajes de contabilidad al servidor, detallando las sesiones anteriores tanto de

solicitantes permitidos como no autorizados.

- **Finalización:** Es crucial para prevenir ataques o violaciones durante la desconexión del puerto. La desconexión debe ser inmediata al terminar la sesión, con mecanismos como tiempos de retardo o inactividad del puerto para asegurar la seguridad.
- **Ventajas del protocolo 802.1x**
  - **Visibilidad**: Permite una gran visibilidad en la red al relacionar usuarios con direcciones IP y MAC, switches y puertos de conexión, lo que facilita la generación de políticas de seguridad, estadísticas y resolución de problemas. [20]
  - **Seguridad**: Es un método robusto de autenticación, controlando el acceso en el borde de la red a través de los suplicantes en los nodos finales. [20]
  - **Servicios basados en identidad**: Permite la asignación de políticas específicas a los usuarios, otorgando acceso a diferentes recursos según las credenciales.
  - **Transparencia**: Facilita el conocimiento del comportamiento y capacidades de los usuarios finales. [20]
  - **Autenticación de equipos y usuarios**: Soporta la autenticación de dispositivos como impresoras o teléfonos que no pueden utilizar el suplicante de autenticación. [20]

- **Desventajas del protocolo 802.1x**
  - **Soporte al punto final**: Para usuarios que no soportan 802.1x, el acceso es denegado. Sin embargo, existen métodos alternativos como la Autenticación Bypass de MAC (MAB) o la autenticación mediante web.
  - **Retraso**: El protocolo no permite el acceso antes de la autenticación, lo que puede causar demoras para los usuarios que necesitan recursos inmediatos.

2.5.1.3 Reglas de autorización de ISE

Ya concluido el proceso de autenticación, el Cisco Identity Services Engine (ISE) procede a la implementación de políticas, conocida como autorización. En este contexto, el ISE tiene la capacidad de emplear una amplia gama de atributos de políticas para cada regla,

los cuales son consolidados para llevar a cabo la autorización, seguido se enumeran los atributos de políticas más utilizados en el ISE:

- Atributos relacionados con el usuario interno, tales como nombre de la empresa, departamento, dirección, cargo, entre otros.
- Ubicación del usuario.
- Método de acceso empleado (ya sea MAB, 802.1X, cableado, inalámbrico, etc.).
- Fecha y hora del acceso.
- Perfiles combinados según el tipo de dispositivo.
- Estado de registro del dispositivo en el ISE.

2.5.1.4 Componentes de Políticas ISE

La centralización en un único motor de políticas confiere a ISE una capacidad innata, ISE comprende el núcleo único motor de políticas dentro de la solución, ofreciendo un control de acceso basado en atributos fuertes y versátiles, integrando autenticación, autorización y contabilidad (AAA), así como servicios de administración de invitados en una sola plataforma. Esta característica permite a los responsables de la red elaborar y gestionar directivas de control de acceso de forma centralizada para usuarios y dispositivos finales, garantizando una coherencia en la aplicación de políticas y proporcionando una visibilidad completa de extremo a extremo sobre todos los elementos conectados a la red. ISE lleva a cabo el descubrimiento y la clasificación automáticos de los dispositivos finales, asegurando un acceso adecuado basado en la identidad y permitiendo la aplicación del cumplimiento del dispositivo mediante la evaluación de la postura de este. [18]

2.5.1.5 Componentes de puntos finales

Los end points de red, conocidos como puntos finales, cumplen una función esencial en la implementación efectiva del Cisco Identity Service Engine (ISE). Estos EP son responsables de facilitar la autenticación a través de diversos métodos, como autenticación web, MAB O 802.1X, así como de suministrar datos de postura al ISE para garantizar el cumplimiento de las políticas de seguridad. Para fortalecer la plataforma de ISE, se recomienda el uso de los siguientes componentes de puntos finales: [18]

- **Agente Cisco NAC**: Disponible para sistemas operativos Windows, Mac OS X y Linux, este agente proporciona información crucial sobre la postura del host al ISE. [18]
- **Suplicante/Agente 802.1X:** Este software es fundamental para la comunicación a través del protocolo de autenticación extensible a través de LAN (EAPoL). Hay una variedad de suplicantes disponibles, incluidos los integrados en sistemas operativos como Windows y Mac OS-X, así como aquellos disponibles a través de aplicaciones como Cisco AnyConnect y agentes de terceros. Además, muchos dispositivos, como teléfonos IP de Cisco, equipos de video e impresoras, vienen con suplicantes incorporados. Prácticamente cualquier dispositivo con capacidad WiFi debería contar con un suplicante nativo. [18]

2.5.1.6 Entidades dentro de ISE

Dentro de la arquitectura del Cisco Identity Services Engine (ISE), se encuentran varios roles que contribuyen a su capacidad para adaptarse a redes de gran escala y a un elevado número de usuarios y dispositivos. La estructura del ISE se caracteriza por su alta disponibilidad y escalabilidad, lo que permite implementaciones tanto independientes como distribuidas.

- **Implementaciones Independientes**: En este caso, el ISE se despliega como una única instancia independiente en la red. Esto significa que todos los componentes del ISE, como el nodo de administración, el nodo de servicio de políticas y el nodo de supervisión, se ejecutan en un solo servidor o en una única infraestructura. Este tipo de implementación es adecuado para redes más pequeñas o entornos donde se requiere una única instancia de ISE para gestionar todos los aspectos de la seguridad de la red.
- **Implementaciones Distribuidas**: En contraste, las implementaciones distribuidas del ISE involucran la distribución de los componentes del sistema en múltiples servidores o ubicaciones físicas. Por ejemplo, puede haber un nodo de administración centralizado que coordina múltiples nodos de servicio de políticas distribuidos en diferentes lugares geográficos. Esta configuración es más escalable y redundante, ya que permite manejar mayores cargas de trabajo y proporciona una mayor disponibilidad al distribuir la carga entre varios servidores.En este contexto,

se identifican tres roles principales, cada uno desempeñando funciones específicas en la gestión y operación del sistema.

El primero de estos roles es el de Administración, el cual permite llevar a cabo todas las tareas administrativas dentro de una implementación del ISE, ya sea independiente o distribuida. El Nodo de Administración de Políticas (PAN), proporciona una interfaz centralizada para la gestión del sistema, abarcando configuraciones y políticas relacionadas al sistema. [18]

El segundo rol es el de Servicio de Políticas, encargado de proporcionar diversos servicios como:

- Portales web
- Servicios de creación de perfiles
- Acceso a la red
- Evaluación de postura
- Gestión de acceso de invitados
- Aprovisionamiento de clientes

Este rol se encarga de analizar las políticas y tomar todas las determinaciones necesarias, es posible que haya más de un nodo que tome este rol. Cuando un nodo está asignado al rol de servicio de políticas, se le denomina nodo de servicio de políticas (PSN); por lo general, en un despliegue distribuido, hay varios nodos PSN. [18]

Por último, se encuentra el rol de Supervisión, el cual permite al ISE funcionar como un recopilador de registros y guarda los mensajes de registro de todos los nodos de administración y servicio de políticas en la red. Este rol ofrece herramientas avanzadas de control y resolución de problemas para una administración eficiente de la red y sus recursos. [18]

2.5.1.7 Licencias, requisitos y performance de ISE

2.5.1.7.1 Licencias ISE

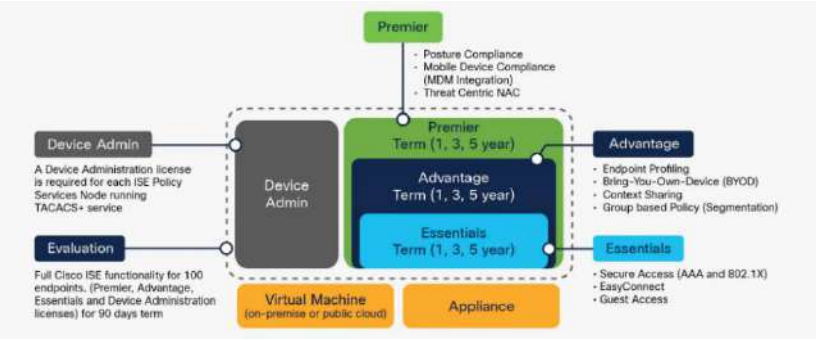

Figura 5. Paquetes de licencias de Cisco ISE [21]

Las licencias del Cisco Identity Services Engine (ISE) proporcionan un conjunto de características que permiten una gestión eficiente y efectiva de la red, brindando visibilidad y control sobre los puntos finales en expansión. Estas licencias están diseñadas para satisfacer las necesidades específicas de cada organización, y se pueden habilitar según sea necesario para aprovechar las capacidades requeridas del ISE. El mecanismo de licencia del Cisco ISE presenta diversas características importantes:

- **Licencia Incorporada**: Al instalar el Cisco ISE, se incluye automáticamente una licencia de evaluación que tiene una validez de 90 días. Esta licencia de evaluación proporciona acceso completo a todas las funcionalidades del ISE durante este período, lo que permite una evaluación exhaustiva del sistema antes de la adquisición de una licencia completa [21]
- **Gestión Centralizada de Licencias**: La gestión de las licencias del Cisco ISE se realiza de manera centralizada a través del nodo de administración primaria (PAN) [21]
- **Recuento de Puntos Finales Activos Simultáneos**: Las licencias del Cisco ISE incluyen un recuento específico de puntos finales activos simultáneos para cada nivel de licencia. Este recuento se refiere al número total de usuarios y dispositivos compatibles que utilizan los servicios del ISE en un momento dado [21]

Además, las licencias del Cisco ISE se proporcionan varios paquetes, que incluyen:

- **Licencias de Nivel**: Estas licencias, denominadas Essentials, Advantage y Premier, sustituyen a las licencias Base, Apex y Plus utilizadas en versiones anteriores del ISE. Permiten el acceso a diferentes conjuntos de funcionalidades del ISE según las necesidades del usuario [21]

Nombre	Capacidades de la licencia
Essentials	• Autenticación, autorización y contabilidad RADIUS, incluido 802.1X, omisión de autenticación MAC y conexión fácil, y autenticación web. • MACsec. • Autenticaciones basadas en estándares de inicio de sesión único (SSO), lenguaje de marcado de afirmación de seguridad (SAML) y conectividad abierta de bases de datos (ODBC). • Acceso de invitados y servicios de patrocinadores. • API de transferencia de estado representacional (REST) para fines de monitoreo y API de servicios RESTful externos para operaciones CRUD. • Servicios de identificación pasiva. • Acceso seguro por cable e inalámbrico.
Advantage	• Todas las funciones habilitadas por la licencia Cisco ISE Essentials. • Registro y aprovisionamiento de dispositivos "Traiga su propio dispositivo (BYOD)", con una autoridad de certificación incorporada. El registro del dispositivo se realiza a través de los portales configurados de Mis dispositivos. • Integración de etiquetado de grupos de seguridad, TrustSec e infraestructura centrada en aplicaciones (ACI) de Cisco. • Servicios de elaboración de perfiles, incluidas funciones básicas de visibilidad de activos y aplicación de la ley. • Servicios de alimentación. • Uso compartido de contexto (como pxGrid) e integraciones de ecosistemas de seguridad. • Contención rápida de amenazas, utilizando control de red adaptativo y servicios de intercambio de contexto. • Visibilidad y aplicación de Cisco AI Endpoint Analytics.
Premier	• Todas las funciones habilitadas por las licencias Cisco ISE Essentials y Advantage. • Visibilidad y cumplimiento de la postura. • Visibilidad y aplicación del cumplimiento a través de Enterprise Mobility Management y Mobile Device Management. • Visibilidad y aplicación del control de acceso a la red centrado en amenazas.

Tabla 1. *Tipos de licencias CISCO ISE [21]*

- **Licencias de Administración de Dispositivos**: Autorizan el uso de los servicios TACACS en un nodo de Servicio de Políticas. En un despliegue de Alta Disponibilidad (HA) independiente [21]
- **Licencias de Dispositivos Virtuales:** Admitidas en versiones específicas del Cisco ISE, estas licencias cubren los nodos virtuales tanto en implementaciones locales como en la nube [21]
- **Licencias de Evaluación:** Estas se ponen en funcionamiento automáticamente al instalar o actualizar a Cisco ISE versión 3.0 y posteriores, y soportan hasta 100 terminales y tiene una duración de 90 días y proporciona acceso completo a todas las funcionalidades de Cisco ISE. [21]

2.5.1.8 Políticas de ISE

Cisco Identity Service Engine (ISE) implementa políticas basadas en reglas para gestionar el acceso a la red de manera eficiente. Este sistema permite la creación de elementos de políticas individuales que pueden ser reutilizados en diversas reglas dentro del entorno de políticas. Durante la ejecución, Cisco ISE evalúa las condiciones de cada política y aplica los resultados definidos en función de si la evaluación de la política devuelve un valor verdadero o falso. [19]

Las políticas de autenticación tienen como objetivo principal determinar la validez de las credenciales de identidad presentadas. Además, estas políticas pueden incluir acciones como rechazar tráfico no permitido, dirigir solicitudes de autenticación al Punto de Identidad correcto, validar la identidad del usuario y pasar autenticaciones exitosas a las políticas de autorización. [19]

Las políticas de autorización, por su parte, determinan si un usuario o dispositivo tendrá acceso a la red según las reglas establecidas. Estas políticas examinan las condiciones para enviar un resultado de autorización al dispositivo de acceso a la red (NAD). Este resultado puede ser una aceptación o rechazo estándar de RADIUS, pero también puede incluir elementos más avanzados, como asignación de VLAN, listas de acceso descargables (DACL) o cambios en la dirección IP. [19]

En relación con las posturas, estas políticas definen los requisitos que un dispositivo debe cumplir para considerarse conforme. Estos requisitos pueden incluir la presencia de antivirus, claves de registro, procesos específicos, aplicaciones, parches de Windows, entre

otros. Cuando no se dispone de datos para determinar el estado de la postura, se clasifica como "Desconocido". Los dispositivos también pueden adoptar este estado mientras se está llevando a cabo el control de posturas. Si la evaluación de la postura revela que uno o más requisitos no se cumplen, el dispositivo se considera "No Cumplimiento", lo que significa que no cumple con las normas establecidas. Por el contrario, si la estación de trabajo cumple con todos los requisitos obligatorios, se clasifica como "En Cumplimiento". En casos donde los dispositivos no cumplen con la política de postura, pueden ser puestos en cuarentena, restringiendo su acceso a la red solo a recursos de postura y remediación. Esta política se suele hacer cumplir mediante listas de control de acceso descargables (DACL) o asignación dinámica de VLAN. [19]

2.5.1.9 Rendimiento de ISE

2.5.1.9.1 Tipos y terminología del nodo ISE

La terminología asociada a los nodos de Cisco ISE abarca una variedad de roles y servicios que estos pueden ofrecer. La disponibilidad de opciones en el portal de administración está determinada por el rol y las funciones que asume cada nodo de ISE.

Tipo de nodo	Información
Nodo de administración de políticas (PAN)	Este nodo posibilita la ejecución de todas las operaciones y ajustes administrativos en la plataforma. Actúa como un punto centralizado para supervisar y gestionar las operaciones administrativas, configuraciones y datos contextuales. Además, garantiza la sincronización de la configuración con los demás nodos dentro del despliegue.
Nodo de servicio de políticas (PSN)	Este nodo habilita el acceso a la red, la postura, el acceso de invitados, el aprovisionamiento de clientes y los servicios de creación de perfiles. Este nodo se encarga de evaluar las políticas y tomar decisiones en función de estas.
Nodo de monitoreo (MnT)	Este nodo actúa como un recolector de registros, almacenando los mensajes de registro de todos los nodos de Servicio de Administración y Políticas en una red. Este nodo proporciona instrumentos de monitoreo y resolución de problemas que pueden ser utilizadas para administrar eficazmente la red y sus recursos. Además, este nodo agrega y correlaciona los datos recopilados, generando informes significativos para su análisis.
Nodo pxGrind	Nodo que posibilita el intercambio de datos de configuración y políticas entre nodos, como la compartición de etiquetas y objetos de políticas entre Cisco ISE y proveedores externos, así como otros intercambios de información relevantes.

Tabla 2. *Tipos de nodo CISCO ISE [19]*

2.5.1.9.2 Referencia en el rendimiento en la implementación ISE CISCO

El desempeño de Cisco Identity Service Engine (ISE) está condicionado por

diversos elementos, aunque su evaluación no siempre resulta ser exacto. Este rendimiento se ve influido por variables como:

- El tipo de nodo.
- Las personas asociadas.
- La complejidad de las políticas.
- El tipo de dispositivos.
- Los puntos finales y otras consideraciones relevantes.

La selección adecuada de la implementación de Cisco Identity Service Engine (ISE) se basa en los límites máximos de escala para puntos finales activos, específicos para cada tipo de implementación. Cada dispositivo con una dirección MAC única se considera una sesión activa.

Es fundamental tener en cuenta que nunca se debe superar el 80% de la capacidad declarada para la implementación y mantener un límite del 50% o menos para el diseño inicial. Este enfoque facilita el crecimiento futuro dentro de la arquitectura y garantiza la disponibilidad de un margen saludable en caso de que el entorno no cumpla con las métricas de rendimiento probadas y documentadas por Cisco.

2.5.2 TACACS+

Es un protocolo de red utilizado para la autenticación, autorización y contabilidad (AAA) en dispositivos de red. Proporciona un mecanismo para que un dispositivo de red se comunique con un servidor TACACS+ y envíe solicitudes de autenticación y autorización, así como para recibir respuestas y realizar acciones en consecuencia. El protocolo TACACS+ es independiente de la plataforma y se puede implementar en diversos sistemas operativos de red. [15]

El protocolo TACACS+ surge como una evolución de su predecesor, TACACS, el cual ha quedado obsoleto y sin soporte debido a la falta de respaldo por parte de su creador, CISCO. Desarrollado originalmente por el Departamento de Defensa de EE. UU., este protocolo fue posteriormente mejorado por Cisco Systems, consolidándose como un protocolo en el ámbito de la seguridad de redes. TACACS+ se distingue por proporcionar soluciones avanzadas en control de acceso y funciones AAA. [22]

Una de las características sobresalientes de TACACS+ radica en su utilización del protocolo de transporte TCP, lo que garantiza una conexión segura y la capacidad de cifrar

el tráfico entre servidores. Funcionando bajo el modelo cliente/servidor, este protocolo opera a través del puerto 49 y emplea el algoritmo de encriptación MD5 para proteger tanto las credenciales como los datos transmitidos, elevando así su nivel de seguridad y confiabilidad en comparación con otros protocolos. [22]

Un aspecto destacable de TACACS+ es su capacidad para reducir la carga en el servidor y detectar de manera eficiente fallos en la comunicación al establecer una sola sesión de cliente/servidor, siempre y cuando el servidor o dispositivo de red se mantengan operativos. Esta característica contribuye a mejorar la eficiencia y la estabilidad del sistema, aspectos fundamentales en entornos de redes críticas como el de una universidad. [22]

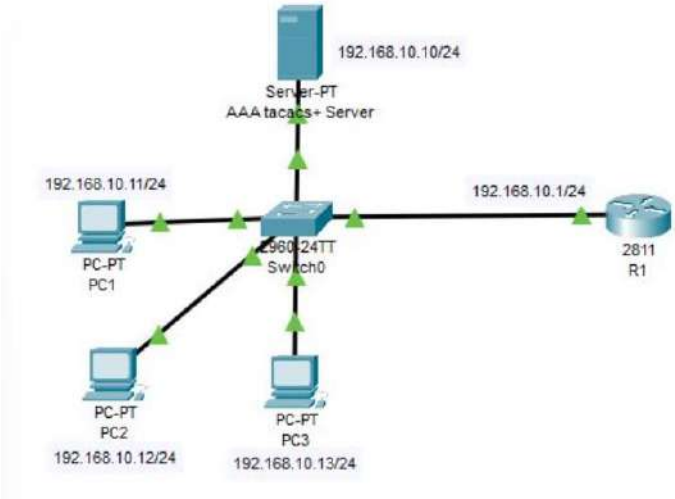

Figura 6. Topología básica TACACS+ [23]

2.5.2.1 Autenticación

El funcionamiento del protocolo TACACS+ se caracteriza por una serie de procesos que tienen lugar cuando un usuario intenta acceder al servidor. En primer lugar, se lleva a cabo el proceso de autenticación, el cual es gestionado por el servidor mismo. Este proceso implica la recopilación de información necesaria para autenticar al usuario, como su nombre de usuario y contraseña, junto con otros datos proporcionados por el usuario, como pasatiempos u otros ítems, a solicitud del servidor. [22]

Si bien la etapa de autenticación puede variar, una de las formas más comunes implica el uso de un nombre de usuario asociado de manera permanente con una contraseña. Sin embargo, este enfoque presenta limitaciones en cuanto a seguridad debido a la fijeza de las credenciales. Para abordar estas limitaciones, los procesos de

autenticación actuales incorporan métodos como preguntas y respuestas para mejorar la seguridad de la información. En este sentido, TACACS+ se destaca por su capacidad para admitir estos métodos de autenticación más robustos que están en constante desarrollo, lo que contribuye a fortalecer su seguridad. [22]

Es importante destacar que en el protocolo TACACS+, la autenticación no es obligatoria, sino que se configura como una opción según los requisitos del usuario. Sin embargo, en otras implementaciones, la autenticación es necesaria para servicios específicos o condiciones particulares, como el inicio de sesión o el acceso a una red específica. En estas situaciones, el usuario debe identificarse y proporcionar las credenciales requeridas para obtener acceso o privilegios especiales. [22]

Al igual que el protocolo RADIUS, TACACS+ establece la comunicación entre el servidor y el usuario a través de un cliente TACACS+. En esta comunicación, el cliente TACACS+ facilita el acceso o deniega el mismo dependiendo de la respuesta del servidor. [22]

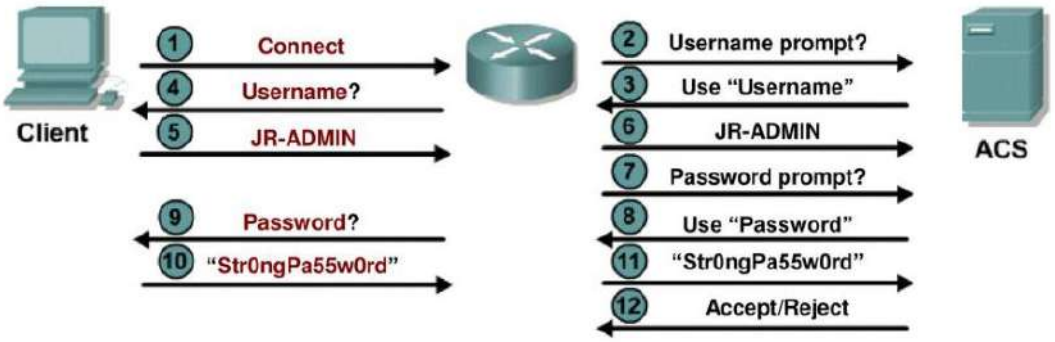

Figura 7. Proceso autenticación TACACS+ [24]

2.5.2.1.1 Tipos de mensajes de autenticación de TACACS+

El protocolo TACACS+ utiliza diversos tipos de mensajes de autorización para gestionar el proceso de autenticación y autorización. Entre estos mensajes se encuentran:

- **ACCEPT (ACEPTAR**): Este mensaje indica que la autenticación ha sido aceptada, siempre y cuando el cliente esté configurado para solicitar la autorización correspondiente.
- **REJECT (RECHAZAR):** Se emite este mensaje cuando la autenticación es rechazada debido a la detección de algún error en los datos proporcionados. Esto puede ocurrir si algún ítem requerido no ha sido proporcionado correctamente.
- **ERROR (ERROR):** Este mensaje señala la ocurrencia de un error durante el

proceso de autenticación. Por lo general, indica problemas de conexión entre el servidor y el usuario. Tras recibir este mensaje, el cliente debe buscar métodos alternativos para realizar la autenticación.

- **CONTINUE (CONTINUAR):** Este mensaje instruye al usuario a realizar autenticaciones adicionales. Puede ser utilizado en situaciones donde se requiere una verificación adicional antes de otorgar el acceso.

Estos mensajes son fundamentales para la interacción entre el servidor y el cliente en el contexto de la autenticación y autorización dentro del protocolo TACACS+. [22]

2.5.2.2 Autorización

La autorización, en el contexto de la seguridad de redes, se refiere al proceso mediante el cual se determinan las acciones que un usuario específico puede llevar a cabo después de haberse autenticado satisfactoriamente en el sistema. Si bien la autenticación generalmente precede a la autorización, es importante destacar que esta secuencia no es obligatoria en todos los casos. Es decir, es posible solicitar autorización sin haberse autenticado previamente, lo que implica que el sistema no tiene conocimiento del usuario que intenta acceder a la red y, por lo tanto, no puede conceder acceso a servicios específicos o privilegiados. [22]

2.5.2.3 Contabilidad

La contabilidad constituye un proceso esencial en el contexto del protocolo TACACS+, donde se lleva a cabo la recopilación y transmisión de datos destinados a la facturación, la contabilidad y el suministro de información al servidor correspondiente.

Dentro de este proceso, los administradores de red pueden emplear la función de contabilidad para monitorear la actividad de los usuarios con el propósito de realizar auditorías de seguridad o para proporcionar detalles sobre las acciones realizadas por los mismos. Los registros de contabilidad contemplan diversos aspectos, tales como:

- Los comandos ejecutados (como PPP)
- El número de paquetes y bytes transferidos.
- Las identidades de los administradores.
- Los horarios de inicio y finalización.

Para llevar a cabo eficientemente el proceso de auditoría, TACACS+ soporta tres

tipos de registros:

- **Registros de inicio:** Indican el inicio de un servicio, brindando información sobre el momento en que dicho servicio se está preparando para iniciar su ejecución.
- **Registros de finalización:** Son registros que informan sobre la conclusión de un servicio en particular, permitiendo tener un seguimiento preciso de los servicios que han sido utilizados y cuándo se han completado.
- **Registros intermedios:** Proporcionan notificaciones acerca de la ejecución de un servicio en curso, ofreciendo una visión detallada del progreso de la actividad en tiempo real.

Estos distintos tipos de registros permiten un exhaustivo seguimiento de la actividad realizada en el sistema, brindando así una base sólida para llevar a cabo auditorías de seguridad y mantener un control riguroso sobre el uso de los recursos de red. [22]

2.5.2.4 Paquetes en TACACS+

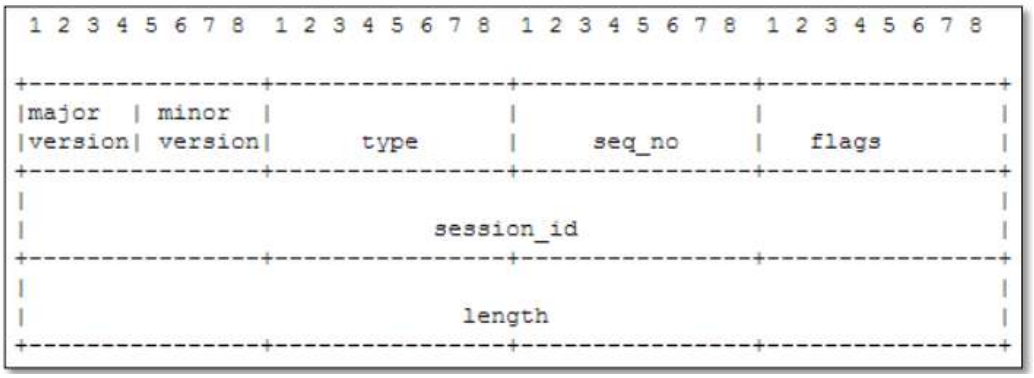

Figura 8. Formato y bits del paquete TACACS+ [22]

El formato y los bits del paquete TACACS+ están estructurados con una cabecera que precede a los datos del paquete, la cual no cuenta con ningún tipo de cifrado y contiene la siguiente información: [25]

- **Versión Mayor y Menor:** Indican el número de versión mayor y menor del protocolo TACACS+. La versión menor se utiliza para permitir la compatibilidad con versiones anteriores del protocolo. En caso de que el servidor reciba un paquete con una versión menor no compatible, responde con un estado de error y la versión menor más cercana compatible.
- **Tipo:** Este campo indica el tipo de paquete y puede tomar los valores 0x01 para una solicitud de autenticación, 0x02 para una solicitud de autorización y 0x03 para una

solicitud de contabilidad.

- **Seq_no:** Consiste en una secuencia de números que permiten identificar los paquetes enviados y la sesión correspondiente para cada paquete. El valor de Seq_no comienza en 1 para el primer paquete de una sesión y se incrementa en uno para cada paquete sucesivo. Cuando se alcanza el límite del contador debido al uso de un gran número de paquetes, se debe cerrar la sesión y abrir una nueva para reiniciar la secuencia.
- **Banderas:** Este bit de la bandera indica si el paquete utiliza algún tipo de cifrado. Cuando la bandera tiene el valor 0x01, el paquete no utiliza cifrado. Además, las banderas también permiten determinar si el protocolo admite y trabaja con múltiples sesiones.
- **ID de Sesión:** Este valor, generado aleatoriamente por el protocolo, sirve como identificador único para cada sesión establecida. Permanece constante durante toda la sesión por razones de seguridad.
- **Longitud:** Indica el tamaño del paquete, incluyendo la cabecera, en bytes de red. Este valor representa el tamaño máximo permitido para cada paquete y no debe ser excedido. Los campos variables no utilizados en el parámetro de longitud deben tener un valor de cero.

Estos componentes del paquete TACACS+ están diseñados para facilitar la comunicación entre el cliente y el servidor, garantizando una correcta identificación, seguridad y control sobre los datos transmitidos durante el proceso de autenticación, autorización y auditoría. [26]

2.5.2.5 Ventajas

El protocolo TACACS+ ofrece diversas ventajas en comparación con otros protocolos de comunicación utilizados en la implementación de sistemas de autenticación, autorización y auditoría (AAA). Estas ventajas se detallan a continuación: [25]

- **UDP (Protocolo de Datagrama de Usuario):** Este protocolo presenta una menor carga de información, lo que permite una respuesta más rápida. Es compatible con la versión simple y es ampliamente soportado por una variedad de equipos.
- **TCP (Protocolo de Control de Transmisión):** La implementación de TCP

es más sencilla, especialmente en equipos que no cuentan con soporte para UDP o tienen recursos limitados. Además, su sintaxis más simple y su robustez permiten la detección de errores, apoyos temporales y una mayor seguridad en el proceso de autenticación de los usuarios.

Es importante tener en cuenta que, independientemente del protocolo utilizado (UDP o TCP), el protocolo TACACS+ transmite la información de usuario y contraseña en texto claro, es decir, sin encriptación. Esto significa que la información enviada a través del medio de transmisión no está protegida, lo que representa un riesgo de seguridad. Por lo tanto, es necesario tomar medidas para mejorar la seguridad de la información, como el uso de enlaces punto a punto o la mejora de la seguridad física del enlace para prevenir accesos no autorizados a la información de usuario y contraseña. [25]

En entornos donde la información debe atravesar varios segmentos de red, la importancia de asegurar el enlace aumenta significativamente. Se recomienda implementar un estricto control de la configuración del router y los protocolos de enrutamiento, así como evitar el uso de puentes. Para los servidores, se sugiere crear listas de acceso especiales para los clientes, reducir los tiempos de respuesta de las solicitudes y llevar un estricto control de los eventos de red. [25]

2.5.3 Radius

RADIUS (Remote Authentication Dial-In User Service) es un protocolo diseñado para asegurar el acceso restringido a redes inalámbricas mediante la implementación de servicios de autenticación, autorización y auditoría (AAA). Este protocolo se ejecuta en un dispositivo que actúa como servidor de acceso, gestionando las tres funciones críticas de AAA: autenticación, autorización y contabilidad. Su principal objetivo es facilitar el acceso remoto seguro a redes y servicios que no tienen mecanismos integrados de control de acceso para los usuarios. RADIUS opera utilizando el protocolo UDP/IP y está compuesto por un servidor que administra y autentica a los usuarios que solicitan acceso a la red. [27]

RADIUS, un protocolo basado en la arquitectura cliente-servidor, se utiliza ampliamente en redes donde el cliente actúa como un elemento autenticador. En el contexto de Cisco ISE, el servidor RADIUS es responsable de recibir y procesar las solicitudes de conexión de los usuarios. Este proceso incluye el envío de mensajes para la autenticación y la aplicación de políticas y configuraciones específicas a los usuarios autenticados.

Además, el protocolo RADIUS permite la función de cliente proxy para la autenticación

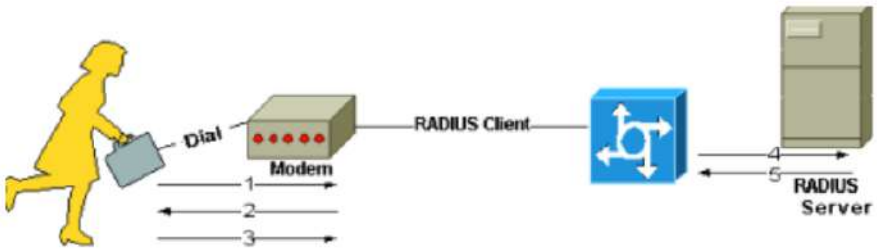

Figura 9. Ejemplo de autenticación de un servidor RADIUS [28]

En el contexto de Cisco ISE, existen tres componentes fundamentales utilizados para la autenticación, los cuales se describen a continuación:

- **Suplicante:** Se emplea un suplicante 802.x para los procesos de autenticación, autorización y auditoría (AAA).
- **Autenticador:** Este componente en este caso es una WLC que recibe la solicitud del suplicante y reenvía una solicitud EAP-Request/Identity utilizando el protocolo de autenticación.
- **Servidor de autenticación:** En este caso, es el servidor Radius implementado a través de Cisco ISE.

2.5.3.1 Proceso de autenticaion y autrizacion del servidor Radius

Este implica una serie de pasos metódicos para garantizar la validación y el control de acceso. A continuación, se describen las fases fundamentales del procedimiento: [29]

- **Solicitud de Autenticación:** El cliente RADIUS envía una solicitud de acceso al servidor RADIUS. Esta solicitud incluye las credenciales del usuario, cifradas para preservar la seguridad, así como un secreto compartido que facilita la verificación del origen del mensaje. [29]

- **Verificación del Usuario:** El servidor RADIUS examina el secreto compartido para confirmar que la solicitud proviene de un usuario autorizado. Si el secreto no concuerda, el mensaje se descarta y el proceso de autenticación no procede. [29]
- **Evaluación del Método de Autenticación:** Si el usuario es autorizado, el servidor RADIUS evalúa el método de autenticación solicitado. Si el método es permitido, se procede a verificar las credenciales del usuario comparándolas con la base de datos de usuarios. [29]

- **Comparación de Credenciales:** Si las credenciales del usuario coinciden con la información almacenada en la base de datos, el servidor RADIUS obtiene detalles adicionales del usuario y busca una política de acceso o perfil que se ajuste a dichas credenciales. [29]
- **Aplicación de Políticas:** Si se encuentra una política que coincide, el servidor RADIUS envía un mensaje de aceptación de acceso al dispositivo cliente. Este mensaje incluye un secreto compartido y un atributo de ID de filtro, que el cliente RADIUS usa para asignar al usuario a un grupo específico. [29]
- **Acceso Final:** El ID de filtro, que es una cadena de texto, permite al cliente RADIUS conectar al usuario con un grupo RADIUS específico, facilitando la categorización en grupos funcionales (por ejemplo, Docentes, Estudiantes, etc). Si el secreto compartido no coincide, el mensaje de aceptación es rechazado. Finalmente, si todo es correcto, el usuario recibe acceso al cliente RADIUS. [29]

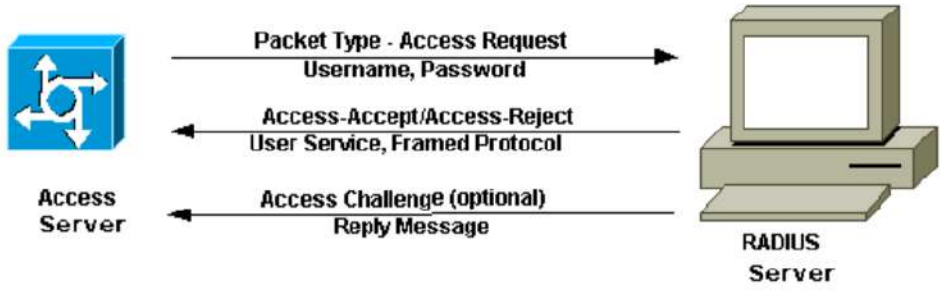

Figura 10. Orden de autenticación y autorización de Radius [29]

2.5.3.2 Autenticación, Autorización y Contabilidad en Radius

2.5.3.2.1 Autenticación RADIUS

Para configurar la autenticación a través de RADIUS, es esencial primero identificar el servidor RADIUS y establecer la clave de autenticación correspondiente. Posteriormente, se deben definir las listas de métodos de autenticación en RADIUS. Dado que la autenticación RADIUS se gestiona a través del sistema AAA, es necesario utilizar el comando aaa authentication y especificar RADIUS como el método de autenticación a implementar. [30]

2.5.3.2.2 Autorización RADIUS

La autorización dentro del marco de AAA permite la definición de parámetros que regulan el acceso de los usuarios a la red. RADIUS facilita un método integral para el control de acceso remoto, que abarca desde la autorización para servicios específicos hasta la gestión de perfiles y listas de cuentas por usuario. Además, ofrece compatibilidad con varios protocolos y servicios, incluyendo IP, IPX, AppleTalk Remote Access (ARA) y Telnet. Para configurar la autorización RADIUS en un entorno AAA, se debe ingresar el comando aaa authorization e indicar RADIUS como el método de autorización deseado. [30]

2.5.3.2.3 Contabilidad RADIUS

La contabilidad en el contexto de AAA permite el monitoreo detallado de los servicios que utilizan los usuarios y el seguimiento de los recursos de red consumidos. La contabilidad a través de RADIUS se gestiona mediante el sistema AAA, requiriendo el comando aaa accounting con RADIUS especificado como el método a emplear. [30]

2.5.3.3 Historia del protocol Radius

El desarrollo del protocolo RADIUS tuvo sus inicios a principios de la década de 1990, en los primeros días de Internet. Merit Network, una organización sin fines de lucro dedicada a proporcionar servicios de redes de alta calidad a diversas instituciones, identificó la necesidad de una solución que integrara los sistemas de autenticación, autorización y contabilidad (AAA). [31]

En respuesta a esta necesidad, Livingston Enterprises, una compañía tecnológica, desarrolló la primera versión del protocolo RADIUS, conocido como Remote Authentication Dial-In User Service. En sus comienzos, RADIUS solo ofrecía autenticación basada en credenciales de usuario. Sin embargo, con el tiempo, el protocolo ha evolucionado para incluir métodos de autenticación más avanzados, como los certificados digitales. Esta evolución ha permitido que RADIUS mantenga su relevancia en la industria de la ciberseguridad, que está en constante transformación. En la actualidad, RADIUS se ha incorporado a los estándares IEEE 802 y está respaldado por el Grupo de Trabajo de Ingeniería de Internet (IETF). [31]

2.5.3.4 Estructura del paquete Radius

El protocolo RADIUS opera sobre UDP/IP, utilizando los puertos 1812 y 1813 para su transporte. La estructura del paquete RADIUS se organiza de manera específica y se presenta en el formato ilustrado a continuación. Los datos dentro del paquete se transmiten en el siguiente orden: primero el código, seguido por el identificador, la longitud, el autenticador y, finalmente, los atributos. [32]

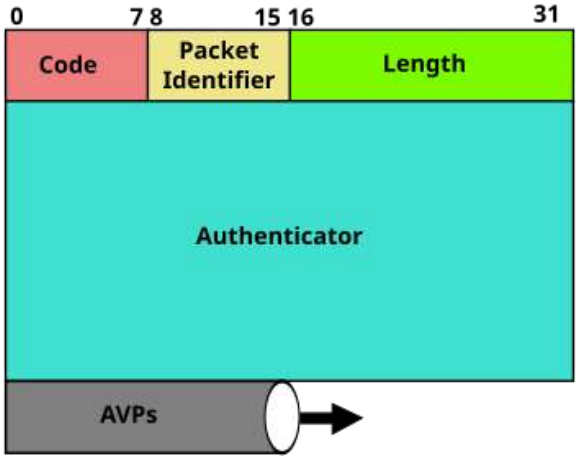

Figura 11. Formato de datos de paquetes RADIUS. [32]

2.6 Controladora Cisco Catalyst 9800-CL

El Cisco Catalyst 9800-CL es un controlador inalámbrico virtualizado diseñado para implementarse en entornos de nube pública, privada o híbrida. Este controlador ofrece una solución flexible y escalable para gestionar redes inalámbricas, permitiendo una integración y gestión eficiente de los puntos de acceso. Sus características avanzadas incluyen soporte para estándares Wi-Fi 6, capacidades de seguridad integradas, y herramientas de análisis y monitoreo en tiempo real. Ideal para instituciones educativas, empresas y centros de datos, el Catalyst 9800-CL garantiza un rendimiento óptimo, alta disponibilidad y una administración simplificada de la infraestructura inalámbrica. [33]

2.6.1 Beneficios de la virtualización

El controlador aprovecha las ventajas de la virtualización para ofrecer los siguientes beneficios:

- **Independencia del hardware:** Al ejecutarse en una VM, el controlador es compatible con cualquier hardware x86 que soporte la plataforma de virtualización utilizada.
- **Compartición de recursos:** Los recursos que el controlador utiliza son gestionados

por el hipervisor, permitiendo que estos recursos sean compartidos entre diferentes máquinas virtuales. La asignación de recursos de hardware a una VM específica puede ser reajustada para otra VM dentro del mismo servidor.

- **Flexibilidad en la implementación:** La capacidad de mover fácilmente una VM de un servidor a otro permite trasladar el controlador de un servidor en una ubicación física a otro servidor en una ubicación diferente sin necesidad de mover físicamente el hardware.

2.6.2 Características clave de la controladora

Métrica	Valor
# máximo de puntos de acceso	Hasta 6000
# máximo de clientes	64.000
Rendimiento máximo (perfil bajo sin SR-IOV)	2,1 Gbps
Rendimiento máximo (perfil alto con SR-IOV)	5 Gbps
WLAN máximas	4096
VLAN máximas	4096
Sistema operativo	Software Cisco IOS XE

Tabla 3. *Características de WLC 9800-CL [33]*

La virtualización Single Root I/O (SR-IOV) permite que múltiples máquinas virtuales, cada una con distintos sistemas operativos invitados, utilicen conjuntamente un único adaptador de red PCIe en un servidor host. SR-IOV habilita la transferencia directa de datos entre una máquina virtual y el adaptador de red, evitando así el paso por el hipervisor. Esto no solo mejora el rendimiento de la red, sino que también disminuye la carga de la CPU del servidor. [34]

CAPÍTULO III. METODOLOGÍA.

3.1. Tipo de investigación

El tipo de investigación utilizada es aplicada y descriptiva, puesto que, la investigación aplicada implica utilizar los conocimientos básicos teóricos existentes, aplicarlos en un contexto y sus descubrimientos en la mejora de estrategias concretas e identificables. En este caso, se analiza y evalúa diferentes tecnologías de Autenticación, Autorización y Auditoría (AAA) con el fin de proponer una solución para mejorar la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo. [35]

A su vez, se utiliza la investigación descriptiva que busca especificar características y elementos importantes de distintos fenómenos actuales, identificando y explicando su naturaleza y comportamiento. En este estudio, se puntualiza las características y el funcionamiento de las principales tecnologías AAA, comparándolas entre sí y evaluando su eficacia en el contexto de la red inalámbrica de la UNACH [36]

3.1 Enfoque de la investigación

La metodología utilizada en esta investigación será de un enfoque mixto para obtener una visión completa y fundamentada; es importante resaltar que el propósito de la investigación mixta no es sustituir a ninguno de los enfoques que la componen, sino que, por el contrario, su meta es utilizar las fortalezas de ambos tipos de indagación, combinándolas y tratando de minimizar sus debilidades potenciales. [37]

Se utilizarán técnicas cuantitativas para recopilar y analizar datos numéricos y estadísticos para obtener resultados objetivos y medibles. El enfoque cuantitativo implica recopilar y analizarla utilizando métodos estadísticos y matemáticos. De igual manera, se emplearán técnicas cualitativas para la recopilación de datos subjetivos y obtención de información acerca de las tecnologías de Autenticación, Autorización y Auditoría (AAA); se enfocará en comprender y explorar las percepciones, opiniones y experiencias de los participantes, expertos en seguridad y personal involucrado en la gestión de la red.

3.2 Proceso de la metodología

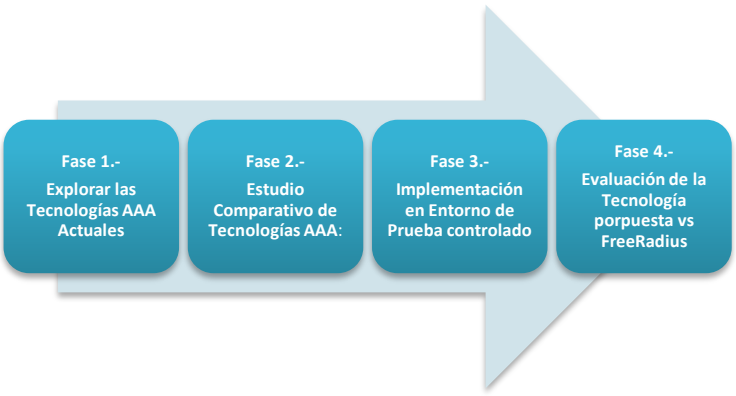

Figura 12. Diagrama del Proceso de la Metodología.

3.2.1 Fase 1: Explorar las Tecnologías AAA Actuales:

Se analizarán las tecnologías de Autenticación, Autorización y Auditoría (AAA) disponibles en la actualidad que facilitan el acceso de usuarios a redes inalámbricas.

3.2.2 Fase 2: Estudio Comparativo de Tecnologías AAA:

Se llevará a cabo un análisis comparativo de las principales tecnologías AAA para identificar la más adecuada para los requisitos específicos de la red inalámbrica de la Universidad Nacional de Chimborazo.

3.2.3 Fase 3: Simulación e Implementación en Entorno de Prueba:

Se implementará la tecnología AAA seleccionada en un entorno de prueba controlado, replicando las condiciones de uso reales del bloque “U” campus “Dolorosa” de la Universidad Nacional de Chimborazo.

3.2.4 Fase 4: Evaluación Sistemática de la Tecnología:

Se realizará una evaluación exhaustiva de la herramienta seleccionada vs la actualmente usada, enfocándose en parámetros clave como las características, soporte, recursos necesarios, implementación y los costos.

3.3 Población y muestra

3.3.1 Población:

La población de estudio del presente trabajo está compuesta por un grupo o conjunto a estudiar. En este caso, la población son las herramientas AAA que se podrán usar para la

red inalámbrica de UNACH; como investigador consideramos que la población sea relativamente homogénea respecto de las variables de mi interés. [38]

3.3.2 Muestra:

La muestra se seleccionará de manera estratificada, todo ello enfocado en adaptabilidad con el hardware CISCO existente en bloque "U" del campus "Dolorosa" de la UNACH, siendo esta muestra una parte representativa de la población. [39]

3.4 Técnicas e instrumentos

En este estudio, se emplearán diversas técnicas e instrumentos para recopilar datos, los cuales consisten en una serie de pasos y acciones que permiten adquirir información necesaria para abordar de manera efectiva la investigación. Se utilizará una revisión bibliográfica y documental para obtener información relevante sobre las tecnologías AAA. Posteriormente, se realizará una comparación que incluirá criterios clave como facilidad de uso, eficiencia, seguridad, escalabilidad e interoperabilidad, con el fin de evaluar y comparar dichas tecnologías, seguido a ello se ejecutaran las pruebas para proponer la herramienta más idónea. [34]

3.5 Operacionalización de variables

A continuación, se muestra una tabla que definirá por un lado la variable independiente que esta se refiere a la característica o factor que se manipula o varía de forma intencionada por el investigador para observar su efecto sobre otras variables. [40]

Por otra parte, la variable dependiente es aquellas cuyos valores se ven alterados o influenciados por la presencia o cambios en una variable independiente. [41]

Variable	Descripción	Indicadores	Técnicas e instrumentación
Independiente	Evaluación del método de autenticación AAA	• Uso de un servidor de autenticación Radius dentro de Cisco ISE	• Revisión de implementación de Radius dentro de Cisco ISE

			• Análisis de resultados de configuración de red
Dependiente	Nivel de seguridad en la autenticación de la red inalámbrica de la Universidad Nacional de Chimborazo.	• Número de incidentes de seguridad reportados • Políticas de seguridad implementadas • Numero de accesos no autorizados	• Revisión de las políticas de seguridad • Observación de los lives logs de cisco ISE

Tabla 4. *Operacionalización de las variables.*

3.6 Comparativa de las herramientas AAA seleccionadas

Comparativa entre RADIUS y TACACS+ como Métodos de Autenticación para Cisco ISE.En el siguiente apartado se analizan y comparan los dos protocolos de seguridad más relevantes empleados en el control de acceso a las redes: Cisco RADIUS y Cisco TACACS+.

La especificación del protocolo RADIUS se encuentra detallada en la RFC 2865, la cual ha sustituido a la RFC 2138. Cisco ha brindado soporte a ambos protocolos sin pretender competir con RADIUS ni influenciar a los usuarios hacia TACACS+. La elección del protocolo debe basarse en las necesidades específicas de cada red. En este contexto, la presente tesis analiza las diferencias entre TACACS+ y RADIUS para facilitar una decisión informada.

Cisco ha ofrecido soporte para RADIUS desde la versión 11.1 del software Cisco IOS en febrero de 1996 y continúa mejorándolo con nuevas funciones y capacidades. Antes de desarrollar TACACS+, Cisco evaluó exhaustivamente el protocolo RADIUS, identificando sus fortalezas y áreas de mejora. La creación de TACACS+ respondió a la necesidad de un protocolo que pudiera escalar con el crecimiento de las redes y adaptarse a nuevas tecnologías de seguridad a medida que estas evolucionan. TACACS+ fue diseñado

para cumplir con las crecientes demandas del mercado de seguridad, incorporando características avanzadas que no se encontraban en RADIUS. La arquitectura de TACACS+ se integra eficientemente con la estructura de autenticación, autorización y contabilidad (AAA) de Cisco, proporcionando una solución robusta y flexible para la gestión de la seguridad en redes complejas.

Las secciones siguientes ofrecen una comparación detallada de las características clave de TACACS+ y RADIUS.

3.6.1 Principal utilización hoy en día

La diferencia fundamental entre RADIUS y TACACS+ radica en sus aplicaciones principales. RADIUS se emplea principalmente como un protocolo de acceso a la red para la autenticación de usuarios. En contraste, TACACS+ se utiliza predominantemente para la gestión y control de dispositivos de red como enrutadores y conmutadores. Esta distinción refleja el enfoque de cada protocolo: RADIUS está orientado hacia la verificación y autorización de usuarios que intentan acceder a la red, mientras que TACACS+ se centra en la administración y control detallado de los comandos y acciones que se ejecutan en los dispositivos de la red.

3.6.2 Protocolo de transporte: UDP vs TCP

RADIUS utiliza el Protocolo de Datagrama de Usuario (UDP), mientras que TACACS+ emplea el Protocolo de Control de Transmisión (TCP). TCP tiene ventajas sobre UDP, como la orientación a la conexión y la entrega garantizada, mientras que UDP ofrece una entrega de mejor esfuerzo. Sin embargo, la naturaleza liviana de UDP hace que RADIUS sea adecuado para entornos donde la velocidad y la eficiencia son cruciales.

3.6.3 Acceso a la red.

El protocolo RADIUS está diseñado para soportar el control de acceso a la red mediante la implementación de 802.1x, permitiendo una gestión eficiente del acceso a la red en función del puerto. Este protocolo está centrado en la autorización de acceso a la red, facilitando la autenticación de usuarios y la aplicación de políticas de acceso. En contraste, TACACS+ no proporciona soporte para el control de acceso a la red basado en puertos

802.1x. En lugar de ello, TACACS+ se enfoca predominantemente en la administración de dispositivos de red a través de servidores de control de acceso (ACS), siendo más adecuado para la gestión y autorización de comandos en dispositivos de red como enrutadores y conmutadores.

3.6.4 Cifrado de paquetes

RADIUS cifra únicamente la contraseña en el paquete de solicitud de acceso enviado del cliente al servidor, mientras que TACACS+ cifra todo el cuerpo del paquete. Aunque el cifrado completo del paquete en TACACS+ proporciona mayor seguridad, el enfoque de RADIUS es suficiente para muchas implementaciones de autenticación de usuarios que es donde se enfoca este trabajo donde el rendimiento y la simplicidad son prioridades.

3.6.5 Autenticación y autorización

RADIUS combina autenticación y autorización en un solo proceso, lo que simplifica la configuración y gestión del sistema, especialmente en entornos universitarios o bancarios. Aunque TACACS+ separa estos procesos, permitiendo una mayor flexibilidad y control, RADIUS ofrece una solución robusta y ampliamente aceptada que es suficiente para muchas organizaciones. La capacidad de RADIUS para integrar autenticación y autorización facilita su implementación y mantenimiento.

3.6.6 Soporte multiprotocolo

TACACS+ admite una variedad de protocolos que RADIUS no soporta, como el Protocolo de Acceso Remoto AppleTalk (ARA) y el Protocolo de Control de Trama NetBIOS. Sin embargo, RADIUS es altamente compatible con los protocolos de red más comunes y utilizados, lo que lo hace ideal para la mayoría de las implementaciones modernas.

3.6.7 Gestión del enrutador

TACACS+ ofrece métodos avanzados para controlar la autorización de comandos en un enrutador, lo que no es posible con RADIUS. Sin embargo, para muchas organizaciones, la funcionalidad de RADIUS en términos de autenticación y autorización

de acceso a la red es suficiente. La simplicidad y eficacia de RADIUS en la gestión de accesos y la implementación de políticas de seguridad hacen que sea una opción preferida en entornos donde la gestión avanzada de comandos no es crítica.

3.6.8 Interoperabilidad

RADIUS, al ser un protocolo de estándar abierto, es ampliamente compatible con casi todos los dispositivos modernos disponibles en el mercado. Esta compatibilidad asegura una mayor flexibilidad y facilidad de integración en diversas redes y entornos de TI. Por otro lado, TACACS+ es un protocolo propietario desarrollado por Cisco, lo que implica que su operatividad está limitada principalmente a dispositivos fabricados por Cisco. Esta limitación puede restringir la interoperabilidad en entornos que no están completamente basados en tecnología Cisco, lo cual puede ser un factor a considerar al elegir entre ambos protocolos.

3.6.9 Tráfico

Las diferencias entre TACACS+ y RADIUS en términos de tráfico generado entre el cliente y el servidor son notables. RADIUS, al utilizar UDP, genera menos sobrecarga en la red, lo que puede ser ventajoso en entornos con recursos limitados como lo son entornos universitarios o donde se prioriza la eficiencia del ancho de banda. La implementación de RADIUS en su red ya existente demuestra su capacidad para manejar las demandas del entorno sin comprometer el rendimiento.

3.6.10 Complejidad y recursos

Al evaluar TACACS+, es esencial considerar el tamaño y la complejidad de la red. TACACS+ es ideal para redes grandes y complejas. No obstante, puede resultar excesivo para redes pequeñas. Para nuestro caso de estudio un solo bloque con infraestructuras de red menos complejas se prefiere RADIUS, debido a su amplio soporte en diversos dispositivos y facilidad de implementación

3.7 Interpretación de resultados

Comparación de Radius frente a TACACS+ mediante la escala de Likert

A continuación, se presentan las comparaciones según varias características de TACACS+ y RADIUS, utilizando la herramienta de la escala de Likert para diferenciar y verificar cuál de los dos protocolos es el más conveniente al implementar una red universitaria. Para realizar la evaluación con la escala de Likert, se detalla en la siguiente tabla el valor cuantitativo de varios aspectos críticos como el protocolo de transporte, cifrado del paquete, autenticación y autorización, soporte multiprotocolo, gestión del enrutador, interoperabilidad, tráfico, complejidad/recursos entre los protocolos RADIUS y TACACS+.

Denominación	**Peso cuantitativo**
Muy alta	5
Buena	4
Media	3
Baja	2
Muy baja	1

Tabla 5. *Denominación de valores de la escala de Likert*

Descripción	**Radius**	**TACACS+**
Protocolo de Transporte	4	5
Cifrado del paquete	4	5
Autenticación y autorización	5	2
Soporte Multiprotocolo	3	5
Gestión del enrutador	2	5
Interoperabilidad	5	3
Complejidad/Recursos	5	3
Trafico	5	3
Total	33	31

Tabla 6. *Escala de pesos mediante escala de Likert*

3.8 **Resultados finales.**

Dada la comparación entre RADIUS y TACACS+, y considerando los factores mencionados, es evidente que RADIUS presenta ventajas significativas para su implementación en Cisco ISE en el contexto de redes universitarias. Las instituciones educativas, como las universidades, que a menudo necesitan una solución escalable para la autenticación Wi-Fi en sus campus, tienden a preferir RADIUS por su excelente integración con una amplia variedad de infraestructuras inalámbricas.

A continuación, se destacan los puntos clave que favorecen la elección de RADIUS:

- **Compatibilidad Amplia:** RADIUS es compatible con una amplia variedad de enrutadores y conmutadores de diferentes fabricantes, no limitándose únicamente a dispositivos Cisco. Esta interoperabilidad facilita la integración en redes heterogéneas y asegura una mayor flexibilidad en la elección de equipos de red.
- **Control de Acceso Basado en Puertos:** A diferencia de TACACS+, RADIUS admite el control de acceso a la red basado en puertos 802.1x. Esta capacidad permite una gestión más eficaz del acceso a la red, proporcionando una capa adicional de seguridad al validar los dispositivos en función del puerto al que se conectan.
- **Mejora en la Contabilidad:** RADIUS ofrece robustas capacidades de contabilidad, registrando de manera efectiva las actividades de los usuarios y los dispositivos. Esta función es crucial para la supervisión y el análisis del uso de la red, contribuyendo a una mejor gestión y seguridad de la misma.

En conclusión, la elección de RADIUS para Cisco ISE es más favorable debido a su amplia compatibilidad con diferentes equipos de red, su capacidad para implementar el control de acceso basado en puertos 802.1x, y su efectividad en la contabilidad. Estas características hacen de RADIUS una opción preferible para mejorar la seguridad y la gestión de la red inalámbrica en una universidad.

3.9 **Implementación de Cisco ISE**

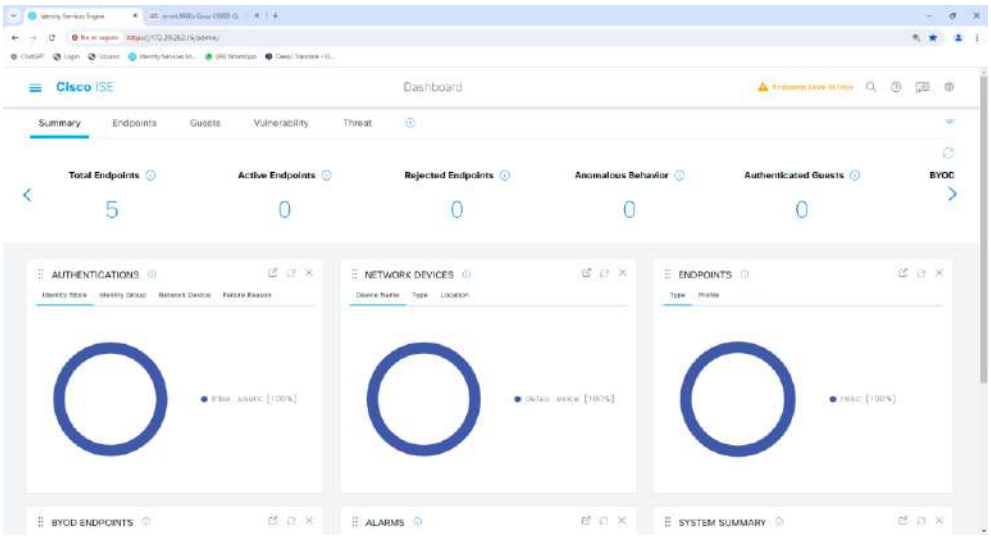

Figura 13. Dashboard inicial de Cisco ISE

Paso 1.-

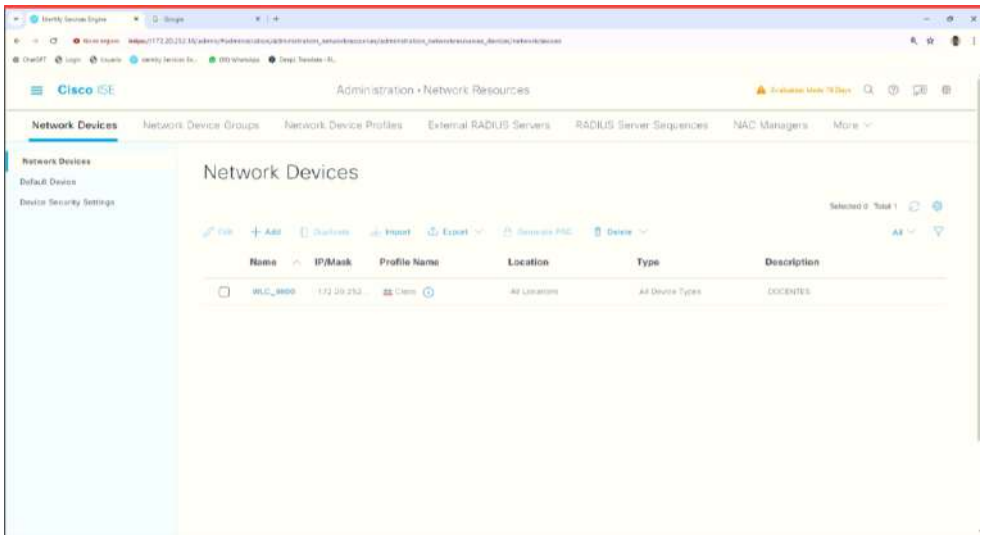

Figura 14. Empezamos agregando el nuevo dispositivo de red: Administration > Network Resources > Network Devices > +Add.

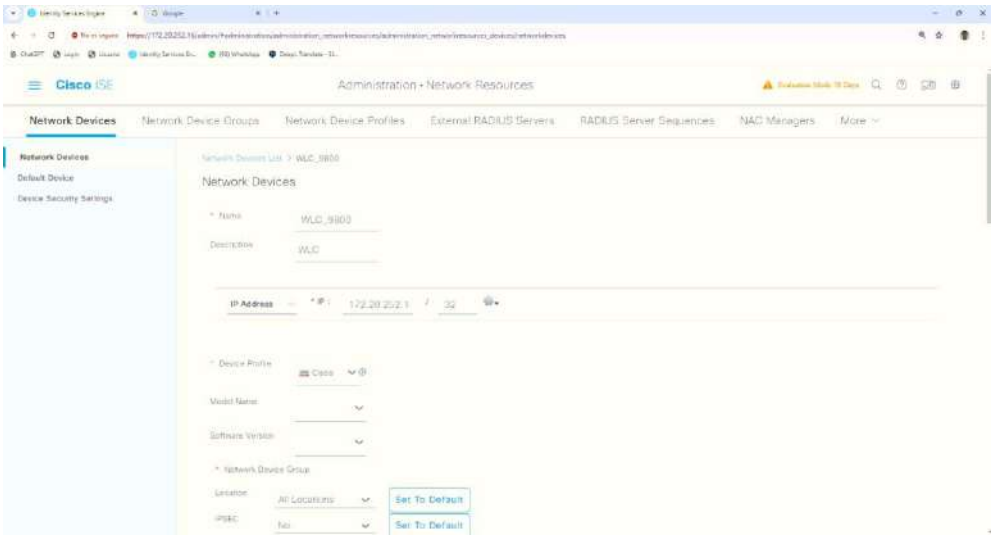

Figura 15. Al ND se le agregara el nombre en este caso es WLC_9800, seguido de la descripción y la dirección IP que se le asigno a este (172.20.252.13)

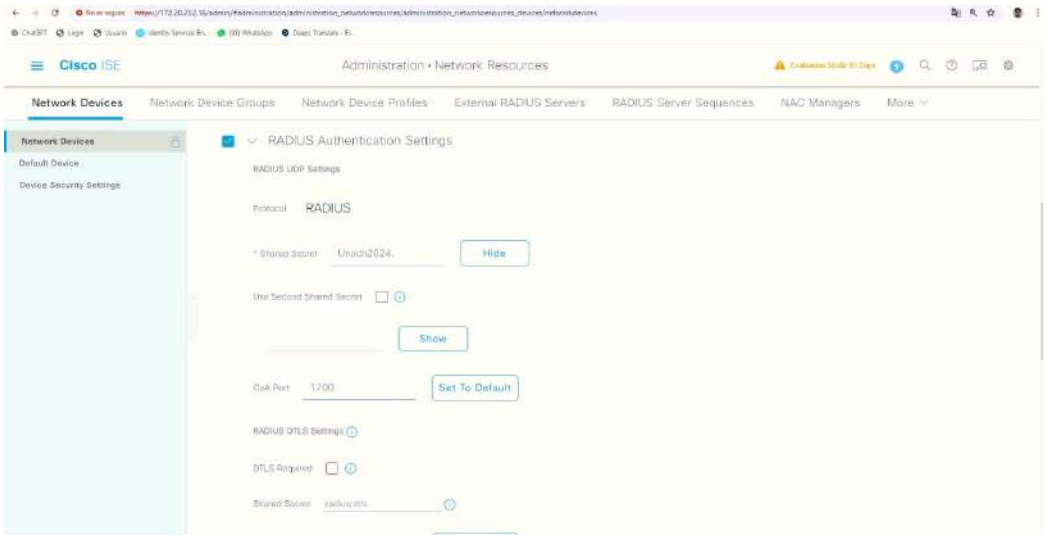

Figura 16. Se marca la casilla de verificación RADIUS dentro del ND y se define el secreto compartido (contraseña= Unach2024.), las demás configuraciones se las dejará por defecto.

Paso 2.-

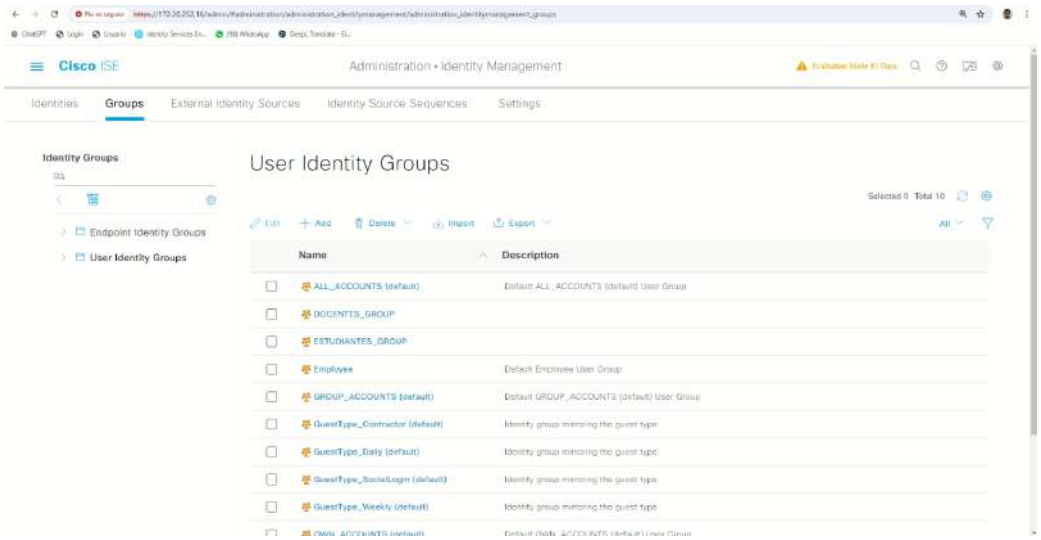

Figura 17. Se creará los grupos de identidades de usuarios, serán dos grupos de usuarios uno llamado DOCENTES_GROUP y ESTUDIANTES_GROUP: > Administration > Identity Management > Groups > User Identity Groups > + Add

Paso 3.-

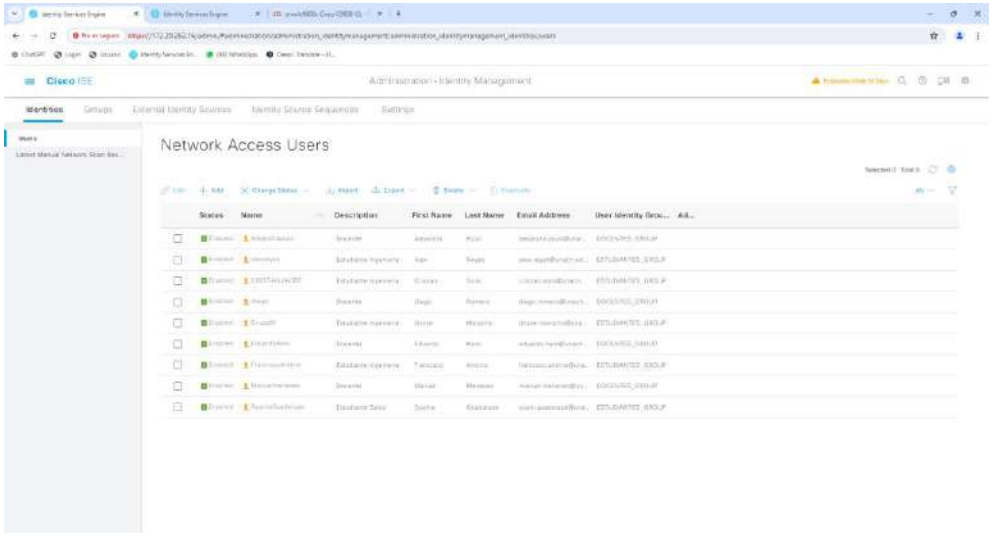

Figura 18. Se realizará la creación los usuarios que vamos a asociar a estos grupos ya sean DOCENTES o ESTUDIANTES: Administration > Identity Management > Identities > + Add.

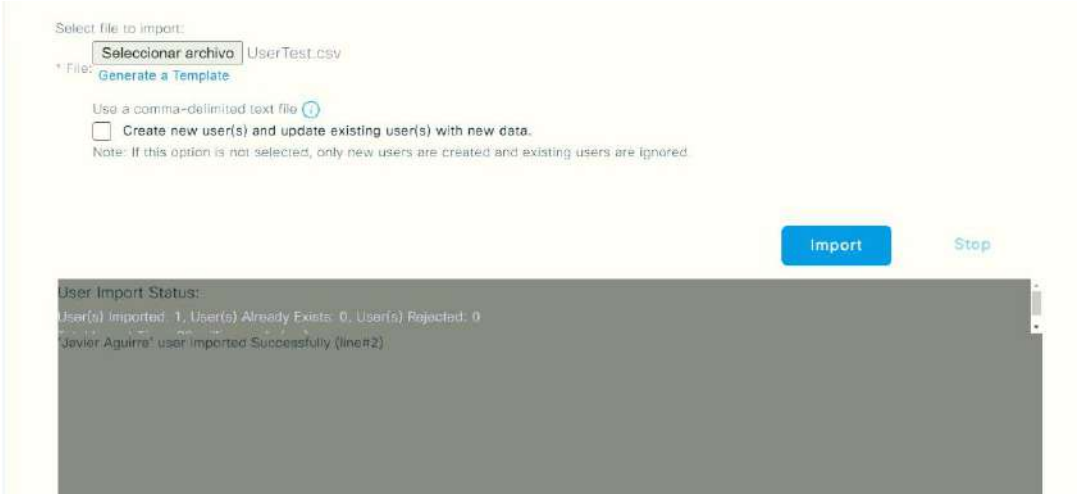

Figura 19. Aquí a su vez se creará una base de datos interna que además se puede importar y exportar mediante archivos con extensión .csv

Figura 20. Archivo Excel con extensión .csv para importación de archivos

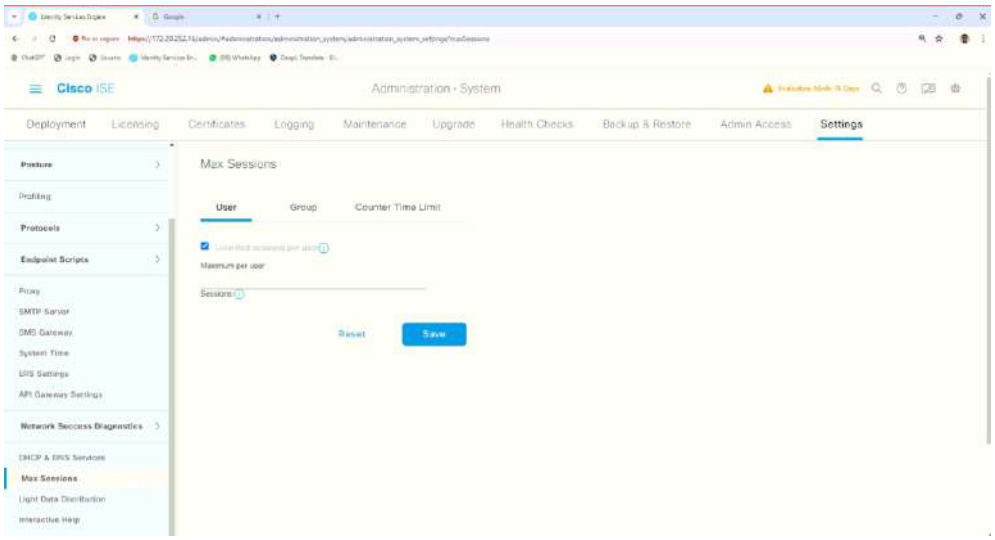

Figura 21. Algo importante a tener en cuenta es sobre el número máximo de sesiones simultaneas con las mismas credenciales, en el caso de Cisco ISE estas se pueden definir por usuario o grupo de usuarios de la siguiente manera: System >Settings >Max Sessions

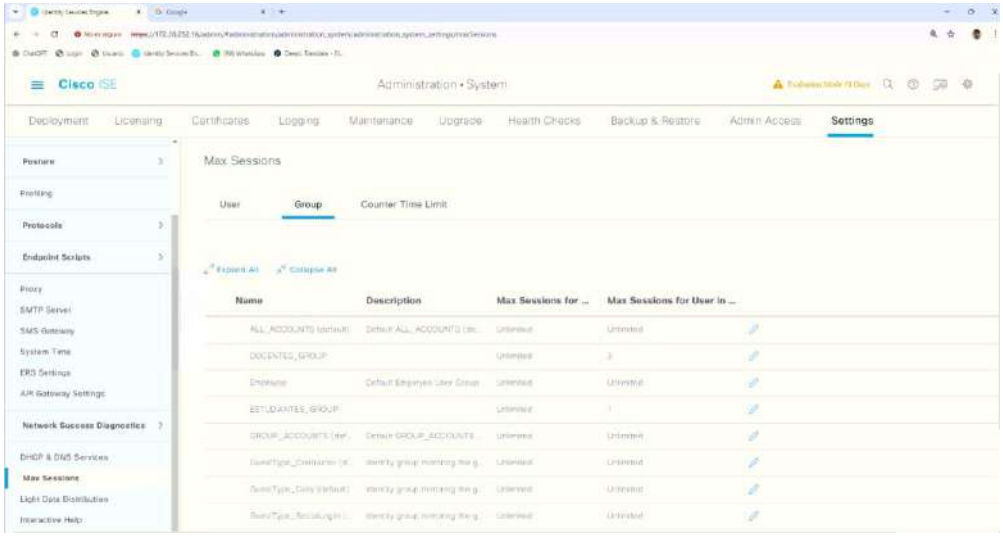

Figura 22. En este caso nosotros definimos un número máximo de 3 sesiones simultaneas por credencial a los usuarios que pertenezcan al grupo DOCENTES_GROUP y una sesión máxima simultánea a los usuarios que pertenezcan al grupo ESTUDIANTES_GROUP.

Figura 23.

Paso 4.-

Seguido se creará dos perfiles de autorización para que podamos diferenciar a los docentes y a los estudiantes, esto configuración se la hace desde: *Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.*

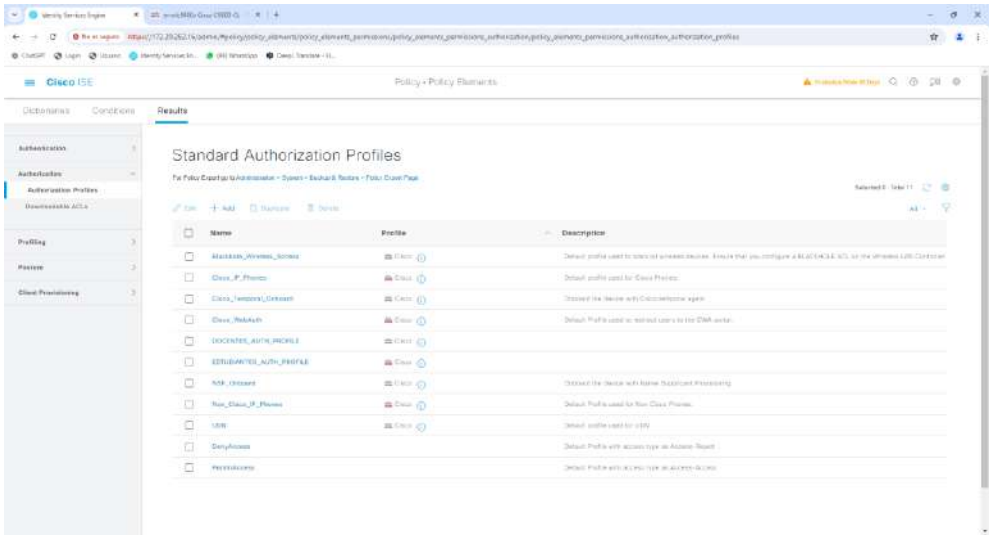

Figura 24. Aquí se observan ambos perfiles de autorización creados: DOCENTES_AUTH_PROFILE y ESTUDIANTES_AUTH_PROFILE

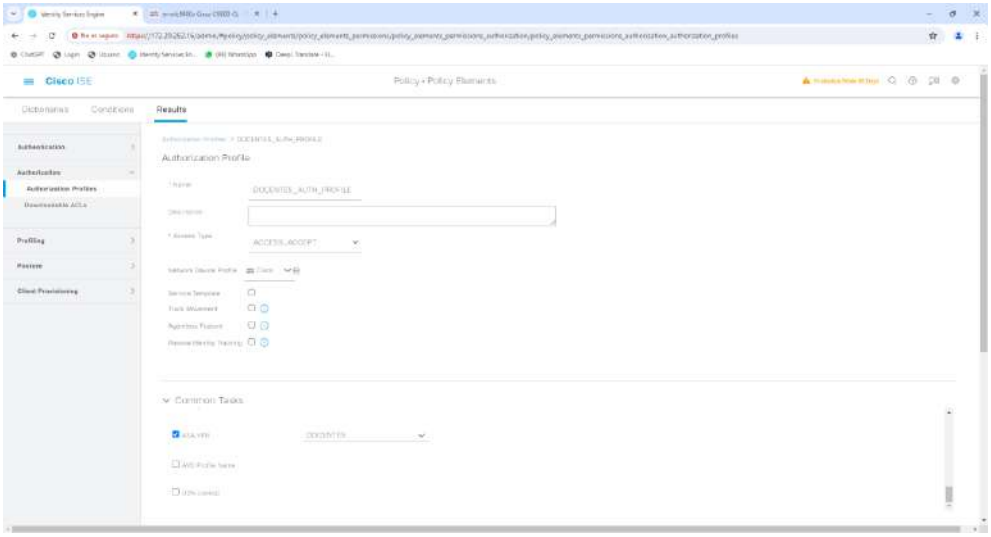

Figura 25. Se define el nombre para el Perfil de autorización

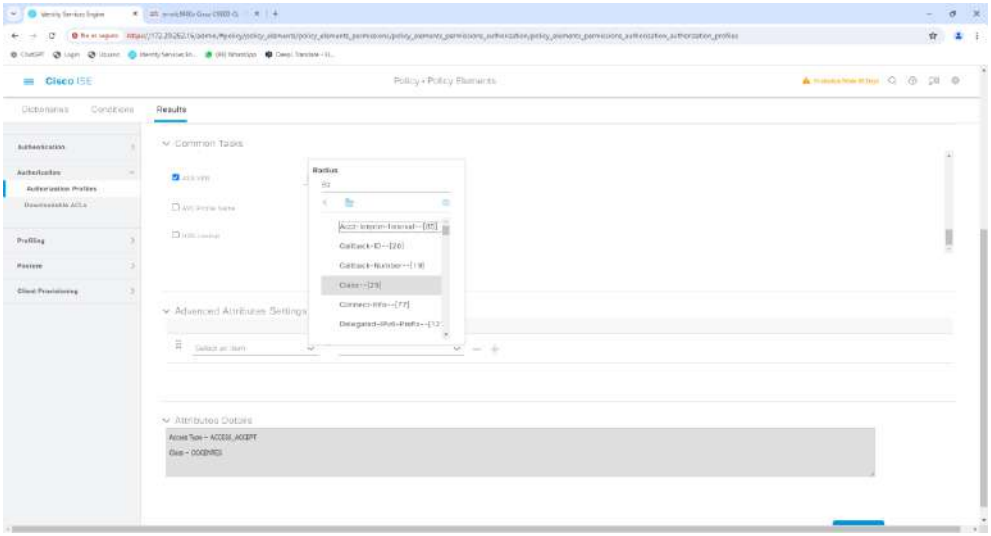

Figura 26. Se deja el Tipo de acceso como ACCESS_ACCEPT y en Configuración de atributos avanzados agregue un Radio > Clase--[25] con el atributo de clase DOCENTES

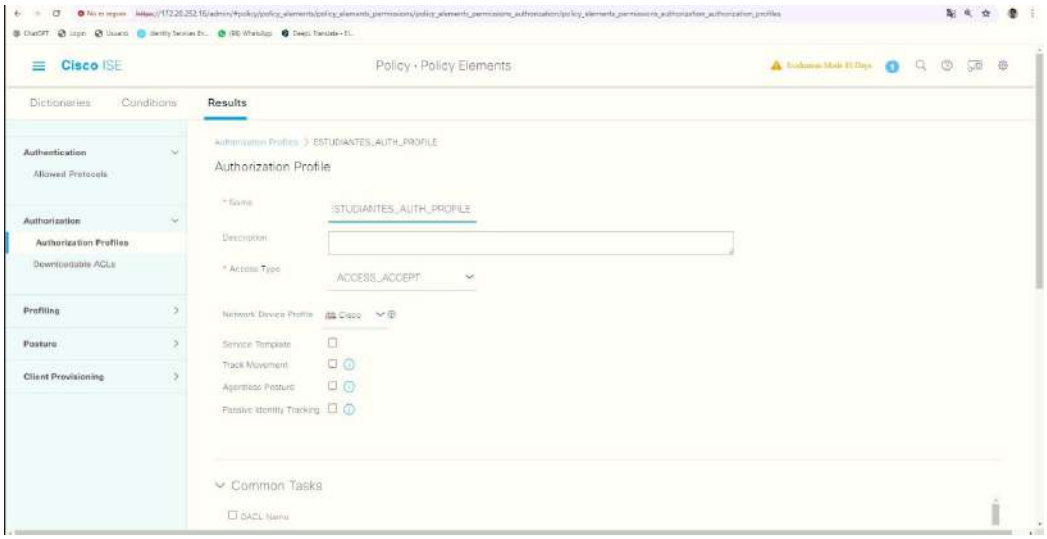

Figura 27. Se define el nombre para el Perfil de autorización

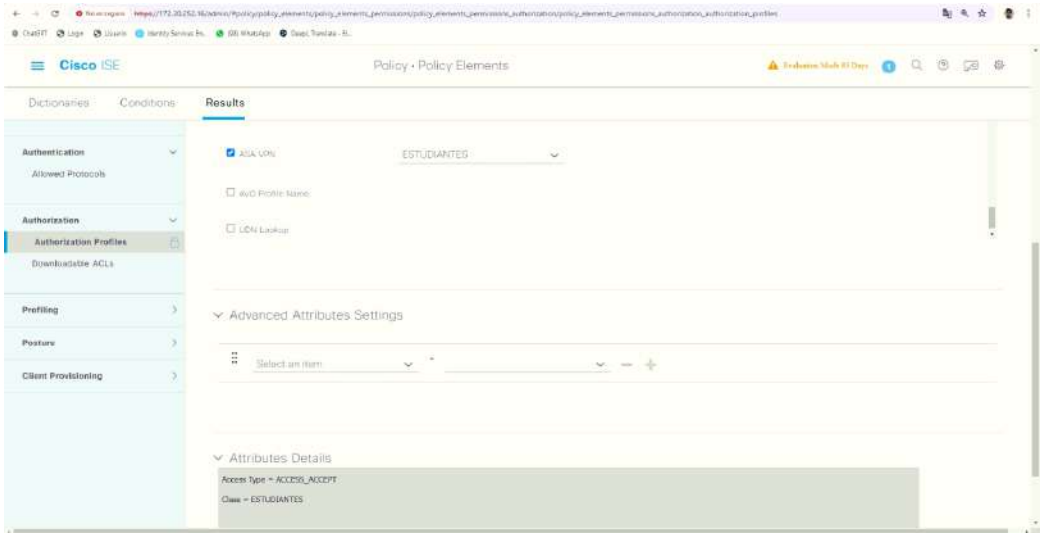

Figura 28. De igual manera se deja el Tipo de acceso como ACCESS_ACCEPT y en Configuración de atributos avanzados agregue un Radio > Clase--[25] con el atributo de clase Estudiantes

Paso 5.-

Seguido se empezará con la creación de los conjuntos de políticas de administración y autorización: > Policy > Policy Sets > +

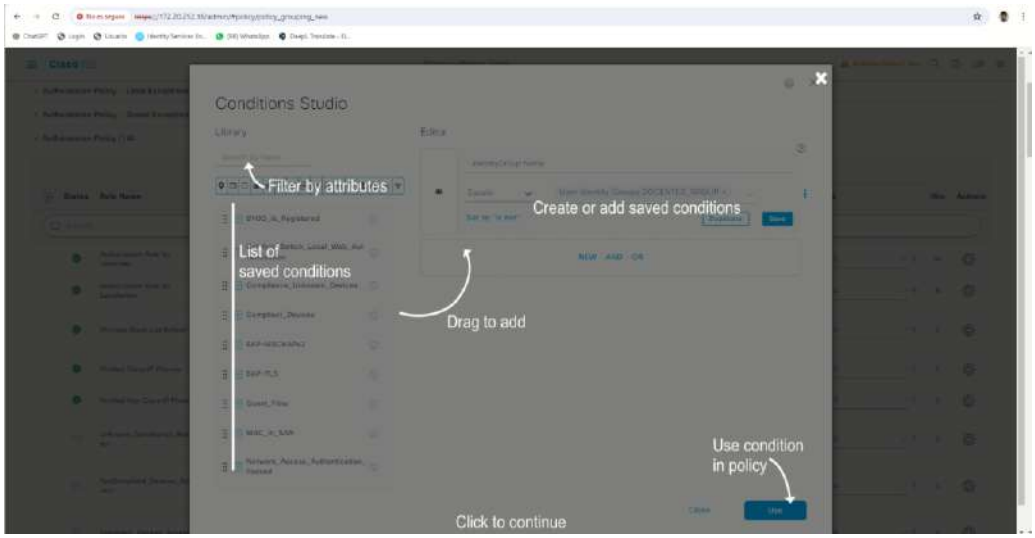

Figura 29. Usaremos una plantilla de política que se encuentra por defecto

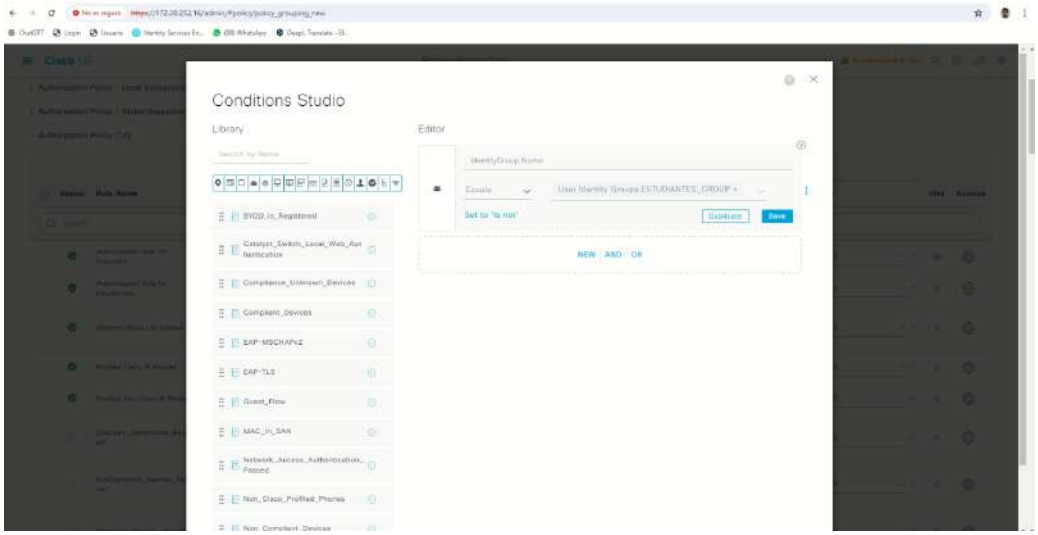

Figura 30. Pero agregaremos dos políticas de autorización adicional, una denominada Autorization Rule for Docentes y otra con el nombre Autorization Rule for Estudiantes

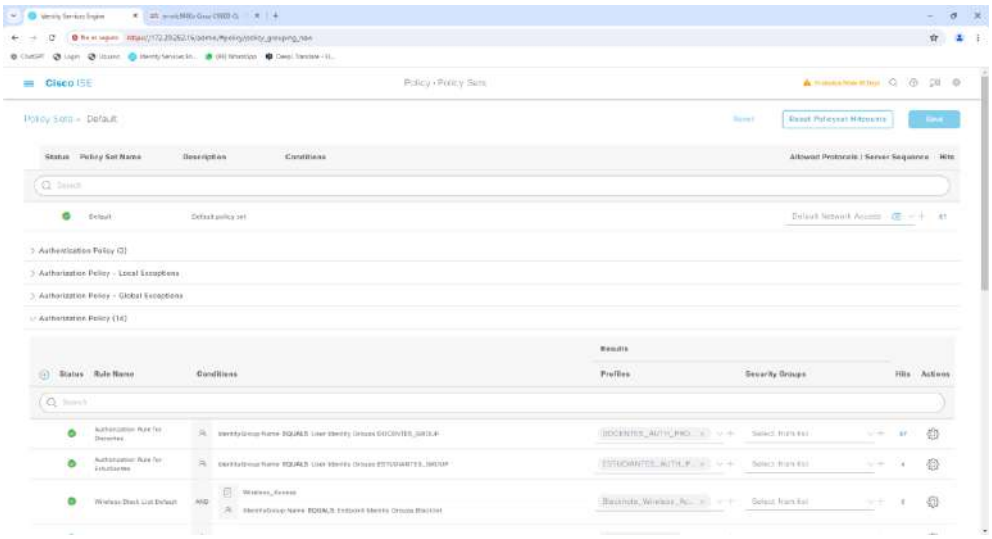

Figura 31. Las condiciones para el Docentes y Estudiantes

Paso 6.-

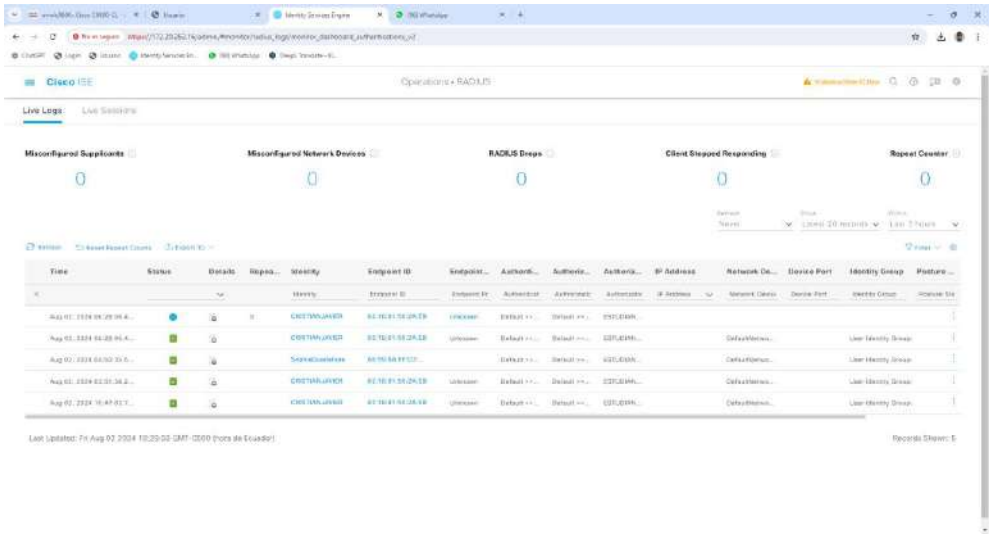

Figura 32. Muestra del dashboard de Lives Logs

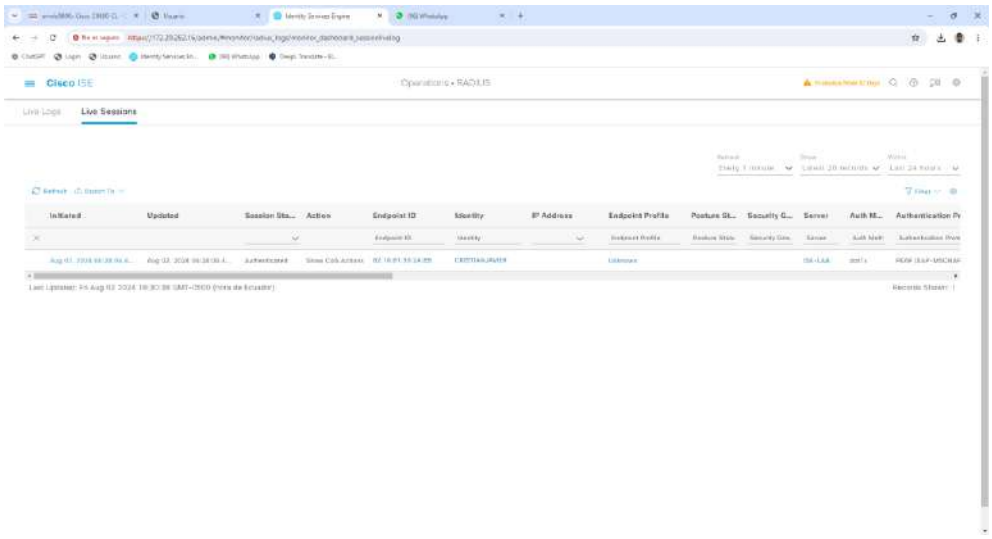

Figura 33. Muestra de el dashboard de los live sessions

Figura 34. Aquí podemos observar que los usuarios creados están cumpliendo las políticas que hemos creado

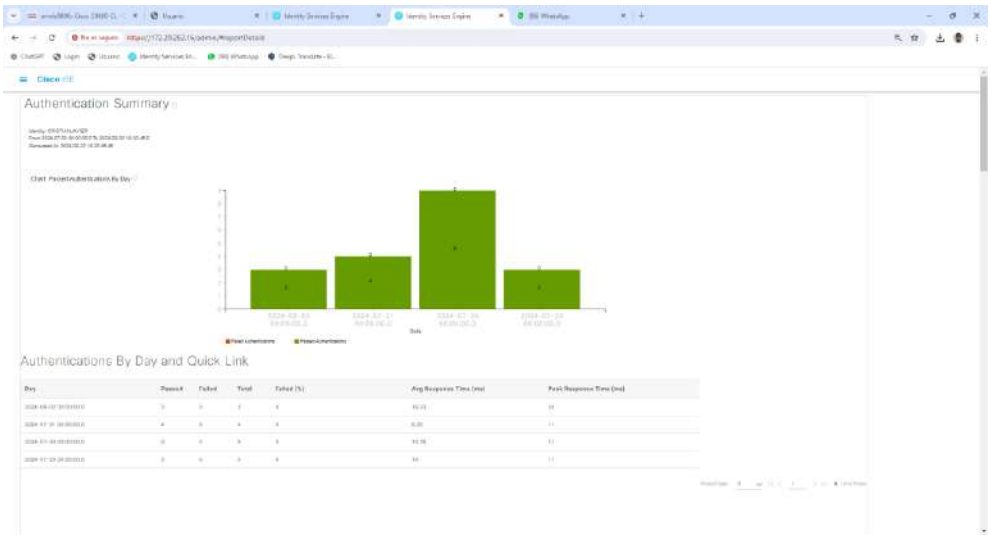

Figura 35. En esta figura se observa el summary authentication de un usuario en especifico

Paso 7.-

Configuración de la Controladora Wireless

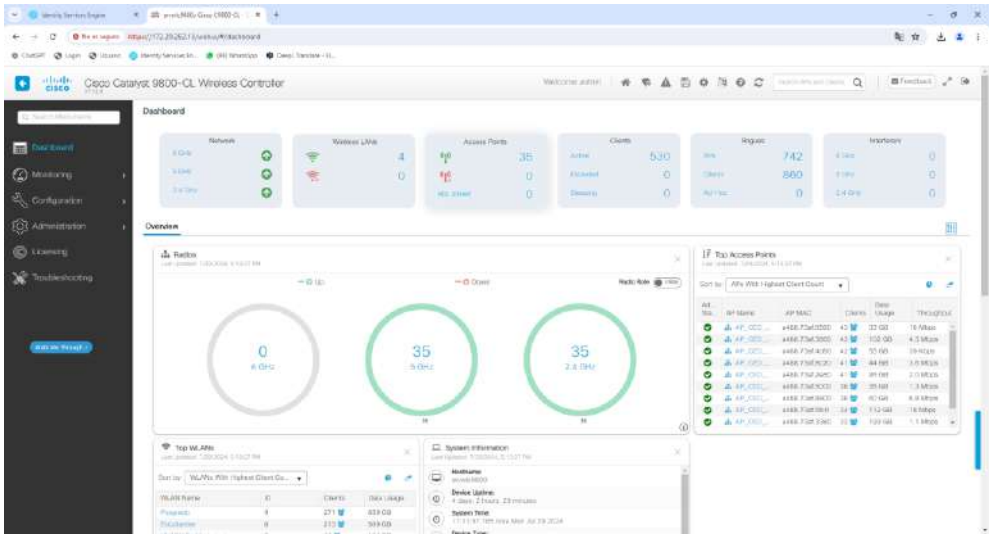

Figura 36. Dashboard de la controladora Catalys 9800-CL

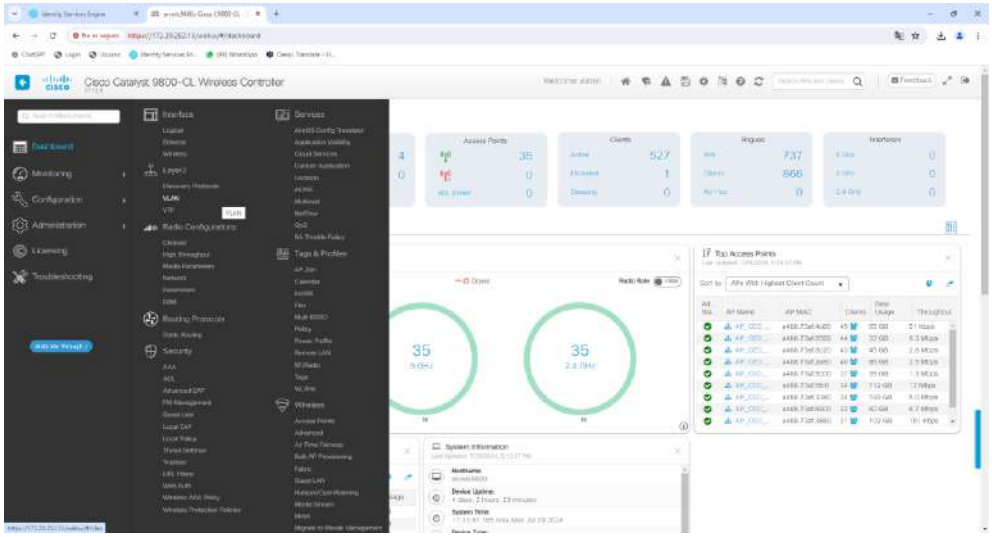

Figura 37. Seguido a ellos elegimos la VLAN que vamos a configurar

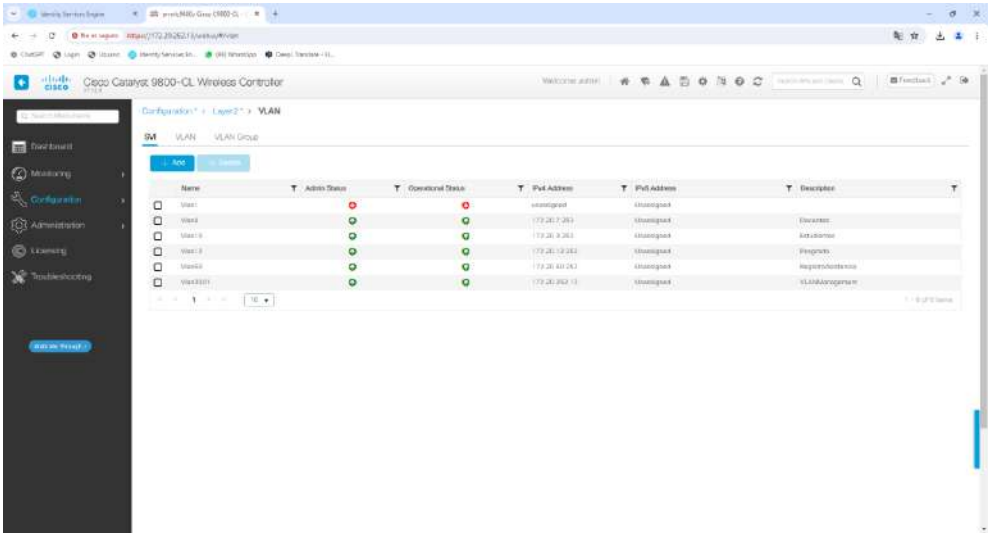

Figura 38. Se elegio hacer la prueba en la VLAN 4 que pertenece a los Docentes con dirección IP (172.20.7.253)

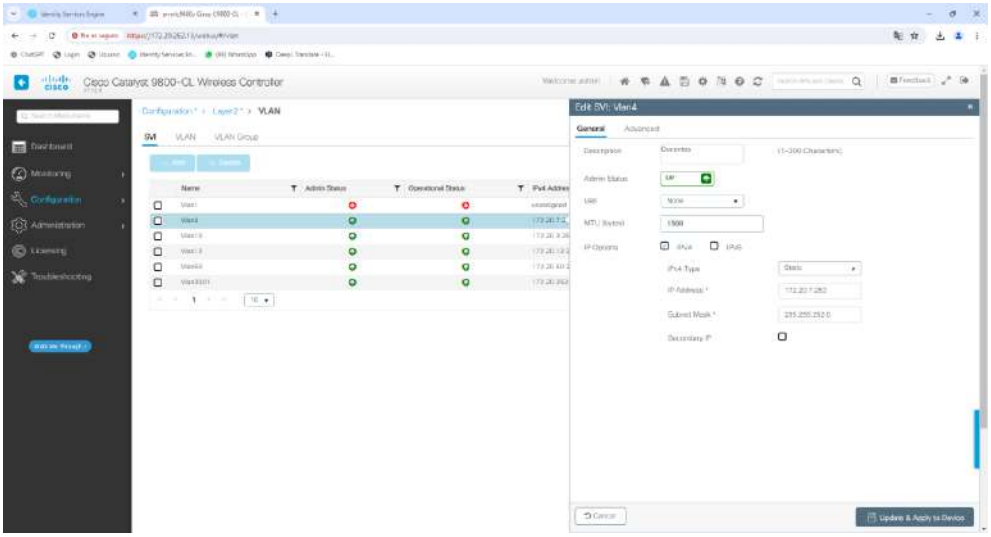

Figura 39. Se puede observar las características asignadas a la VLAN4 a usarse

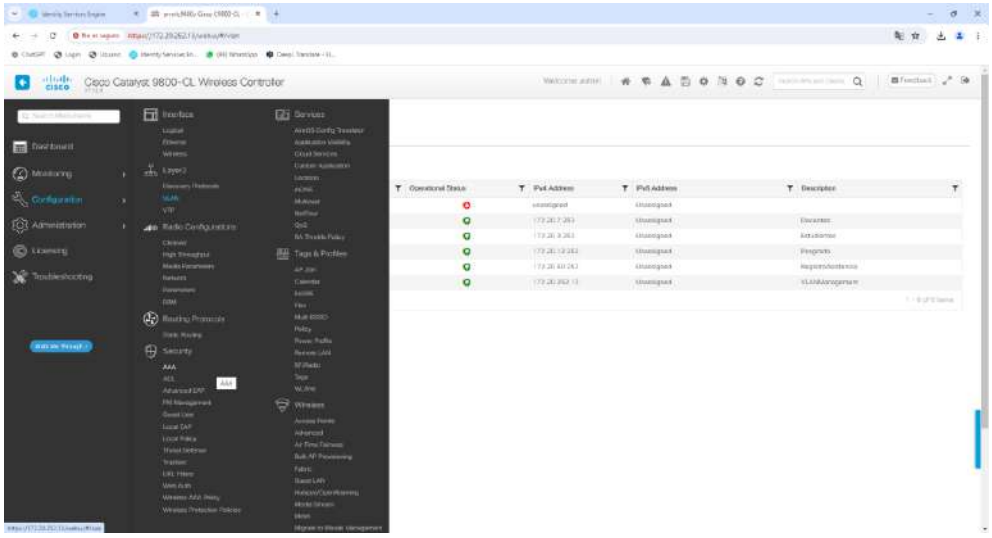

Figura 40. Seguido se ira por la configuración dentro del apartado de Security -- AAA

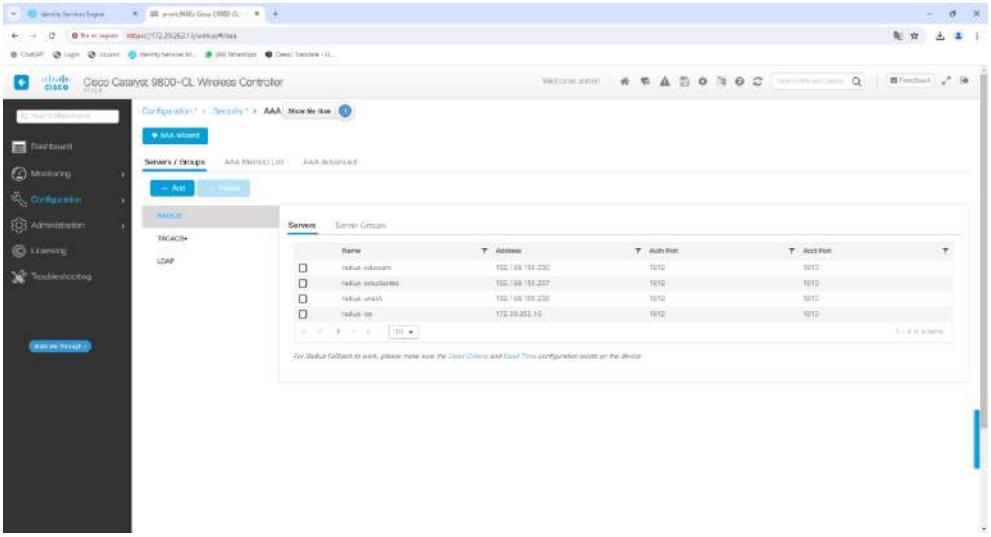

Figura 41. Se procedió a la creación del perfil AAA llamado radius-ise asignándole la dirección IP (172.20.252.16)

- Auth Port 1812: Utilizado para la autenticación de usuarios.
- Acct Port 1813: Utilizado para la contabilidad y el registro de la actividad de los usuarios.

Estos puertos son esenciales para el funcionamiento de los servidores RADIUS, proporcionando seguridad y control sobre quién accede a la red y cómo se utiliza la red una vez que el acceso ha sido otorgado.

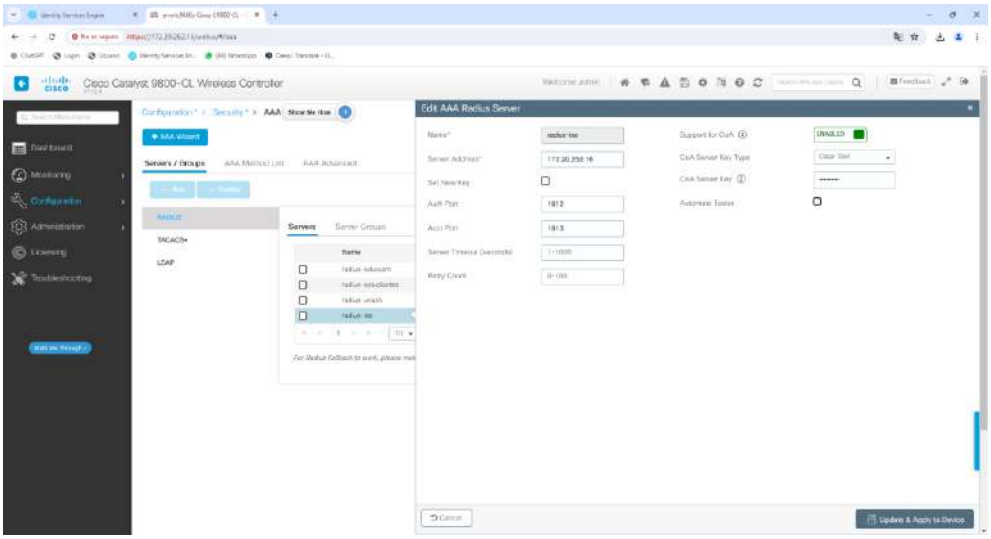

Figura 42. Se asigna una clave al CoA Server Key la que será la misma asignada al protocolo Radius (UNACH2024.)

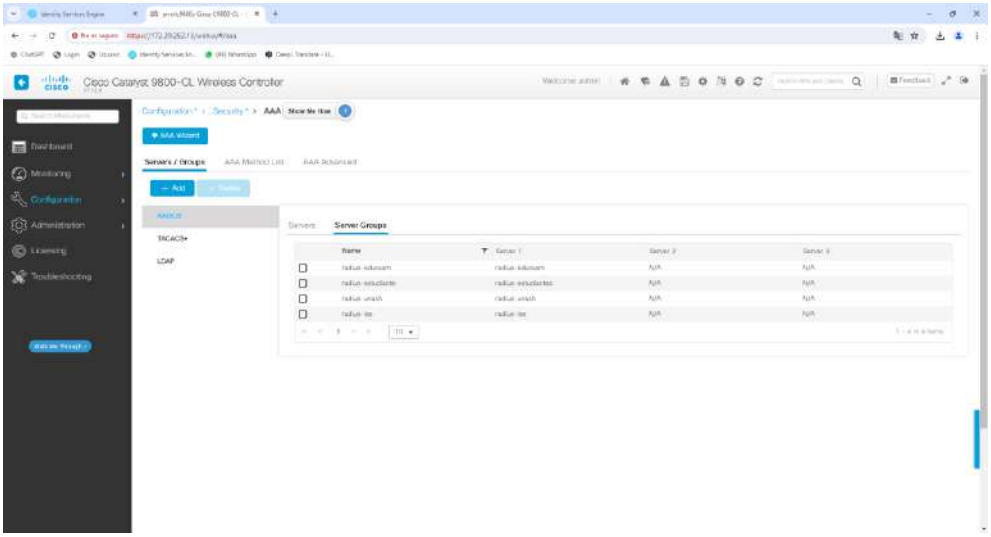

Figura 43. Una vez creado el objeto ISE se declara en un grupo de servidores Radius

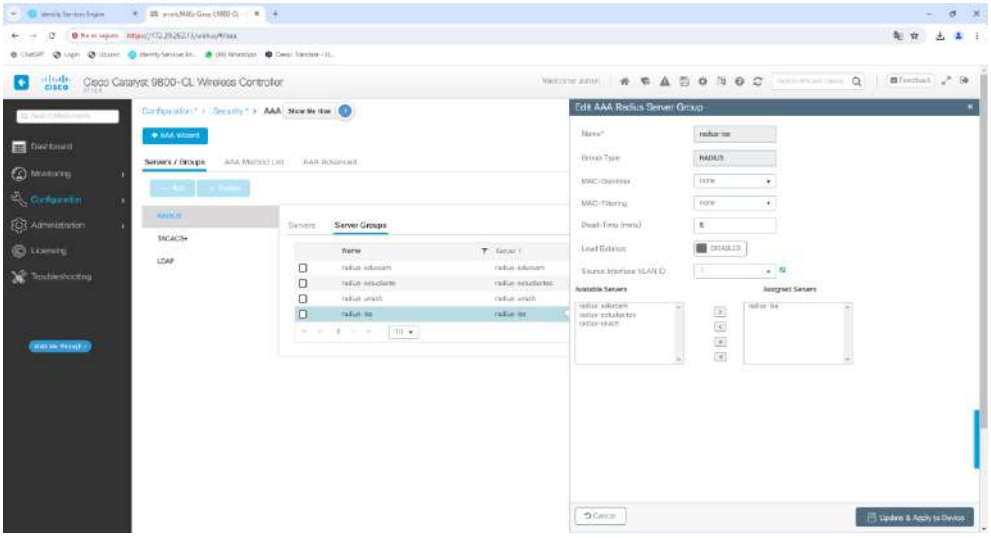

Figura 44. Una vez creado el grupo de radius, de los servidores radius creados tomaremos el servidor ISE creado para las pruebas exclusivamente

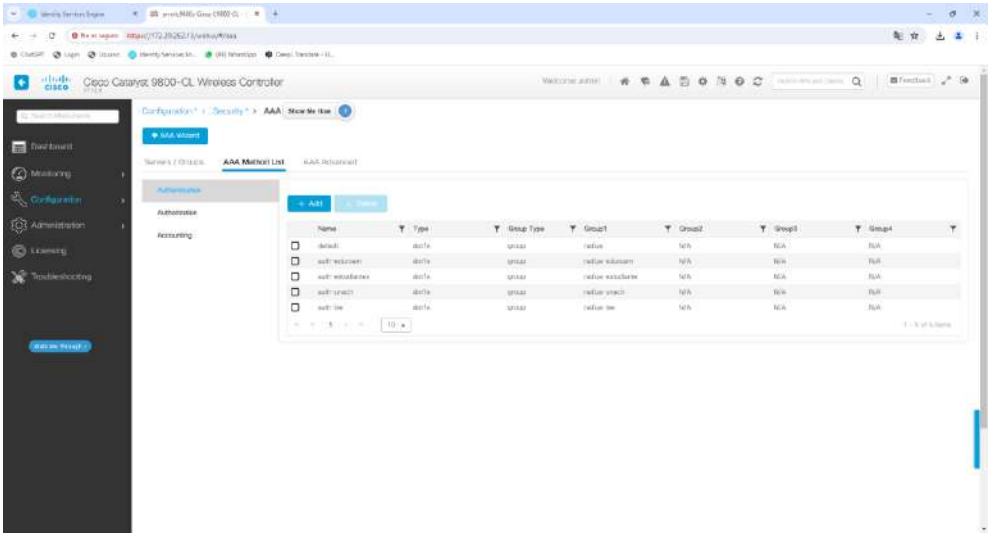

Figura 45. Una vez creado los servidores seguimos con la creación de un objeto en la lista de autenticación con el nombre auth-ise

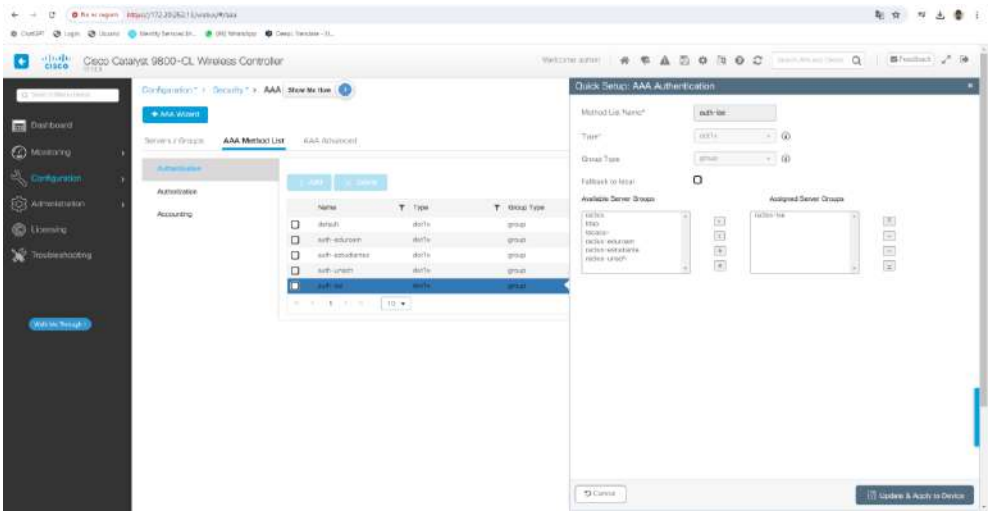

Figura 46. De igual manera de todos los servidores radius disponibles asignamos el creado con los fines específicos radius-ise

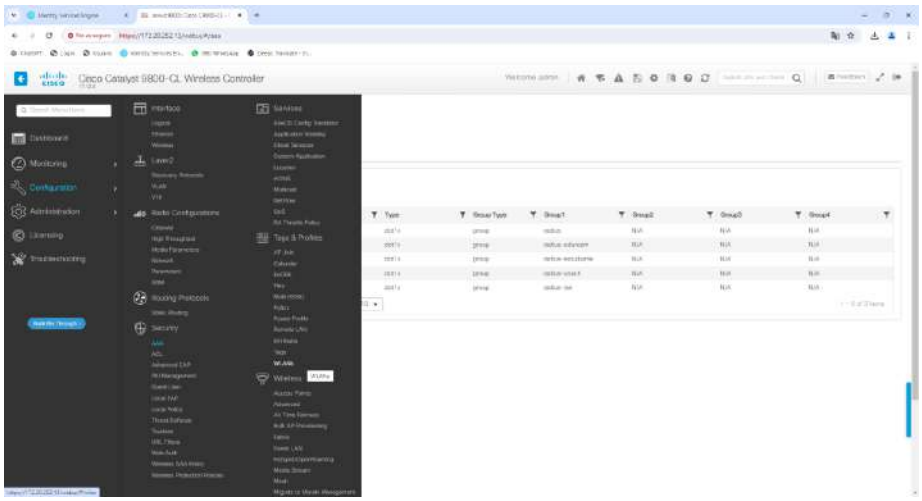

Figura 47. Seguido se prosigue con la configuración de las WLANs

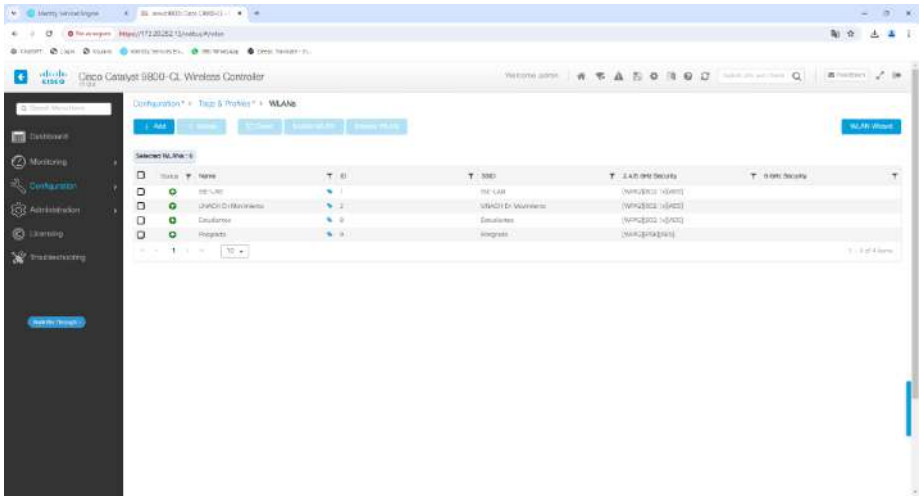

Figura 48. Se prosiguió a crear una WLANs con el nombre ISE-LAB con el SSID del mismo nombre

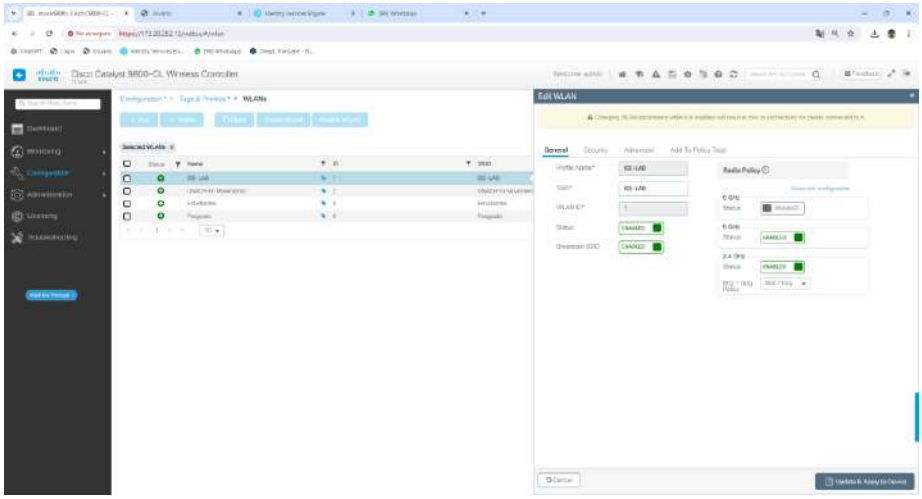

Figura 49. Características de la WLANs y SSID (ISE-LAB)

Dentro de sus configuraciones se deshabilito el uso del 6 GHz por la falta de dispositivos que soporten tal tecnología lo que no es el caso de la banda 5 GHz y 2.4 GHz. Además, coloco en estado activo el Status y el Broadcast SSID estos permiten:

- **Enable Status:** Controla si la WLAN está activa (permitiendo conexiones) o inactiva.
- **Broadcast SSID:** Controla si el SSID de la WLAN se anuncia públicamente (haciendo que la red sea visible para todos los dispositivos).

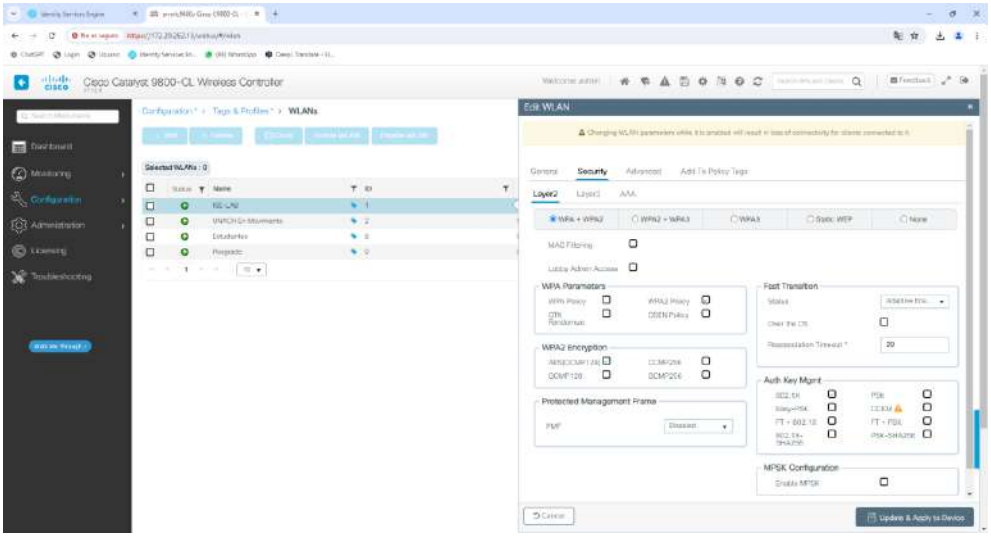

Figura 50. Configuraciones de seguridad de nuestra WLANs

Esta combina la robustez de WPA2 con la flexibilidad de métodos de autenticación tanto 802.1X como PSK, además de soporte para transiciones rápidas que mejoran la experiencia de movilidad del usuario. La encriptación AES-CCMP proporciona un alto nivel de seguridad.

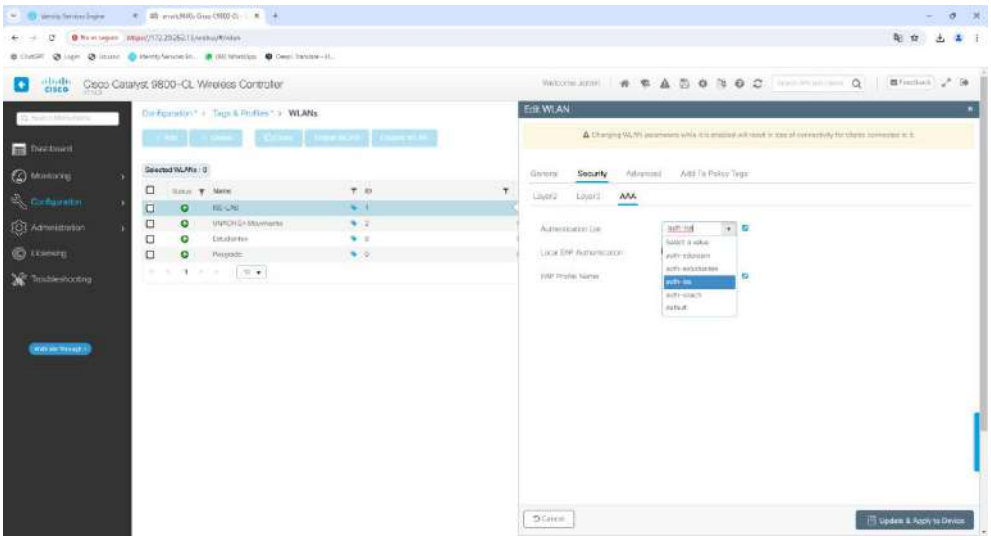

Figura 51. Dentro de la configuración especifica de seguridad AAA en la lista de autenticación elegimos la autorización creada para este propósito especifico.

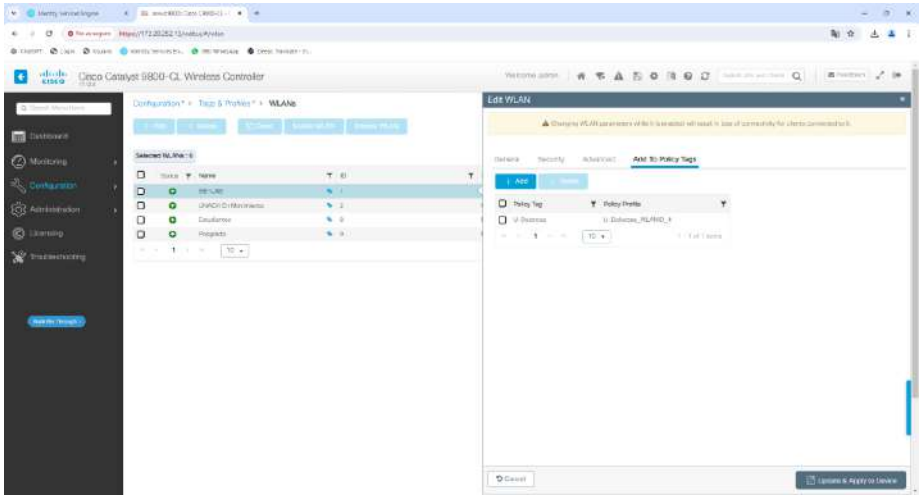

Figura 52. Esta configuración en la pestaña Add To Policy Tags es fundamental para gestionar y aplicar políticas de red específicas a la WLAN.

Al asignar un Policy Tag y un Policy Profile, se agrupan y se aplican configuraciones de red de manera consistente y eficiente, lo que facilita la administración y mejora la seguridad y el rendimiento de la red inalámbrica.

- Policy Tag U-Dolorosa: Agrupa la WLAN con otras que comparten políticas similares.
- Policy Profile U-Dolorosa_WLANID_4: Define las configuraciones específicas de la política que se aplicarán a la WLAN.

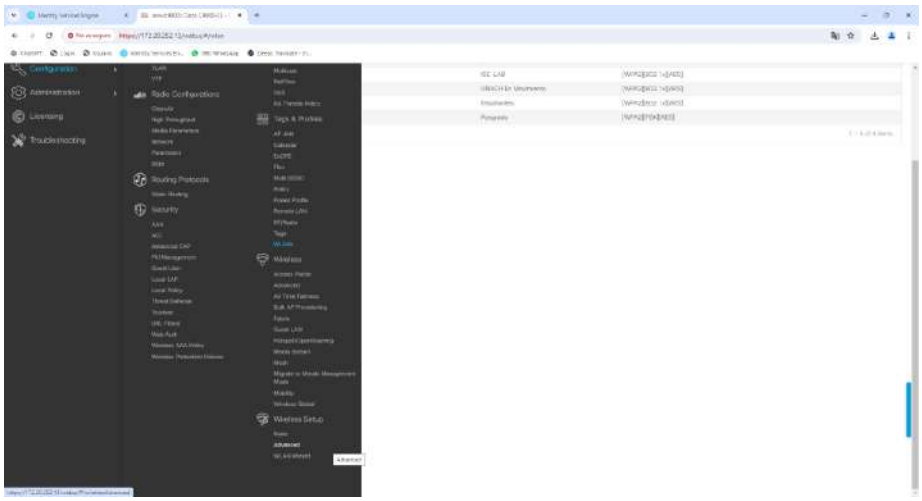

Figura 53. Por último, nos dirigimos a publicar todas nuestras configuraciones

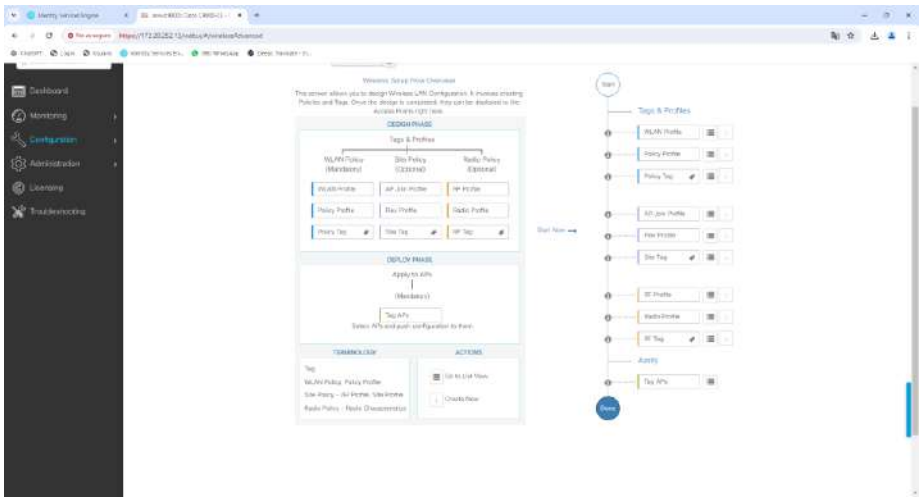

Figura 54. Se seguirá con el Taggeo o etiquetación

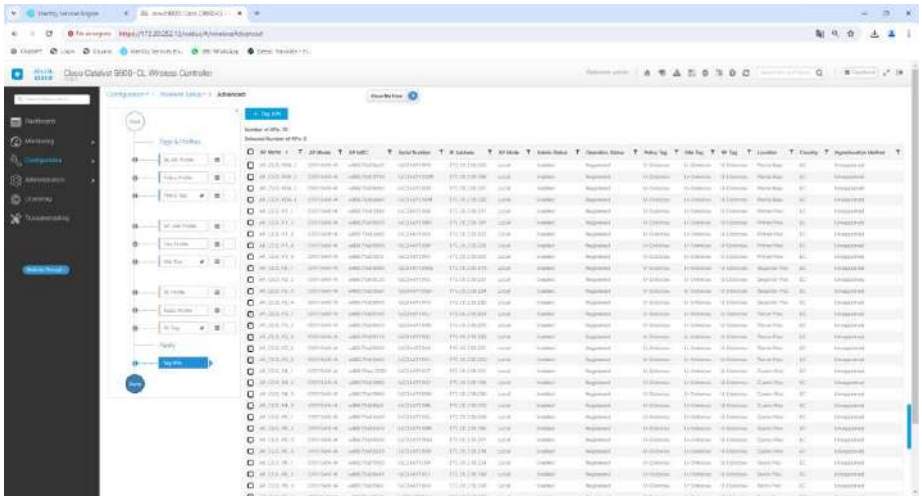

Figura 55. Para efectos de prueba etiquetamos a todos los AP que están instalados en el Piso 3 del bloque U Campus "Dolorosa" para que por ellos se difunda la configuración.

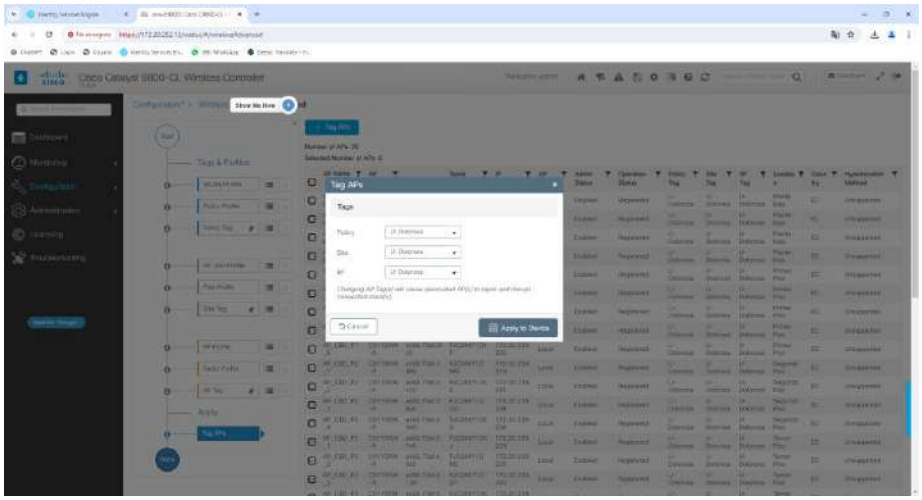

Figura 56. Se colocan los tagg creados que la controladora le va a asignar a los AP donde por medio de los taggs definiremos policy, site y RF.

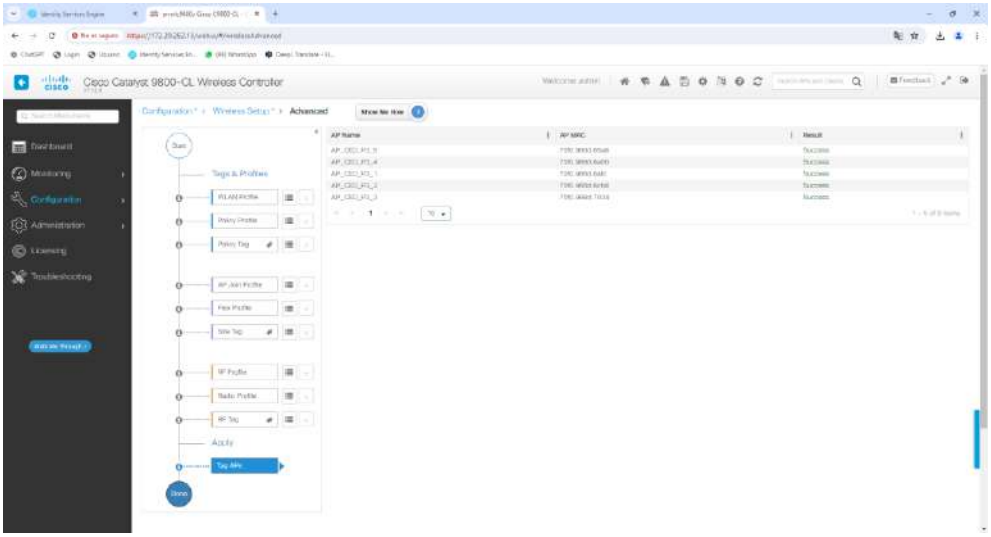

Figura 57. Por último, vemos que la etiquetación se asignó a los AP con éxito.

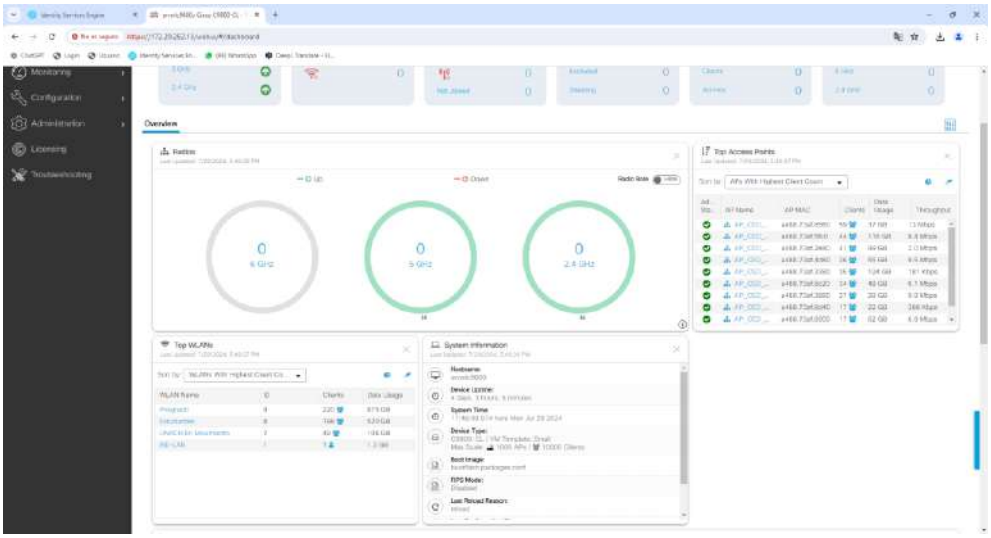

Figura 58. Aquí se puede observar a la publicación exitosa de nuestro WLANs y la vinculación de un dispositivo de prueba en nuestro SSID (ISE-LAB)

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1 Comparación y Evaluación de Cisco ISE vs FreeRADIUS

Cisco ISE Cisco Identity Services Engine (ISE)

Podemos decir que basado en la experiencia al usar este decimos que es un avanzado motor de políticas diseñado para decidir y gestionar el acceso a la red. Utiliza múltiples puntos de datos para determinar quién debe tener acceso y se integra de manera estrecha con los equipos de red de Cisco para implementar estas decisiones. Parte de este proceso incluye que el servidor RADIUS integrado canalice las autenticaciones de sistemas y dispositivos hacia un servicio de directorio.

Una de las mayores ventajas de Cisco ISE es la visibilidad completa que proporciona a los administradores de TI sobre la red. Permite ver en tiempo real quién está conectado, qué usuarios están utilizando (estudiantes o docentes), su ubicación, si la conexión es cableada o inalámbrica, y los tipos de aplicaciones que están utilizando. Toda esta información se presenta en una interfaz gráfica de usuario intuitiva, facilitando la gestión de la red a través de simples acciones de apuntar y hacer clic.

Sin embargo, uno de los principales inconvenientes de Cisco ISE es su alto costo. Además, su uso tiende a requerir una gama de productos Cisco, lo que resultar una ventaja tomando el caso de implementación de prueba en el bloque “U” del campus “Dolorosa” que cuenta en su totalidad con equipos de la marca Cisco.

FreeRADIUS

Por otro lado, FreeRADIUS es una solución de código abierto ampliamente reconocida por su robustez como servidor RADIUS. Es accesible de forma gratuita y su implementación requiere de mucho tiempo y habilidades técnicas. A diferencia de Cisco ISE, FreeRADIUS no funciona como un motor de políticas que decide el acceso, sino que actúa principalmente como un mecanismo de control de acceso que utiliza información de otras soluciones, especialmente de proveedores de identidad (IdP).

Aunque FreeRADIUS no ofrece el mismo nivel de visibilidad sobre la red que Cisco ISE, su flexibilidad es notable. Puede ejecutarse en una amplia variedad de hardware y sistemas operativos basados en Linux, como Ubuntu, Red Hat y Debian, eliminando la necesidad de hardware especializado y permitiendo su uso con una diversidad de

infraestructuras, no solo las de Cisco.

No obstante, FreeRADIUS presenta algunas desventajas. Generalmente se administra a través de una línea de comandos, lo que puede resultar desafiante para algunos administradores de TI. Además, aunque es de código abierto y su uso básico es gratuito, existen costos asociados con la configuración y puesta en marcha del servidor, así como con su adaptación específica al entorno de la red.

4.2 Comparación de FreeRadius frente a Cisco ISE mediante la escala de Likert

Denominación	Peso cuantitativo
Muy alta	5
Buena	4
Media	3
Baja	2
Muy baja	1

Tabla 7. *Denominación de valores de la escala de Likert*

Descripción	FreeRadius	Cisco ISE
Características	3	5
Soporte	2	5
Recursos necesarios	5	3
Implementación	2	4
Costos	4	2
Total	16	19

Tabla 8. *Escala de pesos mediante la escala de Likert*

4.3 Discusión Final

En la comparación entre Cisco ISE y FreeRADIUS para proponer una solución de mejora a la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo. Cisco ISE se destaca por sus características avanzadas, soporte técnico, y facilidad de implementación. Ofrece una visibilidad completa de la red, una interfaz gráfica intuitiva y una integración fluida con otros productos de Cisco, lo que simplifica la gestión y mejora la seguridad. Sin embargo, estas ventajas vienen con altos costos y la necesidad de utilizar productos específicos de Cisco, lo que puede limitar la flexibilidad y aumentar los gastos (este no es el caso del bloque “U” que cuenta con infraestructura Cisco en su totalidad).

Por otro lado, FreeRADIUS es una solución flexible y de bajo costo inicial, adecuada para diversas infraestructuras. A pesar de su menor visibilidad y mayor complejidad de gestión, su naturaleza de código abierto permite una implementación adaptable y económica.

CAPÍTULO V. CONCLUSIONES y RECOMENDACIONES

5.1 Conclusiones

- Al realizar un estudio de las principales tecnologías de autenticación autorización y contabilidad AAA entre ellas se estudió Cisco ISE dentro de esta pudimos evidencia los distintos mecanismos de autenticación de usuarios que estas herramientas nos provee como lo son Radius y TACACS+.
- Al realizar el estudio comparativo de los métodos de autenticación que Cisco ISE nos provee como los son Radius vs TACACS+ estas nos proporcionan diferentes tipos de mecanismos de autenticación para redes inalámbricas como lo son autenticación basada en EAP, MD5, usuario y contraseña, directorio activo entre otras, ya es decisión propia cual de estos métodos se alinea mejor a los requerimientos en nuestro caso se optó por el uso Cisco ISE mediante el método de autenticación Radius ya que esta provee el acceso controlado a la red mientras que TACACS+ provee el acceso controlado a los dispositivo de administración de la red.
- La implementación de Cisco ISE mediante el uso de un servidor Radius como método de autenticación en el entorno de prueba controlado fue una herramienta eficaz para constatar las necesidades en el campo de la autenticación de usuarios se tenían por el uso de una solución de código abierto como lo es FreeRadius.
- Se puede concluir mediante la evaluación de la implementada Cisco ISE frente a la actualmente usada por la universidad como lo es FreeRadius, que la herramienta propietaria de Cisco se debería tomar en cuenta si se desea hacer una mejora en el tema de seguridad AAA por parte de la Universidad, destacamos sus avanzadas características en el campo de la contabilidad, soporte técnico y facilidad de implementación sin embargo sus altos costes son un defecto a tomar en cuenta, frente a esta encontramos una solución flexible y de bajo costo inicial como es FreeRadius a pesar de su menor visibilidad, altos costes en materia de soporte y mayor complejidad de gestión.

5.2 **Recomendaciones**

- Para maximizar el aprovechamiento de las capacidades que ofrece Cisco Identity Services Engine (ISE), se recomienda implementar una infraestructura compuesta exclusivamente por dispositivos Cisco, que abarque desde la capa de core hasta la capa de acceso. Esta integración permite utilizar de manera óptima las funcionalidades avanzadas de ISE, tales como la descarga de Listas de Control de Acceso (ACL), la asignación dinámica de VLANs, la re-autenticación de usuarios y la integración de Redes Privadas Virtuales (VPN) a través de dispositivos ASA. La implementación de una infraestructura heterogénea puede limitar significativamente los beneficios que ISE es capaz de proporcionar, dado que muchas de sus características avanzadas están diseñadas para operar de manera más eficaz en un entorno completamente Cisco.
- Se recomienda tener un conocimiento sólido en áreas relacionadas con la seguridad de redes, hipervisores, ciberseguridad, topologías de red, direccionamiento y otros temas pertinentes. Un entendimiento profundo de estos conceptos es fundamental para optimizar el uso de la herramienta y garantizar su correcta configuración y operación dentro del entorno de red de la universidad.
- Es aconsejable que el personal encargado de la implementación tenga conocimientos básicos sobre dispositivos Cisco, incluyendo controladores de puntos de acceso (AP) y otros equipos relevantes. Este conocimiento específico facilitará considerablemente la implementación y la gestión efectiva de Cisco ISE, al asegurar que el personal esté familiarizado con la configuración y operación de los dispositivos que interactuarán con la solución de AAA.
- En el caso de que la implementación de Cisco ISE no se realice utilizando dispositivos locales, se recomienda adquirir un conocimiento moderado en la configuración y gestión de Active Directory u otros métodos de autenticación externa. Esto es crucial para asegurar una integración fluida entre Cisco ISE y los sistemas de autenticación existentes, lo que garantizará la correcta sincronización y el funcionamiento eficiente del sistema de control de acceso.

- Se sugiere utilizar dispositivos con altas capacidades de procesamiento computacional para la implementación de Cisco ISE y del controlador de red inalámbrico WLC 9800-CL, especialmente si estos se implementan en un entorno de hipervisor. La capacidad computacional asignada a los sistemas virtualizados debe ser equivalente a la requerida para los equipos físicos, para asegurar que el rendimiento y la estabilidad del sistema sean adecuados y cumplan con los requisitos de la red universitaria.

BIBLIOGRÁFIA

[1] S. J. E. Pilicita, *"DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD A.A.A (AUTHENTICATION AUTHORIZATION AND ACCOUNTING) EN LAS REDES WI-FI DEL GAD MUNICIPAL DEL CANTÓN MEJÍA",* Latacunga: UNIVERSIDAD TÉCNICA DE COTOPAXI , 2019.

[2] E. Espinoza, *Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS,* Lima: Universidad Nacional Mayor de San Marcos , 2018.

[3] A. Otero, *"Herramienta de auditoría de seguridad en redes inalámbricas para pequeñas empresas",* Coruña: Universidade da Coruña, 2021.

[4] F. P. Diez, «Advanced aaa system for interoperable distributed architectures,» Universidad Carlos III de Madrid, Madrid, 2020.

[5] N. Lazo, «DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN CON SISTEMA DE CONTROL DE ACCESO MEDIANTE SERVIDORES AAA,» PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ , Lima, 2012.

[6] Y. Alvarado, «DESARROLLO DE UN MECANISMO AGIL DE AUDITORIA A LA SEGURIDAD INFORMATICA DE LA RED INALAMBRICA,» Universidad Espíritu Santo, Guayaquil, 2017.

[7] C. P. Sanchez Almeida, «"Sistema de autenticación y políticas de seguridad mediante un servidor AAA, haciendo uso del estándar IEEE 802.1 X y los protocolos radius para la red institucional de la unidad educativa "San Juan Diego" en la ciudad de Ibarra ",» *Universidad Pontifica del Ecuador,* 2023.

[8] S. Perez, «Conociendo el concepto de AAA en el ámbito de la seguridad informática.,» HUAWEI, 19 Octubre 2022. [En línea]. Available: https://forum.huawei.com/enterprise/es/conociendo-el-concepto-de-aaa-en-el-%C3%A1mbito-de-la-seguridad-inform%C3%A1tica/thread/667218838057533440-667212881550258176. [Último acceso: 5 Agosto 2024].

[9] V. P. Kriss Chichay, «Comparación de protocolos de autenticación de usuarios en el control de acceso a redes inalámbricas,» Universidad Nacional Pedro Ruiz Gallo, Lambayeque, 2021.

[10] J. Kim, I. Lee y S. Noh, «VoIP QoS(Quality of Service) Diseño del Modelo de Proceso de Gestión de la Medición,» IEEE Explorer, 2010.

[11] S. Banquete, *"Implementación de un módulo didáctico para la administración y seguridad en redes de datos WLAN aplicado a la asignatura de redes inalámbricas de la carrera de ingeniería en computación y redes",* Jipijapa: Universidad estatal del sur de Manabí, 2019.

[12] K. Carhuaz, *"La seguridad en redes inalámbricas",* Lima: UNIVERSIDAD NACIONAL DE EDUCACIÓN Enrique Guzman y Valle, 2021.

[13] C. Gonzales, *"Desafíos de Seguridad en Redes 5G",* Chiriquí: Universidad Autónoma de Chiriquí , 2019.

[14] J. Marquez, «"Riesgos y vulnerabilidades de la denegación de servicio",» *Revista de Bioética y Derecho,* p. 100, 2019.

[15] A. Navarro, *"Diseño de una infraestructura de red WAN segura con un servidor de autenticación AAA basado en el protocolo TACACS+ para la empresa Sintelcom",* Huancayo: Escuela Académico Profesional de Ingeniería de Sistemas e Informática, 2020.

[16] N. Vargas, *"MODELO DE CONTROL DE ACCESO Y SEGURIDAD EN REDES WLAN Y WI-FI",* La Paz: UNIVERSIDAD MAYOR DE SAN ANDRÉS, 2015.

[17] D. Ñauta y J. Vizñay, «Acceso y seguridad a la red wifi mediante la tecnología CISCO identity services engine (ise) para los,» *Polo de Conocimiento,* vol. 5, nº 02, p. 697, 2020.

[18] O. M. y. O. Morales, «Estudio de la tecnología Cisco Identity Services Engine (ISE) para mejorar la seguridad de los usuarios de la infraestructura WLAN de la ESPOCH.,» Escuela Superior Politécnica de Chimborazo, Riobamba, 2017.

[19] CISCO, «Politicas de ISE,» 2018. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_introduction.html. [Último acceso: 18 Abril 2024].

[20] A. Sanchez, «Diseño de solución para el control de acceso y movilidad a partir del protocolo 802.1x empleando la plataforma ISE de Cisco,» Universidad Santo Tomas, Bogota, 2017.

[21] CISCO, «CISCO ISE LICENCIAS,» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/security/ise. [Último acceso: 19 Abril 2024].

[22] I. Alonso, «Análisis comparativo de dos protocolos para control de acceso y administración de equipos de telecomunicaciones,» Universidad Catolica de Colombia, Bogota, 2013.

[23] I. U. Khan, «CCNA PRACTICAL LABS,» [En línea]. Available: https://ccnapracticallabs.com/fortify-your-network-the-ultimate-guide-to-tacacs-server-implementation/. [Último acceso: 25 Abril 2024].

[24] J. L. D. Guzmán, «CISCO Learning Institute,» 2009. [En línea]. Available: www.ciscolearning.org. [Último acceso: 25 Abril 2024].

[25] G. Andrade, *"ANÁLISIS DE PRESTACIONES DE LOS PROTOCOLOS DE AUTENTICACIÓN REMOTA RADIUS Y TACACS+ EN INFRAESTRUCTURA DE COMUNICACIONES CORPORATIVAS",* Riobamba: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, 2019.

[26] G. A. A. Tubun, «"ANÁLISIS DE PRESTACIONES DE LOS PROTOCOLOS DE,» ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, Riobamba, 2019.

[27] G. R. J. R. Gabrile Huaman, «Propuesta de implementación de políticas de seguridad basado en CISCO ISE (identity services engine) en la red LAN de Caja Huancayo,» Universidad Continental, Huancayo, 2022.

[28] A. Sanchez, «Diseño de solución para el control de acceso y movilidad a partir del protocolo 802.1x empleando la plataforma ISE de Cisco,» Universidad Santo Tomas, Bogotá, 2017.

[29] CISCO.USA, «Examine how the RADIUS Works,» CISCO, San Francisco, 2024.

[30] CISCO, «RADIUS Configuration Guide,» CISCO, San Francisco, 2016.

[31] ClodRadius, «Everything You Need to Know About RADIUS Server Authentication,» Securew2, 2024.

[32] Wikipedia, «Radius,» 2024.

[33] CISCO, «Ccontrolador inalámbrico Cisco Catalyst 9800-CL,» CISCO, 09 Febrero 2023. [En línea]. Available: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-cl-wireless-controller-cloud/nb-06-cat9800-cl-cloud-wirel-data-sheet-ctp-en.html. [Último acceso: 03 Junio 2024].

[34] CISCO, «Configuration Guide,» CISCO, [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Configuration/3-2/b_GUI_KVM_VM-FEX_UCSM_Configuration_Guide_3_2/b_GUI_KVM_VM-FEX_UCSM_Configuration_Guide_3_2_chapter_00.pdf. [Último acceso: 03 Junio 2024].

[35] A. ALVAREZ, «Clasificación de las Investigaciones,» Universidad de Lima, Lima, 2020.

[36] R. Hernandez, "Definición del alcance de la investigación que se realizará: exploratorio, descriptivo, correlacional o explicativo.", Ciudad de Mexico: McGraw-Hill, 2014.

[37] M. Albayero, M. Tejada y J. d. J. Cerritos, «"Una aproximación teórica para la aplicación de la metodología del enfoque mixto en la investigación en enfermería",» *Revista Entorno,* vol. 1, nº 69, p. 50, 2020.

[38] L. Mucha, R. Chamorro, M. Oseda y R. Alania, «"Evaluación de procedimientos empleados para determinar la población y muestra en trabajos de investigación de posgrado",» *Revista Cientifica de Ciencias Sociales y Humanindades,* vol. 12, nº 1, pp. 50-51, 2020.

[39] P. Condori, «"Universo, población y muestra.",» Universidad Nacional de Juliaca, Juliaca, 2020.

[40] E. Espinoza, «LAS VARIABLES Y SU OPERACIONALIZACIÓN EN LA INVESTIGACIÓN EDUCATIVA.,» *Revista pedagógica de la Universidad de Cienfuegos,* vol. 14, nº 65, pp. 39-49, 2018.

[41] L. Fornetti y V. Martello, «Las variables en investigacion,» Universidad Nacional de la Plata, La Plata, 2021.

[42] NetworkRadius, «NetworkRadius,» 2021. [En línea]. Available: https://www.networkradius.com/support/. [Último acceso: 5 Agosto 2024].

ANEXOS

Anexo 1.- Costo del soporte de FreeRadius

Fuente: [42]

Anexo 2.- Precio estimado de costo de licencias Cisco ISE.

All Prices Shown in USD

Part Number	Description	Service Duration (Months)	Estimated Lead Time (Days)	Unit List Price	Pricing Term	Qty	Unit Net Price	Disc(%)	Extended Net Price
ISE-SEC-SUB	Cisco Identity Service Engine Subscription	--	N/A	0.00		1	0.00	0.00	0.00
Initial Term - 36.00 Months | Auto Renewal Term - 12 Months | Billing Model - Prepaid Term | Requested Start Date - 10-Aug-2024 | Requested End Date - 09-Aug-2027									
ISE-E-LIC	Cisco Identity Service Engine Essentials Subscription	---	3	2.31	12	1000	2.31	0.00	6,930.00
SVS-ISE-SUP-B	Basic Support for Identity Service Engine Subscription	---	N/A	0.00	1	1	0.00	0.00	0.00
L-ISE-TACACS-ND=	Cisco ISE Device Admin Node License	---	3	10,700.00		1	10,700.00	0.00	10,700.00
R-ISE-VMC-K9=	Cisco ISE Virtual Machine Common PID	---	7	6,420.00		1	6,420.00	0.00	6,420.00
CON-ECMUS-RISE9KVM	SOLN SUPP SWSS Cisco ISE Virtual Machine Common PID	12	N/A	2,118.88		1	2,118.88	0.00	2,118.88

Product Total	17,120.00
Service Total :	2,118.88
Subscription Total	6,930.00
Total Price:	**26,168.88**

Signed: _____

Cristian Javier Solis Aguirre

Fuente: [43]

Sr. Cristian Javier Solís Aguirre

ESTUDIANTE

C.I. 0604573956