Universidad Nacional de Ingeniería

Facultad de Ingeniería Mecánica

Tesis

Análisis Comparativo de los Protocolos RADIUS y TACACS+ en el Control de Acceso Centralizado a la Configuración de Switches.

Para Obtener el Título Profesional de Ingeniero Mecatrónico

Elaborado por

Cynthia Mori Córdova

0009-0006-6154-7570

Asesor

Mg. Alcides Guillermo Joo Aguayo

0000-0002-8459-8489

LIMA – PERÚ

2025

Citar/How to cite	(Mori, 2025)
Referencia/Reference Estilo/Style: APA (7ma ed.)	Mori, C. (2025). *Análisis Comparativo de los Protocolos RADIUS y TACACS+ en el Control de Acceso Centralizado a la Configuración de Switches.* [Tesis, Universidad Nacional de Ingeniería]. Repositorio institucional Cybertesis UNI.

Dedicatoria

Dedico este trabajo a mi madre, quien constantemente me ha impulsado a salir adelante a través de sus consejos y amor incondicional.

Agradecimientos

Quisiera expresar mi más sincero agradecimiento a todas las personas que hicieron posible la realización de este trabajo. En primer lugar, a mi madre, por su inquebrantable apoyo, amor y motivación constante, que fueron el motor principal para culminar esta tesis. Asimismo, mi profundo agradecimiento a mi asesor, cuya guía, conocimiento y dedicación fueron fundamentales para el desarrollo y la dirección de esta investigación.

Lista de Contenidos

Lista de Figuras

Lista de Tablas

Resumen

El presente trabajo de investigación analiza y compara los protocolos de autenticación, autorización y auditoría (AAA) RADIUS y TACACS+ para determinar cuál ofrece mejor desempeño, seguridad y disponibilidad en el acceso de forma centralizada a la configuración un switch. La investigación es de tipo aplicada, enfoque cuantitativo, nivel descriptivo y diseño cuasi-experimental.

La muestra está conformada por dos sistemas AAA implementados, uno basado en RADIUS y otro en TACACS+. Los datos se recolectan mediante la técnica experimental, utilizando como instrumentos las interfaces de línea de comandos del switch y el servidor AAA, así como las herramientas de análisis de tráfico de red Wireshark y tcpdump. El análisis se realiza mediante la comparación de métricas asociadas al desempeño, seguridad y disponibilidad de cada protocolo.

Los resultados demuestran que RADIUS presenta mejor desempeño operacional al generar menor número de paquetes, volumen de datos y latencia en la red. RADIUS generó 2 paquetes con un tamaño total de 226 bytes, mientras que TACACS+ generó 22 paquetes con 1517 bytes transmitidos. La latencia promedio registrada con RADIUS es de 0.137 segundos, frente a los 0.169 segundos de TACACS+. No obstante, TACACS+ demostró un nivel superior de seguridad, ya que presenta un mayor porcentaje de cifrado en los paquetes AAA. Asimismo, TACACS+ ofrece un control más granular de privilegios, permitiendo denegar hasta el 95.2% de los comandos ejecutables por un usuario con nivel de privilegio 1, característica inexistente en RADIUS. En cuanto a auditoría, TACACS+ generó 10 paquetes de registro, incluyendo los comandos ejecutados por el usuario, mientras que RADIUS registró únicamente el inicio y cierre de sesión con 4 paquetes. En términos de disponibilidad, TACACS+ presentó un tiempo promedio de conmutación (fail-over) de 1.570 segundos, significativamente menor que el registrado por RADIUS (40.259 segundos), evidenciando una mejor capacidad de recuperación ante fallos.

Se concluye que TACACS+ ofrece ventajas sustanciales en seguridad y disponibilidad

del servicio AAA, mientras que RADIUS mantiene un desempeño operativo más eficiente. Esta comparación aporta evidencia técnica relevante para la selección del protocolo más adecuado según las necesidades específicas de rendimiento o seguridad en entornos de red corporativos.

***Palabras clave*:** TACACS+, RADIUS, AAA, desempeño, seguridad, disponibilidad.

Abstract

This research study analyzes and compares the authentication, authorization, and accounting (AAA) protocols RADIUS and TACACS+ to determine which one offers better performance, security, and availability in centralized access to switch configuration. The study is applied in nature, with a quantitative approach, descriptive level, and a quasi-experimental design.

The sample consists of two implemented AAA systems: one based on RADIUS and the other on TACACS+. Data were collected through an experimental technique, using as instruments the command-line interfaces (CLI) of the switch and the AAA server, as well as the Wireshark and tcpdump network traffic analysis tools. The analysis was carried out by comparing metrics associated with the performance, security, and availability of each protocol.

The results show that RADIUS exhibits better operational performance by generating a smaller number of packets, lower data volume, and reduced network latency. RADIUS generated 2 packets with a total size of 226 bytes, while TACACS+ generated 22 packets with 1517 bytes transmitted. The average latency recorded with RADIUS was 0.137 seconds, compared to 0.169 seconds with TACACS+. However, TACACS+ demonstrated a higher level of security, as it achieved a greater percentage of encryption in AAA packets. Likewise, TACACS+ provides more granular privilege control, allowing up to 95.2% of commands executable by a privilege level 1 user to be denied— a feature not available in RADIUS. Regarding auditing, TACACS+ generated 10 log packets that included user-executed commands, whereas RADIUS recorded only session start and end events with 4 packets. In terms of availability, TACACS+ achieved an average failover time of 1.570 seconds, significantly lower than that of RADIUS (40.259 seconds), demonstrating superior fault recovery capability.

In conclusion, TACACS+ offers substantial advantages in AAA service security and availability, while RADIUS maintains higher operational performance efficiency. This comparison provides relevant technical evidence for selecting the most appropriate protocol

according to specific performance or security requirements in corporate network environments.

Keywords**:** TACACS+, RADIUS, AAA, performance, security, availability.

INTRODUCCIÓN

Entre los protocolos más utilizados para la gestión de autenticación, autorización y auditoría se encuentran RADIUS y TACACS+. Ambos proporcionan mecanismos para autenticar usuarios, autorizar sus privilegios y registrar sus actividades, pero difieren en su arquitectura, en el tipo de cifrado que utilizan y en la forma en que manejan las transacciones entre el cliente y el servidor. Estas diferencias pueden impactar significativamente en el desempeño, la seguridad y la disponibilidad del servicio de autenticación en entornos empresariales.

El presente trabajo de investigación compara estos protocolos para determinar cuál de ellos ofrece un mejor rendimiento operativo y mayor nivel de seguridad y disponibilidad en el acceso centralizado a la configuración de un switch.

La investigación está estructurada en cuatro capítulos. En el **Capítulo I** se presentan los aspectos generales de la investigación, incluyendo los antecedentes, la identificación y descripción del problema, la formulación del problema (general y específicos), la justificación e importancia del estudio, los objetivos (general y específicos), las hipótesis (general y específicas), la operacionalización de las variables y la metodología.

El **Capítulo II** desarrolla el marco teórico y conceptual que sustenta la estudio, abordando conceptos técnicos y académicos relacionados con redes de comunicación y el control de acceso.

En el **Capítulo III** se describe el desarrollo del trabajo de investigación, detallando los componentes que integran los sistemas implementados para el estudio de los protocolos TACACS+ y RADIUS, así como la arquitectura de ambos y el detalle de su configuración.

El **Capítulo IV** expone los resultados obtenidos a partir de la comparación entre el sistema basado en el protocolo RADIUS y el sistema basado en TACAS+, con el fin de evaluar específicamente a cada protocolo en cuanto a su desempeño, nivel de seguridad y disponibilidad. En esta sección también se validan las hipótesis planteadas (general y específicas) y se discuten los resultados obtenidos en relación con estudios previos.

Finalmente, se enuncian las conclusiones y recomendaciones derivadas de los hallazgos del estudio.

CAPITULO I Generalidades

1.1. Antecedentes de la Investigación

1.1.1. Antecedentes Nacionales

Navarro (2020) en su trabajo de investigación titulado "*Diseño de una infraestructura de red WAN segura con un servidor de autenticación AAA basado en el protocolo TACACS+ para la empresa Sintelcom*" investigó el problema de la falta de control en el acceso a los recursos tecnológicos de la empresa Sintelcom. El objetivo es diseñar una infraestructura de red WAN segura con un servidor de autenticación AAA basado en el protocolo TACACS, para mejorar el control de acceso a los recursos tecnológicos y aumentar los niveles de seguridad en la red corporativa. La investigación es aplicada, de nivel descriptiva, enfoque cualitativo y diseño no experimental. Se utiliza la herramienta GNS3 para el diseño y la simulación de la propuesta. Los resultados señalan que el diseño propuesto y su simulación prevé el funcionamiento real de la red. Se concluye que el diseño propuesto y su simulación es viable desde el aspecto tecnológico, técnico y económico, sobre todo mejora la tecnología tradicional de las redes VPN y genera impacto positivo dentro de la organización al ser más rápida y factible al momento de ser usada.

Chinchay & Peña (2021) en su tesis titulada "*Comparación de protocolos de autenticación de usuarios en el control de acceso a redes inalámbricas*" investigaron el problema de la seguridad de la información en redes inalámbricas. El objetivo la investigación es analizar los protocolos de autenticación de usuarios RADIUS, TACACS+, DIAMETER y KERBEROS en el control de acceso a datos en redes inalámbricas de área local. La metodología empleada es de tipo aplicada, nivel descriptivo, enfoque cuantitativo y diseño no experimental. Se utiliza una matriz que pondera las características básicas de autenticación, forma de trabajo y funcionalidad AAA de cada protocolo. La ponderación se realiza con una escala de 0 a 3, donde 0 equivale a "no cuenta", 1 a "nivel bajo", 2 a "nivel medio" y 3 a "nivel alto". Los resultados indican que el protocolo RADIUS alcanza un total de 20 puntos, seguido por DIAMETER con 17 puntos, TACACS+ con 16 puntos, y KERBEROS con 15 puntos. Se

concluye que el protocolo RADIUS es el protocolo más competente para la autenticación de usuarios.

Ramos & Torres (2021) en su investigación titulada "S*ervidor radius en el control de acceso a la red inalámbrica de la escuela profesional de ingeniería de sistemas de la Universidad Nacional de Huancavelica*", estudiaron el control de acceso a la red inalámbrica de la Universidad Nacional de Huancavelica. El objetivo es determinar la influencia de los servidores RADIUS en el control del acceso a la red inalámbrica en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Huancavelica. La investigación es de tipo aplicada, nivel descriptivo, enfoque cuantitativo, diseño pre experimental. Se utilizan fichas de observación y listas de cotejo para la recolección de datos. Los resultados muestran mejoras significativas, el tiempo de respuesta en el nivel WAN mejoró de 78 ms a 40 ms, y en el nivel WLAN de 78 ms a 17 ms. El porcentaje de autenticaciones exitosas de usuarios WLAN a WAN aumentó de 80% a 87%, mientras que las peticiones de autenticación de usuarios WLAN a WAN disminuyeron de 88% a 9%. Además, las peticiones de autenticación de usuarios WAN a WLAN a servicios autorizados mejoraron de 87% a 95%, y las peticiones WAN a WLAN a servicios no autorizados se redujeron de 89% a 2%. Se concluye que los servidores RADIUS optimizan la autenticación, el control de acceso y la confidencialidad de la información en la red inalámbrica de la Escuela Profesional de Ingeniería de Sistemas.

Huaman et. al. (2022) en su investigación titulada "*Propuesta de implementación de políticas de seguridad basado en CISCO ISE (identity services engine) en la red LAN de Caja Huancayo*" abordan la seguridad de la red LAN de Caja Huancayo. El objetivo es elaborar una propuesta de implementación de políticas de seguridad utilizando la tecnología Cisco ISE (Identity Services Engine) y los protocolos TACACS+ y RADIUS. La investigación es aplicada, nivel explicativo, enfoque cualitativo y diseño pre experimental. Se realiza la encuesta a 10 expertos en seguridad informática que laboran en empresas establecidas en Lima para seleccionar la tecnologia más adecuada. Los resultados demuestra que la tecnología de seguridad CISCO ISE consigue la prioridad más alta en siete aspectos y prioridad media en dos aspectos por lo que se recomienda su uso. Se concluye que Cisco ISE permitiría

optimizar la seguridad interna en la agencia principal de Caja Huancayo mediante políticas de seguridad centralizada, gestionando switches de acceso, switches Core Campus, switches Core Datacenter y Wireless LAN Controller con TACACS+, y las PCs con RADIUS.

1.1.2. Antecedentes Internacionales

Andrade (2019) en su trabajo de investigación "*Análisis de prestaciones de los protocolos de autenticación remota RADIUS y TACACS+ en infraestructura de comunicaciones corporativas*" investigó los protocolos de autenticación remota RADIUS y TACACS+ para determinar el más adecuado para mejorar la seguridad de acceso a redes inalámbricas. El objetivo es analizar las prestaciones de los protocolos de autenticación remota RADIUS y TACACS+ en infraestructura de comunicaciones corporativas. La investigación es aplicada, de nivel descriptiva, enfoque mixto y diseño cuasi-experimental. Se utiliza la escala de Likert para medir y comparar criterios como el protocolo de transporte, cifrado de paquetes, autenticación y autorización, soporte multiprotocolo, capacidad de administración de routers, interoperabilidad, complejidad y RFC, y la seguridad. Los resultados confirman que TACACS+ posee mejores ventajas sobre RADIUS tales como el uso de TCP que es más seguro, el cifrado de todo el contenido del paquete, se puede utilizar para administrar routers, es multiprotocolo y finalmente englobando a todo lo antes mencionado TACACS+ ofrece mejores beneficios en cuanto a la seguridad. Se concluye que ambos protocolos funcionan correctamente en entornos corporativos, sin embargo, TACACS+ es más recomendable en entornos que priorizan seguridad y RADIUS es más óptimo en tiempo de autenticación.

Pozo & Solis (2024) en su 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*" investigaron el problema de utilizar FreeRADIUS para la autenticación de usuarios a redes inalámbricas. El objetivo es mejorar la seguridad y el control del acceso a la red inalámbrica del bloque "U" del campus "Dolorosa" de la Universidad Nacional de Chimborazo (UNACH). La metodología es de tipo aplicada, de nivel descriptiva,

enfoque mixto y diseño cuasi experimental. Se utiliza la escala de Likert para comparar FreeRADIUS y la tecnología de autenticación, autorización y auditoría (AAA) Cisco ISE según 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 y 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. Se concluye que Cisco ISE utilizando el método de autenticación RADIUS es 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.

Alimatov (2025) en su artículo "*Aplicación y capacidad de seguridad de las tecnologías TACACS+ y RADIUS en el control de acceso centralizado en redes de telecomunicaciones*" investiga la función de los protocolos TACACS+ y RADIUS en los procesos de autenticación, autorización y contabilidad (AAA) en sistemas de control de acceso centralizados. Su objetivo es realizar un análisis comparativo de los aspectos técnicos de estos dos protocolos y su papel en la seguridad de la red. Los resultados del análisis indican que el protocolo TACACS+ brinda alta seguridad, cifrado completo, sistema de auditoría sólido y granular. Se caracteriza por sus capacidades de gestión y es ideal para grandes organizaciones de alta seguridad. Por otro lado, RADIUS es abierto, compatibilidad entre plataformas, arquitectura ligera y amplia. Se utiliza ampliamente en la práctica debido a su amplia gama de aplicaciones y es eficaz en sistemas de autenticación de propósito general. Se concluye que la elección del protocolo a utilizar depende de la estructura de la red, el nivel de seguridad y las necesidades de gestión. En muchos casos, el sistema puede mejorarse aún más implementando ambos protocolos conjuntamente o por etapas.

1.2. Identificación y Descripción del Problema de Estudio

En la gestión de infraestructuras de red, la seguridad del acceso a la configuración de los switches es crítica para proteger la red. Actualmente, este acceso puede gestionarse de dos maneras: mediante autenticación local en el propio dispositivo, o a través de un esquema de Autenticación, Autorización y Auditoría (AAA) centralizado en un servidor AAA utilizando protocolos como RADIUS o TACACS+ (Juniper Networks, 2025).

Los fabricantes líderes en redes, como Cisco recomiendan el uso de AAA centralizado para entornos empresariales, ya que la autenticación local presenta limitaciones significativas en términos de escalabilidad, trazabilidad y control granular (Cisco, 2011). Sin embargo, la decisión entre implementar RADIUS o TACACS+ no siempre está clara, dado que ambos protocolos poseen ventajas y desventajas según el escenario de uso.

El problema radica en que, a pesar de las recomendaciones de los fabricantes, existen pocos antecedentes que muestren un análisis comparativo empírico y cuantitativo que contraste de manera objetiva las diferencias entre la autenticación, autorización y auditoria centralizada con RADIUS y TACACS+. Con frecuencia, las supuestas ventajas de cada enfoque se presentan únicamente en términos cualitativos en documentación técnica y foros especializados, sin datos medibles que respalden dichas afirmaciones.

La falta de información medible limita la capacidad de los responsables de TI, administradores de red y líderes de negocio para tomar decisiones estratégicas fundamentadas, ya que no cuentan con una referencia cuantitativa que demuestre con evidencia cuál de los dos protocolos ofrece el mejor rendimiento en términos de desempeño, seguridad y disponibilidad.

1.3. Formulación del Problema

1.3.1. Problema Principal

¿Cuál protocolo proporciona mejor desempeño, seguridad y disponibilidad en el control de acceso centralizado a la configuración de un switch entre RADIUS y TACACS+?

1.3.2. Problemas Específicos

a) ¿Cómo difiere el tráfico de red que genera un usuario al solicitar y obtener acceso de forma centralizada a la configuración de un switch cuando se utilizan los protocolos RADIUS y TACACS+?

b) ¿Qué nivel de cifrado de datos y granularidad se puede lograr con RADIUS y TACACS+ durante los procesos de autenticación, autorización y auditoría?

c) ¿Cuál es el impacto sobre el acceso de un usuario debido a fallas en la comunicación entre el cliente y el servidor AAA al utilizar RADIUS y TACACS+?

1.4. Justificación e Importancia

La presente investigación es importante porque permitirá a los responsables de la gestión de infraestructuras de red disponer de un análisis comparativo y empírico entre dos protocolos ampliamente utilizados para la autenticación, autorización y auditoria (AAA) centralizada de usuarios que administran la configuración de un switch. Esto facilitará la toma de decisiones más objetivas y fundamentadas, en lugar de depender únicamente de experiencias previas o supuestos poco comprobados.

La seguridad en la administración de switches y la gestión de usuarios son componentes críticos de la infraestructura tecnológica de cualquier organización. Mejorar la gestión y control de accesos mediante la elección adecuada del protocolo AAA contribuye directamente a la protección de la información corporativa, la prevención de ataques cibernéticos y la continuidad operativa de los servicios. Por lo tanto, los resultados de este estudio tienen un impacto práctico para empresas, instituciones gubernamentales y organizaciones que gestionan redes.

Este estudio contribuye a la literatura sobre seguridad de redes y control de acceso, ya que establece métricas cuantitativas para los evaluar los protocolos RADIUS y TACACS+, lo que generalmente se aborda de manera cualitativa. Este aporte permitirá enriquecer los marcos de referencia existentes en materia de autenticación, autorización y auditoría.

Finalmente, esta investigación servirá como un modelo para futuros estudios comparativos en el campo de la seguridad de TI, demostrando cómo se pueden

operacionalizar y medir conceptos abstractos como el desempeño, la seguridad y la disponibilidad del servicio AAA.

1.5. Objetivos

1.5.1. Objetivo General

Comparar los protocolos RADIUS y TACACS+, para determinar cuál ofrece mejor desempeño, seguridad y disponibilidad en el acceso de forma centralizada a la configuración de un switch.

1.5.2. Objetivos Específicos

a) Evaluar el tráfico de red que genera un usuario al solicitar y obtener acceso de forma centralizada a la configuración de un switch cuando se utilizan los protocolos RADIUS y TACACS+, para determinar el protocolo que tiene mejor desempeño operacional.
b) Comparar el nivel de cifrado y granularidad que se puede lograr con RADIUS y TACACS+ durante los procesos de autenticación, autorización y auditoría, para establecer el protocolo que ofrece mayor nivel de seguridad.
c) Analizar el impacto sobre el acceso de un usuario debido a fallas en la comunicación entre el cliente y el servidor AAA al utilizar RADIUS y TACACS+, para identificar el protocolo que garantiza mayor disponibilidad del servicio AAA.

1.6. Hipótesis

1.6.1. Hipótesis General

La comparación de los protocolos RADIUS y TACACS+, determinará que TACACS+ ofrece mejor desempeño, seguridad y disponibilidad en el acceso a la configuración de un switch.

1.6.2. Hipótesis Específicas

a) La evaluación del tráfico de red que genera un usuario al solicitar y obtener acceso de forma centralizada a la configuración de un switch, cuando se utilizan los protocolos RADIUS y TACACS+, determinará que el protocolo TACACS+ tiene mejor desempeño operacional.
b) La comparación del nivel de cifrado y granularidad que se puede lograr con RADIUS

y TACACS+, establecerá que protocolo TACACS+ ofrecerá mayor nivel de seguridad.

c) El análisis del impacto sobre el acceso de un usuario debido a fallas en la comunicación entre el cliente y el servidor AAA al utilizar RADIUS y TACACS+, identificará a TACACS+ como el protocolo que garantiza mayor disponibilidad del servicio AAA.

1.7. Variables y Operacionalización de Variables

VI: Protocolo AAA

VD1: Eficiencia, VD2: seguridad y VD3: disponibilidad.

1.7.1. Operacionalización de Variables

Tabla 1.

Operacionalización de variables.

Variable	Definición Conceptual	Definición Operacional	Operacionalización	
			Dimensiones	**Indicadores**
Desempeño	Capacidad del protocolo AAA para otorgar acceso a usuarios legítimos utilizando la menor cantidad de recursos y en el menor tiempo.	Se medirá evaluando el número de paquetes transmitidos, el tamaño total de los datos intercambiados y la latencia en la red cuando un usuario legítimo solicita y obtiene acceso al switch.	Eficiencia operacional	• Número de paquetes necesarios para otorgar el acceso. • Tamaño total de datos transmitidos en la autenticación y autorización del usuario. • Latencia en la red cuando un usuario solicita y obtiene acceso.
Seguridad	Capacidad del protocolo AAA para proteger la información y garantizar el control del acceso de los usuarios.	Se medirá evaluando el porcentaje de datos cifrados en cada fase, la granularidad en la asignación de privilegios y el registro de eventos de seguridad.	Cifrado de datos	• Porcentaje de datos cifrados en los paquetes de autenticación y autorización. • Porcentaje de datos cifrados en los paquetes de auditoría.
			Control del privilegio	• Porcentaje de comandos denegados sobre un conjunto representativo.
			Registro y auditoría	• Número de paquetes de auditoría generados desde el inicio hasta el fin de sesión.
Disponibilidad	Capacidad del protocolo AAA para transmitir datos de manera continua y confiable.	Se medirá evaluando la tolerancia a fallos en la comunicación entre el servidor AAA y el switch.	Tolerancia a fallos	• Tiempo promedio de fail-over.

1.8. Metodología de la Investigación

1.8.1. Unidad de Análisis

La presente investigación tiene como unidad de análisis los protocolos de autenticación, autorización y auditoría (AAA) RADIUS y TACACS+.

1.8.2. Tipo, Enfoque y Nivel de Investigación

Según Hernández Sampieri et al. (2014), la presente investigación es de tipo aplicada, ya que busca resolver un problema práctico en el ámbito de la seguridad de redes.

El enfoque es cuantitativo porque se basa en la recolección y análisis de datos numéricos para probar la hipótesis.

El nivel de esta investigación es descriptivo porque se centra en recopilar información que permita comparar las características de los dos protocolos AAA que se someten a análisis.

1.8.3. Diseño de la Investigación

El diseño de la investigación es cuasi-experimental, porque se manipula la variable independiente (el protocolo AAA) para observar su impacto en las variables dependientes, pero no se asignan aleatoriamente grupos experimentales (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).

1.8.4. Fuentes de Información

El desarrollo de la investigación se apoya en los datos obtenidos de pruebas controladas y mediciones experimentales realizadas sobre el switch y los servidores AAA. Además, la revisión bibliográfica de manuales técnicos, guías de configuración, documentos de fabricantes y artículos científicos fundamentan la base teórica de este estudio.

1.8.5. Población y muestra

La población es el conjunto de sistemas que implementan protocolos de autenticación, autorización y contabilización (AAA) para el control de acceso a switches.

La muestra corresponde a los dos sistemas AAA, uno basado en RADIUS y otro en TACACS+, configurados para gestionar el acceso centralizado a la configuración de un switch. Estos sistemas son observados para medir el desempeño, la seguridad y la

disponibilidad que ofrece cada protocolo.

1.8.6. Técnicas e Instrumentos de Recolección de Datos

Los datos son recolectados mediante la técnica experimental y los instrumentos utilizados para la medición y recolección de estos datos son las interfaces de línea de comandos (CLI) del switch y del servidor AAA que permiten ejecutar comandos de diagnóstico y monitoreo, y las herramientas de análisis de tráfico de red Wireshark y tcpdump que permiten capturar, inspeccionar y analizar los paquetes de datos que viajan entre el switch y el servidor AAA.

1.8.7. Análisis y Procesamiento de Datos

El análisis de los datos recolectados se realiza mediante la comparación de métricas asociadas al desempeño, seguridad y disponibilidad de los protocolos AAA. Para el desempeño, se evalúa el número de paquetes intercambiados, el tamaño total de los datos y la latencia en la red cuando un usuario solicita y obtiene acceso al switch. Para la seguridad, se evalúa el porcentaje de datos cifrados en los paquetes de autenticación, autorización y auditoría; el porcentaje de comandos denegados sobre un conjunto representativo y el número de paquetes de auditoría generados desde el inicio hasta el fin de sesión de un usuario legítimo. Para la disponibilidad, se mide el tiempo de fail-over.

Tabla 2.

Resumen de la metodología de investigación.

Unidad de Análisis	Tipo, Enfoque y Nivel de Investigación	Diseño de la Investigación
La presente investigación tiene como unidad de análisis los protocolos de autenticación, autorización y auditoría (AAA) RADIUS y TACACS+.	La presente investigación es de tipo aplicada, ya que busca resolver un problema práctico en el ámbito de la seguridad de redes. El enfoque es cuantitativo porque se basa en la recolección y análisis de datos numéricos para probar la hipótesis. El nivel de esta investigación es descriptivo porque se centra en recopilar información que permita comparar las características de los dos protocolos AAA que se someten a análisis.	El diseño de la investigación es cuasi-experimental, porque se manipula la variable independiente (el protocolo AAA) para observar su impacto en las variables dependientes, pero no se asignan aleatoriamente grupos experimentales.
Fuentes de Información	**Técnicas e Instrumentos de Recolección de Datos**	**Análisis y Procesamiento de Datos**
El desarrollo de la investigación se apoya en los datos obtenidos de pruebas controladas y mediciones experimentales realizadas sobre el switch y los servidores AAA. Además, la revisión bibliográfica de manuales técnicos, guías de configuración, documentos de fabricantes y artículos científicos fundamentan la base teórica de este estudio.	Los datos son recolectados mediante la técnica experimental y los instrumentos utilizados para la medición y recolección de estos datos son las interfaces de línea de comandos (CLI) del switch y del servidor AAA que permiten ejecutar comandos de diagnóstico y monitoreo, y las herramientas de análisis de tráfico de red Wireshark y tcpdump que permiten capturar, inspeccionar y analizar los paquetes de datos que viajan entre el switch y el servidor AAA.	El análisis de los datos recolectados se realiza mediante la comparación de métricas asociadas al desempeño, seguridad y disponibilidad de los protocolos AAA. Para el desempeño, se evalúa el número de paquetes intercambiados, el tamaño total de los datos y la latencia en la red cuando un usuario solicita y obtiene acceso al switch. Para la seguridad, se evalúa el porcentaje de datos cifrados en los paquetes de autenticación, autorización y auditoría; el porcentaje de comandos denegados sobre un conjunto representativo y el número de paquetes de auditoría generados desde el inicio hasta el fin de sesión de un usuario legítimo. Para la disponibilidad, se mide el tiempo de fail-over.

Nota. Adaptado de Hernández Sampieri et al. (2014).

CAPÍTULO II

Marco Teórico y Marco Conceptual

2.1. Bases Teóricas

2.1.1. Redes de Comunicación

Una red se define como la conexión de dos o más computadoras para que puedan intercambiar información entre sí. Todas las redes, requieren de hardware de red especializado para su funcionamiento. (Lowe, 2005).

2.1.1.1. Tipos de Redes

Las infraestructuras de red pueden variar en gran medida en términos de tamaño del área que abarcan, cantidad de usuarios conectados, cantidad y tipos de servicios disponibles y el área de responsabilidad. A continuación, se definen los dos tipos de infraestructuras de red más comunes.

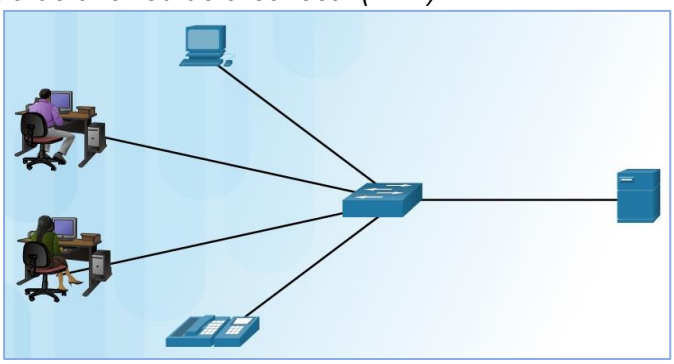
- **Redes LAN**

Una red de área local (LAN) conecta dispositivos que están físicamente cerca unos de otros mediante conectores como enrutadores y conmutadores. Permite que los dispositivos intercambien datos y se comuniquen de forma segura a pequeña escala (Amazon Web Services, 2025).

La Figura 1 muestra un ejemplo de topología de una red de área local (LAN), donde se evidencia la interconexión de múltiples dispositivos dentro de un mismo entorno físico.

Figura 1.

Topología de una red de área local (LAN).



Nota. Adaptado de “LAN y WAN - CCNA V6.0” por K. Linares, 2017, Blogspot (https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-LAN-y-WAN.html)

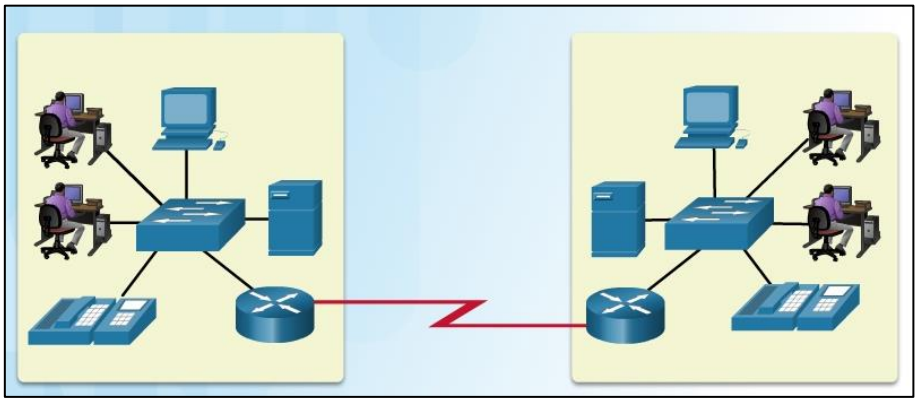
- **Redes WAN**

Una red de área extendida (WAN) se extiende más allá de un edificio o de un gran recinto para incluir múltiples ubicaciones repartidas a lo largo de una zona geográfica concreta, o incluso del mundo. Las organizaciones utilizan las WAN para facilitar las interacciones digitales y el intercambio de datos entre empleados y clientes en diferentes regiones o países (Amazon Web Services, 2025).

La Figura 2 muestra un ejemplo de topología de una red de área amplia (WAN), en el cual se representa cómo dos redes locales se enlazan mediante enlaces de comunicación de largo alcance.

Figura 2.

Topología de una red de área amplia (WAN).



Nota. Adaptado de "LAN y WAN - CCNA V6.0" por K. Linares, 2017, Blogspot (https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-LAN-y-WAN.html).

2.1.1.2. Componentes de la Red

La infraestructura de red contiene tres categorías de componentes de red:

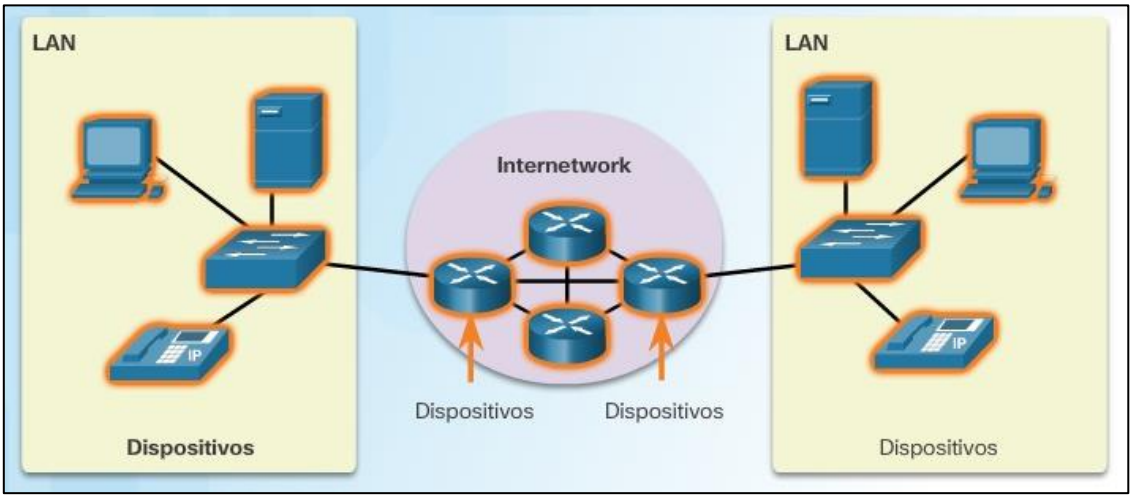
- **Dispositivos de Red**

Los dispositivos de red son los elementos físicos o hardware de la red. Pueden ser dispositivos finales o dispositivos de red intermedios (Linares, 2017).

La Figura 3 muestra algunos de los dispositivos que se encuentran dentro de una red.

Figura 3.

Dispositivos en una red.



Nota. Adaptado de “Componentes de la red - CCNA V6.0” por K. Linares, 2017, Blogspot (https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-Componentes-de-la-red.html).

- **Dispositivos finales.** Un dispositivo final es el origen o el destino de un mensaje transmitido a través de la red. Por ejemplo, computadoras, impresoras de red, teléfonos VoIP, cámaras de seguridad, etc (Linares, 2017). La Figura 4 muestra los principales dispositivos finales de una red.

Figura 4.

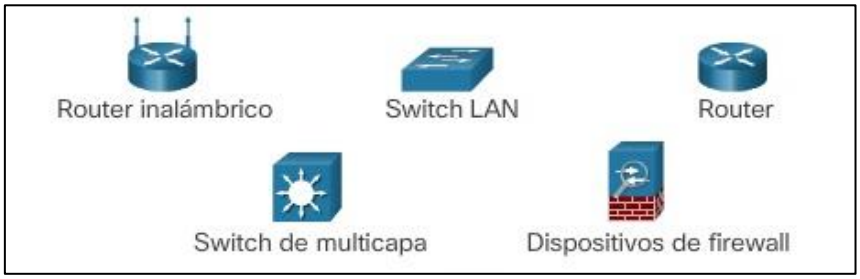
Dispositivos finales de una red.

Nota. Adaptado de “Componentes de la red - CCNA V6.0” por K. Linares, 2017, Blogspot (https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-Componentes-de-la-red.html).

- **Dispositivos de red intermedios.** Los dispositivos intermedios conectan los dispositivos finales a la red y garantizan el flujo de datos en toda la red. Por ejemplo, switches, routers, firewalls, puntos de acceso, etc (Linares, 2017). La Figura 5 muestra los principales dispositivos de red intermedios utilizados para garantizar la conectividad y el flujo de información en una red.

Figura 5.

Dispositivos de red intermedios.



Nota. Adaptado de “Componentes de la red - CCNA V6.0” por K. Linares, 2017, Blogspot (https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-Componentes-de-la-red.html).

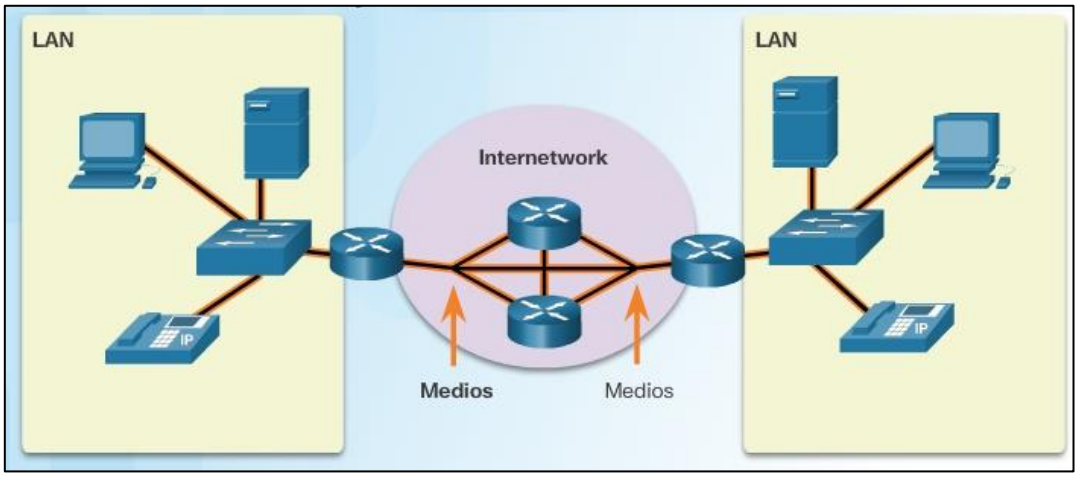
- **Medios**

La comunicación a través de una red es transportada por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino (Linares, 2017).

La Figura 6 muestra un ejemplo de medio de comunicación cableada, el cual constituye la base de muchas infraestructuras de red.

Figura 6.

Topología de red cableada.



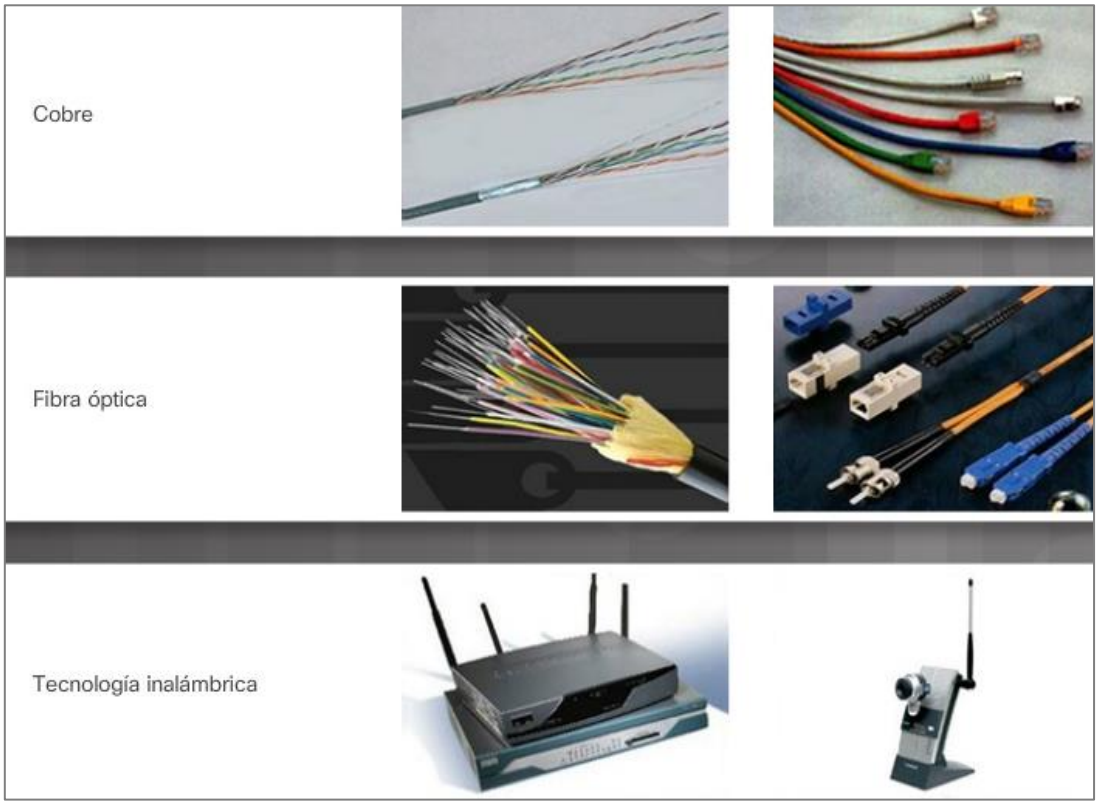
Nota. Adaptado de “Componentes de la red - CCNA V6.0” por K. Linares, 2017, Blogspot (https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-Componentes-de-la-red.html).

Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos: cobre, fibra óptica e inalámbrico (Linares, 2017).

La Figura 7 presenta los principales tipos de medios de comunicación para una red.

Figura 7.

Tipos de medios de comunicación para una red.



Nota. Adaptado de “Componentes de la red - CCNA V6.0” por K. Linares, 2017, Blogspot (https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-Componentes-de-la-red.html).

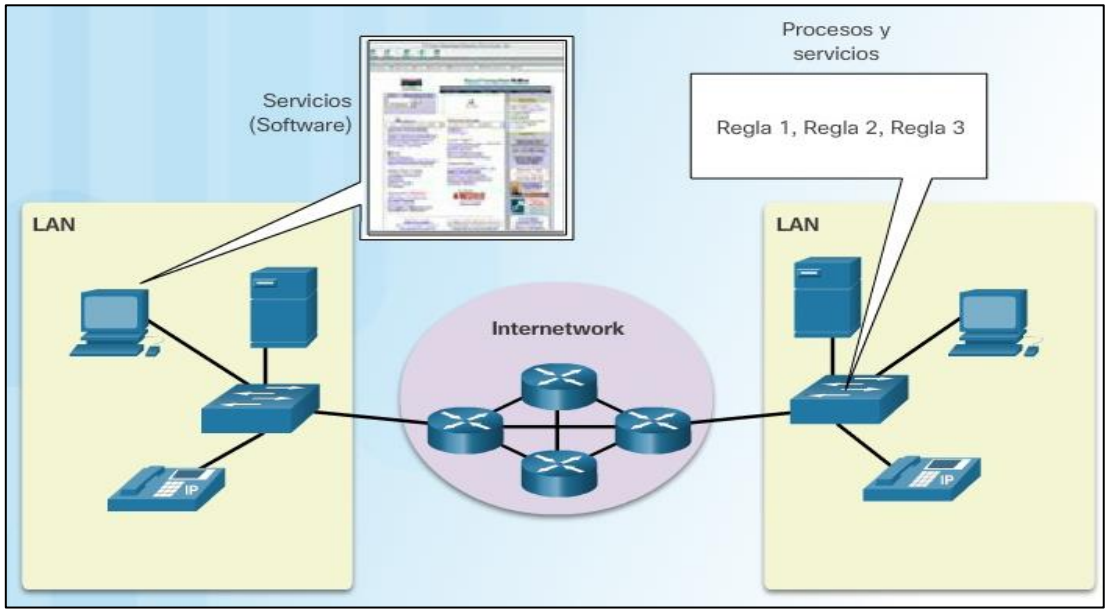
- **Servicios y procesos**

Los servicios incluyen aplicaciones de red que utilizan las personas a diario, como los servicios de alojamiento de correo electrónico y los servicios de alojamiento web. Los procesos proporcionan la funcionalidad que direcciona y traslada mensajes a través de la red, son menos obvios para el ser humano, pero son críticos para el funcionamiento de las redes (Linares, 2017).

La Figura 8 muestra un ejemplo de los servicios y procesos que se ejecutan dentro de una red.

Figura 8.

Servicios y procesos en una red.



Nota. Adaptado de “Componentes de la red - CCNA V6.0” por K. Linares, 2017, Blogspot (https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-Componentes-de-la-red.html).

2.1.2. Modelos de Referencia para las Comunicaciones de Red

Los dos modelos de referencia para las comunicaciones en red son el modelo TCP/IP y el modelo OSI (Open Systems Interconnection). TCP/IP es un modelo práctico que aborda desafíos de comunicación específicos y se basa en protocolos estandarizados. Por el contrario, OSI sirve como un marco integral e independiente del protocolo, diseñado para abarcar varios métodos de comunicación de red (Fortinet, 2025).

2.1.2.1. Modelo TCP/IP

El modelo de protocolo de control de transmisión/protocolo de Internet (TCP/IP) se presentó antes que el modelo de interconexión de sistemas abiertos (OSI) y tiene cinco capas:

1. **Capa de aplicación.** La capa de aplicación es donde los datos se originan del lado del remitente. Las aplicaciones se utilizan para crear los datos. Un navegador web, por ejemplo, se utiliza para generar los datos que se envían a través del resto de las capas, asistidos por el Sistema de Nombres de Dominio (DNS), que asocia los nombres de dominio web con sus direcciones de protocolo de Internet (IP).
2. **Capa de transporte.** En la capa de transporte, los datos se codifican para que puedan

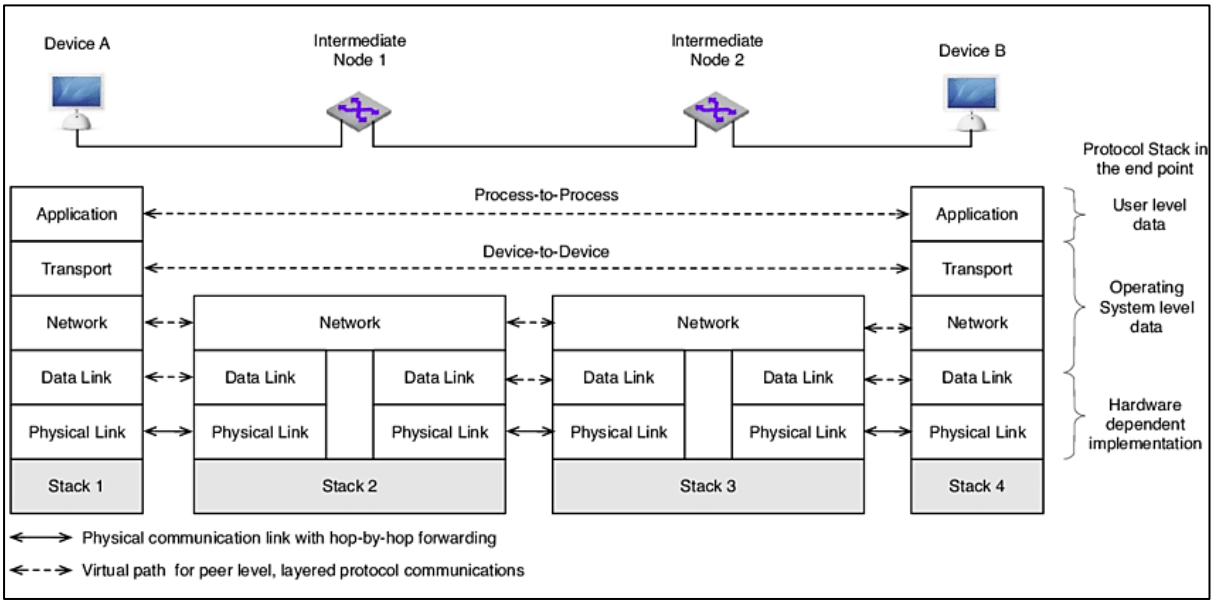
transportarse a través de Internet mediante el Protocolo de Datagrama de Usuario (UDP) o el Protocolo de Control de Transmisión (TCP).

3. **Capa de acceso a la red.** En la capa de acceso a la red, los datos obtienen un encabezado y un remolque, y estos indican a los datos a dónde ir. Esta información luego se transmite a la capa de interfaz de red.
4. **Capa de interfaz de red.** En la capa de interfaz de red, el paquete de datos se formatea y prepara para ser transportado y enrutado a través de la red.
5. **Capa de hardware**. En la capa de hardware, los datos se convierten en algo que se puede enviar a una computadora u otro dispositivo y leer. Por ejemplo, el protocolo IEEE 802.3 se utiliza para convertir datos en lo que se utiliza en una conexión Ethernet.

La Figura 10 presenta la comunicación entre dispositivos de red utilizando el modelo TCP/IP, mostrando cómo los datos viajan a través de las diferentes capas hasta llegar al destino.

Figura 9.

Comunicación entre dispositivos de red utilizando el modelo TCP/IP.



Nota. Adaptado de “On analyzing poblems of distributed systems and current internet in front of the future internet architectures” por M. Alberti, 2016, ResearchGate (https://www.researchgate.net/figure/TCP-IP-layered-protocol-communication-between-two-end-point-devices-Functionally_fig1_310317068)

2.1.2.2. Modelo OSI

La mayor diferencia entre los modelos OSI y TCP/IP es que el modelo OSI tiene siete capas. Aunque los modelos TCP/IP y OSI transportan datos, las formas en que los envían son ligeramente diferentes, por lo que a veces se utiliza TCP/IP en lugar de OSI. Sin embargo, en el análisis de TCP/IP frente a OSI, hay más similitudes entre los modelos OSI y TCP/IP que las diferencias. Ambos proporcionan servicios de comunicación de datos, lo que permite a los usuarios enviar y recibir información (Fortinet, 2025).

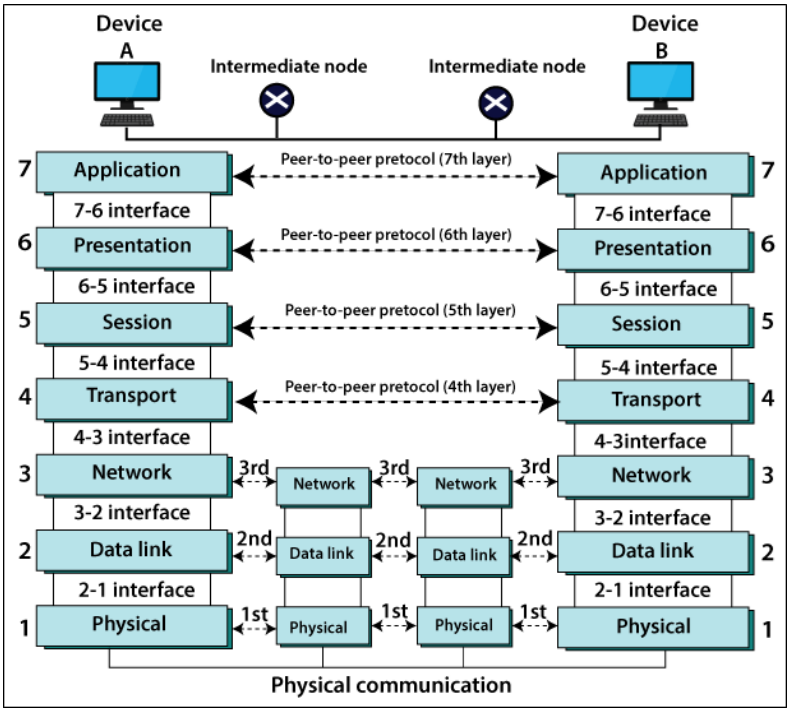
El modelo OSI tiene las siguientes capas:

1. **Físico**. Esto consiste en una conexión de datos entre un dispositivo que genera datos y la red.
2. **Enlace de datos**. La capa de enlace de datos es la conexión punto a punto que transmite los datos a la capa de red.
3. **Red**. En la capa de red, los datos obtienen su dirección e instrucciones de enrutamiento para prepararse para su recorrido por la red.
4. **Transporte**. En la capa de transporte, los datos saltan entre diferentes puntos de la red en camino a su destino.
5. **Sesión**. La capa de sesión tiene una conexión que administra las sesiones que ocurren entre aplicaciones.
6. **Presentación**. La capa de presentación es donde los datos se cifran, descifran y convierten en una forma a la que puede acceder la capa de aplicación,
7. **Aplicación**. En la capa de aplicación, una aplicación, como un navegador de Internet, obtiene los datos y un usuario puede interactuar con ellos.

La Figura 10 presenta la comunicación entre dispositivos de red utilizando el modelo OSI, mostrando cómo los datos viajan a través de las diferentes capas hasta llegar al destino.

Figura 10.

Comunicación entre dispositivos de red utilizando el modelo OSI.



Nota. Adaptado de "OSI Model" por O. Ozturk, 2021, Medium (https://ztrkouzhan.medium.com/osi-model-b77a4351aae0)

2.1.3. Encapsulación y Desencapsulación de Datos

La encapsulación marca el inicio y el fin de un paquete, o unidad de datos. El inicio se denomina encabezado y el final tráiler. Los datos entre el encabezado y el tráiler se denominan a veces *payload*.

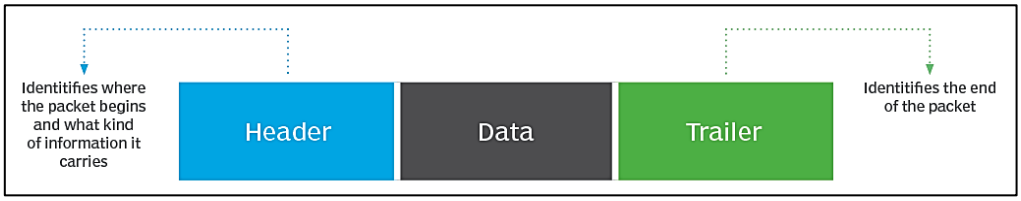
El encabezado del paquete contiene información en sus primeros bytes para marcar su inicio e identificar el tipo de información que contiene. A medida que un paquete viaja desde su origen hasta su destino, las diferentes capas de un sistema informático contribuyen a su encabezado. La información del encabezado varía según el protocolo utilizado, ya que cada uno tiene un formato definido.

El tráiler del paquete indica al dispositivo receptor que ha llegado al final del paquete. Suele contener un valor de comprobación de errores que el dispositivo receptor puede usar para confirmar que ha recibido el paquete completo (Jacobs, 2022).

La Figura 11 muestra la incorporación de la cabecera y el tráiler de datos en el proceso de encapsulación.

Figura 11.

Cabecera y tráiler de datos.



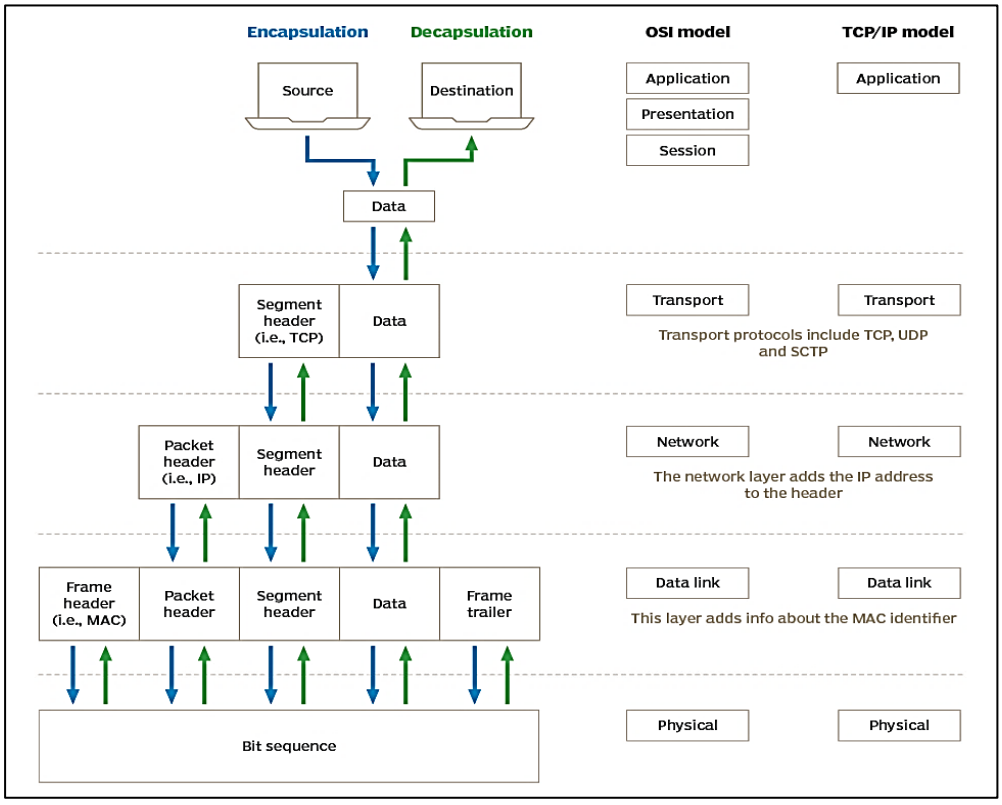
Nota. Adaptado de "Intro to encapsulation and decapsulation in networking" por D. Jacobs, 2022, TechTarget(https://www.techtarget.com/searchnetworking/tip/Intro-to-encapsulation-and-decapsulation-in-networking)

La desencapsulación es el proceso de eliminar la información del encabezado y el tráiler de un paquete a medida que avanza hacia su destino. El dispositivo de destino recibe los datos en su formato original (Jacobs, 2022).

La Figura 12 ilustra el proceso de encapsulamiento y desencapsulamiento de datos, destacando la interacción entre las diferentes capas de la comunicación.

Figura 12

Proceso de encapsulamiento y desencapsulamiento de datos.



Nota. Adaptado de "Intro to encapsulation and decapsulation in networking" por D. Jacobs, 2022, TechTarget(https://www.techtarget.com/searchnetworking/tip/Intro-to-encapsulation-and-decapsulation-in-networking)

2.1.4. Acceso a la Administración de Dispositivos de Red

El acceso a la administración de dispositivos de red es la capacidad de iniciar sesión, solucionar problemas y monitorear dispositivos de red. Estos dispositivos se pueden administrar mediante una interfaz de línea de comandos (CLI) o una interfaz gráfica de usuario (GUI) (Mikac, 2024).

2.1.4.1. Acceso a la CLI mediante puerto de consola

El puerto de consola en un dispositivo de red es una interfaz dedicada que se utiliza para establecer una conexión directa entre una computadora y el dispositivo, generalmente a través de un cable serie.

La Figura 13 muestra el switch de la marca FS, modelo S3240-8P, destacando la ubicación de su puerto de consola, utilizado para la administración local del dispositivo.

Figura 13.

Switch marca FS, modelo S3240-8P.

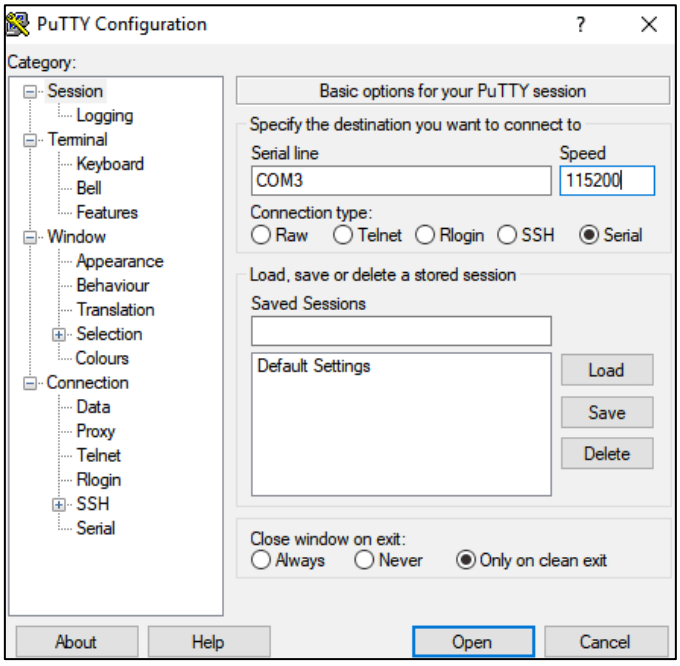
Nota. Adaptado de *"S3240-8P, switch Gigabit Ethernet L2+ PoE+ de 8 puertos, 8 x PoE+ puertos@120W, con 4 x 10Gb SFP+ enlaces ascendentes, switch apilable, sin ventilador"* por FS, 2025, FS (https://www.fs.com/es/products/329355.html?now_cid=3150)

Al conectar una computadora al puerto de la consola, el administrador puede acceder a la interfaz de línea de comandos (CLI) del conmutador para realizar tareas de configuración, actualizar firmware y diagnosticar problemas de red. Para ello, la computadora del administrador debe contar con un software de emulación de terminal, como PuTTY o la propia terminal del sistema operativo como OpenSSH (FS, 2022).

La Figura 14 muestra una conexión serial utilizando PuTTY con el puerto COM3 seleccionado.

Figura 14.

Conexión serial al switch mediante Putty.



Nota. Adaptado de “How to Log into a Network Switch: 3 Methods” por FS, 2025, FS (https://www.fs.com/eu-en/blog/three-approaches-to-log-in-to-your-network-switch-1256.html).

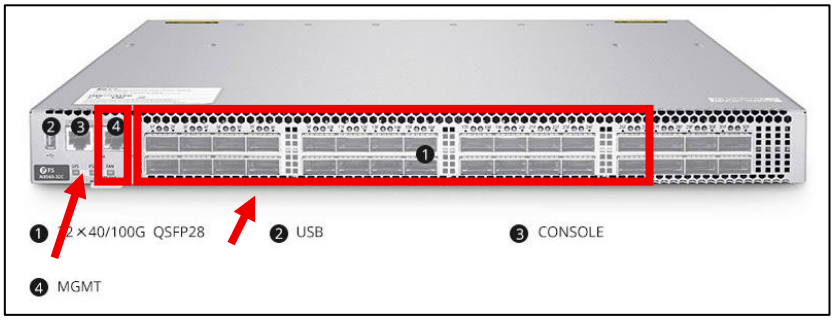
2.1.4.2. Acceso a la CLI mediante Telnet o SSH

Este método permite la administración local o remota de un dispositivo de red que cuenta con una dirección IP de gestión asignada a su interfaz de administración (MGMT) o a una VLAN destinada exclusivamente a tareas de gestión y se ha activado el servicio Telnet o SSH.

La Figura 15 muestra el switch marca FS, modelo N8560-32C, destacando la ubicación de los puertos MGMT y de acceso, los cuales permiten establecer comunicación administrativa con el equipo a través de la red.

Figura 15.

Switch marca FS, modelo N8560-32C.



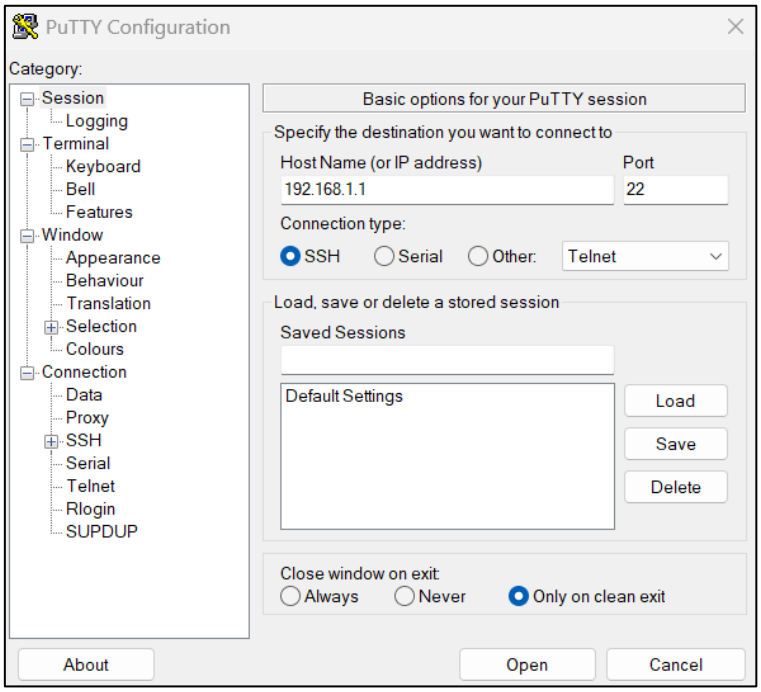
Nota. Adaptado de “Switch de centro de datos Ethernet capa 3 de 32 puertos, N8560-32C, 32 x 100Gb QSFP28, soporta MLAG/apilamiento, Chip Broadcom, FSOS instalado” por FS, 2025, FS (https://www.fs.com/es/products/110480.html?now_cid=3404).

De esta manera, el administrador puede conectarse desde un cliente remoto a la CLI del switch utilizando un emulador de terminal, como PuTTY o la propia terminal del sistema operativo como OpenSSH.

La Figura 16 muestra una conexión SSH utilizando PuTTY y la Figura 17 una conexión Telnet mediante la terminal del sistema operativo.

Figura 16.

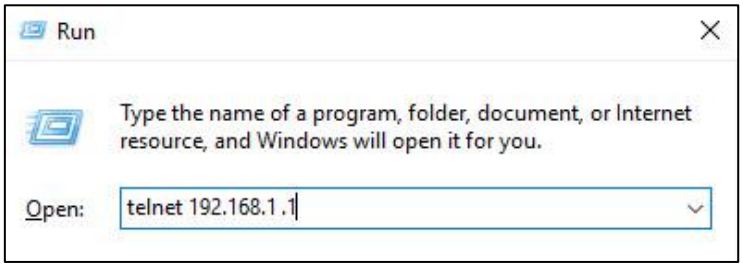
Conexión SSH al switch mediante Putty.



Nota. Elaboración propia.

Figura 17.

Conexión telnet mediante la terminal del sistema operativo.



Nota. Adaptado de "How to Log into a Network Switch: 3 Methods" por FS, 2025, FS (https://www.fs.com/eu-en/blog/three-approaches-to-log-in-to-your-network-switch-1256.html).

2.1.4.3. Acceso a la GUI mediante HTTP o HTTPS

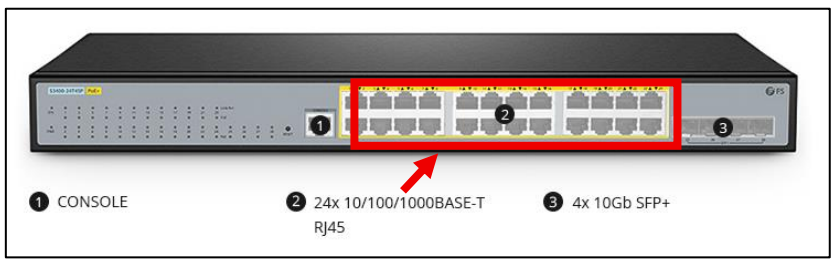
Es posible configurar y administrar un dispositivo de red a través del navegador web cuando el dispositivo tiene una dirección IP de gestión asignada a su interfaz de administración (MGMT) o a una VLAN destinada exclusivamente a tareas de gestión y se ha activado el servicio HTTP o HTTPS.

El acceso puede ser local o remoto, según desde dónde esté disponible la IP de gestión. Es local si el administrador se conecta directamente al switch con un cable de red en el puerto de administración (MGMT) o en uno de los puertos de acceso. Es remoto si el switch es accesible desde cualquier lugar, siempre que exista conectividad (FS, 2022).

La Figura 18 muestra el switch de la marca FS, modelo S3400-24T4SP destacando la ubicación de sus puertos de acceso y la Figura 19 ilustra la conexión al switch mediante HTTPS desde un navegador web.

Figura 18.

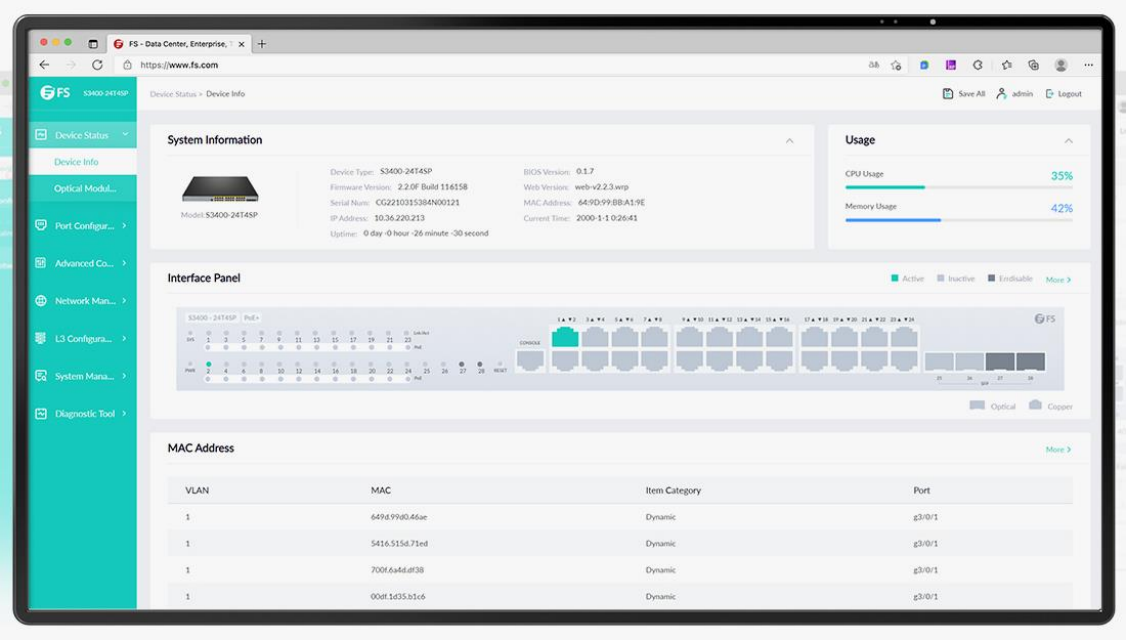
Switch marca FS, modelo S3400-24T4SP.



Nota. Adaptado de "S3400-24T4SP, Switch Gigabit Ethernet L2+ PoE+ de 24 puertos, 24 x PoE+ puertos @370W, con 4 x 10Gb SFP+ enlaces ascendentes, soporta apilamiento" por FS, 2025, FS (https://www.fs.com/es/products/165979.html?attribute=115361&id=4486351).

Figura 19.

Conexión HTTPS al switch mediante web.



Nota. Adaptado de “S3400-24T4SP, Switch Gigabit Ethernet L2+ PoE+ de 24 puertos, 24 x PoE+ puertos @370W, con 4 x 10Gb SFP+ enlaces ascendentes, soporta apilamiento” por FS, 2025, FS (https://www.fs.com/es/products/165979.html?attribute=115361&id=4486351).

2.1.4.4. Protocolos de Acceso Remoto para la Administración de Dispositivos

Los protocolos de acceso remoto permiten establecer sesiones interactivas con dispositivos de red a través de redes IP. A continuación, se mencionan los más relevantes:

- **Telnet:** Protocolo de acceso remoto que opera sobre TCP/23, pero no cifra los datos transmitidos, incluyendo credenciales. Debido a sus vulnerabilidades, su uso está desaconsejado en redes modernas (Postel & Reynolds, 2013).
- **SSH (Secure Shell):** Protocolo seguro que cifra todo el canal de comunicación. Opera sobre TCP/22 y permite una administración remota protegida de dispositivos de red, siendo actualmente el estándar recomendado (Ylonen & Lonvick, 2015).
- **HHTP (Hypertext Transfer Protocol):** Protocolo o conjunto de reglas de comunicación que opera sobre TCP/80 para la comunicación cliente-servidor. Es el método de comunicación que utilizan el navegador y los servidores web (Amazon Web Services, 2025).

- **HTTPS (Hypertext Transfer Protocol Secure):** Es una versión más segura o una extensión del protocolo HTTP y opera sobre TCP/443. En HTTPS, el navegador y el servidor establecen una conexión segura y cifrada antes de transferir datos (Amazon Web Services, 2025).

2.1.5. Control de Acceso

El control de acceso es un proceso de seguridad que permite a las organizaciones gestionar quién está autorizado a acceder a los datos y recursos corporativos. Utiliza políticas que verifican que los usuarios sean quienes afirman ser y garantiza que se otorguen niveles de acceso de control adecuados a los usuarios. Existen varios tipos de controles de acceso que las organizaciones pueden implementar para proteger sus datos y usuarios. Estos incluyen: controles físicos, lógicos y administrativos (Fortinet, 2024).

2.1.5.1. Controles físicos

Abordan las necesidades de seguridad basadas en procesos utilizando dispositivos físicos de hardware, como un lector de credenciales, torniquete o candado. La Figura 20 muestra un ejemplo de control de acceso físico mediante torniquete, empleado para garantizar que solo individuos previamente identificados y validados puedan acceder a las instalaciones.

Figura 20.

Control de acceso físico utilizando torniquetes.

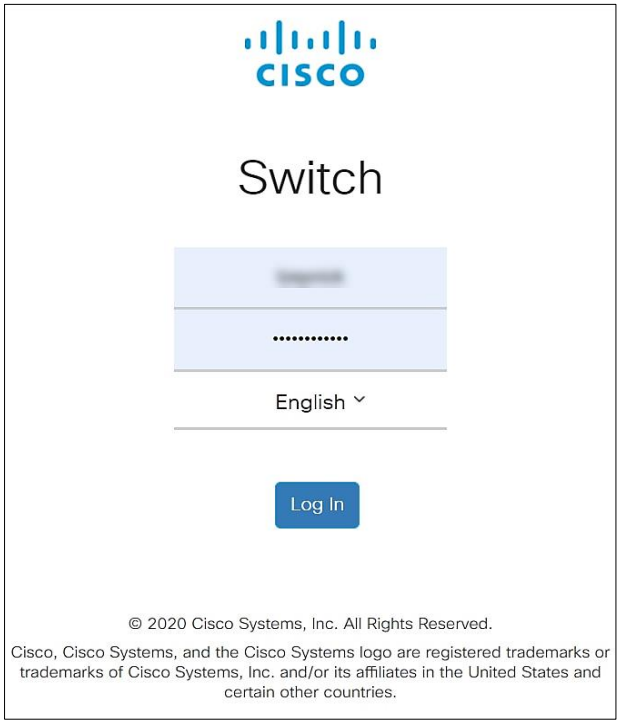
Nota. Adaptado de “Torniquetes CAME, control de acceso multipropósito respaldado con calidad y experiencia” por Tecnoseguro, 2019, Tecnoseguro (https://www.tecnoseguro.com/analisis/control-de-acceso/torniquetes-came-control-acceso-calidad-experiencia)

2.1.5.2. Controles lógicos

También llamados controles técnicos, son controles de seguridad que los sistemas informáticos y las redes implementan para proteger sus objetos (datos, servicios, aplicaciones ejecutables, dispositivos de red u otro tipo de tecnología de la información) de operaciones no autorizadas como descubrir, leer, crear, editar, eliminar y ejecutar objetos. La Figura 21 ilustra el control de acceso lógico mediante inicio de sesión, donde se evidencia el proceso de verificación de identidad previo al acceso a los recursos tecnológicos.

Figura 21.

Control de acceso lógico utilizando usuario y contraseña.



Nota. Adaptado de “Cómo iniciar sesión en la interfaz de usuario (UI) web de un switch Cisco Business” por Cisco, 2022, Cisco (https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-550x-series-stackable-managed-switches/1238-tz-log-into-the-gui-of-a-switch.html)

2.1.5.3. Controles Administrativos

También conocidos como controles gerenciales, son directivas lineamientos o avisos dirigidos a las personas dentro de la organización, como las políticas de uso aceptable, procedimientos de emergencia o entrenamientos de seguridad de los empleados. La Figura 22 es un ejemplo de la aplicación de control de acceso administrativo mediante políticas de uso de USB.

Figura 22.

Control de acceso administrativo mediante políticas de uso.

Nota. Adaptado de “Las USB siguen siendo un importante riesgo para la ciberseguridad” por Saynet, 2020, Saynet (https://saynet.com.mx/las-usb-siguen-siendo-un-importante-riesgo-para-la-ciberseguridad/).

2.1.6. Marco de Seguridad AAA

La autenticación, autorización y auditoría (AAA) es un marco de seguridad para el control de acceso a la red y la administración de dispositivos. Determina qué usuarios pueden acceder a la red y qué recursos o servicios están disponibles para los usuarios autorizados (Huawei Technologies, 2023).

2.1.6.1. Componentes del Marco de Seguridad AAA

Huawei Technologies (2025), señala que los principales componentes que participan en la aplicación del marco AAA son:

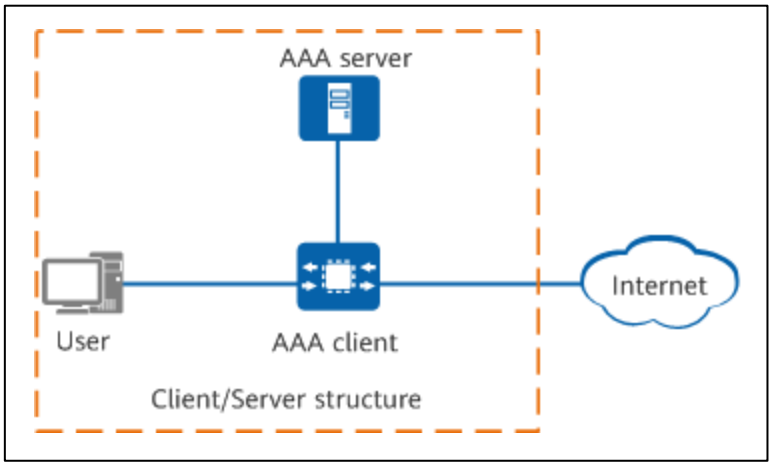
- **Usuario.** Usuario que intenta acceder a un recurso de la red desde una computadora.
- **Cliente AAA.** También llamado NAS (Network Access Server). Es un dispositivo de red (por ejemplo, un switch, router, firewall o punto de acceso) que recibe la conexión del usuario final y reenvía su solicitud al servidor AAA.

- **Servidor AAA.** Servidor que toma las decisiones de autenticación, autorización y auditoría. Según los protocolos de comunicación utilizados en AAA, los servidores AAA se clasifican en servidores de Servicio de Usuario de Acceso Telefónico de Autenticación Remota (RADIUS) y servidores de Sistema de Control de Acceso del Controlador de Acceso de Terminal (TACACS).

  La Figura 23 representa la conexión lógica de los componentes que participan en la aplicación del marco de seguridad AAA.

Figura 23.

Componentes del marco de seguridad AAA.



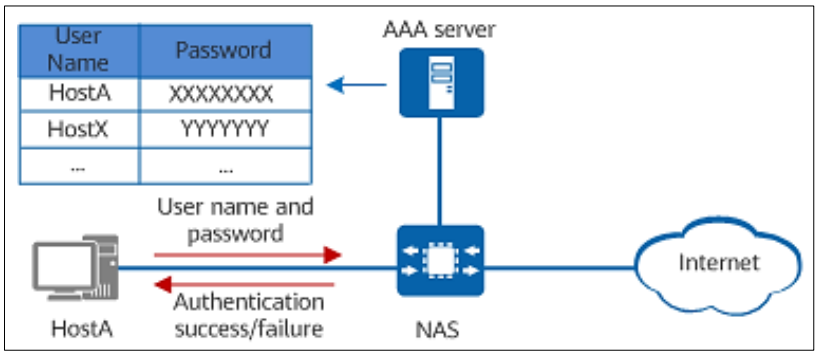
Nota. Adaptado de “What Is AAA?” por Huawei Technologies, 2023, Huawei (https://info.support.huawei.com/info-finder/encyclopedia/en/AAA.html).

2.1.6.2. Funciones del Marco de Seguridad AAA

- **Autenticación.** Se refiere al proceso de verificar la identidad de un usuario, dispositivo o sistema. Es el acto de confirmar que la entidad que intenta acceder a un sistema es quien dice ser. Para aplicarla, es preciso acreditar su identidad, por ejemplo, mediante la entrega de unas credenciales, un testigo, un certificado digital, etc. También es posible usar protocolos de autenticación que permiten demostrar la posesión de esas credenciales. La Figura 24 representa el funcionamiento de la autenticación de un usuario mediante el uso de credenciales.

Figura 24.

Autenticación mediante nombre de usuario y contraseña.

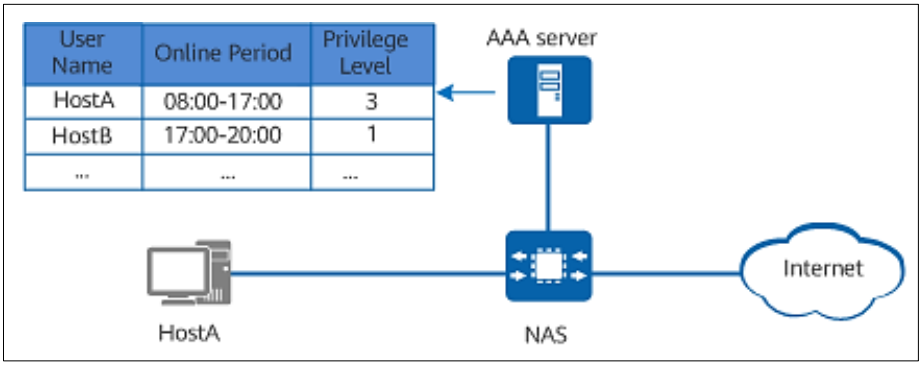


Nota. Adaptado de “What Is AAA?” por Huawei Technologies, 2023, Huawei (https://info.support.huawei.com/info-finder/encyclopedia/en/AAA.html).

- **Autorización.** Se refiere a la legitimidad de una entidad o persona para la ejecución. Para ello, el sistema debe reconocerle unos permisos o privilegios, y garantizarlos mediante técnicas como el control de acceso. La Figura 25 representa el funcionamiento de la autorización de un usuario.

Figura 25.

Autorización del usuario.

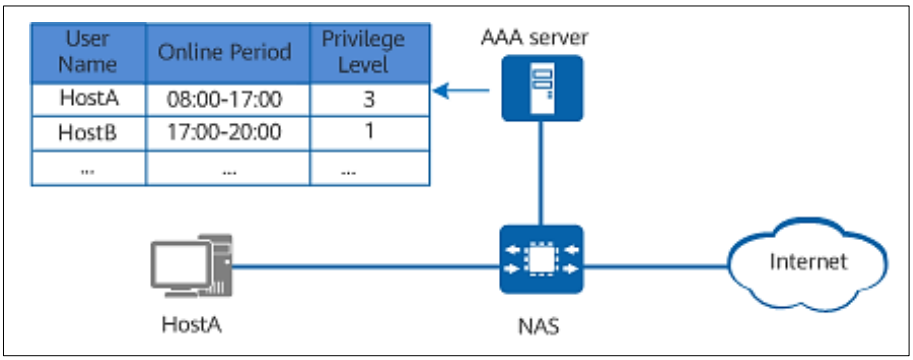


Nota. Adaptado de “What Is AAA?” por Huawei Technologies, 2023, Huawei (https://info.support.huawei.com/info-finder/encyclopedia/en/AAA.html).

- **Auditoría.** También conocida como contabilidad, implica el registro y el seguimiento de las actividades de usuarios y sistemas. Registra eventos como inicios de sesión, intentos de acceso, cambios en la configuración y otras operaciones críticas. La Figura 26 representa el funcionamiento de la auditoría de un usuario.

Figura 26.

Auditoría del usuario.



Nota. Adaptado de “What Is AAA?” por Huawei Technologies, 2023, Huawei (https://info.support.huawei.com/info-finder/encyclopedia/en/AAA.html).

2.1.6.3. Flujo de Operación del Marco de Seguridad AAA

AAA utiliza la estructura cliente/servidor, que es simple, escalable y facilita la gestión centralizada de la información del usuario.

El proceso de implementación de AAA inicia cuando el usuario establece una conexión con el cliente AAA antes de acceder a la red. Luego, el cliente envía las credenciales de autenticación del usuario al servidor AAA para que gestione la autenticación y autorización del usuario en función de sus credenciales y devuelve los resultados de autenticación y autorización al cliente. Finalmente, el cliente determina si se permite que el usuario acceda en función de los resultados de autenticación y autorización recibidos. Si se establece la sesión, se inicia el proceso de auditoría (Huawei Technologies, 2023).

2.1.6.4. Protocolos de Autenticación, Autorización y Auditoría.

El marco de seguridad AAA implementa autenticación, autorización y auditoría a través de múltiples protocolos. Los principales protocolos AAA son RADIUS y TACACS+.

2.1.6.5. Aplicaciones del Marco de Seguridad AAA

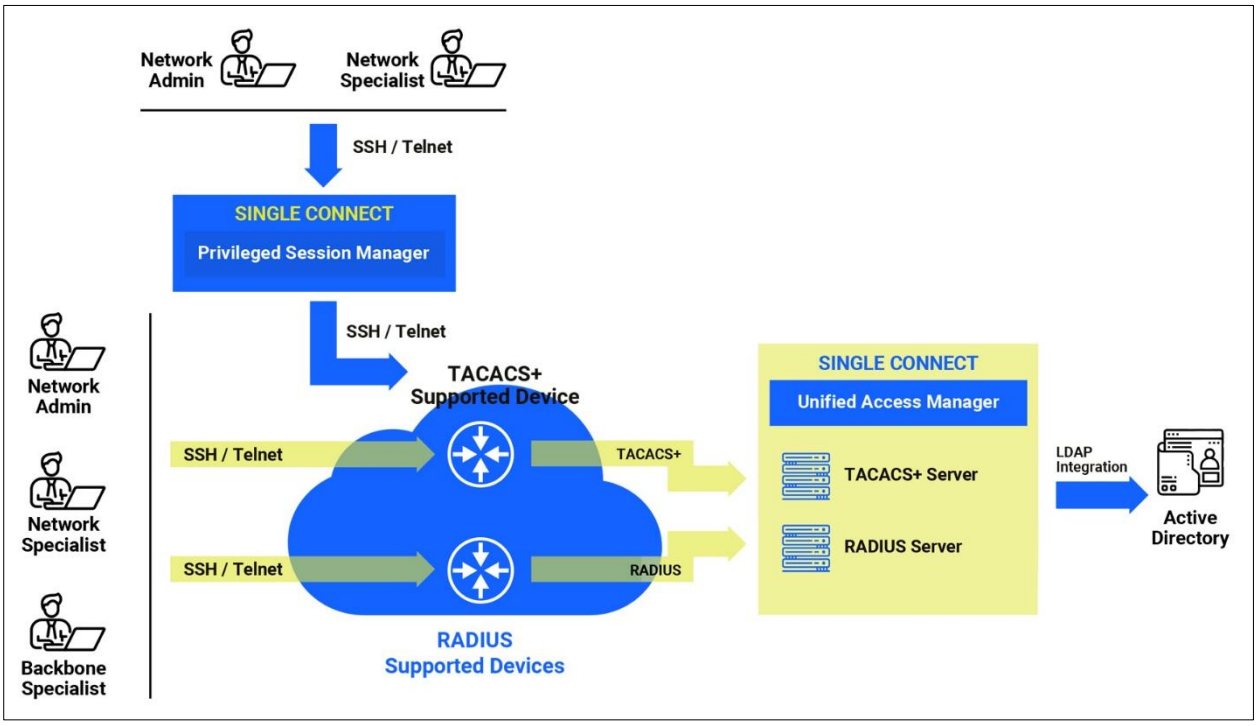
Según el modo de acceso de usuario, el marco de seguridad AAA se puede aplicar en los siguientes escenarios:

- **Administración de dispositivos**. Implica el control del acceso del usuario a sesiones, puertos de consolas de dispositivos de red, shell seguro (SSH) y más. AAA se puede utilizar para determinar los usuarios que pueden iniciar sesión en el dispositivo, los

comandos que se pueden ejecutar después del inicio de sesión y registrar las operaciones realizadas por los usuarios (Fortinet, 2025). La Figura 27 muestra los casos de uso del marco de seguridad AAA para la administración de dispositivos.

Figura 27.

Administración de dispositivos de red con RADIUS y TACACS+.

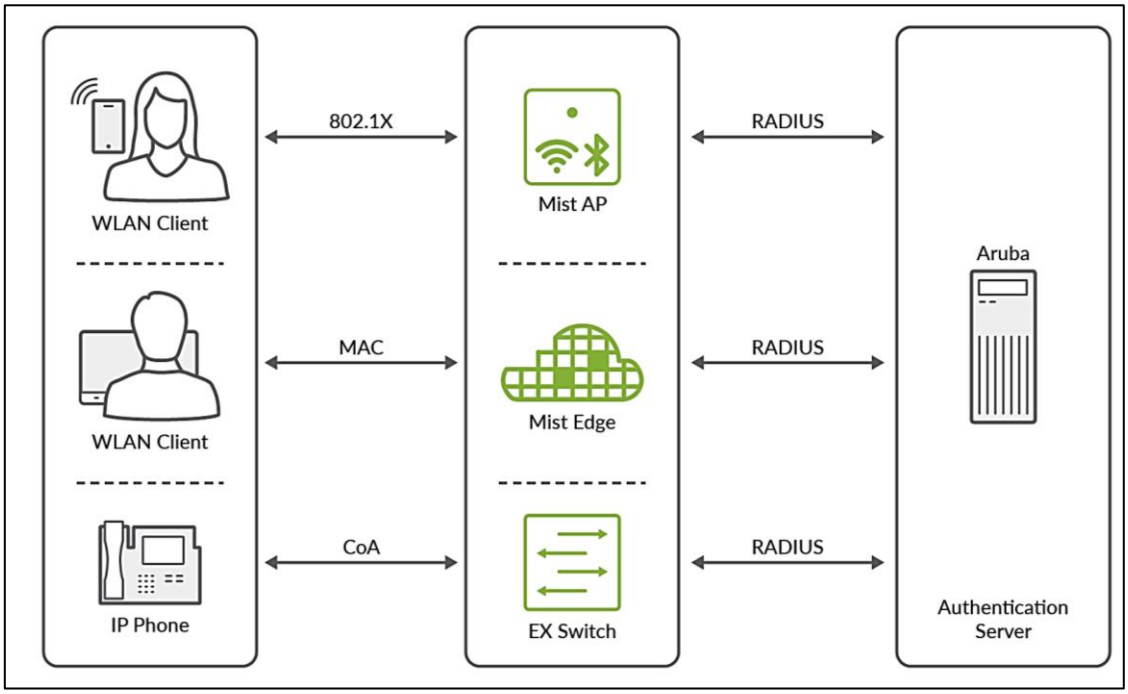


Nota. Adaptado de "¿Qué es la gestión de acceso TACACS+/RADIUS? ¿Cómo funciona?" por Kron Technologies, 2025, Kron Technologies (https://krontech.com/what-is-tacacs-radius-access-management-how-does-it-work#)

- **Control de acceso a la red**. Implica bloquear, otorgar o limitar el acceso en función de las credenciales de un usuario. AAA verifica la identidad de un dispositivo o usuario comparando la información presentada o ingresada con una base de datos de credenciales aprobadas. Si la información coincide, se otorga acceso a la red (Fortinet, 2024). La Figura 28 muestra los casos de uso del marco de seguridad AAA para el control de acceso a la red.

Figura 28.

Control de acceso a la red con RADIUS.



Nota. Adaptado de “Juniper Mist Wireless Assurance Configuration Guide”, por HPE Juniper Networking, 2025, Juniper (https://www.juniper.net/documentation/us/en/software/mist/mist-wireless/topics/task/arubaguestintegration.html)

2.1.7. Principio de Mínimo Privilegio

El principio del mínimo privilegio es un concepto relacionado con la seguridad de la información según el cual un usuario o entidad solo debe tener acceso a los datos, los recursos y las aplicaciones que necesite para llevar a cabo una determinada tarea (Palo Alto Networks, 2025).

2.1.8. Cifrado de Datos

El cifrado implica convertir texto sin formato legible por humanos en un texto incomprensible, conocido como texto cifrado. Esto significa tomar datos legibles y cambiarlos para que se vean como algo aleatorio. El cifrado implica utilizar una clave criptográfica; un conjunto de valores matemáticos que acuerdan tanto el emisor como el receptor. El receptor utiliza la clave para descifrar los datos y volver a convertirlos en texto sin formato legible (Kaspersky, 2025).

2.2. Marco Conceptual

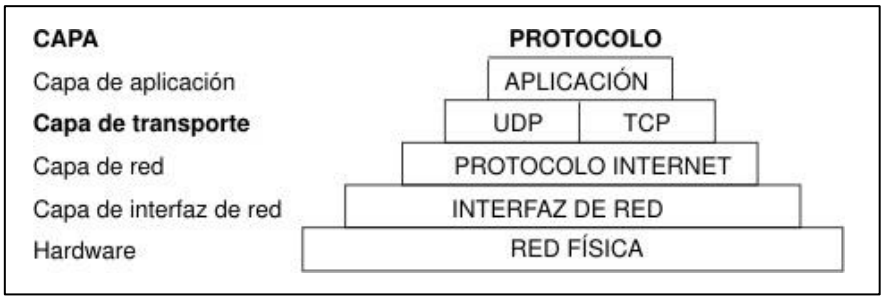
2.2.1. Protocolos de la Capa de Transporte

La capa de transporte contiene los protocolos UDP (User Datagram Protocol) y TCP (Transmission Control Protocol). Estos protocolos son necesarios para realizar conexiones entre sistemas. Ambos permiten que los programas envíen mensajes a las aplicaciones de otros sistemas principales y reciban mensajes de dichas aplicaciones. Cuando una aplicación envía a la capa de transporte una petición de envío de un mensaje, UDP y TCP dividen la información en paquetes, añaden una cabecera de paquete, incluida la dirección de destino, y envían la información a la capa de red para su proceso adicional. TCP y UDP utilizan puertos de protocolo para identificar el destino específico del mensaje (IBM, 2021).

La Figura 29 representa el modelo en capas TCP/IP, destacando la capa de transporte.

Figura 29.

Capa de transporte del modelo TCP/IP.



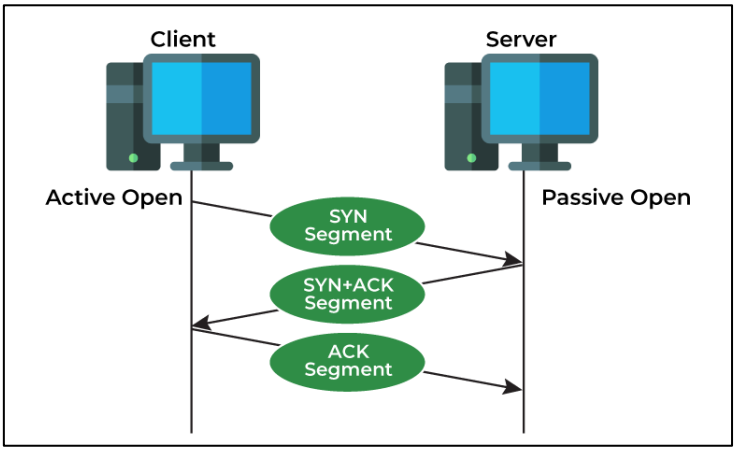
Nota. Adaptado de “Protocolos a nivel de transporte de Internet”, por IBM, 2021, IBM (https://www.ibm.com/docs/es/aix/7.1.0?topic=protocols-internet-transport-level)

2.2.1.1. Transmission Control Protocol (TCP)

Es un protocolo de la capa de transporte orientado a la conexión que facilita el intercambio de mensajes entre diferentes dispositivos a través de una red (Geeksforgeeks, 2025). La Figura 30 muestra el proceso de establecimiento de una conexión TCP mediante el intercambio de tres vías.

Figura 30.

Comunicación usando el protocolo TCP.

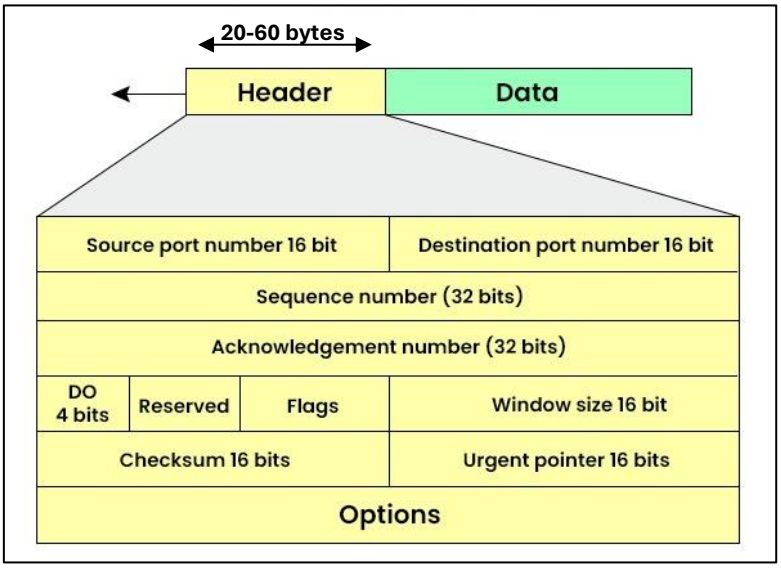


Nota. Adaptado de "Differences between TCP and UDP", por GeekforGeeks, 2021, GeekforGeeks (https://www.geeksforgeeks.org/computer-networks/differences-between-tcp-and-udp/)

La Figura 31 presenta el formato de la cabecera TCP, en el cual se especifican los campos que permiten identificar los puertos de origen y destino, el control de secuencias, las banderas de control y otros parámetros esenciales para la transmisión de datos.

Figura 31.

Cabecera TCP.



Nota. Adaptado de "TCP Header – Definition, Diagram and its Format (2025)", por PyNetLabs, 2025, PyNetLabs (https://www.pynetlabs.com/transmission-control-protocol-tcp-header/)

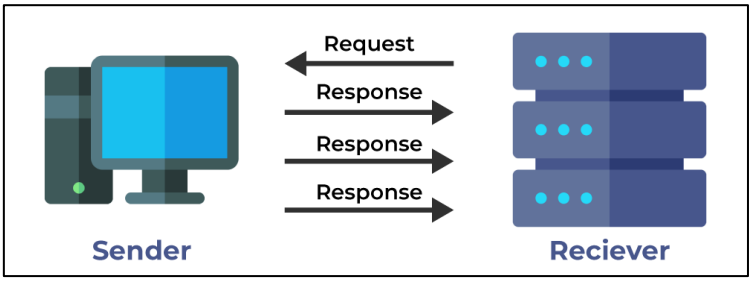
2.2.1.2. User Datagram Protocol (UDP)

Es un protocolo de la capa de transporte poco fiable y sin conexión. Por lo tanto, no es necesario establecer una conexión antes de la transferencia de datos. UDP ayuda a establecer conexiones de baja latencia y con tolerancia a pérdidas en la red (Geeksforgeeks, 2025).

La Figura 32 ilustra el modelo de comunicación basado en UDP, en el cual se observa el intercambio de mensajes bajo el esquema *request–response*, donde un cliente envía una solicitud y el servidor responde sin que exista un establecimiento previo de conexión.

Figura 32.

Comunicación usando el protocolo UDP.

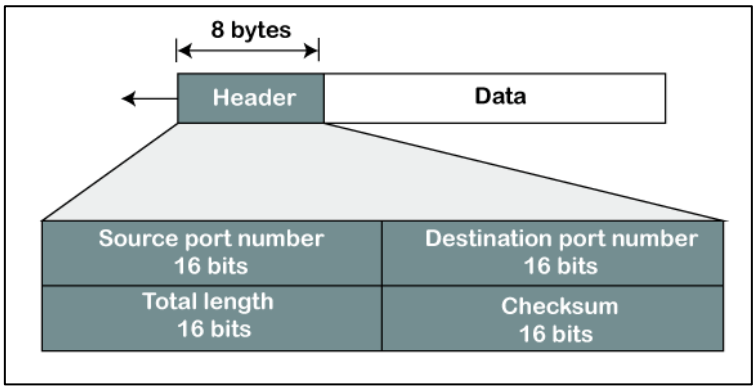


Nota. Adaptado de "Differences between TCP and UDP, por GeekforGeeks, 2021, GeekforGeeks (https://www.geeksforgeeks.org/computer-networks/differences-between-tcp-and-udp/)

La Figura 33 muestra el formato de la cabecera UDP, compuesta por los campos de puerto de origen, puerto de destino, longitud y suma de verificación (*checksum*), los cuales permiten gestionar el intercambio básico de datagramas entre aplicaciones.

Figura 33.

Cabecera UDP.



Nota. Adaptado de "UDP Frame Format", por K. Tae, 2023, K. Tae (https://ystc1247.tistory.com/entry/UDP-Frame-Format)

2.2.1.3. Diferencias entre TCP y UDP

Los protocolos TCP y UDP cumplen funciones distintas que impactan directamente en la confiabilidad, velocidad y modo de transmisión de los datos. Para comprender mejor estas diferencias y su aplicación en diversos escenarios de red, la Tabla 3 presenta una comparación entre las características de TCP y UDP.

Tabla 3.

Diferencias entre los protocolos de capa de transporte TCP y UDP.

Característica	TCP	UDP
Tipo de servicio	Protocolo orientado a la conexión. Esto significa que los dispositivos que se comunican deben establecer una conexión antes de transmitir datos y cerrarla después de transmitirlos.	Protocolo orientado a datagramas. Esto se debe a que no hay sobrecarga para abrir, mantener ni terminar una conexión. UDP es eficiente para transmisiones de red de difusión y multidifusión.
Fiabilidad	TCP es confiable ya que garantiza la entrega de datos al enrutador de destino.	No se puede garantizar la entrega de datos al destino en UDP.
Mecanismo de comprobación de errores	Proporciona amplios mecanismos de comprobación de errores , ya que proporciona control de flujo y reconocimiento de datos.	Solo tiene el mecanismo básico de verificación de errores mediante sumas de comprobación.
Reconocimiento	Hay un segmento de reconocimiento.	Sin segmento de reconocimiento.
Secuencia	La secuenciación de datos es una característica del Protocolo de Control de Transmisión (TCP). Esto significa que los paquetes llegan en orden al receptor.	En UDP no hay secuenciación de datos. Si se requiere el orden, la capa de aplicación debe gestionarlo.
Velocidad	TCP es comparativamente más lento que UDP.	UDP es más rápido, más simple y más eficiente que TCP.
Retransmisión	La retransmisión de paquetes perdidos es posible en TCP, pero no en UDP.	No hay retransmisión de paquetes perdidos en el Protocolo de datagramas de usuario (UDP).
Longitud del encabezado	Tiene un encabezado de longitud variable de (20-60) bytes.	Tiene un encabezado de longitud fija de 8 bytes.
Peso	TCP es pesado.	UDP es ligero.
Técnicas de handshake	Utiliza handsahke como SYN, ACK, SYN-ACK	Es un protocolo sin conexión, es decir, sin protocolo de enlace.
Radiodifusión	TCP no admite transmisión.	UDP admite transmisión.
Protocolos	TCP es utilizado por HTTP, HTTPS , FTP , SMTP y Telnet .	UDP es utilizado por DNS , DHCP, TFTP, SNMP , RIP y VoIP .
Tipo de flujo	La conexión TCP es un flujo de bytes.	La conexión UDP es un flujo de mensajes.
Arriba	Bajo pero superior al UDP.	Muy bajo.
Aplicaciones	Se utiliza principalmente en situaciones en las que es necesario un procedimiento de comunicación seguro y confiable, como en el correo electrónico, la navegación web y en los servicios militares.	Se utiliza en situaciones donde es necesaria una comunicación rápida pero la confiabilidad no es una preocupación, como VoIP, transmisión de juegos, transmisión de video y música, etc.

Nota. Adaptado de “Differences between TCP and UDP, por GeekforGeeks, 2021, GeekforGeeks (https://www.geeksforgeeks.org/computer-networks/differences-between-tcp-and-udp/)

2.2.2. Secure Shell (SSH)

Secure Shell, también conocido como SSH, es un protocolo de seguridad de red que utiliza mecanismos de cifrado y autenticación. Permite a los clientes SSH conectarse de forma segura a un servidor SSH en ejecución y que puedan ejecutar operaciones remotas utilizando el puerto TCP 22 (García, 2025).

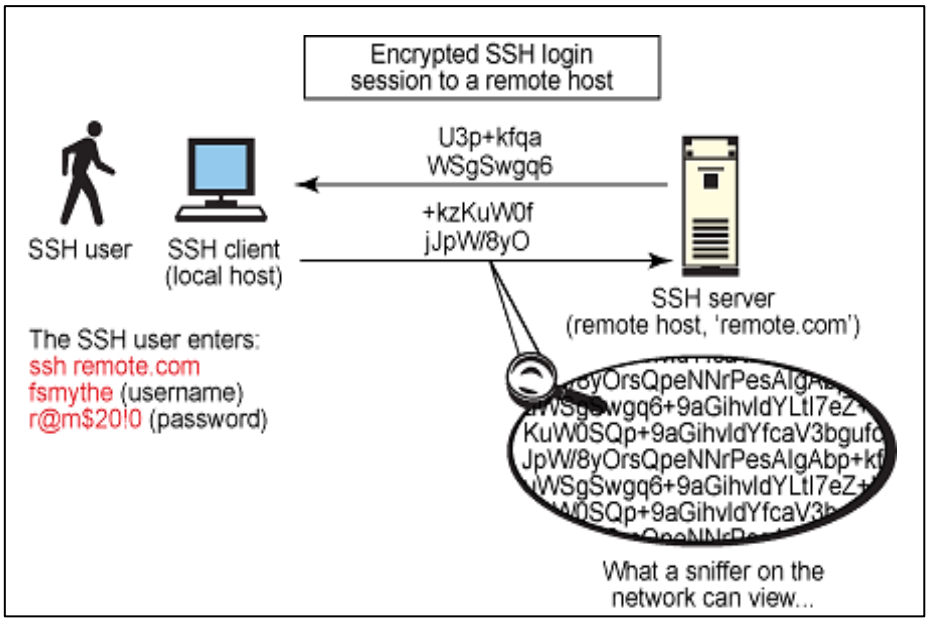
El protocolo SSH utiliza una arquitectura cliente-servidor para establecer conexiones seguras. Sus principales componentes son:

- **Cliente SSH**. Es la aplicación que se utiliza para la conexión a un servidor remoto. Se puede utilizar diferentes clientes SSH, como OpenSSH en sistemas Linux o PuTTY en Windows.
- **Servidor SSH**. Se ejecuta en el servidor remoto al que se desea acceder. Este servidor está configurado para aceptar conexiones SSH y autenticar a los usuarios.

La Figura 34 ilustra el intercambio de datos cifrados en la comunicación entre el cliente y servidor SSH.

Figura 34.

Sesión cifrada con el protocolo SSH.



Nota. Adaptado de “Getting started with SSH security and configuration”, por R. Hill, 2014, IBM (https://developer.ibm.com/articles/au-sshsecurity/).

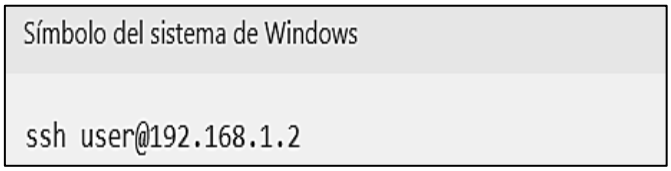
2.2.3. OpenSSH

Las compilaciones más recientes de Windows 10 y Windows 11 incluyen un servidor SSH integrado y un cliente basados en OpenSSH, la cual es una herramienta de conectividad para el inicio de sesión remoto que usa el protocolo SSH (Microsoft, 2024).

Como se observa en la Figura 35, para iniciar una sesión de SSH en el símbolo del sistema de Windows, se ejecuta el comando *ssh* con el nombre de usuario y la dirección IP del equipo al que se desea acceder de forma remota.

Figura 35.

Conexión mediante SSH desde el símbolo del sistema de Windows.



Nota. Adaptado de “Differences between TCP and UDP, por Microsoft, 2021, Microsoft Learn (https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/factoryos/connect-using-ssh?view=windows-11)

2.2.4. Remote Authentication Dial-In User Service (RADIUS)

RADIUS es un protocolo de red que proporciona autenticación, autorización y contabilidad a los usuarios que acceden a una red remota utilizando un modelo cliente/servidor.

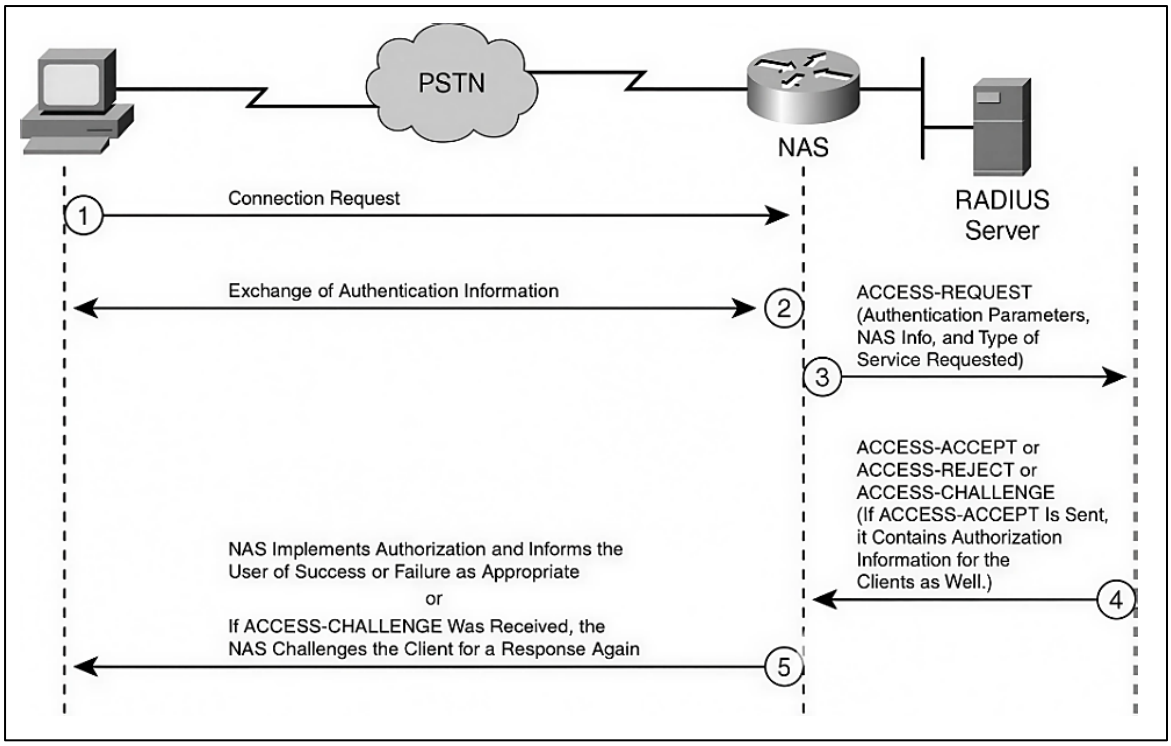
Dado que RADIUS se definió antes que el marco de seguridad AAA, combina autenticación y autorización. La autenticación y la contabilidad de RADIUS pueden ejecutarse en diferentes servidores (Huawei, 2025).

RADIUS opera en el puerto UDP 1812 para la autenticación y autorización (Rigney, et al.,2000). Por otro lado, el puerto UDP 1813 se utiliza para la auditoría en la comunicación entre el cliente (NAS) y el servidor (Rigney, 2000).

Las Figuras 36, 37 y 38 ilustran el flujo de paquetes de autenticación, autorización y auditoría entre el cliente y el servidor RADIUS.

Figura 36.

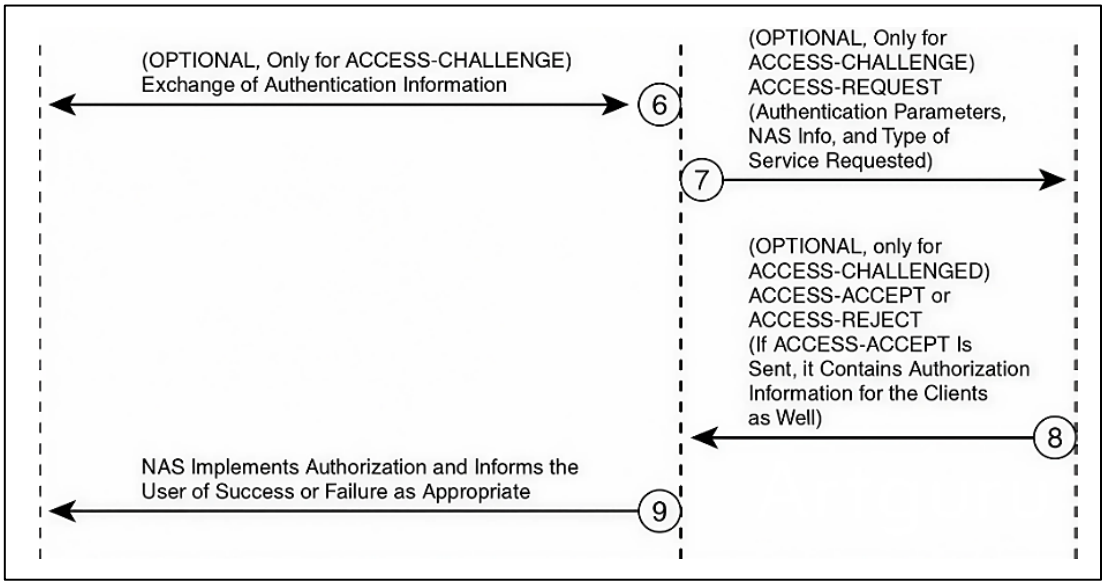
Flujo de paquetes de autenticación y autorización RADIUS.



Nota. Adaptado de “Overview of Authentication, Authorization, and Accounting (AAA)”, por M. Hoda, 2006, Flylib (https://flylib.com/books/en/1.233.1.70/1/).

Figura 37.

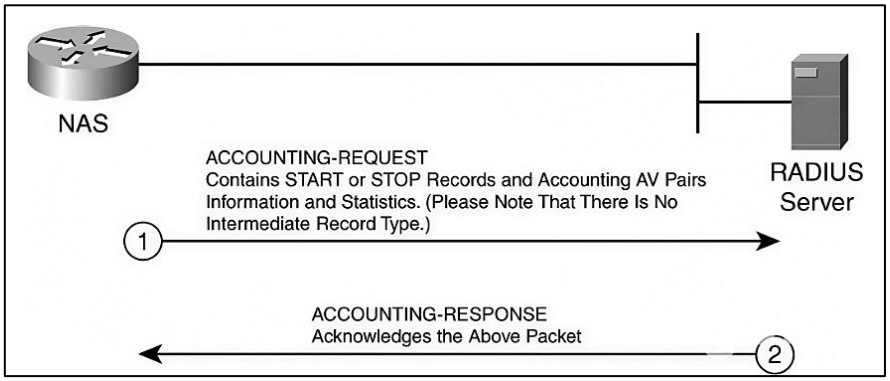
Flujo de paquetes de autenticación y autorización RADIUS (opcional).



Nota. Adaptado de “Overview of Authentication, Authorization, and Accounting (AAA)”, por M. Hoda, 2006, Flylib (https://flylib.com/books/en/1.233.1.70/1/)

Figura 38.

Flujo de paquetes de auditoría TACACS+.



Nota. Adaptado de “Overview of Authentication, Authorization, and Accounting (AAA)”, por M. Hoda, 2006, Flylib (https://flylib.com/books/en/1.233.1.70/1/).

El detalle del formato del paquete RADIUS, los cuerpos de cada tipo de paquete (autenticación, autorización y auditoría), así como los procesos correspondientes, se presentan en el **Anexo B**.

2.2.5. Terminal Access Controller Access-Control System Plus (TACACS+)

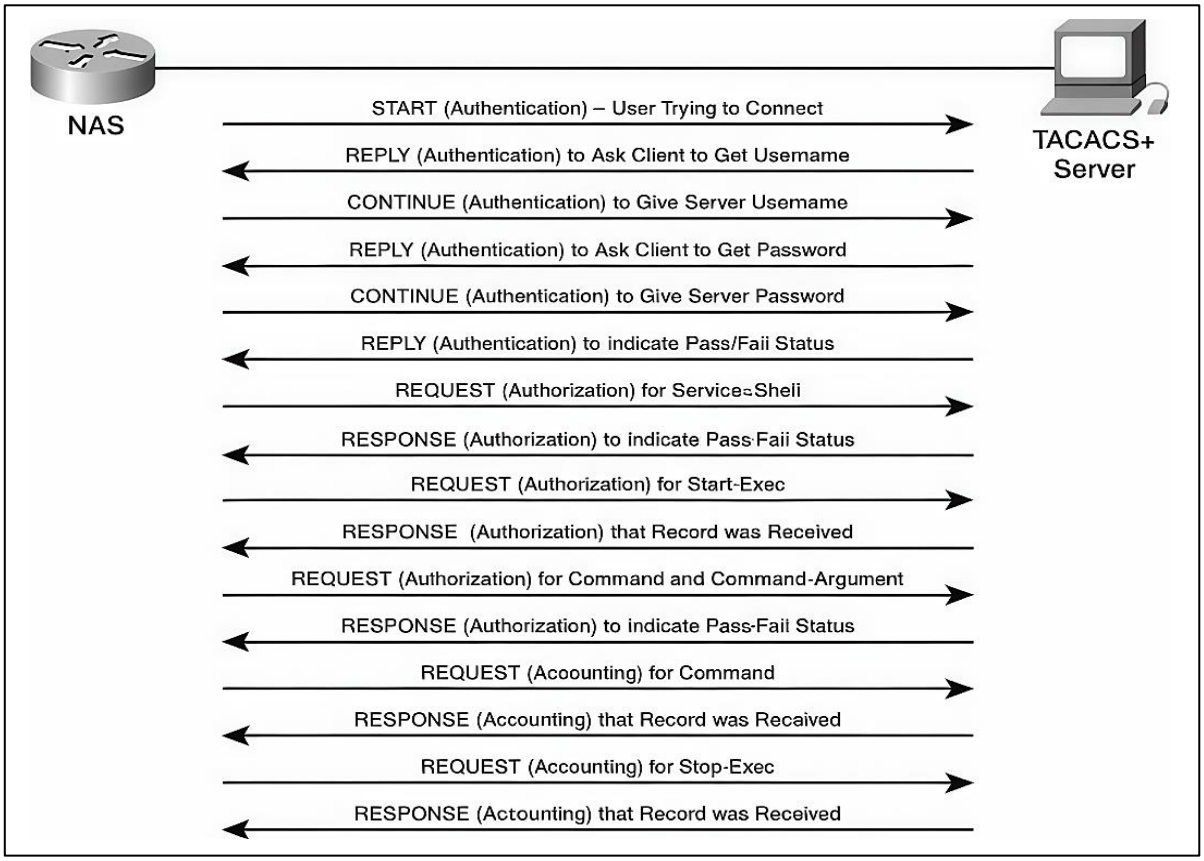
TACACS+ es un protocolo de autenticación, autorización y auditoría para controlar el acceso a equipos de red que utiliza un modelo cliente/servidor. Separa las funciones de autenticación, autorización y auditoría, y cada función puede implementarse de forma independiente y en servidores diferentes si es necesario (Dahm, et al., 2020).

TACACS+ utiliza el puerto TCP 49 para la comunicación entre el cliente (NAS) y el servidor. La sesión de autenticación puede implicar el intercambio de un número arbitrario de paquetes. En cambio, las sesiones de auditoría y autorización constan de un único par de paquetes (solicitud y respuesta) (Dahm, et al., 2020).

La Figura 39 ilustra el flujo de paquetes de autenticación, autorización y auditoría entre el cliente y el servidor TACACS+.

Figura 39.

Flujo de paquetes AAA TACACS+.



Nota. Adaptado de “Overview of Authentication, Authorization, and Accounting (AAA)”, por M. Hoda, 2006, Flylib (https://flylib.com/books/en/1.233.1.70/1/).

El detalle del encabezado del paquete TACACS+, los cuerpos de cada tipo de paquete (autenticación, autorización y auditoría), así como los procesos correspondientes, se presentan en el **Anexo C**.

2.2.6. FreeRADIUS

FreeRADIUS es un servidor RADIUS de código abierto que ofrece servicios de autenticación, autorización y auditoría (AAA) para el acceso a la red (FreeRADIUS, 2025).

La Figura 40 muestra una captura de la página oficial de FreeRADIUS, donde se pueden encontrar sus principales características y documentación disponible para su implementación.

Figura 40.

Página oficial de FreeRADIUS.

Nota. Elaboración propia.

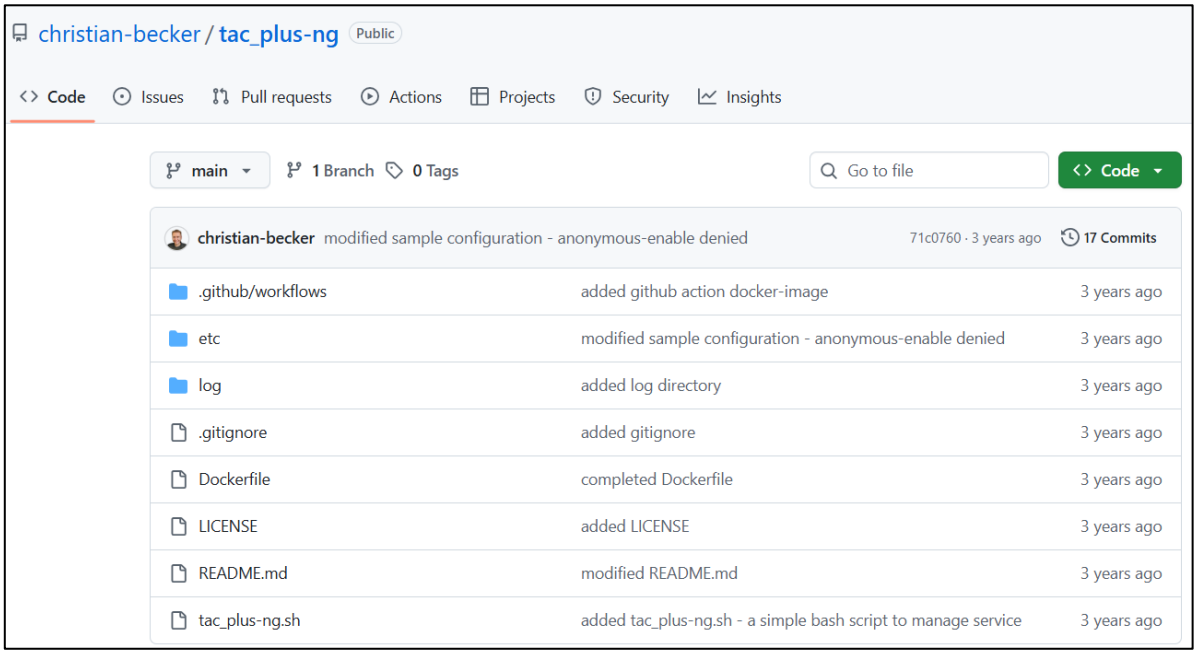
2.2.7. Tac_plus-ng

Tac_plus-ng es un demonio TACACS+ que proporciona servicios de autenticación, autorización y contabilidad a componentes de red como routers y switches. Es una reescritura importante del código fuente público original de Cisco y, a su vez, se basa en tac_plus (Huber, 2025).

La Figura 41 muestra el repositorio oficial de *tac_plus-ng* en GitHub, donde se encuentran los archivos fuente, documentación técnica y recursos necesarios para su implementación.

Figura 41.

Repositorio en GitHub de Tac_plus-ng.



Nota. Elaboración propia.

2.2.8. Wireshark

Wireshark es un analizador de paquetes de red. Un analizador de paquetes de red presenta los datos de los paquetes capturados con el mayor detalle posible (Wireshark, 2025). Algunas de las características que ofrece Wireshark son:

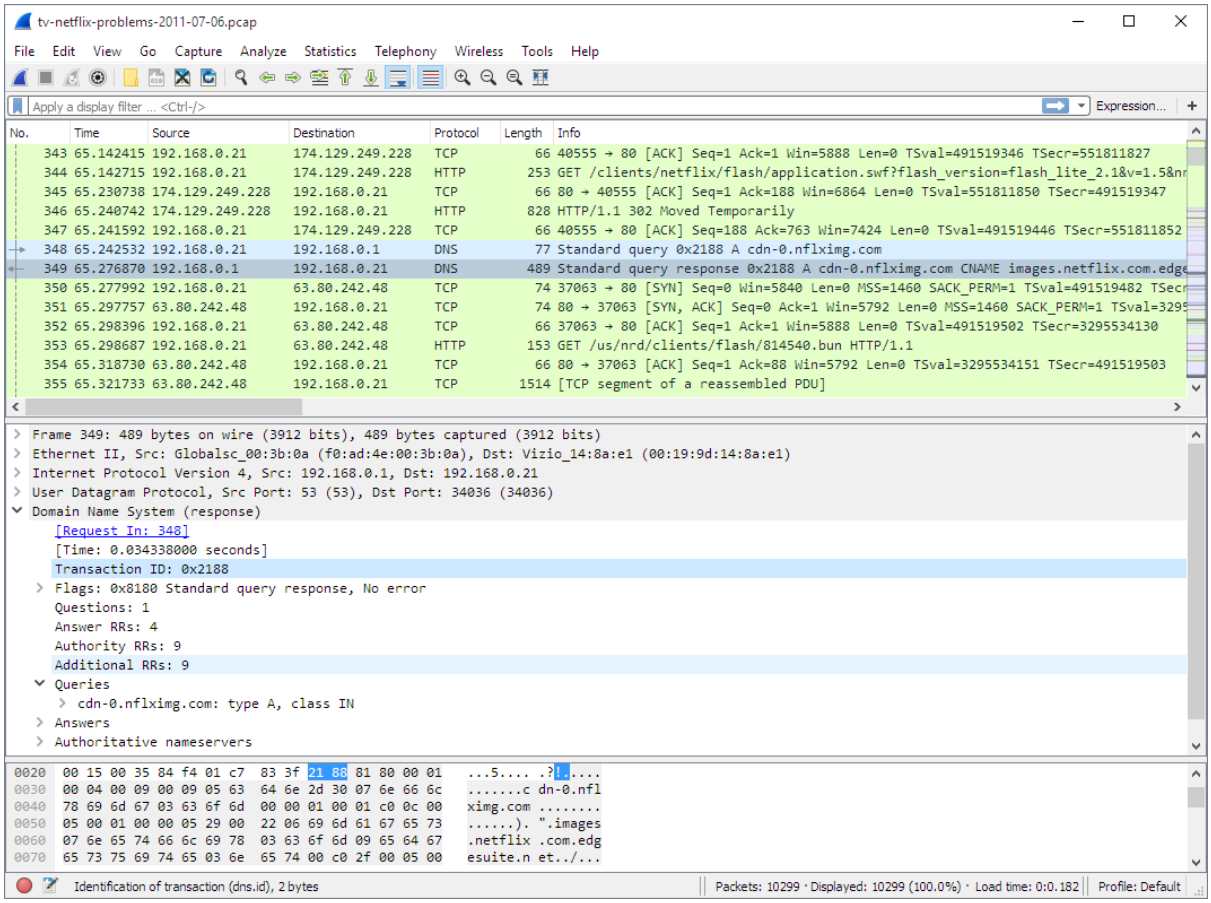
- Está disponible para UNIX y Windows.
- Captura paquetes de datos en vivo desde una interfaz de red.
- Permite abrir archivos que contengan datos de paquetes capturados con tcpdump/WinDump, Wireshark y muchos otros programas de captura de paquetes.
- Permite importar paquetes desde archivos de texto que contienen volcados hexadecimales de datos de paquetes.
- Muestra paquetes con información de protocolo muy detallada.
- Guarda paquetes de datos capturados.
- Exporta algunos o todos los paquetes en varios formatos de archivos de captura.
- Busca y filtra paquetes según criterios establecidos.
- Colorea la visualización de paquetes basándose en filtros.

- Permite crear varias estadísticas.

La Figura 42 presenta un ejemplo de captura de paquetes realizada con Wireshark, donde se observan los encabezados y detalles de los datagramas intercambiados durante la comunicación en la red.

Figura 42.

Captura de paquetes con Wireshark.



Nota. Adaptado de "Capítulo 1. Introducción" por Wireshark, 2025, Wireshark (https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs).

2.2.9. Latencia de Red

La latencia de red es el retraso en la comunicación de la red. Muestra el tiempo que tardan los datos en transferirse a través de la red y se mide mediante la métrica del tiempo de ida y vuelta (RTT). Un tiempo de ida y vuelta (RTT) idóneo debe ser inferior a 100 milisegundos para obtener un rendimiento óptimo. Un RTT de 100 a 200 milisegundos significa que el rendimiento puede verse afectado, pero los usuarios podrán seguir accediendo al servicio. Un RTT de 200 milisegundos o más significa que el rendimiento es

deficiente y los usuarios experimentan tiempos de espera o de carga de página prolongados.

Un RTT de más de 375 milisegundos normalmente provoca la finalización de una conexión (Amazon Web Services, 2024).

Varios factores influyen en el tiempo de ida y vuelta (RTT), por ejemplo:

- La distancia física entre el equipo de origen y el equipo de destino.
- Medio de transmisión (cobre, fibra o tecnología inalámbrica).
- Congestión de red.
- Tiempo de respuesta del destino.
- Tráfico de red de área local.

CAPÍTULO III

Desarrollo del Trabajo de Investigación

3.1. Sistema con RADIUS

A continuación, se describe el sistema que utiliza el protocolo RADIUS para la gestión centralizada de la autenticación, autorización y auditoría de los usuarios que acceden al switch.

3.1.1. Componentes del Sistema

El sistema se compone de los siguientes elementos de hardware y software:

- **Servidor de Acceso a la Red (NAS):** Switch marca Cisco, modelo C9200-24P, que actúa como cliente RADIUS. Su función principal es conectar físicamente los dispositivos de la red y, al mismo tiempo, redireccionar las solicitudes de autenticación de los usuarios hacia el servidor RADIUS.

Figura 43.

Switch Cisco C9200-24P.

Nota. Elaboración propia.

Figura 44.

Modelo, versión de software e imagen del switch Cisco C9200-24P.

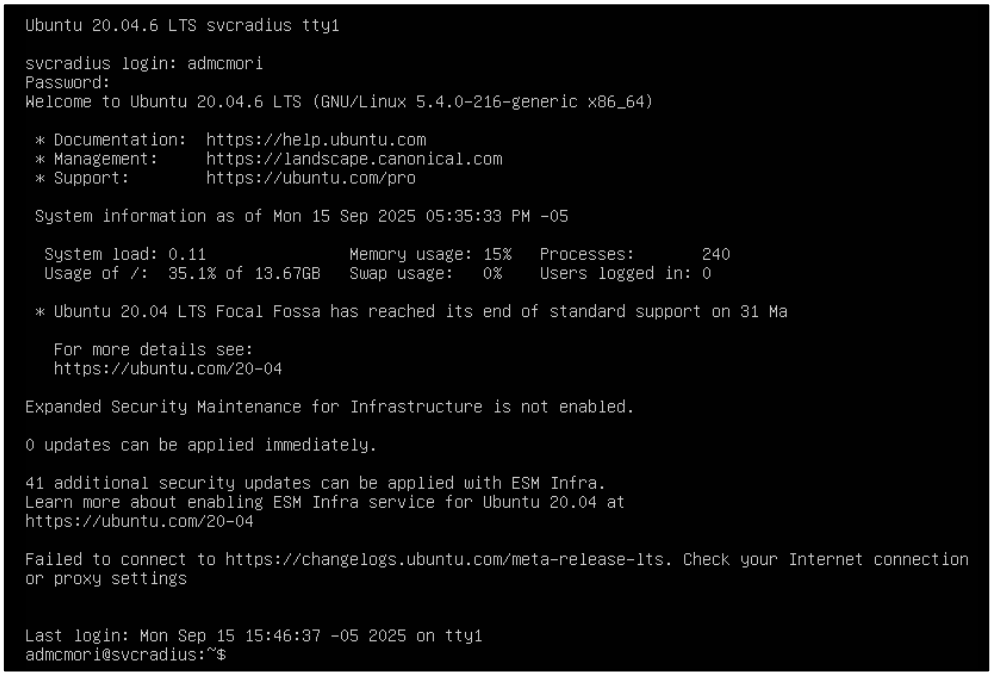
```
Switch Ports Model              SW Version        SW Image
------ ----- -----              ----------        ----------
*    1 32    C9200-24P          17.06.04          CAT9K_LITE_IOSXE
```

Nota. Elaboración propia.

- **Servidor RADIUS:** Máquina virtual en un host físico, corriendo el software FreeRADIUS. Este servidor centraliza la gestión de autenticación, autorización y auditoría (AAA) para los usuarios que intentan acceder al NAS.

Figura 45.

Máquina virtual del servidor RADIUS.

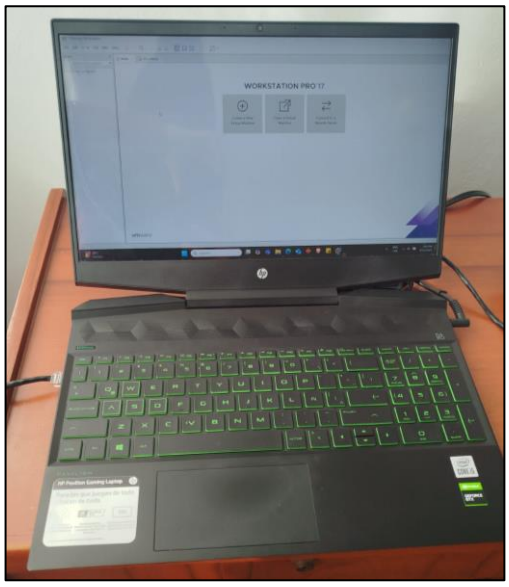


Nota. Elaboración propia.

- **Host del servidor RADIUS:** Máquina anfitriona donde se aloja el servidor RADIUS virtual y proporciona los recursos de hardware necesarios para su correcto funcionamiento.

Figura 46

Host del servidor RADIUS.



Nota. Elaboración propia.

- **Laptop del usuario:** Computadora desde donde el usuario inicia una conexión para acceder a la configuración del switch.

Figura 47.

Laptop del usuario.

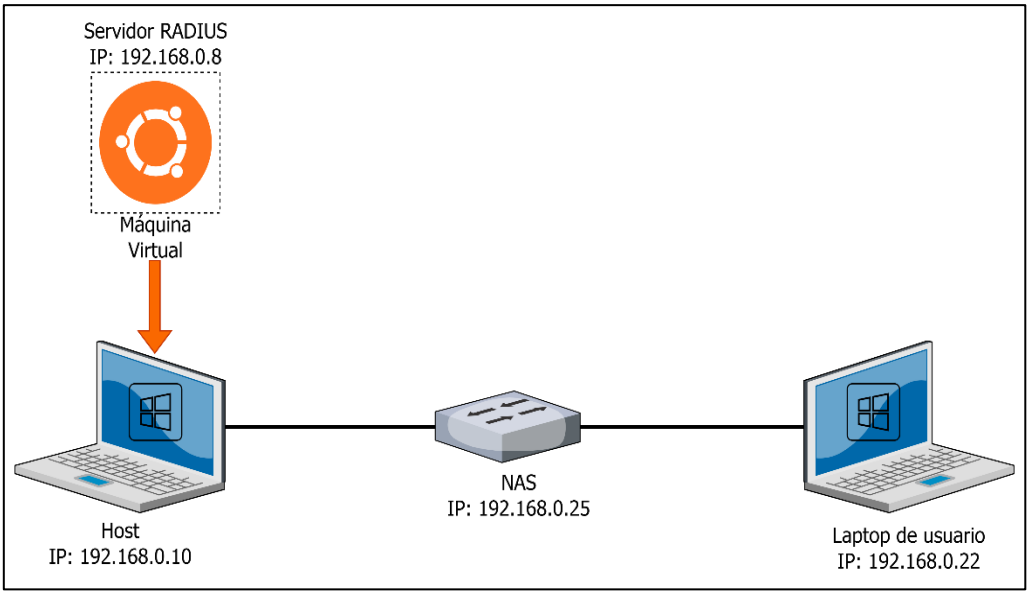
Nota. Elaboración propia.

3.1.2. Arquitectura de Red del Sistema

La arquitectura del sistema que utiliza el protocolo RADIUS se basa en la interconexión del switch, el servidor RADIUS y la laptop del usuario. La Figura 48 muestra la conexión física y lógica entre los componentes, así como el direccionamiento IP utilizado.

Figura 48.

Diagrama de topología de red del sistema con RADIUS.



Nota. Elaboración propia.

3.1.3. Implementación del Sistema

A continuación, se detallan las configuraciones realizadas para el despliegue del sistema con RADIUS

3.1.3.1. Configuración en el Switch

Las conexiones remotas al switch se restringen exclusivamente mediante el protocolo SSH a su dirección IP de gestión.

Figura 49.

Dirección IP para la gestión del switch.

```
interface Vlan1
 ip address 192.168.0.25 255.255.255.0
```

Nota. Elaboración propia.

Se crean credenciales locales como contingencia ante un fallo en la comunicación con el servidor RADIUS.

Figura 50.

Configuración de usuario local.

```
username local_user privilege 2 password 0 cisco
```

Nota. Elaboración propia.

Se crea y protege el acceso al modo privilegiado del switch con una contraseña cifrada.

Figura 51.

Configuración de contraseña para el modo privilegiado.

```
enable secret 9 $9$HiLjyQQT1KCmdE$koCDxAtiMTHpIxDnuOy8fkdcRqO0eA64m9p50iNo9cY
```

Nota. Elaboración propia.

Se activa el soporte para los procesos de autenticación, autorización y auditoría (AAA).

Figura 52.

Activación del soporte AAA.

```
aaa new-model
```

Nota. Elaboración propia.

Luego, se especifica que la interfaz Vlan1 se utilizará para la comunicación con el

servidor RADIUS.

Figura 53.

Interfaz de switch utilizada para la comunicación con el servidor RADIUS.

```
ip radius source-interface Vlan1
```

Nota. Elaboración propia.

Se crea el grupo de servidores RADIUS con el nombre *radius_group* y el servidor que pertenece a este grupo con el nombre *server01*.

Figura 54.

Configuración de grupo de servidores RADIUS.

```
aaa group server radius radius_group
 server name server01
```

Nota. Elaboración propia.

Se configura la dirección IP del servidor RADIUS *server01*. Además, se establece la clave compartida *testing123*, el timeout de 10 segundos y *retransmit* de 3 veces.

Figura 55.

Configuración de los parámetros del servidor RADIUS.

```
radius server server01
 address ipv4 192.168.0.8 auth-port 1812 acct-port 1813
 timeout 10
 retransmit 3
 key testing123
```

Nota. Elaboración propia.

Se habilita el servicio AAA, definiendo las credenciales locales como opción principal y al grupo de servidores RADIUS como respaldo.

Figura 56.

Configuración de autenticación, autorización y auditoría RADIUS.

```
aaa authentication login default local group radius_group
aaa authorization exec default local group radius_group
aaa accounting exec default start-stop group radius_group
```

Nota. Elaboración propia.

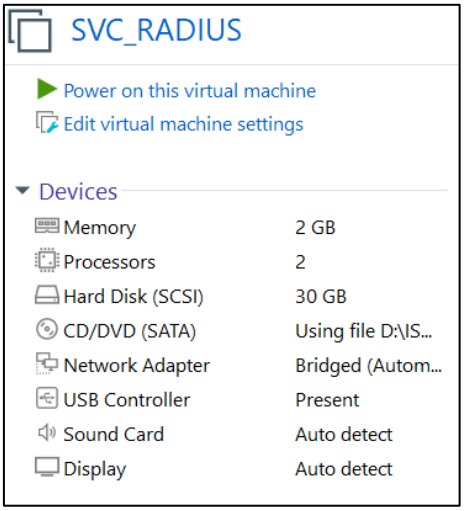
3.1.3.2. Despliegue y Configuración del Servidor RADIUS

Para la implementación del sistema de autenticación centralizada, se configura el servidor RADIUS en una máquina virtual y se definen los recursos necesarios, tales como

memoria, procesador y almacenamiento.

Figura 57.

Características de la máquina virtual del servidor RADIUS.

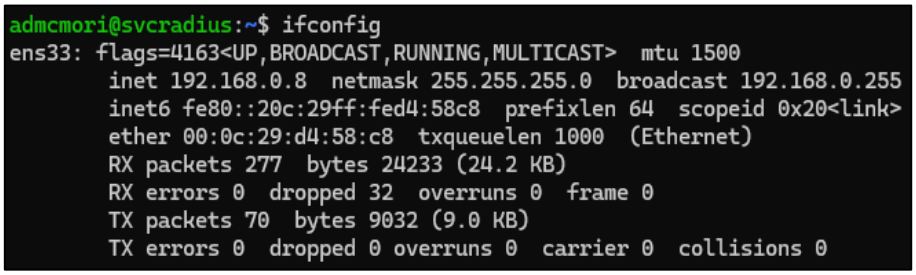


Nota. Elaboración propia.

Posteriormente, se configura la interfaz de red de la máquina virtual y se sincroniza la hora y la fecha del servidor, aspecto fundamental para la trazabilidad de registros.

Figura 58

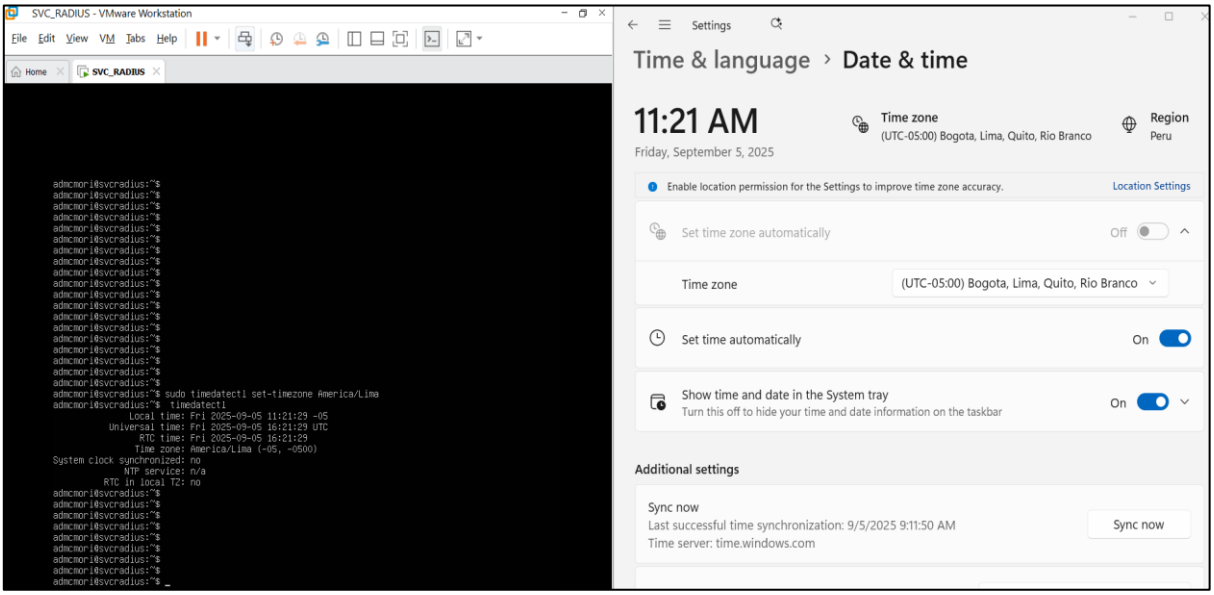
Configuración de interfaz de red del servidor RADIUS.



Nota. Elaboración propia.

Figura 59.

Sincronización de hora y fecha del servidor RADIUS.



Nota. Elaboración propia.

Luego, se instala el software FreeRADIUS. Una vez instalado, se crean los usuarios “admin” y “readonly” con sus respectivas contraseñas y niveles de privilegio, lo que permitirá establecer un esquema de acceso diferenciado.

Figura 60.

Instalación de FreeRADIUS.

```
admcmori@svcradius:~$ sudo apt install freeradius
[sudo] password for admcmori:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl libfreeradius3 libtalloc2
  libtevent0 libwbclient0 make ssl-cert
Suggested packages:
  freeradius-ldap freeradius-postgresql freeradius-mysql freeradius-krb5 snmp freeradius-python3 libclone-perl
  libmldbm-perl libnet-daemon-perl libsql-statement-perl make-doc openssl-blacklist
The following NEW packages will be installed:
  freeradius freeradius-common freeradius-config freeradius-utils freetds-common libct4 libdbi-perl libfreeradius3
  libtalloc2 libtevent0 libwbclient0 make ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,527 kB of archives.
After this operation, 9,655 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 libtalloc2 amd64 2.3.3-0ubuntu0.20.04.1 [29.6 kB]
Get:2 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 libtevent0 amd64 0.11.0-0ubuntu0.20.04.1 [36.2 kB]
Get:3 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 libwbclient0 amd64 2:4.15.13+dfsg-0ubuntu0.20.04.8 [211 kB]
Get:4 http://pe.archive.ubuntu.com/ubuntu focal/main amd64 freetds-common all 1.1.6-1.1 [24.8 kB]
Get:5 http://pe.archive.ubuntu.com/ubuntu focal/main amd64 libct4 amd64 1.1.6-1.1 [152 kB]
Get:6 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 freeradius-common all 3.0.20+dfsg-3ubuntu0.5 [218 kB]
Get:7 http://pe.archive.ubuntu.com/ubuntu focal/main amd64 make amd64 4.2.1-1.2 [162 kB]
Get:8 http://pe.archive.ubuntu.com/ubuntu focal/main amd64 ssl-cert all 1.0.39 [17.0 kB]
Get:9 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 freeradius-config amd64 3.0.20+dfsg-3ubuntu0.5 [166 kB]
Get:10 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 libfreeradius3 amd64 3.0.20+dfsg-3ubuntu0.5 [183 kB]
Get:11 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 freeradius amd64 3.0.20+dfsg-3ubuntu0.5 [504 kB]
```

Nota. Elaboración propia.

Figura 61.

Configuración de credenciales de acceso y niveles de privilegio.

```
admcmori@svcradius:/etc/freeradius/3.0$ cat users

# Users

admin Cleartext-Password := "adminpass"
    Service-Type = NAS-Prompt-User,
    Cisco-AVPair = "shell:priv-lvl=15"

readonly Cleartext-Password := "readonlypass"
    Service-Type = NAS-Prompt-User,
    Cisco-AVPair = "shell:priv-lvl=1"
```

Nota. Elaboración propia.

Finalmente, se registran en el servidor los parámetros correspondientes al cliente RADIUS, incluyendo el nombre de host, la dirección IP y la clave compartida.

Figura 62.

Configuración del cliente RADIUS.

```
# Define clients

client sw_cisco {

        ipaddr= 192.168.0.25/24
        secret = testing123
```

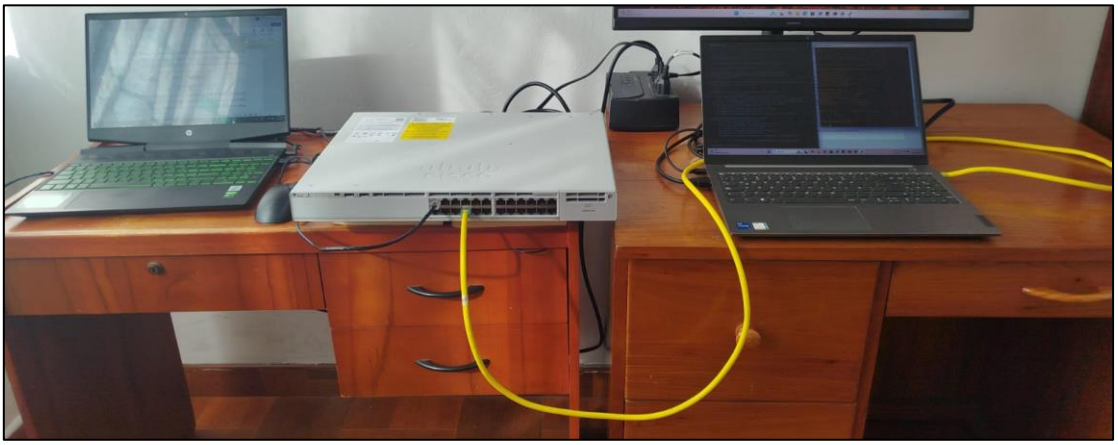
Nota. Elaboración propia.

3.1.3.3. Integración de los Componentes

Una vez realizadas las configuraciones, se procede con la integración física de los equipos. En la Figura 63 se observa el escenario real, donde el host del servidor RADIUS, el switch y la laptop del usuario se encuentran interconectados.

Figura 63.

Implementación física del sistema con RADIUS.

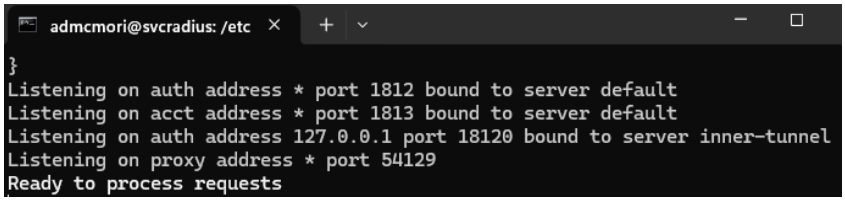


Nota. Elaboración propia.

Finalmente, se pone en marcha el servicio FreeRADIUS y se valida que tanto el usuario local creado en el switch y los usuarios creados en el servidor RADIUS se puedan conectar.

Figura 64.

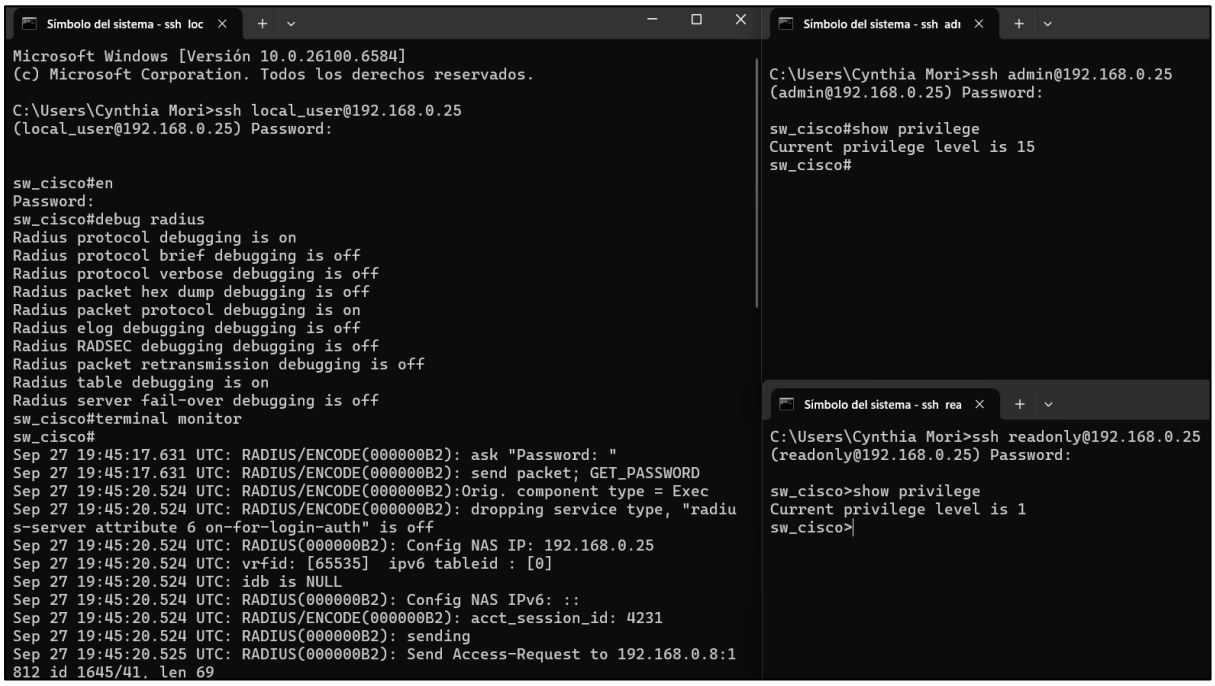
Puesta en marcha del servicio RADIUS.



Nota. Elaboración propia.

Figura 65.

Acceso exitoso con usuario local, admin y readonly usando RADIUS.



Nota. Elaboración propia.

3.2. Sistema con TACACS+

A continuación, se presenta el sistema que utiliza el protocolo TACACS+ para la gestión centralizada de la autenticación, autorización y auditoría de los usuarios que acceden al switch.

3.2.1. Componentes del Sistema

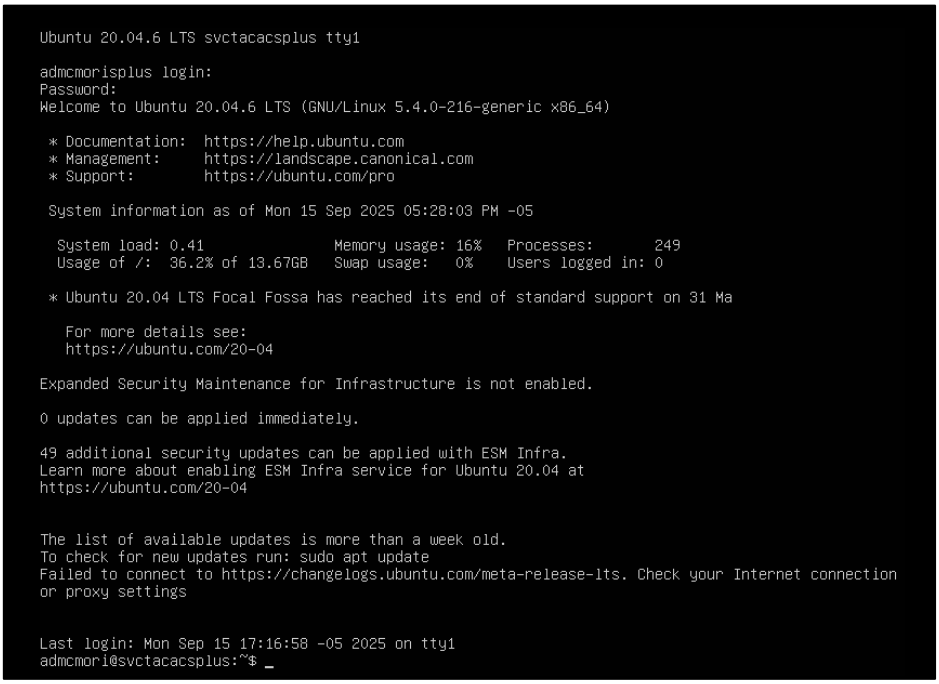
El sistema TACACS+ reutiliza la infraestructura física del sistema RADIUS, pero

incorpora nuevas configuraciones en algunos de los componentes:

- **Servidor de Acceso a la Red (NAS):** Switch Cisco C9200-24P utilizado en el sistema RADIUS, pero configurado como cliente TACACS+. Su función principal es conectar físicamente los dispositivos de la red y, al mismo tiempo, redireccionar las solicitudes de autenticación de los usuarios hacia el servidor TACACS+.
- **Servidor TACACS+:** Máquina virtual independiente del servidor RADIUS, aunque alojado en el mismo host físico. Ejecuta el software Tac_plus-ng, encargado de centralizar los procesos de autenticación, autorización y auditoría (AAA) de los usuarios que intentan acceder al NAS.

Figura 66.

Máquina virtual del servidor TACACS+.



Nota. Elaboración propia.

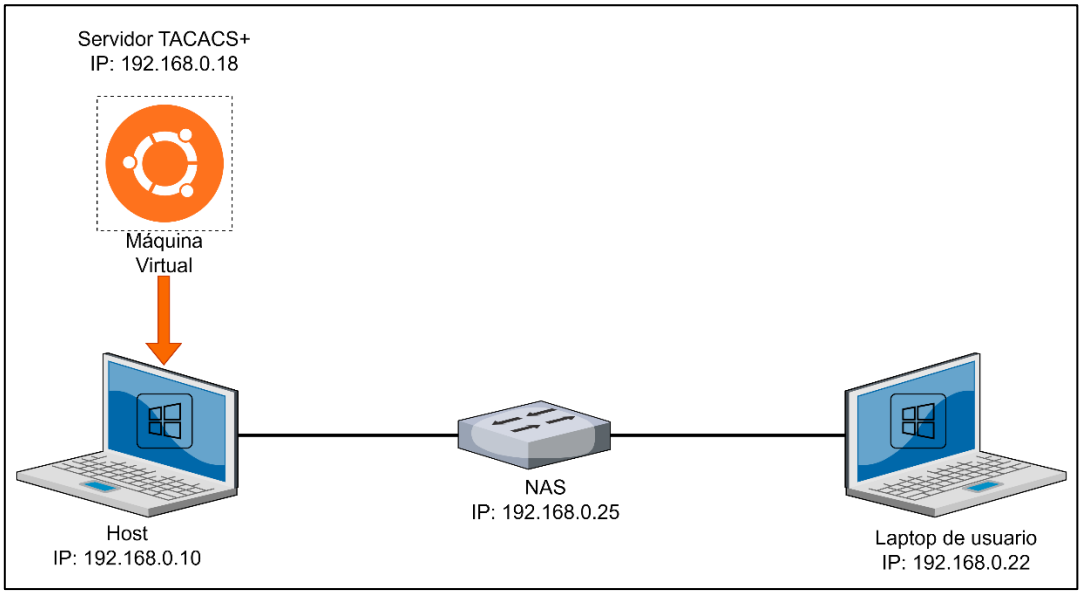
- **Host del servidor TACACS+:** Equipo anfitrión que también es utilizado en el sistema RADIUS, pero que ahora proporciona los recursos de hardware para alojar la máquina virtual del servidor TACACS+.
- **Laptop del usuario:** Computadora reutilizada del sistema RADIUS, desde la cual se establecen las conexiones al switch.

3.2.2. Arquitectura de Red del Sistema

La arquitectura del sistema que utiliza el protocolo TACACS+ se basa en la interconexión del switch con el servidor TACACS+ y la laptop del usuario. La figura 67 muestra la conexión física y lógica entre los componentes, así como el direccionamiento IP utilizado.

Figura 67.

Diagrama de topología de red del sistema con TACACS+.



Nota. Elaboración propia.

3.2.3. Implementación del Sistema

A continuación, se detallan las configuraciones realizadas para el despliegue del sistema con TACACS+.

3.2.3.1. Configuración del Switch

Se mantienen las siguientes configuraciones que se realizaron para el sistema RADIUS:

- Dirección IP de gestión.
- Credenciales de usuario local.
- Protección del modo privilegiado.
- Soporte para autenticación, autorización y auditoría (AAA).

Se especifica que la interfaz vlan1 se utilizará como dirección IP de origen para la comunicación con el servidor TACACS+.

Figura 68.

Interfaz de switch utilizada para la comunicación con el servidor TACACS+.

```
ip tacacs source-interface Vlan1
```

Nota. Elaboración propia.

Se crea el grupo de servidores TACACS+ con el nombre *tacacs_group* y el servidor que pertenece a este grupo con nombre el *server01*.

Figura 69.

Configuración de grupo de servidores TACACS+.

```
aaa group server tacacs+ tacacs_group
 server name server01
```

Nota. Elaboración propia.

Se configura la dirección IP del servidor TACACS+ *server01*. Además, se establece la clave compartida *testing123* y el timeout de 10 segundos.

Figura 70.

Configuración de los parámetros del servidor TACACS+.

```
tacacs server server01
 address ipv4 192.168.0.18
 key testing123
 timeout 10
```

Nota. Elaboración propia.

Se habilita el servicio AAA, definiendo las credenciales locales como opción principal y al grupo de servidores TACACS+ como respaldo.

Figura 71.

Configuración de autenticación, autorización y auditoría TACACS+.

```
aaa authentication login default local group tacacs_group
aaa authorization exec default local group tacacs_group
aaa authorization commands 1 default local group tacacs_group
aaa authorization commands 15 default local group tacacs_group
aaa accounting exec default start-stop group tacacs_group
aaa accounting commands 1 default start-stop group tacacs_group
aaa accounting commands 15 default start-stop group tacacs_group
```

Nota. Elaboración propia.

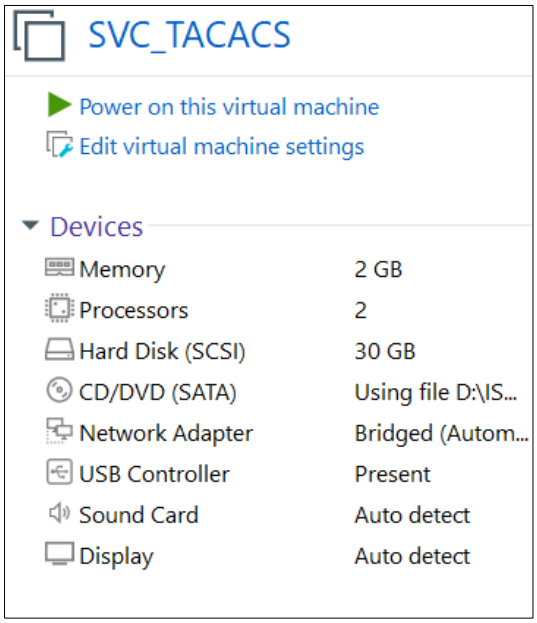
3.2.3.2. Despliegue y configuración del Servidor TACACS+

Para la implementación del sistema de autenticación centralizada, se configura el servidor TACACS+ en una máquina virtual y se definen los recursos necesarios, tales como

memoria, procesador y almacenamiento.

Figura 72.

Características de la máquina virtual del servidor TACACS+.



Nota. Elaboración propia.

Posteriormente, se configura la interfaz de red de la máquina virtual y se sincroniza la hora y la fecha del servidor.

Figura 73.

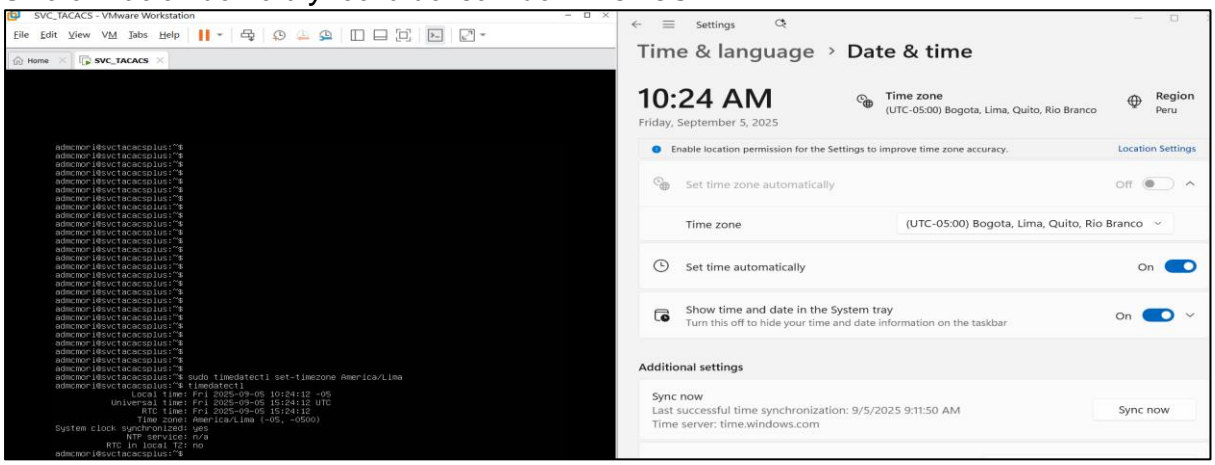
Configuración de interfaz de red del servidor TACACS+.

```
admcmori@svctacacsplus:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.18  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::20c:29ff:fe87:e1e2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:87:e1:e2  txqueuelen 1000  (Ethernet)
        RX packets 157  bytes 11799 (11.7 KB)
        RX errors 0  dropped 115  overruns 0  frame 0
        TX packets 46  bytes 7096 (7.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Nota. Elaboración propia.

Figura 74.

Sincronización de hora y fecha del servidor TACACS+.



Nota. Elaboración propia.

Luego, se instala el software Tac_plus-ng. Una vez instalado, se crean los usuarios “admin” y “readonly” con sus respectivas contraseñas y niveles de privilegio, lo que permitirá establecer un esquema de acceso diferenciado.

Figura 75.

Instalación de Tac_plus-ng.

```
install -c -m 0755 /home/admcmori/event-driven-servers/tac_plus-ng/sample/tac_plus-ng.cfg /usr/local/etc/mavis/sample/tac_plus-ng.cfg
install -c -m 0755 /home/admcmori/event-driven-servers/tac_plus-ng/sample/tac_plus-ng-simple.cfg /usr/local/etc/mavis/sample/tac_plus-ng-simple.cfg
make[3]: Entering directory '/home/admcmori/event-driven-servers/tac_plus-ng/extra'
make[3]: Nothing to be done for 'install'.
make[3]: Leaving directory '/home/admcmori/event-driven-servers/tac_plus-ng/extra'
make[2]: Leaving directory '/home/admcmori/event-driven-servers/build/linux-5.4.0-216-generic-x86_64/tac_plus-ng'
make[1]: Leaving directory '/home/admcmori/event-driven-servers/tac_plus-ng'
make[1]: Entering directory '/home/admcmori/event-driven-servers/tcprelay'
make[2]: Entering directory '/home/admcmori/event-driven-servers/tcprelay/extra'
make[2]: Nothing to be done for 'all'.
make[2]: Leaving directory '/home/admcmori/event-driven-servers/tcprelay/extra'
make[2]: Entering directory '/home/admcmori/event-driven-servers/build/linux-5.4.0-216-generic-x86_64/tcprelay'
make[3]: Entering directory '/home/admcmori/event-driven-servers/build/linux-5.4.0-216-generic-x86_64/tcprelay'
make[4]: Entering directory '/home/admcmori/event-driven-servers/tcprelay/extra'
make[4]: Nothing to be done for 'install'.
make[4]: Leaving directory '/home/admcmori/event-driven-servers/tcprelay/extra'
make[3]: Leaving directory '/home/admcmori/event-driven-servers/build/linux-5.4.0-216-generic-x86_64/tcprelay'
make[2]: Leaving directory '/home/admcmori/event-driven-servers/build/linux-5.4.0-216-generic-x86_64/tcprelay'
make[2]: Entering directory '/home/admcmori/event-driven-servers/build/linux-5.4.0-216-generic-x86_64/tcprelay'
install -c -m 0755 tcprelay /usr/local/sbin/tcprelay
install -c -m 0755 /home/admcmori/event-driven-servers/tcprelay/sample/tcprelay.cfg /usr/local/etc/mavis/sample/tcprelay.cfg
make[3]: Entering directory '/home/admcmori/event-driven-servers/tcprelay/extra'
make[3]: Nothing to be done for 'install'.
make[3]: Leaving directory '/home/admcmori/event-driven-servers/tcprelay/extra'
make[2]: Leaving directory '/home/admcmori/event-driven-servers/build/linux-5.4.0-216-generic-x86_64/tcprelay'
make[1]: Leaving directory '/home/admcmori/event-driven-servers/tcprelay'
admcmori@svctacacsplus:~/event-driven-servers$ whereis tac_plus-ng
tac_plus-ng: /usr/local/sbin/tac_plus-ng
admcmori@svctacacsplus:~/event-driven-servers$ sudo mkdir -p /var/log/tac_plus-ng/{authentication,accounting,access}
admcmori@svctacacsplus:~/event-driven-servers$ tac_plus-ng -v
tac_plus-ng version dc63dc9c6b01ca1559ab2a8f432239b14c2bf596/PCRE2/CRYPTO/ARES/CURL/SSL
admcmori@svctacacsplus:~/event-driven-servers$
```

Nota. Elaboración propia.

Figura 76.

Configuración de credenciales de acceso y niveles de privilegio.

```
# Profiles

  profile netadmin {
        script {
            if (service == shell) {
                    if (cmd == "") {
                        set priv-lvl = 15
                        permit
                    }
                permit
              }
        }
    }

  profile netreadonly {
        script {
            if (service == shell) {
                    if (cmd == "") {
                        set priv-lvl = 1
                        permit
                        }
                if (cmd =~ /^ping/){ permit
                    }
                if (cmd =~ /^traceroute/){ permit
                    }
                  deny
            }
        }
  }

# Groups

group admins
group readonlys

# Users

  user admin {
   password login = clear adminpass
   member = admins
      }

  user readonly {
   password login = clear readonlypass
   member = readonlys
      }
```

Nota. Elaboración propia.

Finalmente, se registran en el servidor los parámetros correspondientes al cliente, incluyendo el nombre de host, la dirección IP y la clave compartida.

Figura 77.

Configuración del cliente TACACS+.

```
# Define clients

host = sw_cisco {

  address = 192.168.0.25/24

  key = testing123
```

Nota. Elaboración propia.

3.2.3.3. Integración de los Componentes

Una vez realizadas las configuraciones, se pone en marcha el servicio Tac_plus-ng. Finalmente, se valida que tanto el usuario local creado en el switch y los usuarios creados en

el servidor TACACS+ se puedan conectar.

Figura 78.

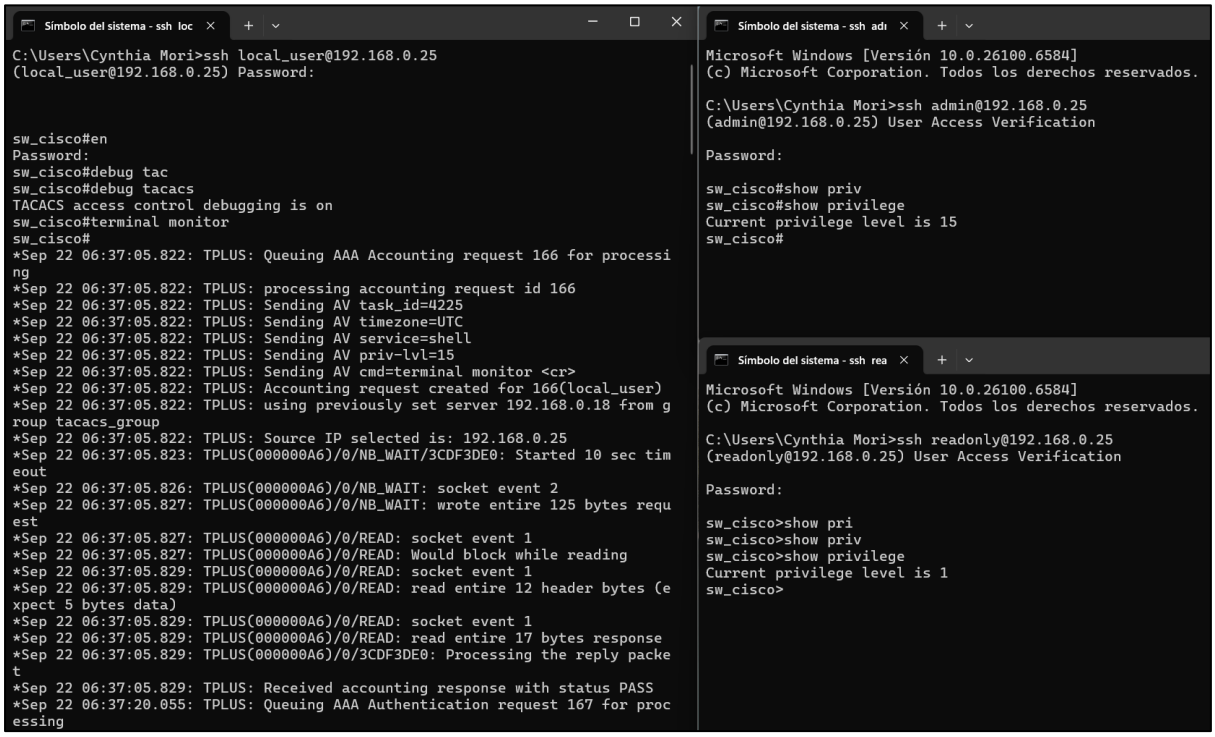
Puesta en marcha del servicio TACACS+.

```
admcmori@svctacacsplus:~$ sudo tac_plus-ng -f /etc/tacplusng.cfg -d 16
3182: 00:49:45.734 0/00000000: - creating profile netadmin in realm default
3182: 00:49:45.734 0/00000000: - creating profile netreadonly in realm default
3182: 00:49:45.734 0/00000000: - creating user admin in realm default
3182: 00:49:45.734 0/00000000: - creating user readonly in realm default
3182: 00:49:45.734 0/00000000: - Version dc63dc9c6b01ca1559ab2a8f432239b14c2bf596 initialized
```

Nota. Elaboración propia.

Figura 79.

Acceso exitoso con usuario local, admin y readonly usando TACACS+.



Nota. Elaboración propia.

CAPÍTULO IV

Resultados, Contrastación de Hipótesis y Discusión de Resultados

4.1. Resultados

Los sistemas basados en los protocolos RADIUS y TACACS+, fueron evaluados bajo condiciones controladas e idénticas de red: se utilizó la misma topología física, los mismos dispositivos de red, configuraciones equivalentes en los switches, y el mismo sistema operativo en las máquinas virtuales donde se ejecutaron los servidores AAA. La única variable fue el software correspondiente a cada protocolo: FreeRADIUS y Tac_plus-ng. Por tanto, las diferencias observadas en el comportamiento de la red pueden atribuirse exclusivamente a las particularidades de cada protocolo.

4.1.1. Desempeño

Se evalúa el desempeño de los protocolos RADIUS y TACACS+ considerando el número de paquetes requeridos para el acceso del usuario, volumen de datos transmitidos, y latencia total en el proceso de autenticación y autorización. Estos indicadores permiten determinar la eficiencia operacional de cada protocolo en cuanto al uso de recursos de red y tiempo de respuesta.

4.1.1.1. Número de paquetes necesarios para otorgar el acceso

Se captura el tráfico entre el switch y los servidores AAA durante los procesos de autenticación y autorización mediante tcpdump y se analizan los paquetes en Wireshark.

Figura 80.

Captura de paquetes con "tcpdump" desde el servidor RADIUS.

```
admcmori@svcradius:~$ sudo tcpdump -n -i any udp port 1812 or port 1813 -w /tmp/freerad_authen1.pcap
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
```

Nota. Elaboración propia.

Figura 81.

Captura de paquetes con "tcpdump" desde el servidor TACACS+.

```
admcmori@svctacacsplus:/tmp$ sudo tcpdump -n -i any tcp port 49 -w /tmp/tacplus_authen1.pcap
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
```

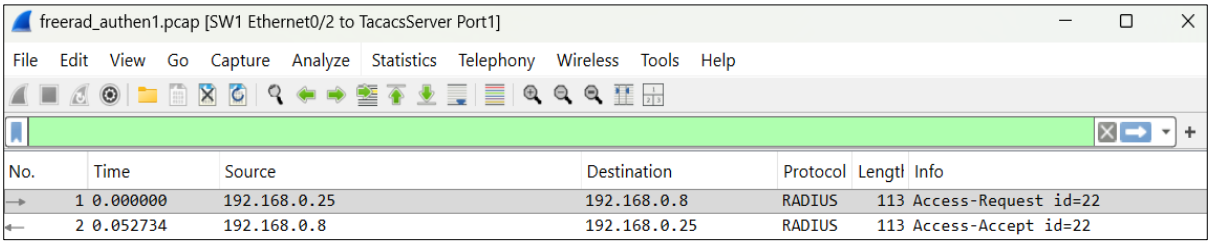
Nota. Elaboración propia.

En el intercambio de paquetes, RADIUS completa la autenticación y autorización de un usuario legítimo con solo 2 paquetes: un paquete Access-Request enviado por el switch al servidor y un paquete Access-Accept de respuesta que incluye tanto la confirmación de autenticación como los atributos de autorización.

La Figura 82 muestra la captura realizada con Wireshark de los paquetes de autenticación y autorización intercambiados entre el switch y el servidor RADIUS.

Figura 82.

Captura de paquetes RADIUS durante el proceso de autenticación y autorización.



Nota. Elaboración propia.

La Tabla 4 describe cada paquete RADIUS intercambiado durante la autenticación y autorización.

Tabla 4.

Intercambio de paquetes durante el proceso de autenticación y autorización con RADIUS.

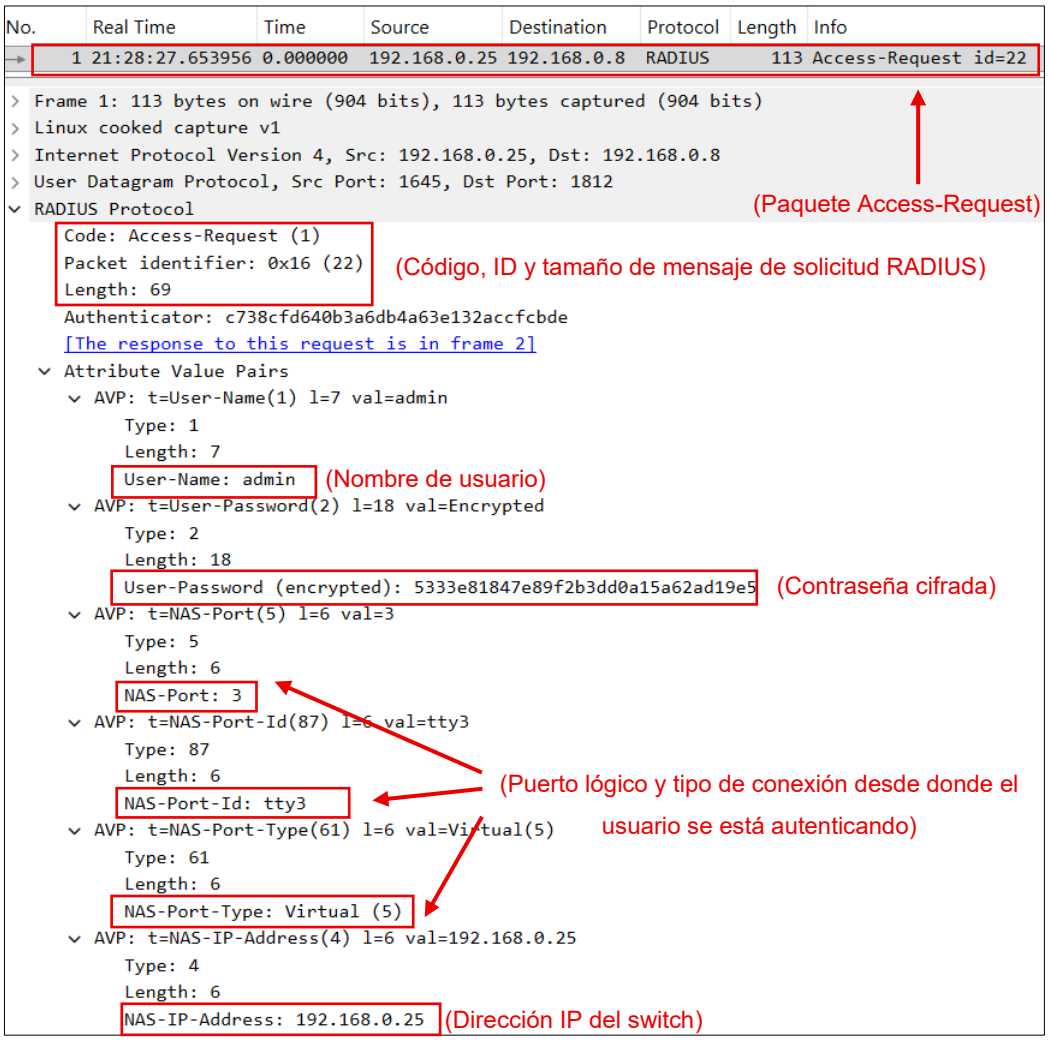
N° Paquete	Paquete	Descripción
1	Access-Request	Solicitud de acceso enviada por el switch al servidor. El switch envía el nombre de usuario, contraseña y atributos de la sesión.
2	Access-Accept	Respuesta del servidor al switch en la que, además de confirmar la autenticación exitosa del usuario, se incluyen los atributos de autorización, como el nivel de privilegio asignado en el dispositivo.

Nota. Elaboración propia.

La Figura 83 ilustra el contenido del paquete *Access-Request*. Como se observa en la figura, el paquete Access-Request inicia el proceso AAA y transporta los atributos relevantes para la autenticación y autorización del usuario como el nombre de usuario, contraseña, parámetros del contexto de conexión (NAS-Port, NAS-Port-Id y NAS-Port-Type) y la dirección IP del switch (NAS) hacia el servidor RADIUS para que se inicie la validación.

Figura 83.

Contenido del paquete Access-Request en el protocolo RADIUS.

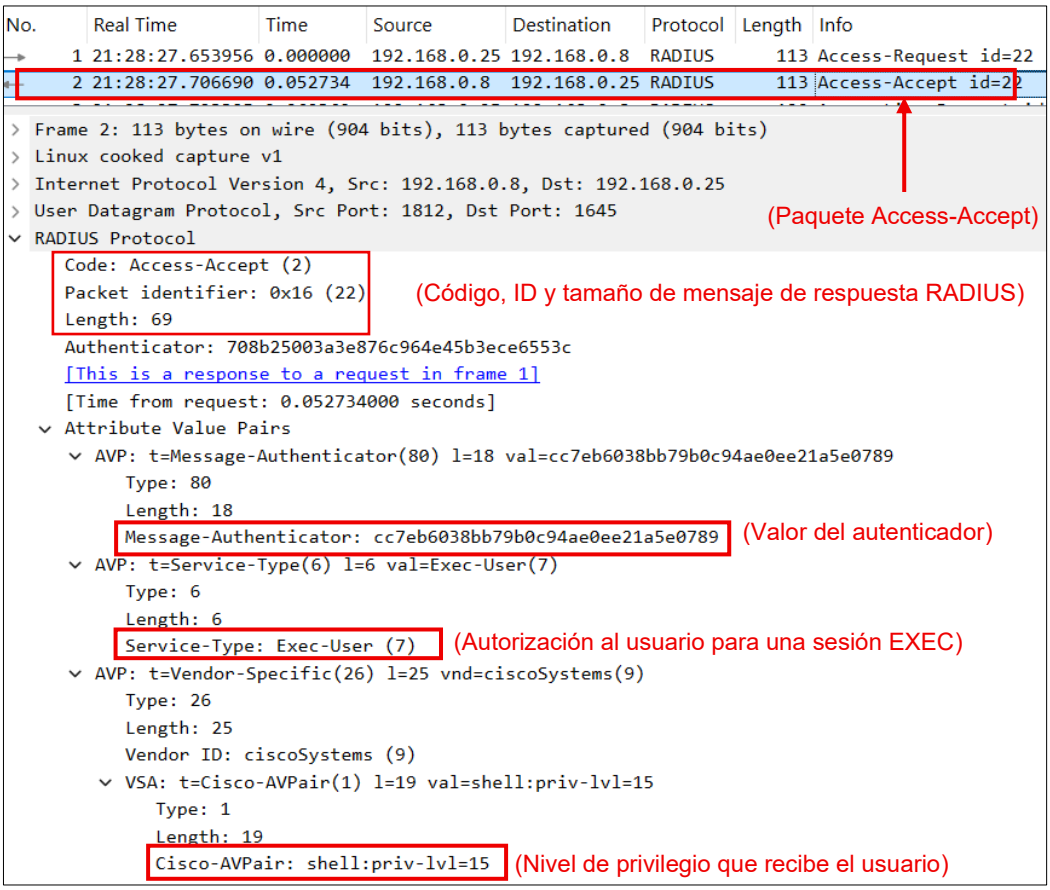


Nota. Elaboración propia.

La Figura 84 muestra el contenido del paquete *Access-Accept*, correspondiente a la respuesta del servidor RADIUS frente al paquete Access-Request previamente enviado por el switch. El paquete *Access-Accept* indica que las credenciales del usuario fueron correctamente validadas e incluye el atributo *Cisco-AVPair: shell:priv-lvl=15*, que corresponde al nivel EXEC privilegiado que se otorga al usuario para el acceso a la CLI del switch. Esta combinación de los procesos de autenticación y autorización en un mismo paquete coincide con lo descrito en la teoría, donde se establece que el protocolo RADIUS integra ambas funciones en un único intercambio.

Figura 84.

Contenido del paquete Access-Accept en el protocolo RADIUS.



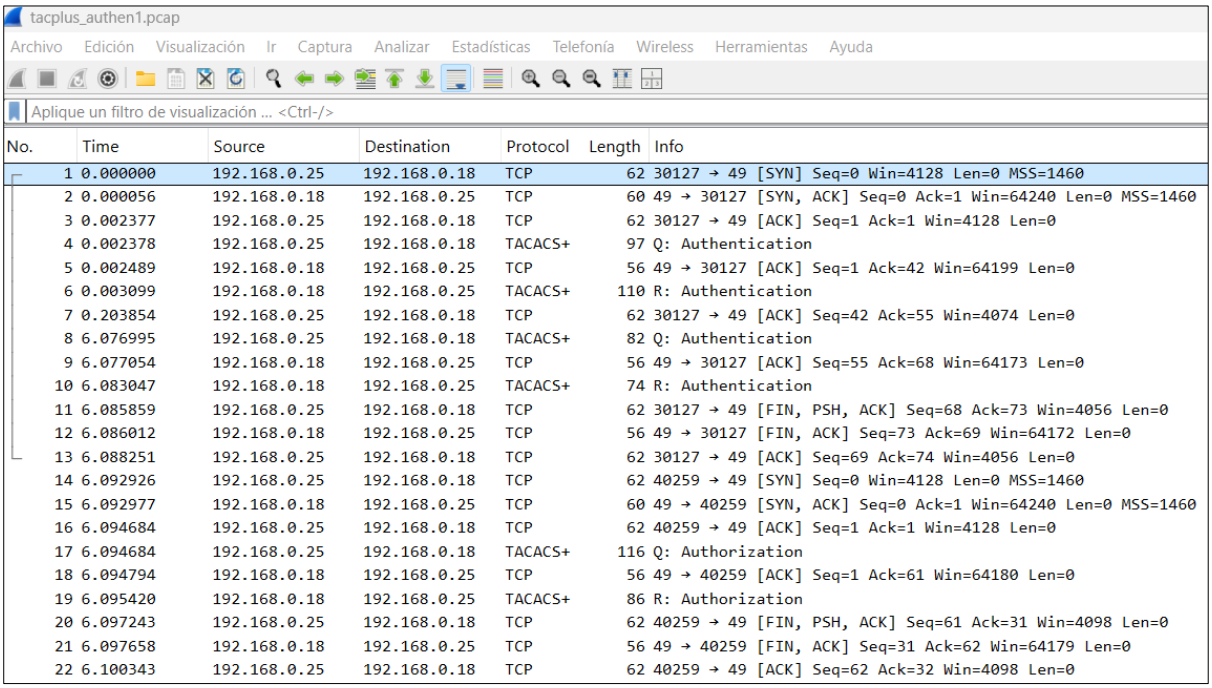
Nota. Elaboración propia.

El acceso de un usuario legítimo mediante el protocolo TACACS+ requirió el intercambio de 22 paquetes entre el switch (NAS) y el servidor. Este intercambio incluye tanto el proceso de autenticación como el de autorización, los cuales se ejecutan de manera independiente, en correspondencia con la arquitectura funcional del protocolo.

Como se observa en la Figura 85, el proceso inicia con el establecimiento de una conexión TCP en el puerto 49. Una vez establecida la conexión, el switch envía una solicitud de autenticación *Q: Authentication*. El servidor responde con un mensaje de desafío *R: Authentication,* tras lo cual el switch envía una nueva solicitud *Q: Authentication* y el servidor emite una respuesta *R: Authentication*. Finalmente, el switch establece una nueva conexión TCP para ejecutar la fase de autorización, en la que se intercambian los mensajes Q: Authorization y R: Authorization.

Figura 85.

Captura de paquetes TACACS+ durante el proceso de autenticación y autorización.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [SYN] Seq=0 Win=4128 Len=0 MSS=1460
2	0.000056	192.168.0.18	192.168.0.25	TCP	60	49 → 30127 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.002377	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [ACK] Seq=1 Ack=1 Win=4128 Len=0
4	0.002378	192.168.0.25	192.168.0.18	TACACS+	97	Q: Authentication
5	0.002489	192.168.0.18	192.168.0.25	TCP	56	49 → 30127 [ACK] Seq=1 Ack=42 Win=64199 Len=0
6	0.003099	192.168.0.18	192.168.0.25	TACACS+	110	R: Authentication
7	0.203854	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [ACK] Seq=42 Ack=55 Win=4074 Len=0
8	6.076995	192.168.0.25	192.168.0.18	TACACS+	82	Q: Authentication
9	6.077054	192.168.0.18	192.168.0.25	TCP	56	49 → 30127 [ACK] Seq=55 Ack=68 Win=64173 Len=0
10	6.083047	192.168.0.18	192.168.0.25	TACACS+	74	R: Authentication
11	6.085859	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [FIN, PSH, ACK] Seq=68 Ack=73 Win=4056 Len=0
12	6.086012	192.168.0.18	192.168.0.25	TCP	56	49 → 30127 [FIN, ACK] Seq=73 Ack=69 Win=64172 Len=0
13	6.088251	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [ACK] Seq=69 Ack=74 Win=4056 Len=0
14	6.092926	192.168.0.25	192.168.0.18	TCP	62	40259 → 49 [SYN] Seq=0 Win=4128 Len=0 MSS=1460
15	6.092977	192.168.0.18	192.168.0.25	TCP	60	49 → 40259 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16	6.094684	192.168.0.25	192.168.0.18	TCP	62	40259 → 49 [ACK] Seq=1 Ack=1 Win=4128 Len=0
17	6.094684	192.168.0.25	192.168.0.18	TACACS+	116	Q: Authorization
18	6.094794	192.168.0.18	192.168.0.25	TCP	56	49 → 40259 [ACK] Seq=1 Ack=61 Win=64180 Len=0
19	6.095420	192.168.0.18	192.168.0.25	TACACS+	86	R: Authorization
20	6.097243	192.168.0.25	192.168.0.18	TCP	62	40259 → 49 [FIN, PSH, ACK] Seq=61 Ack=31 Win=4098 Len=0
21	6.097658	192.168.0.18	192.168.0.25	TCP	56	49 → 40259 [FIN, ACK] Seq=31 Ack=62 Win=64179 Len=0
22	6.100343	192.168.0.25	192.168.0.18	TCP	62	40259 → 49 [ACK] Seq=62 Ack=32 Win=4098 Len=0

Nota. Elaboración propia.

La Tabla 5 describe cada paquete intercambiado durante la autenticación y autorización utilizando el protocolo TACACS+.

Tabla 5.

Intercambio de paquetes durante el proceso de autenticación y autorización con TACACS+.

N° Paquete	Paquete	Descripción
1	SYN	Solicitud enviada por el switch al servidor para establecer una conexión TCP en el puerto 49.
2	SYN, ACK	Respuesta del servidor confirmando la petición de conexión del cliente.
3	ACK	Establecimiento de la conexión TCP.
4	Q: Authentication	Solicitud de acceso enviada por el switch al servidor. El switch envia el nombre de usuario y atributos de la sesión.
5	ACK	Confirmación de recepción de paquete Q: Authentication por parte del servidor.
6	R: Authentication	Respuesta del servidor al switch, en la que solicita la contraseña.
7	ACK	Confirmación de recepción de paquete R: Authentication por parte del switch.
8	Q: Authentication	Continuación de la solicitud de acceso. El switch envia la contraseña.
9	ACK	Confirmación de recepción de paquete Q: Authentication por parte del servidor.
10	R: Authentication	Respuesta del servidor al switch, confirmando la autenticación exitosa del usuario.
11	FIN, PSH, ACK	El switch reconoce la información recibida y notifica que no enviará más.
12	FIN, ACK	El servidor acepta el cierre, reconoce la petición y, a la vez, comunica que también finaliza su transmisión.
13	ACK	Cierre de la conexión TCP.
14	SYN	Solicitud enviada por el switch al servidor para establecer una nueva conexión TCP en el puerto 49.
15	SYN, ACK	Respuesta del servidor confirmando la petición de conexión del cliente.
16	ACK	Establecimiento de la conexión TCP.
17	Q: Authorization	Solicitud de autorización enviada por el switch al servidor. El switch envia el nombre de usuario y atributos de la sesión.
18	ACK	Confirmación de recepción de paquete Q: Authorization por parte del servidor.
19	R: Authorization	Respuesta del servidor al switch en la que, además de confirmar la autorización exitosa del usuario, se incluyen los atributos de autorización, como el nivel de privilegio asignado.
20	FIN, PSH, ACK	El switch reconoce la información recibida y notifica que no enviará más.
21	FIN, ACK	El servidor acepta el cierre, reconoce la petición y, a la vez, comunica que también finaliza su transmisión.
22	ACK	Cierre de la conexión TCP.

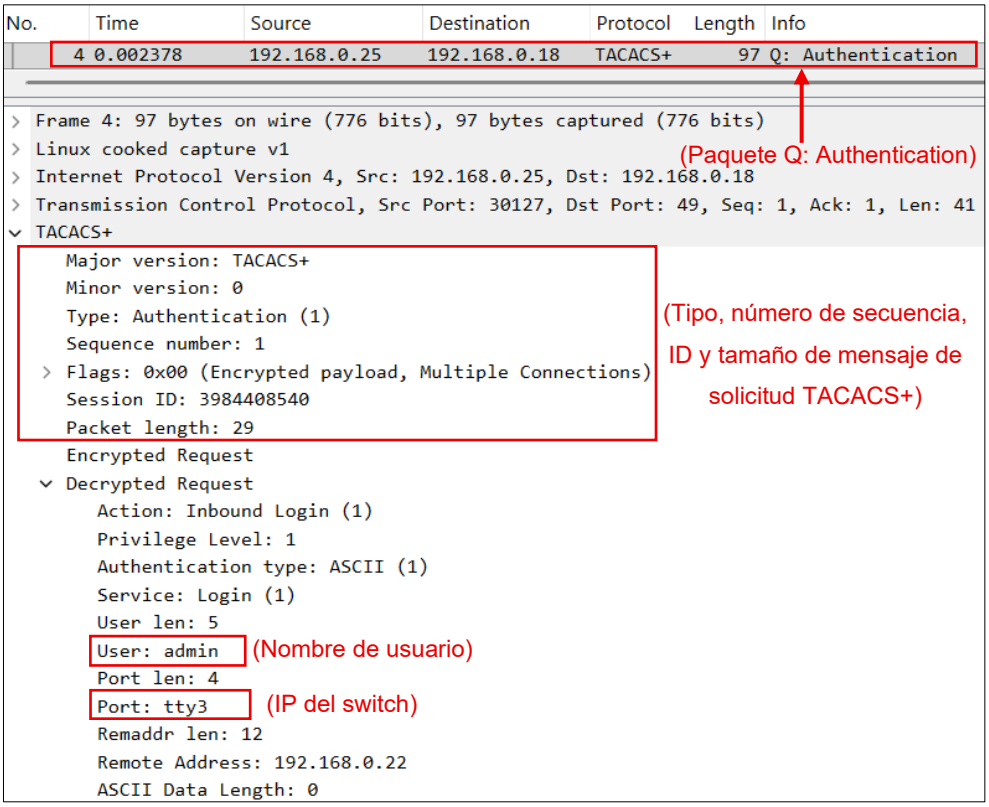
Nota. Elaboración propia.

Para visualizar el contenido de los paquetes en detalle, se configuró en Wireshark la clave compartida *testing123*, lo que permitió descifrar los mensajes TACACS+ y analizar los atributos transmitidos en cada fase.

En la Figura 86 se muestra el contenido del primer paquete *Q: Authentication* del protocolo TACACS+. Además del nombre de usuario y el tipo de servicio requerido, el paquete incluye información relevante de red, como la dirección IP remota del usuario y el puerto desde el cual se origina la conexión. También se observa que el paquete contiene el nivel de privilegio del usuario, el cual es asignado automáticamente por el switch al generar la solicitud de autenticación. Este valor funciona como un nivel de privilegio predeterminado y no representa los permisos reales del usuario.

Figura 86.

Contenido del primer paquete Q: Authentication en el protocolo TACACS+.

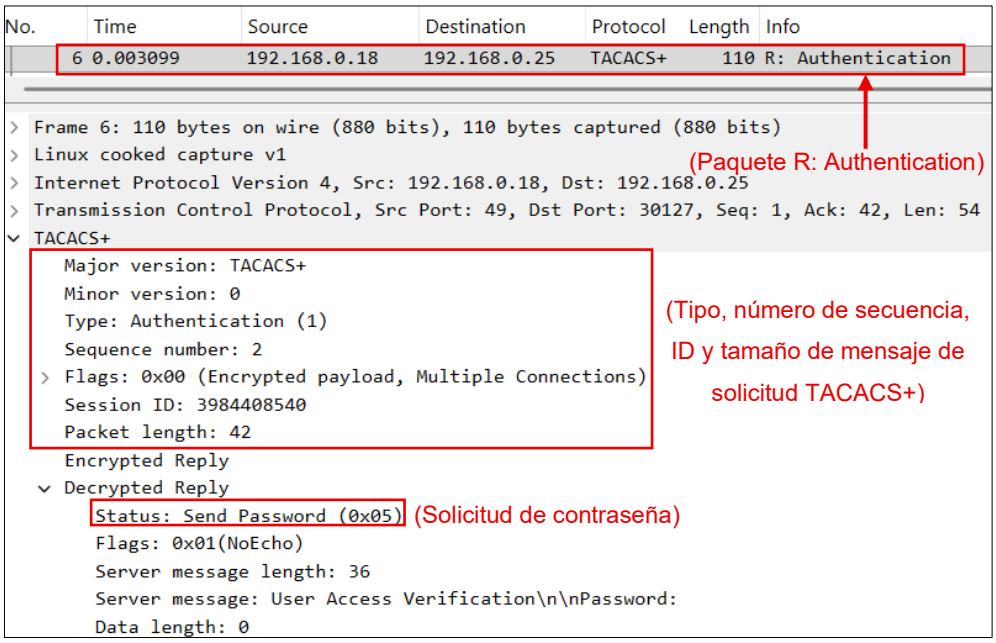


Nota. Elaboración propia.

La Figura 87 muestra el contenido del primer paquete *R: Authentication*, correspondiente a la respuesta del servidor TACACS+ en el que solicita al switch la contraseña del usuario previamente identificado.

Figura 87.

Contenido del primer paquete R: Authentication en el protocolo TACACS+.

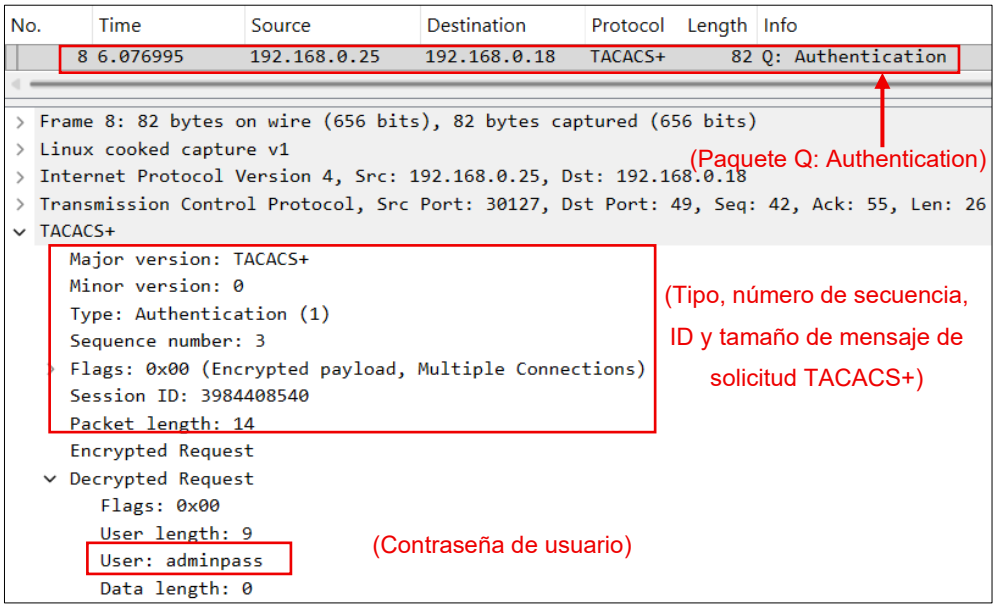


Nota. Elaboración propia.

En la Figura 88 se presenta el contenido del segundo paquete *Q: Authentication*, correspondiente a la respuesta del switch ante la solicitud del servidor TACACS+, en la cual se incluye la contraseña del usuario.

Figura 88.

Contenido del segundo paquete Q: Authentication en el protocolo TACACS+.

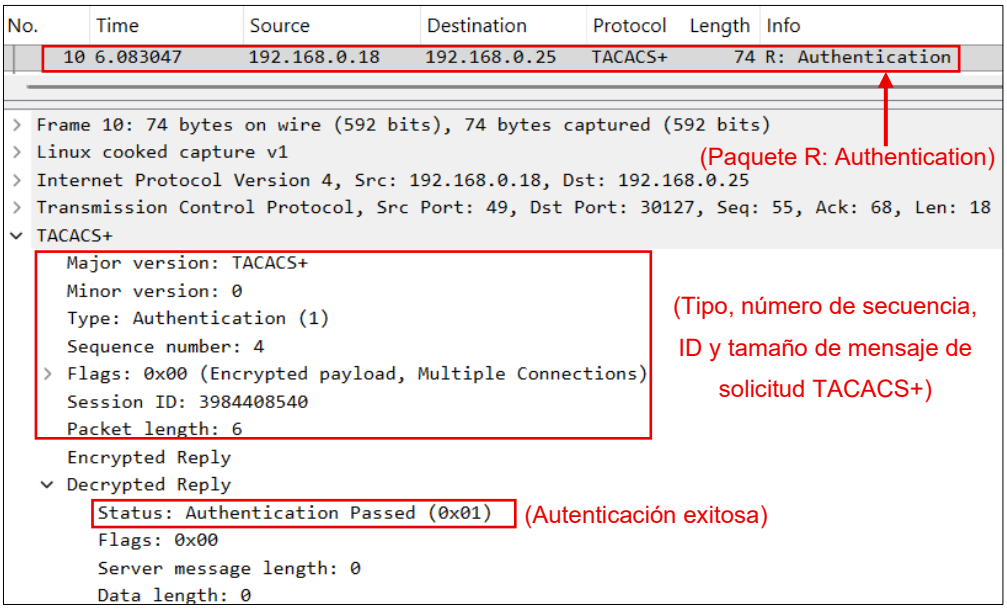


Nota. Elaboración propia.

La Figura 89 muestra el contenido del segundo paquete *R: Authentication*, correspondiente a la respuesta del servidor TACACS+ luego de validar las credenciales del usuario. En este mensaje, el servidor responde indicando que la autenticación es exitosa.

Figura 89.

Contenido del segundo paquete R: Authentication en el protocolo TACACS+.

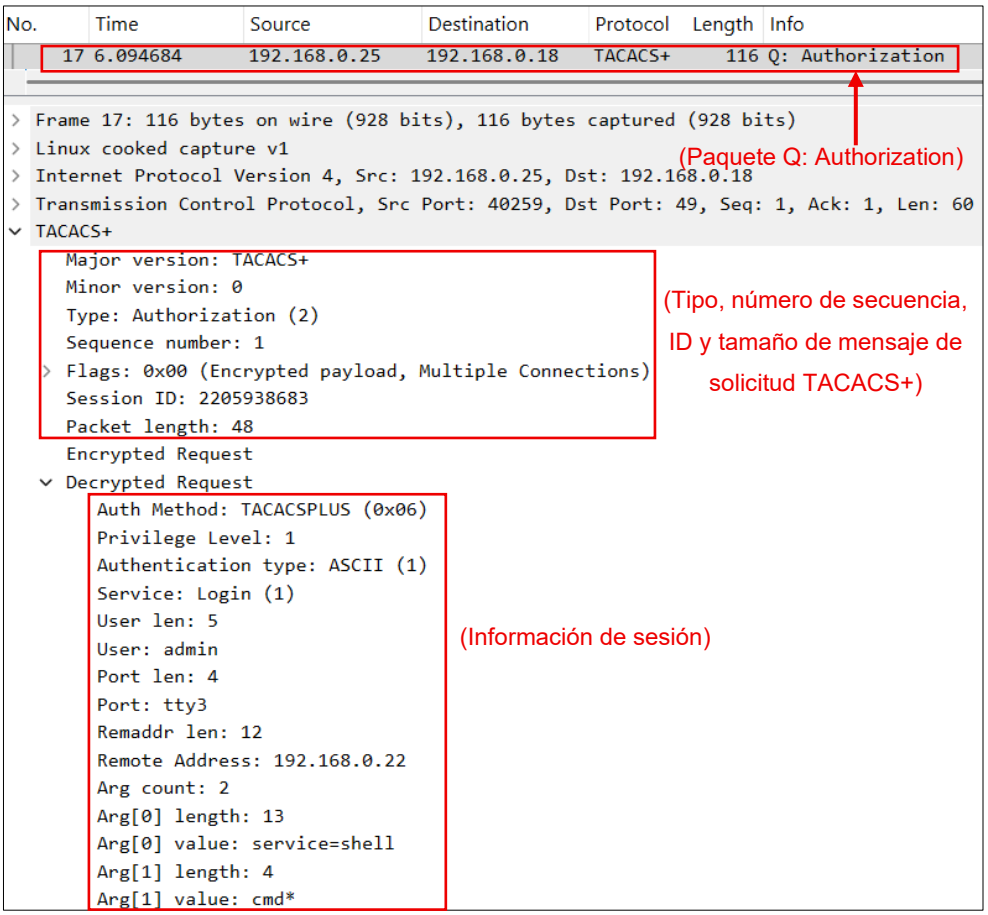


Nota. Elaboración propia.

En la Figura 90 se presenta el contenido del paquete *Q: Authorization*, mediante el cual el switch solicita autorización al servidor TACACS+. En este mensaje, el campo *privilege level* aparece con valor 1, lo que representa el nivel mínimo de privilegio por defecto que envía el switch en la solicitud. No obstante, este valor no refleja el nivel de privilegio real del usuario. Como se observa en la Figura 91, en el contenido del paquete de respuesta *R: Authorization* emitido por el servidor TACACS+, el atributo *priv-lvl= 15* indica el nivel de privilegio que finalmente se asigna al usuario durante en la sesión.

Figura 90.

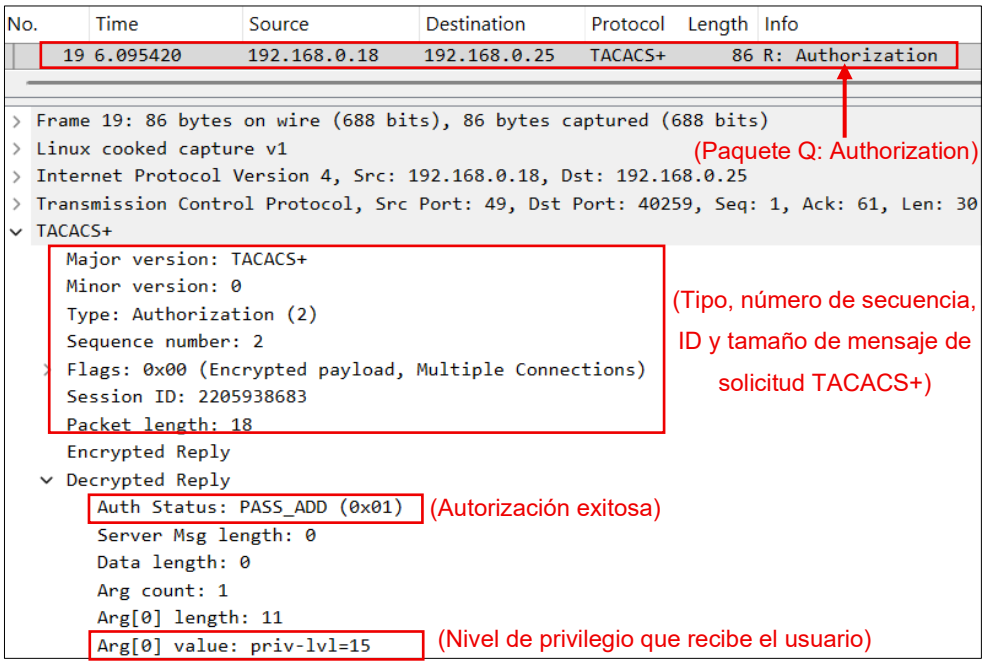
Contenido del paquete Q: Authorization en el protocolo TACACS+.



Nota. Elaboración propia.

Figura 91.

Contenido del paquete R: Authorization en el protocolo TACACS+.



Nota. Elaboración propia.

Con estos resultados, se evidencia que RADIUS requiere un menor número de paquetes para otorgar el acceso a un usuario legítimo.

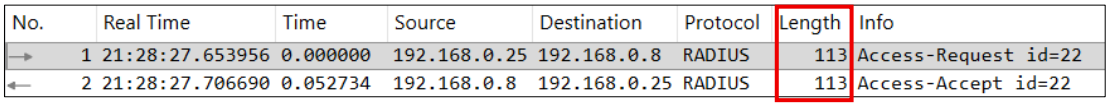
4.1.1.2. Tamaño total de datos transmitidos en la autenticación y autorización del usuario

Se analizan los paquetes capturados con Wireshark de la sección 4.1.2, tomando los valores de la columna *Length* de cada paquete y sumando los bytes transmitidos entre el switch y el servidor AAA.

En cuanto al protocolo RADIUS, el tamaño total de datos transmitidos durante la autenticación y autorización del usuario alcanzó los 226 bytes.

Figura 92.

Tamaño de bytes transmitidos en la autenticación y autorización con RADIUS.



Nota. Elaboración propia.

El detalle del tamaño de bytes por cada paquete RADIUS durante la autenticación y autorización del usuario se presenta en la Tabla 6.

Tabla 6.

Tamaño de datos transmitidos por paquete RADIUS.

N° Paquete	Paquete	Tamaño (bytes)
1	Access-Request	113
2	Access-Accept	113
Total		**226**

Nota. Elaboración propia.

En el caso del protocolo TACACS+, el tamaño total de los datos transmitidos durante la autenticación y autorización del usuario es de 1517 bytes.

Figura 93.

Tamaño de bytes transmitidos en la autenticación y autorización con TACACS+.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [SYN] Seq=0 Win=4128 Len=0 MSS=1460
2	0.000056	192.168.0.18	192.168.0.25	TCP	60	49 → 30127 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.002377	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [ACK] Seq=1 Ack=1 Win=4128 Len=0
4	0.002378	192.168.0.25	192.168.0.18	TACACS+	97	Q: Authentication
5	0.002489	192.168.0.18	192.168.0.25	TCP	56	49 → 30127 [ACK] Seq=1 Ack=42 Win=64199 Len=0
6	0.003099	192.168.0.18	192.168.0.25	TACACS+	110	R: Authentication
7	0.203854	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [ACK] Seq=42 Ack=55 Win=4074 Len=0
8	6.076995	192.168.0.25	192.168.0.18	TACACS+	82	Q: Authentication
9	6.077054	192.168.0.18	192.168.0.25	TCP	56	49 → 30127 [ACK] Seq=55 Ack=68 Win=64173 Len=0
10	6.083047	192.168.0.18	192.168.0.25	TACACS+	74	R: Authentication
11	6.085859	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [FIN, PSH, ACK] Seq=68 Ack=73 Win=4056 Len=0
12	6.086012	192.168.0.18	192.168.0.25	TCP	56	49 → 30127 [FIN, ACK] Seq=73 Ack=69 Win=64172 Len=0
13	6.088251	192.168.0.25	192.168.0.18	TCP	62	30127 → 49 [ACK] Seq=69 Ack=74 Win=4056 Len=0
14	6.092926	192.168.0.25	192.168.0.18	TCP	62	40259 → 49 [SYN] Seq=0 Win=4128 Len=0 MSS=1460
15	6.092977	192.168.0.18	192.168.0.25	TCP	60	49 → 40259 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16	6.094684	192.168.0.25	192.168.0.18	TCP	62	40259 → 49 [ACK] Seq=1 Ack=1 Win=4128 Len=0
17	6.094684	192.168.0.25	192.168.0.18	TACACS+	116	Q: Authorization
18	6.094794	192.168.0.18	192.168.0.25	TCP	56	49 → 40259 [ACK] Seq=1 Ack=61 Win=64180 Len=0
19	6.095420	192.168.0.18	192.168.0.25	TACACS+	86	R: Authorization
20	6.097243	192.168.0.25	192.168.0.18	TCP	62	40259 → 49 [FIN, PSH, ACK] Seq=61 Ack=31 Win=4098 Len=0
21	6.097658	192.168.0.18	192.168.0.25	TCP	56	49 → 40259 [FIN, ACK] Seq=31 Ack=62 Win=64179 Len=0
22	6.100343	192.168.0.25	192.168.0.18	TCP	62	40259 → 49 [ACK] Seq=62 Ack=32 Win=4098 Len=0

Nota. Elaboración propia.

El detalle del tamaño de bytes por cada paquete TACACS+ durante la autenticación y autorización del usuario se presenta en la Tabla 7.

Tabla 7.

Tamaño de datos transmitidos por paquete TACACS+.

N° Paquete	Paquete	Tamaño (bytes)
1	SYN	62
2	SYN, ACK	60
3	ACK	62
4	Q: Authentication	97
5	ACK	56
6	R: Authentication	110
7	ACK	62
8	Q: Authentication	82
9	ACK	56
10	R: Authentication	74
11	FIN, PSH, ACK	56
12	FIN, ACK	62
13	ACK	56
14	SYN	62
15	SYN, ACK	60
16	ACK	62
17	Q: Authorization	116
18	ACK	56
19	R: Authorization	86
20	FIN, PSH, ACK	62
21	FIN, ACK	56
22	ACK	62
Total		**1517**

Nota. Elaboración propia.

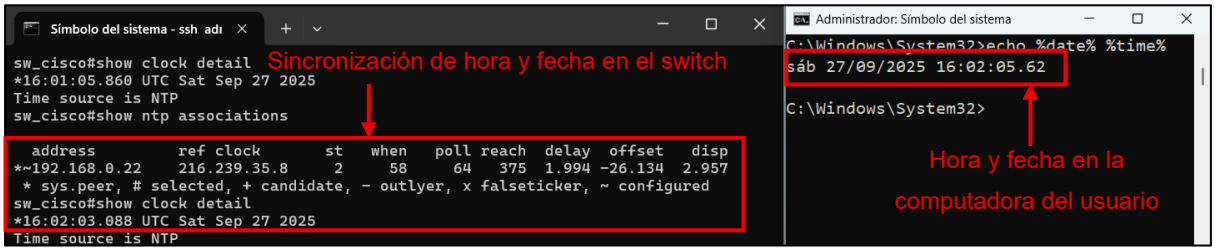
Estos resultados exponen una diferencia importante en el volumen de datos que transmiten ambos protocolos en la red durante la autenticación y autorización del usuario. RADIUS requiere menos volumen de datos debido a que intercambia menor número de paquetes y además concentra la autenticación y autorización. Por otro lado, TACACS+ requiere más paquetes y, por ende, mayor volumen de datos en la transmisión.

4.1.1.3. Latencia en la red cuando un usuario solicita y obtiene acceso

Para medir la latencia en la autenticación y autorización de un usuario legítimo, se sincronizan los relojes de la computadora del usuario y el switch mediante el servicio NTP, configurando la IP de la computadora como servidor NTP del switch.

Figura 94.

Sincronización de relojes entre el switch y la computadora del usuario.

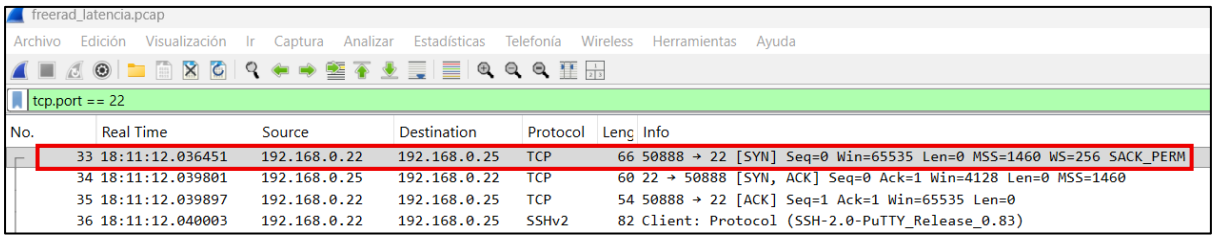


Nota. Elaboración propia.

Posteriormente, se registra el tiempo total que transcurre desde que el usuario envía la solicitud SSH hasta que el servidor autoriza el acceso con el nivel de privilegio correspondiente. Para ello se utilizan capturas de paquetes con Wireshark y los logs generados en el switch.

Figura 95

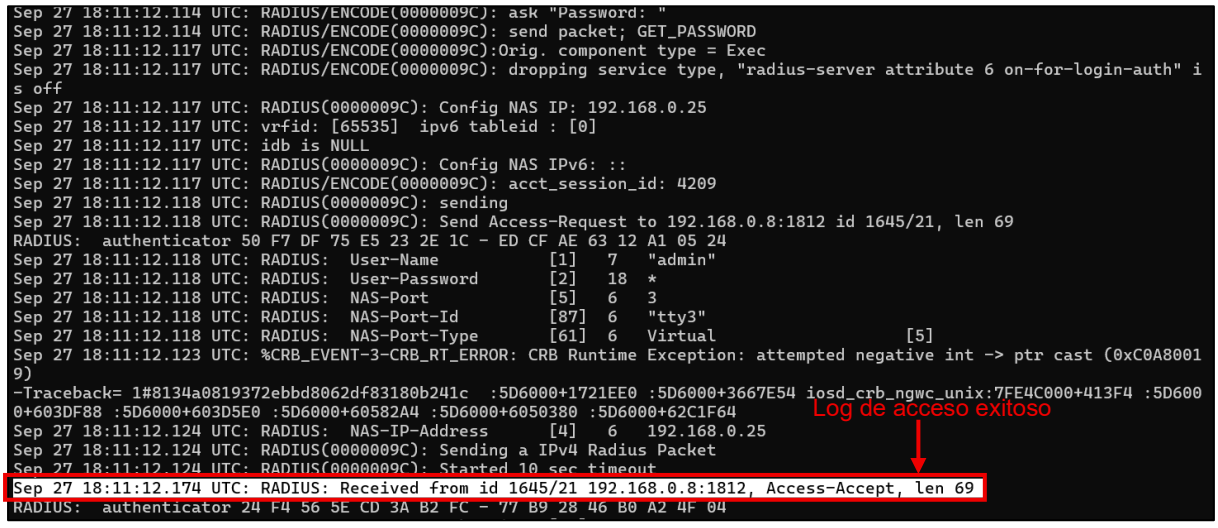
Captura de paquetes SSH durante la prueba de RADIUS.



Nota. Elaboración propia.

Figura 96.

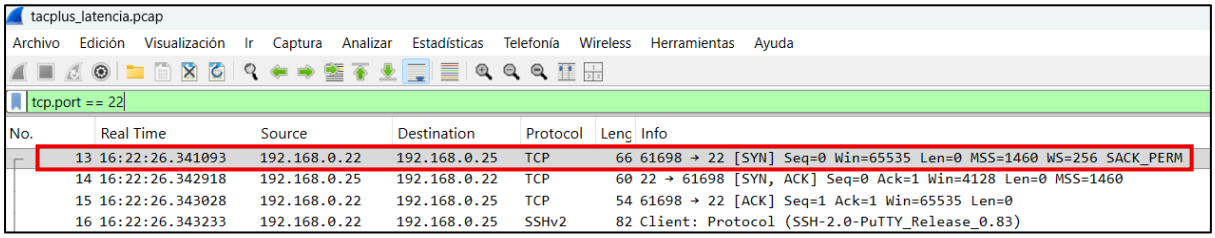
Logs generados en el switch por el protocolo RADIUS.



Nota. Elaboración propia.

Figura 97.

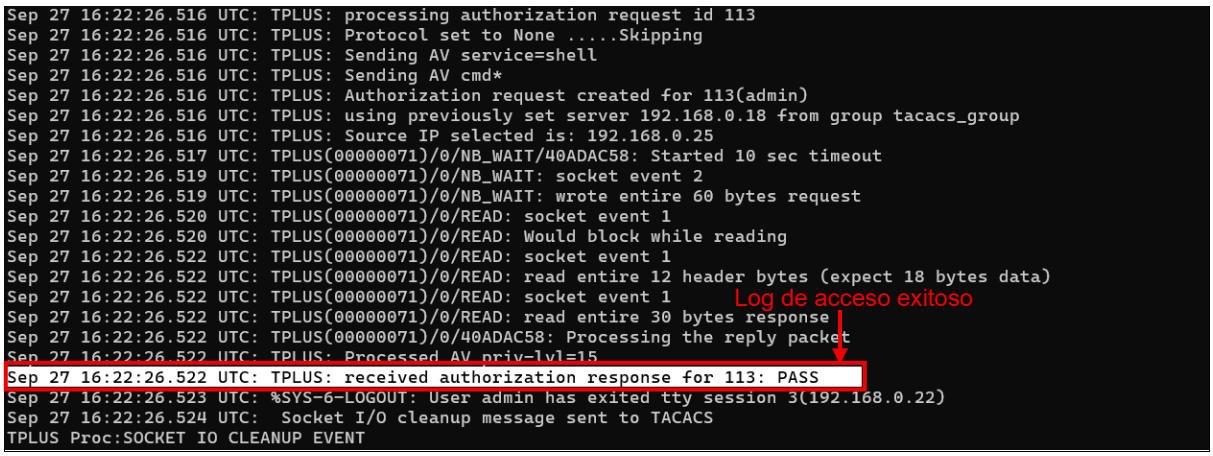
Captura de paquetes SSH durante la prueba de TACACS+.



Nota. Elaboración propia.

Figura 98.

Logs generados en el switch por el protocolo TACACS+.

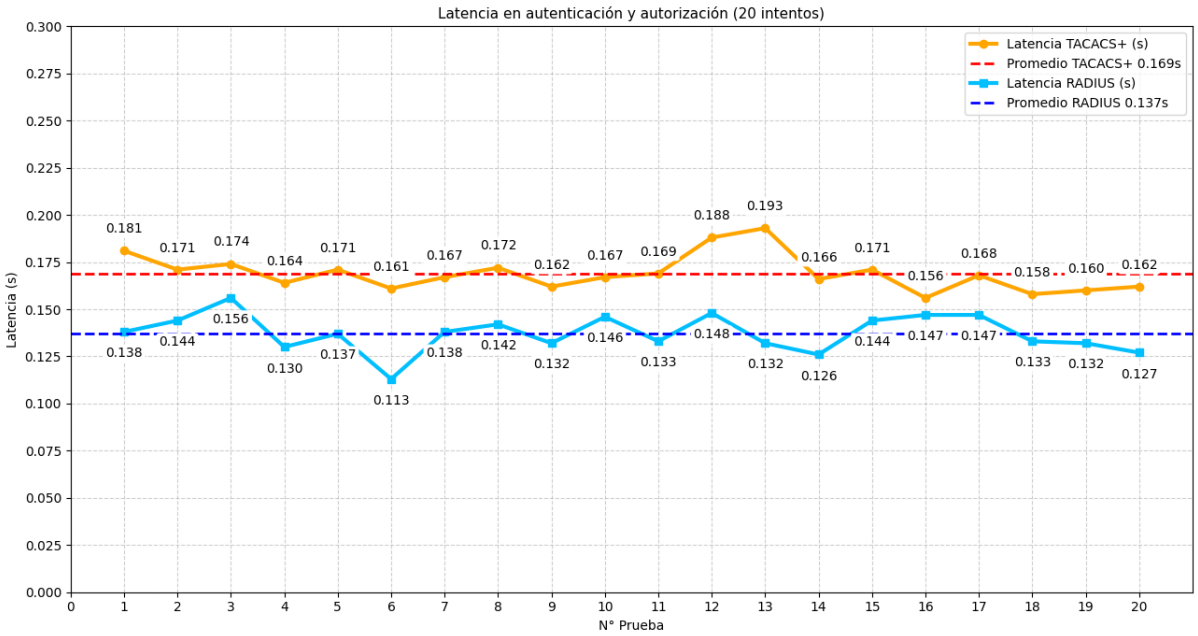


Nota. Elaboración propia.

Los resultados demuestran que, en 20 pruebas de conexión con RADIUS, el tiempo promedio desde la solicitud de acceso hasta la autorización del usuario fue de 0.137 segundos, con un mínimo de 0.113 segundos registrado en la sexta prueba y un máximo de 0.156 segundos observado en la tercera prueba. Por otro lado, el protocolo TACACS+ presentó un tiempo promedio de 0.169 segundos, con un mínimo de 0.156 segundos registrado en la decimosexta prueba y un máximo de 0.193 segundos alcanzado en la decimotercera prueba. Ver Figura 99.

Figura 99.

Resultados de latencia para RADIUS y TACACS+.



Nota. Elaboración propia.

La diferencia en latencia se explica por el mayor número de paquetes y el volumen de datos que TACACS+ intercambia durante el proceso de autenticación y autorización. Mientras que RADIUS completa el proceso con solo 2 paquetes, TACACS+ requiere 22, lo que incrementa el tiempo total para otorgar acceso al usuario. Este comportamiento confirma que RADIUS ofrece un mejor tiempo en la validación y la autorización del acceso a un usuario legítimo, mientras que TACACS+, aunque más detallado, introduce mayor latencia en la red.

Considerando los resultados obtenidos, se demuestra que, desde la perspectiva del desempeño, el protocolo RADIUS presenta una mejor eficiencia operacional ya que intercambia un menor número de paquetes y volumen de datos reducido en un tiempo más corto al otorgar el acceso a un usuario legítimo. De esta manera, se cumple con el primer objetivo de esta investigación.

4.1.2. Seguridad

Se evalúa la seguridad de los protocolos RADIUS y TACACS+ considerando el porcentaje de datos cifrados en los paquetes de autenticación, autorización y auditoría, la capacidad para denegar comandos específicos y el número de paquetes de auditoría generados durante la sesión de un usuario legítimo. Estos indicadores permiten determinar la capacidad del cifrado de datos, control del privilegio y registro de eventos de seguridad que ofrece cada protocolo.

4.1.2.1. Porcentaje de datos cifrados en los paquetes de autenticación y autorización

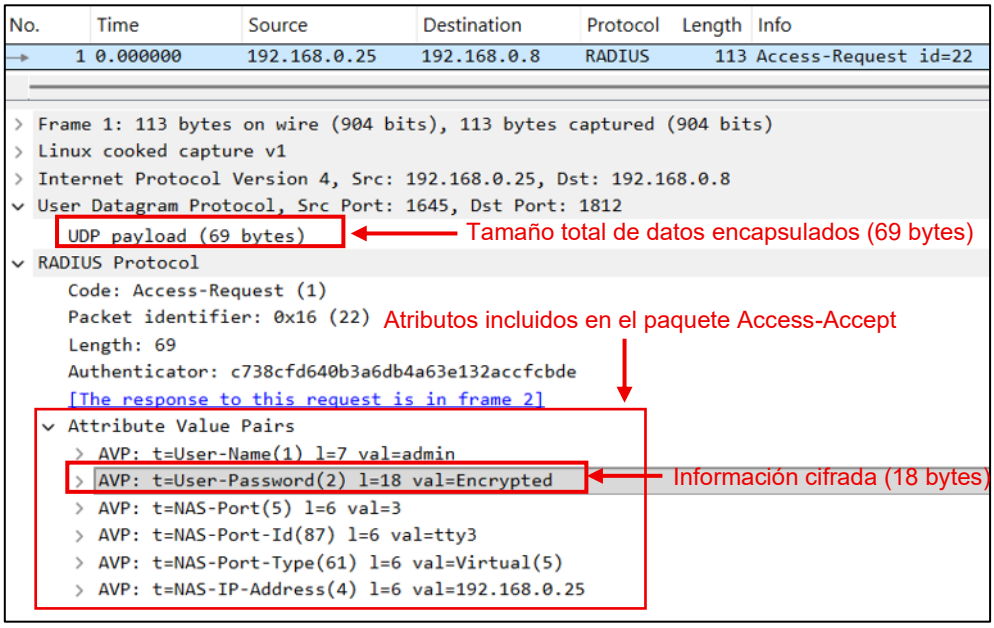
Para medir el porcentaje de datos cifrados en los paquetes de autenticación y autorización, se captura el tráfico con Wireshark y se identifica el tamaño total del *payload* en cada paquete. Posteriormente, se calcula la razón entre la longitud del dato cifrado y el tamaño total del *payload*.

En RADIUS, se evidencia que información sensible como la dirección IP del switch (NAS) y el nombre de usuario se transmiten en texto claro, lo cual representa un riesgo significativo de exposición ante un posible ataque de interceptación.

Como se observa en la Figura 1000, en el paquete Access-Request, únicamente el campo User-Password se encuentra cifrado, lo que corresponde al 26% del payload UDP.

Figura 100.

Contenido del paquete Access-Request con el campo User-Password cifrado.

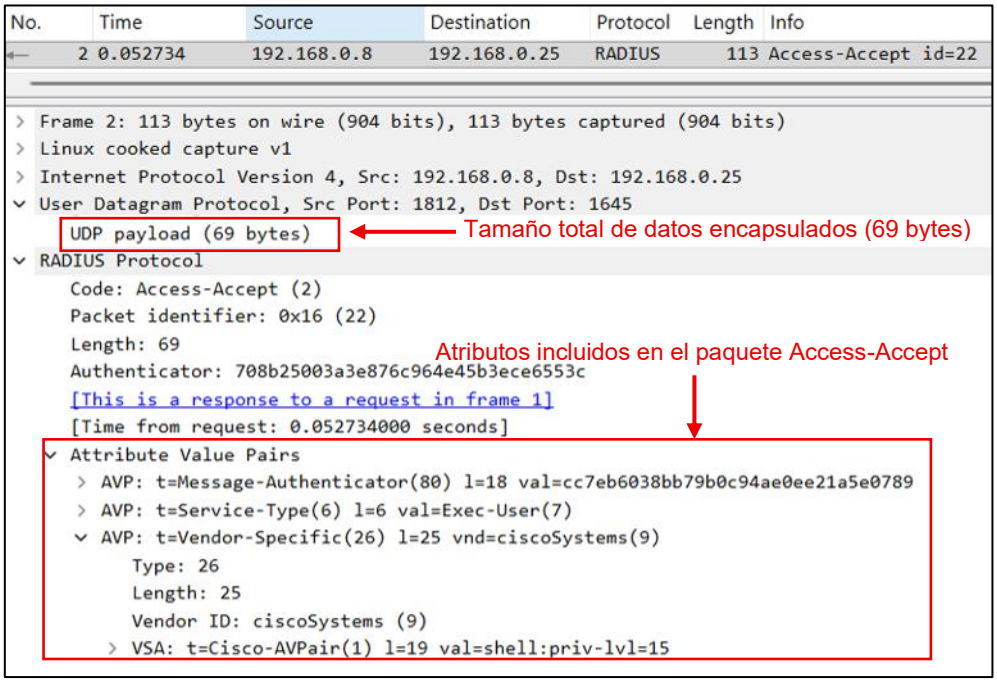


Nota. Elaboración propia.

En el paquete *Access-Accept*, toda la información viaja en texto claro, es decir, el 0% está cifrado. Esto es crítico, ya que en dicho paquete se incluyen atributos relacionados a características del switch y privilegios del usuario, como se aprecia en la Figura 101.

Figura 101.

Contenido del paquete Access-Accept sin ningún campo cifrado.

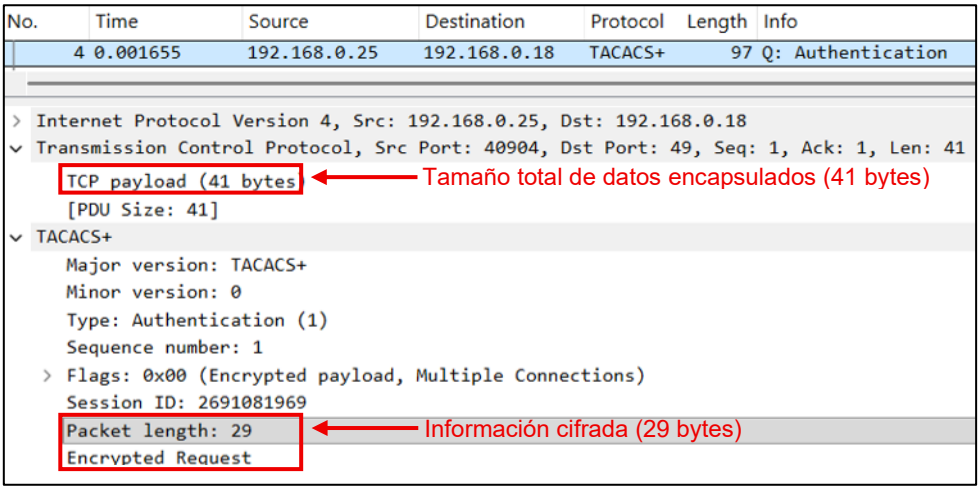


Nota. Elaboración propia.

En contraste, TACACS+ presenta un cifrado mucho más robusto. En el primer paquete *Q: Authentication*, el 70.731% del *payload* TCP está cifrado y en el paquete *R: Authentication,* el cifrado alcanza el 70.778%. Ver Figura 102 y Figura 103.

Figura 102.

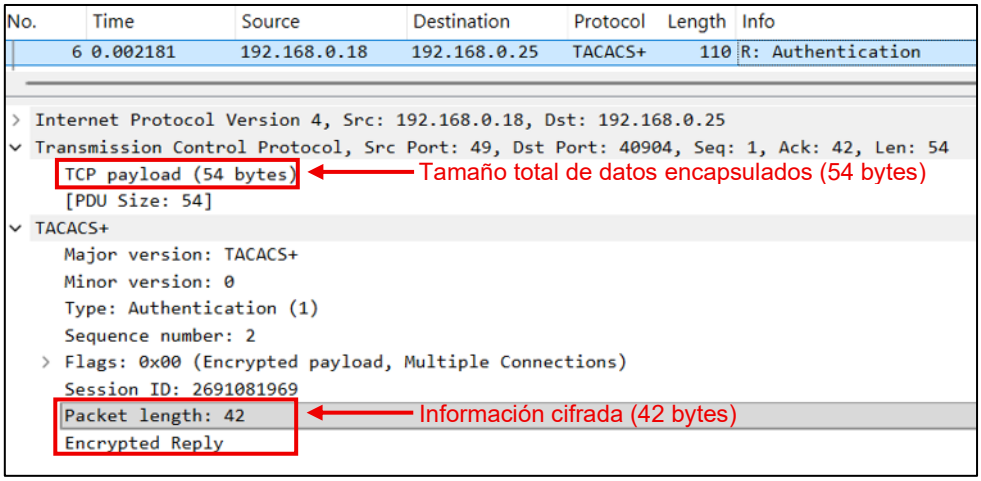
Contenido del primer paquete Q: Authentication con sus respectivos campos cifrados.



Nota. Elaboración propia.

Figura 103.

Contenido del primer paquete R: Authentication con sus respectivos campos cifrados.

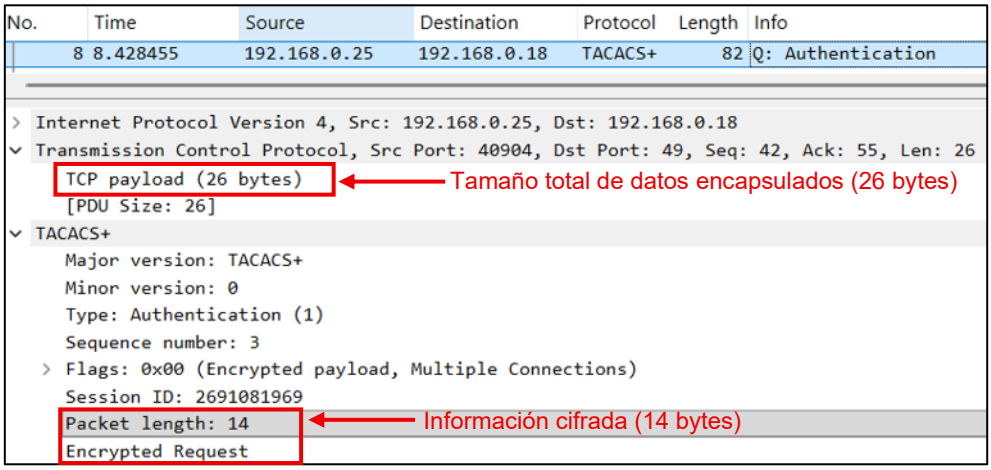


Nota. Elaboración propia.

En el segundo paquete *Q: Authentication,* el cifrado representa el 53.846% del payload TCP y en el paquete *R: Authentication* se alcanza el 33.333% de cifrado. Ver Figura 104 y Figura 105.

Figura 104.

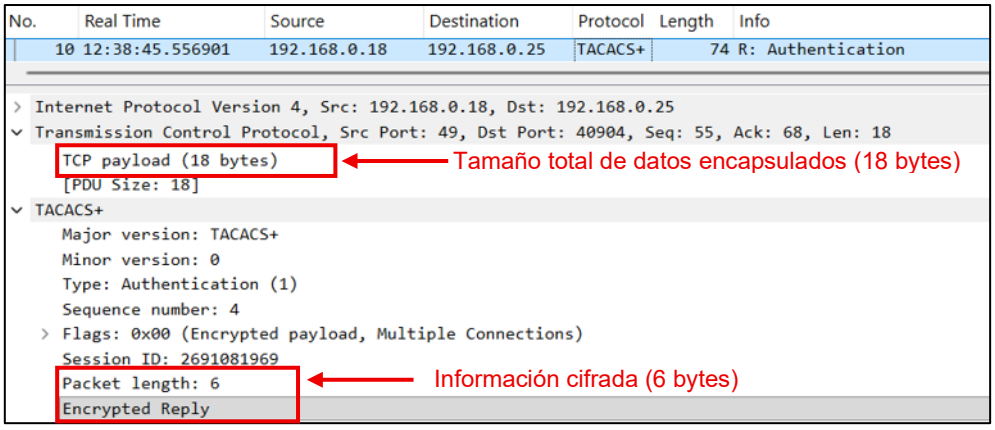
Contenido del segundo paquete Q: Authentication con sus respectivos campos cifrados.



Nota. Elaboración propia.

Figura 105.

Contenido del segundo paquete R: Authentication con sus respectivos campos cifrados.

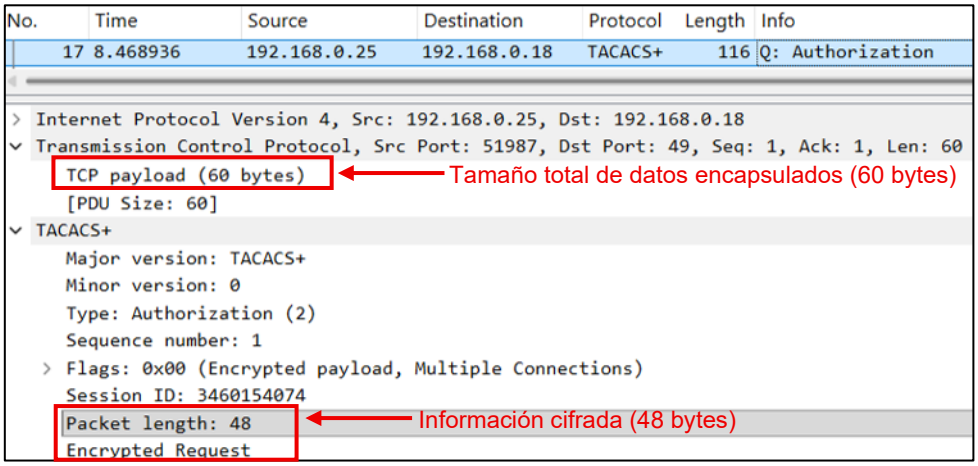


Nota. Elaboración propia.

En los paquetes de autorización, los valores alcanzan el 80% en el paquete *Q: Authorization* y el 60% en el paquete *R: Authorization*. Ver Figura 106 y Figura 107.

Figura 106.

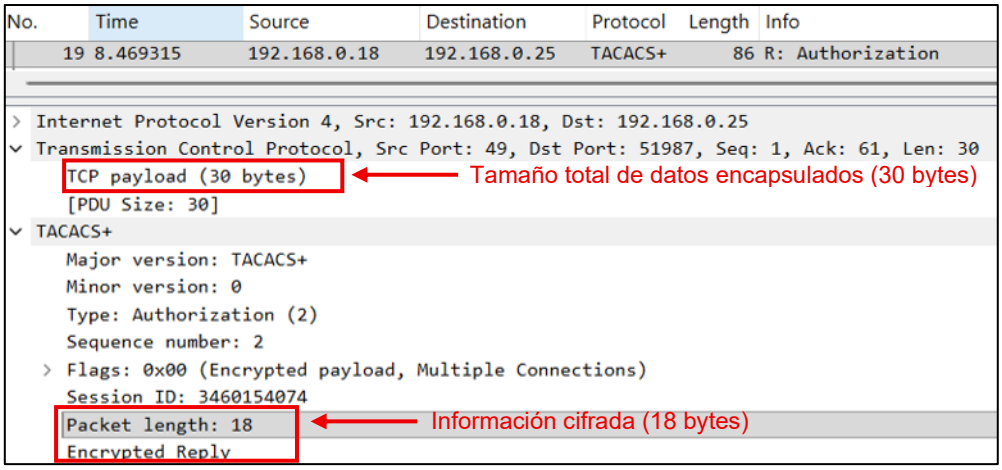
Contenido del segundo paquete Q: Authorization con sus respectivos campos cifrados.



Nota. Elaboración propia.

Figura 107.

Contenido del segundo paquete R: Authorization con sus respectivos campos cifrados.



Nota. Elaboración propia.

Los resultados confirman que TACACS+ cifra la totalidad de la información sensible transmitida, exceptuando únicamente la cabecera fija de 12 bytes, que no contiene datos críticos. Por tanto, TACACS+ ofrece una protección significativamente superior frente a RADIUS en los procesos de autenticación y autorización, reduciendo la probabilidad de exposición de datos ante ataques de interceptación.

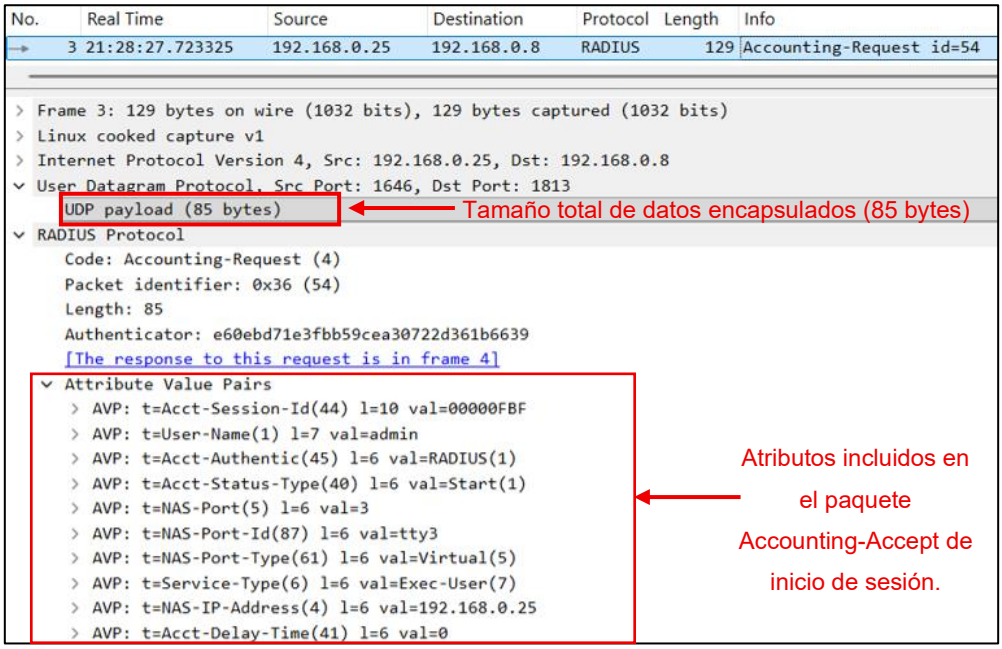
4.1.2.2. Porcentaje de datos cifrados en los paquetes de auditoría

En el análisis de los paquetes de auditoría, se verifica que los mensajes *Accounting-Request* y *Accounting-Response* de RADIUS, tanto en el inicio como en el fin de sesión, se

transmiten completamente en texto plano, es decir, con 0% de cifrado. Esto implica que atributos como el nombre de usuario, la dirección IP del switch (NAS) y los detalles de la sesión pueden ser visualizados por un atacante que intercepte el tráfico. La ausencia de cifrado en los registros de auditoría constituye un riesgo grave, ya que dicha información puede ser utilizada para perfilar usuarios legítimos o ejecutar ataques dirigidos. Ver Figuras 108, 109, 110, y 111.

Figura 108.

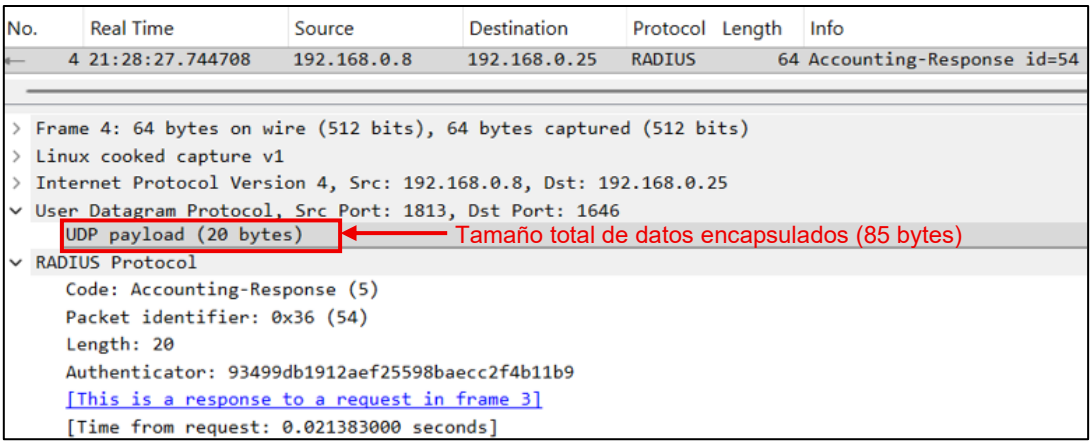
Contenido del paquete Accounting-Accept de inicio de sesión sin ningún campo cifrado.



Nota. Elaboración propia.

Figura 109.

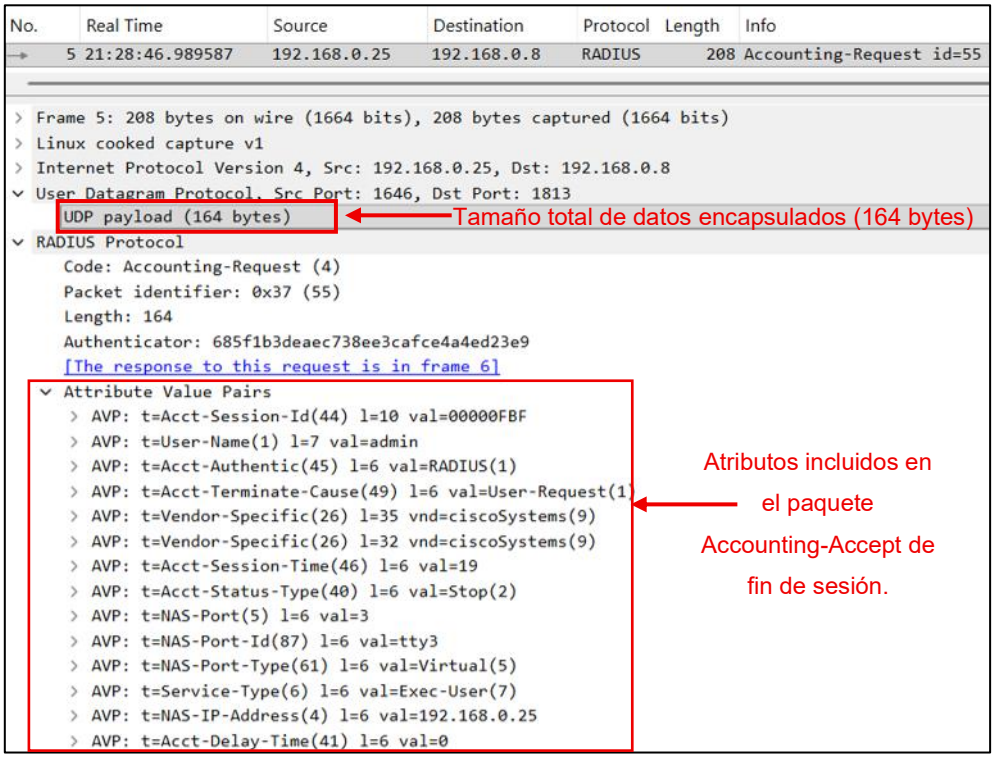
Contenido del paquete Accounting-Response de inicio de sesión sin ningún campo cifrado.



Nota. Elaboración propia.

Figura 110.

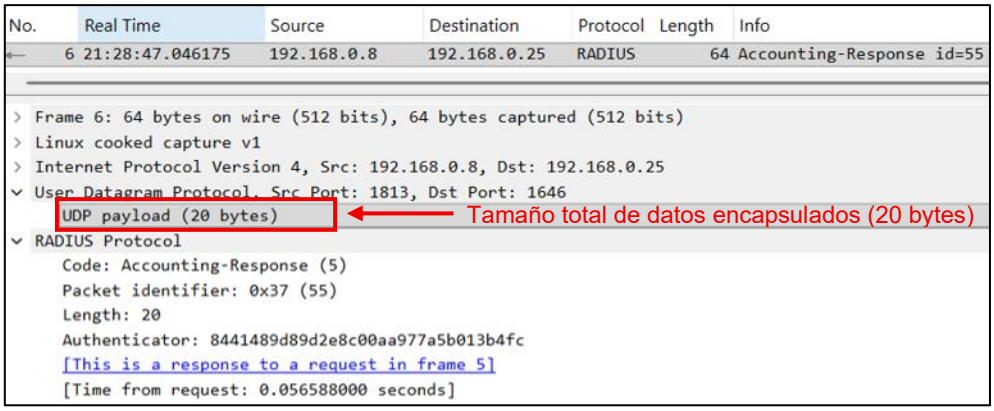
Contenido del paquete Accounting-Accept de fin de sesión sin ningún campo cifrado.



Nota. Elaboración propia.

Figura 111.

Contenido del paquete Accounting-Response de fin de sesión sin ningún campo cifrado.

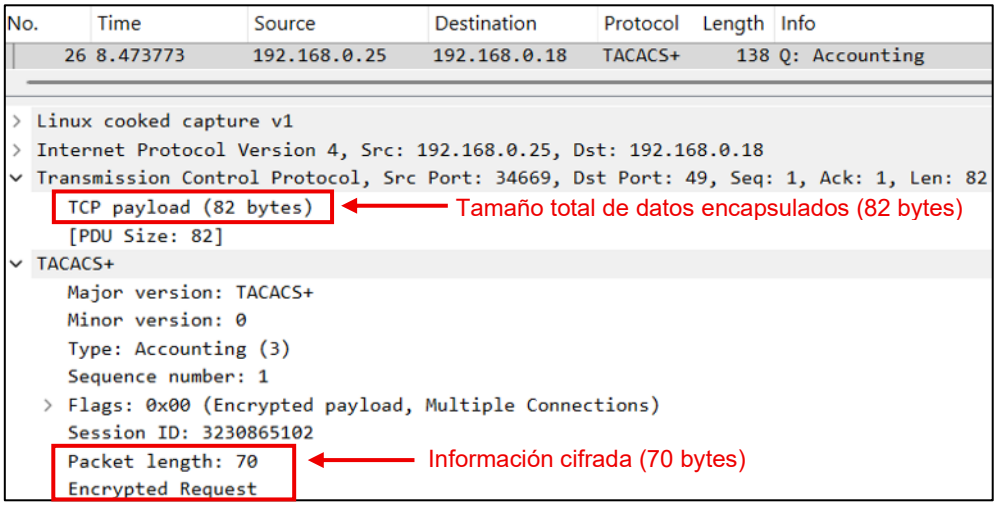


Nota. Elaboración propia.

En el caso de TACACS+, los mensajes de auditoría se transmiten cifrados, garantizando que la información de auditoría permanezca confidencial durante su tránsito por la red. En el primer paquete *Q: Accounting*, el 87.5% del *payload* TCP está cifrado, mientras que en el *R: Accounting*, el cifrado representa el 29.412%.

Figura 112.

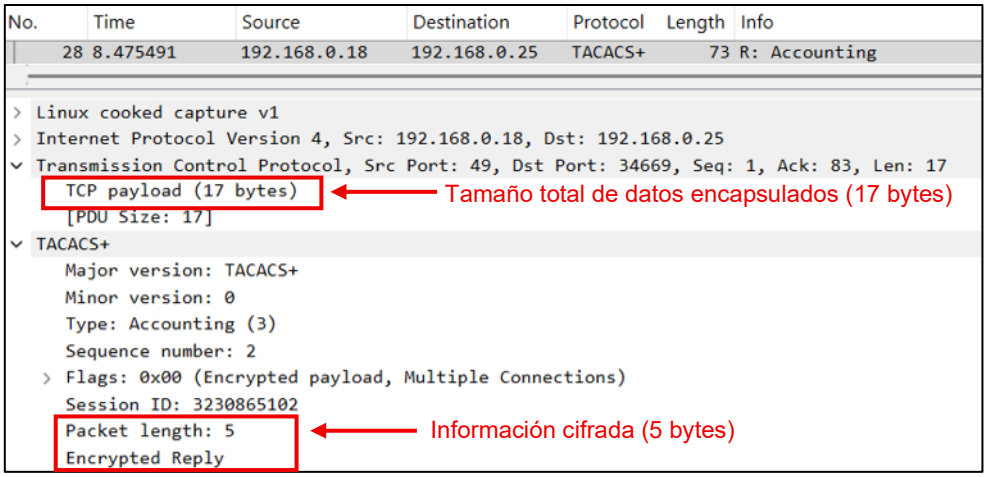
Contenido del paquete Q: Accounting de inicio de sesión cifrado.



Nota. Elaboración propia.

Figura 113.

Contenido del paquete R: Accounting de inicio de sesión cifrado.

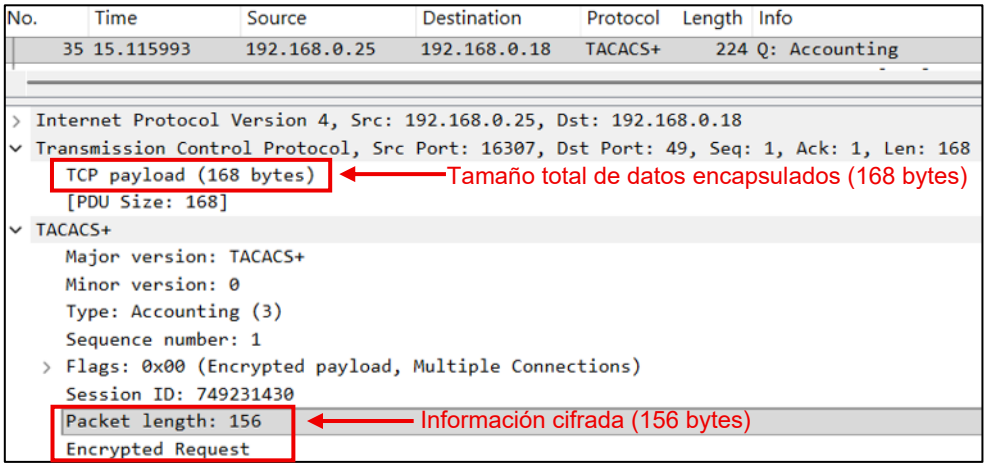


Nota. Elaboración propia.

En el segundo intercambio, el 92.857% del *payload* TCP está cifrado en el paquete *Q: Accounting* y el 29.412% en el paquete *R: Accounting*.

Figura 114.

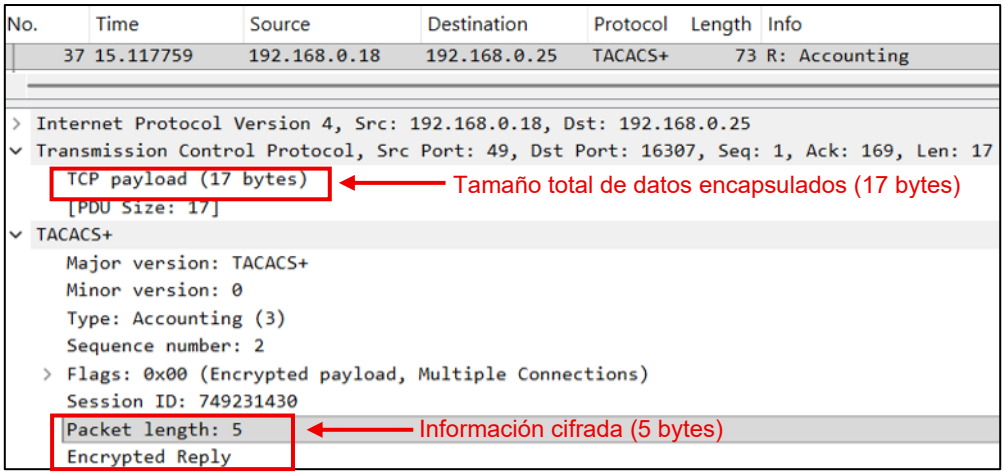
Contenido del paquete Q: Accounting de fin de sesión cifrado.



Nota. Elaboración propia.

Figura 115.

Contenido del paquete R: Accounting de fin de sesión cifrado.



Nota. Elaboración propia.

Los resultados evidencian que TACACS+ implementa un esquema de cifrado más sólido para los mensajes de auditoría, evitando la exposición de información sensible durante la transmisión. A diferencia de RADIUS, que carece de mecanismos de protección, TACACS+ asegura la confidencialidad de los registros y contribuye a mantener la trazabilidad de las actividades de los usuarios sin comprometer su seguridad.

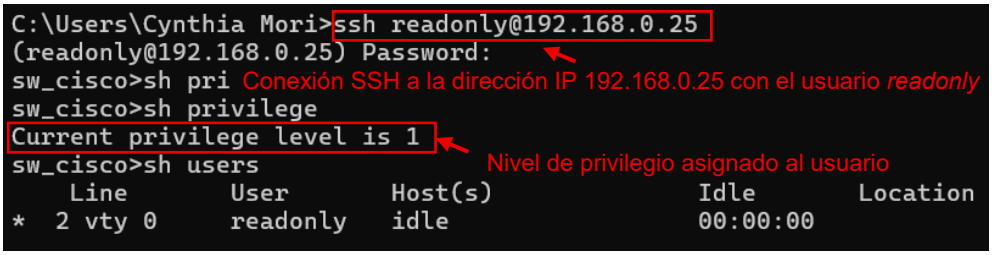
4.1.2.3. Porcentaje de comandos que se pueden denegar sobre un conjunto representativo

Para evaluar la capacidad de control del privilegio otorgado a los usuarios, se analiza la posibilidad de denegar comandos específicos al usuario con nivel de privilegio 1, aplicando el principio del mínimo privilegio.

La Figura 116 muestra la conexión del usuario *readonly* y el nivel de privilegio 1 que se le otorga.

Figura 116.

Conexión del usuario con nivel de privilegio 1.

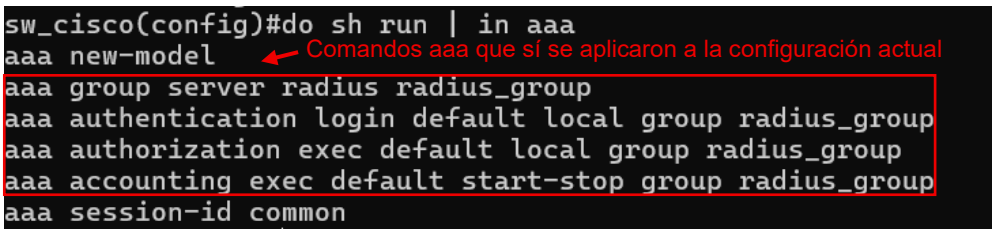


Nota. Elaboración propia.

En RADIUS, debido a que la configuración de los comandos *aaa authorization commands* en el switch no activa ningún control funcional el control, se limita a validar las credenciales y a asignar atributos de acceso, sin permitir una restricción detallada de los comandos ejecutados en la CLI del dispositivo. Como resultado, el 0% de los comandos disponibles para un usuario determinado puede ser denegado.

Figura 117.

Verificación de configuración con los comandos aaa authorization commands en el switch.



Nota. Elaboración propia.

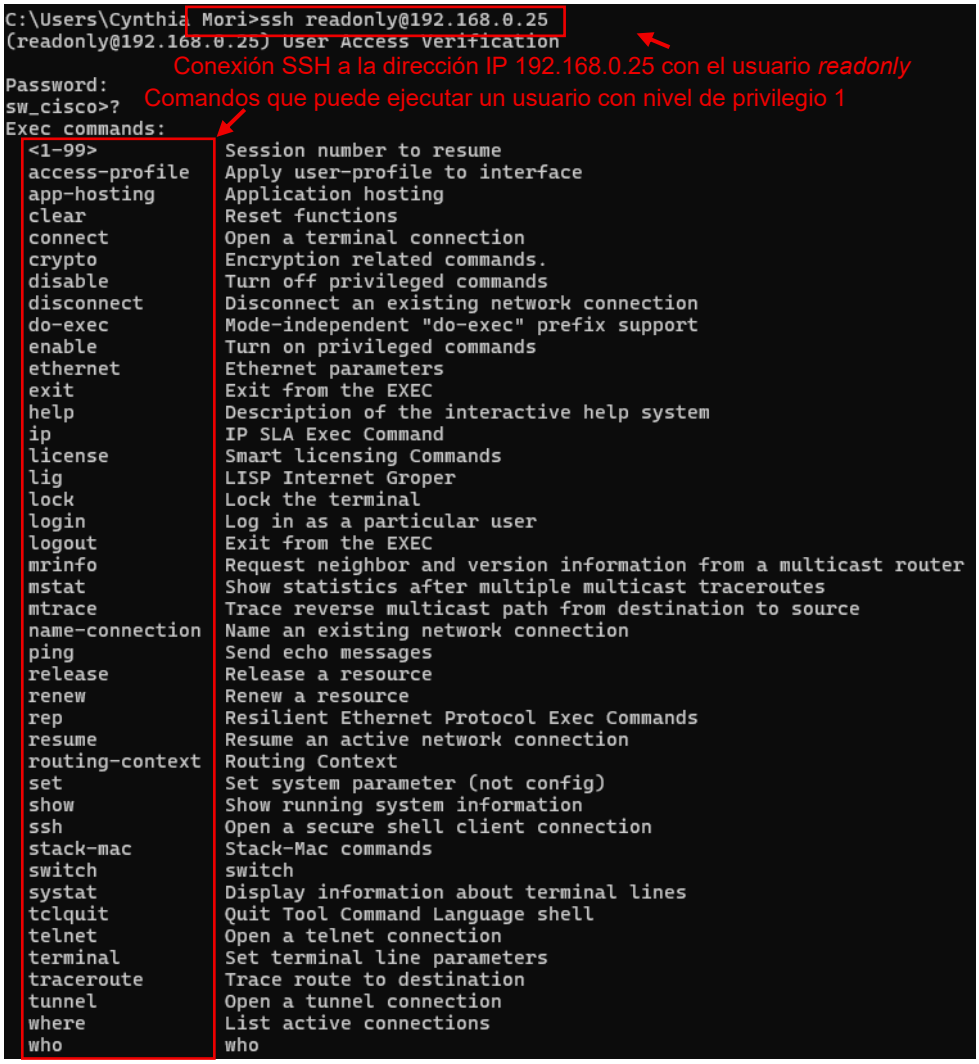
Por el contrario, TACACS+ ofrece un control detallado sobre los comandos permitidos al usuario de nivel de privilegio 1. En las pruebas realizadas, de un total de 42 comandos disponibles para el usuario, se restringieron 40, permitiendo únicamente los comandos

básicos de diagnóstico como *ping* y *traceroute*. Esto representa un 95.2% de comandos denegados.

La Figura 118 presenta todos comandos que pueden ser ingresados en la CLI del switch por un usuario con nivel de privilegio 1 y la Figura 119 evidencia que solo los comandos *ping* y *traceroute* son permitidos.

Figura 118.

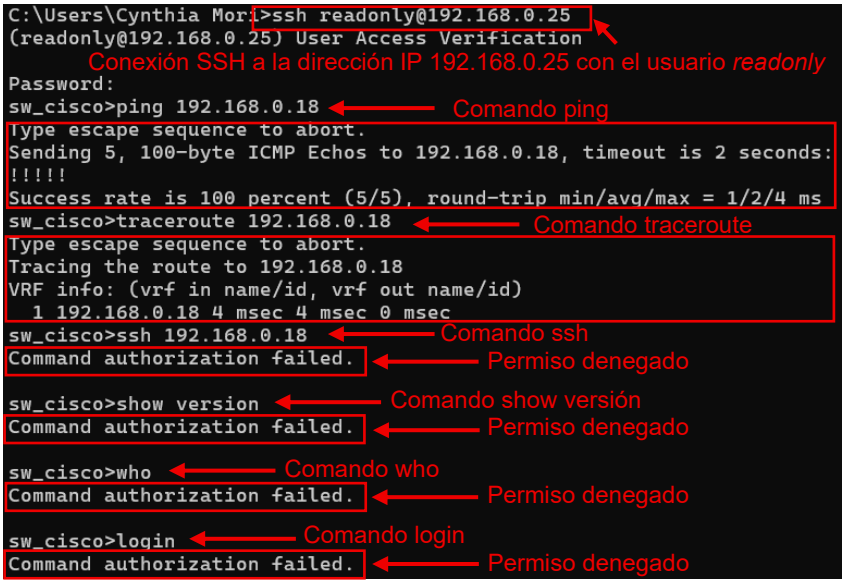
Comandos que pueden ser utilizados por un usuario con nivel de privilegio 1.



Nota. Elaboración propia.

Figura 119.

Verificación de comandos permitidos y denegados para el usuario de privilegio 1.



Nota. Elaboración propia.

Estos resultados demuestran que TACACS+ garantiza un control más granular del nivel de privilegio asignado, evitando que los usuarios realicen cambios no autorizados en la configuración del equipo y asegurando que solo realicen las funciones específicas que les han sido asignadas.

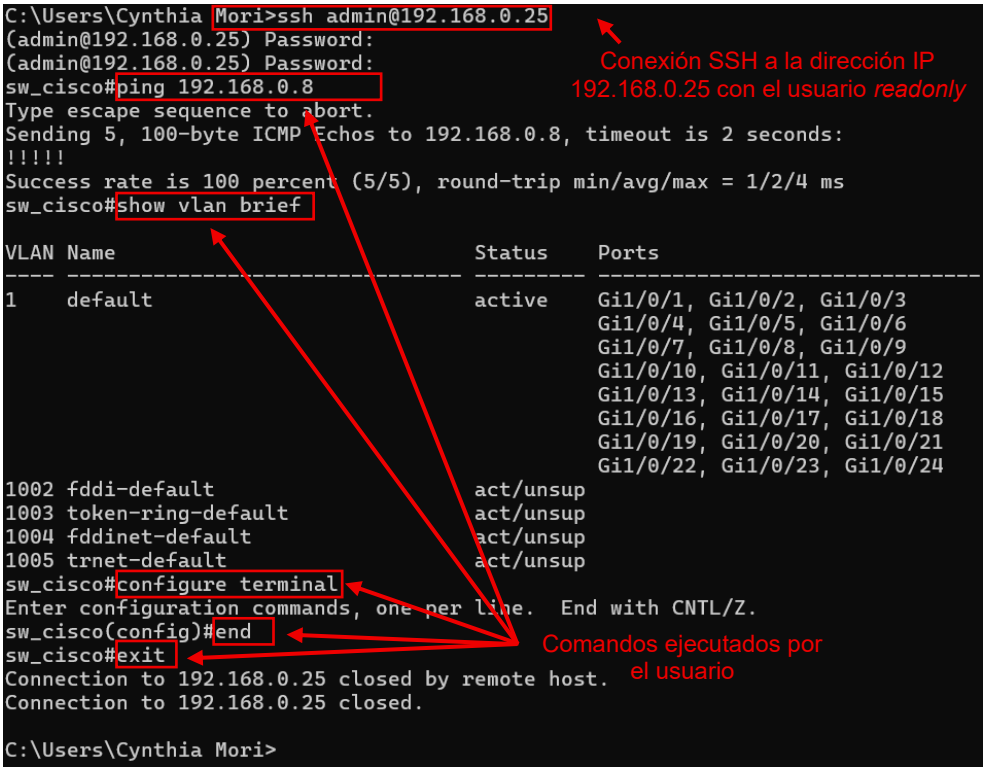
4.1.2.4. Número de paquetes de auditoría generados desde el inicio hasta el fin de sesión

Para evaluar las capacidades de auditoría de cada protocolo, se contabiliza el número de paquetes *Accounting* generados durante la sesión completa de un usuario legítimo, la cual incluye el inicio de sesión, la ejecución de comandos y el cierre de sesión.

La Figura 120 muestra la actividad del usuario en la interfaz de línea de comandos (CLI) del switch.

Figura 120.

Actividad del usuario admin en la CLI de switch.

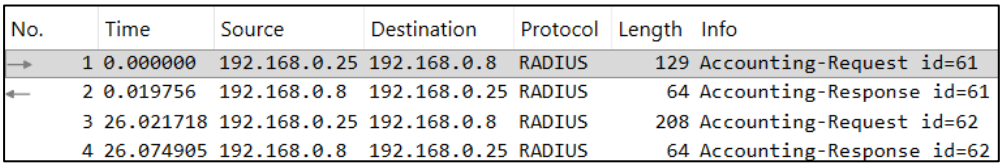


Nota. Elaboración propia.

Con RADIUS, se tienen en total 4 paquetes *Accounting,* correspondientes únicamente al inicio y fin de sesión. Ver Figura 121.

Figura 121.

Paquetes Accounting RADIUS capturados con Wireshark.



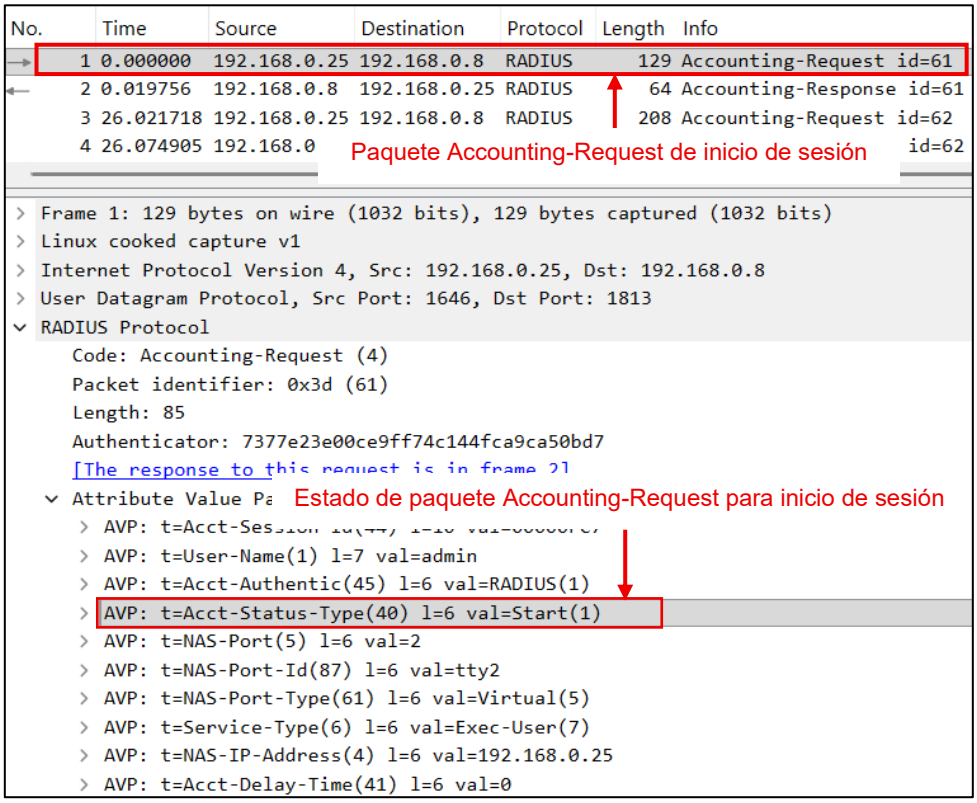
No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000	192.168.0.25	192.168.0.8	RADIUS	129	Accounting-Request id=61
← 2	0.019756	192.168.0.8	192.168.0.25	RADIUS	64	Accounting-Response id=61
3	26.021718	192.168.0.25	192.168.0.8	RADIUS	208	Accounting-Request id=62
4	26.074905	192.168.0.8	192.168.0.25	RADIUS	64	Accounting-Response id=62

Nota. Elaboración propia.

Los paquetes *Accounting* de RADIUS no incluyen los comandos ejecutados por el usuario en la CLI del switch, lo que limita la trazabilidad de las acciones realizadas durante la sesión. Ver Figura 122 y Figura 123.

Figura 122.

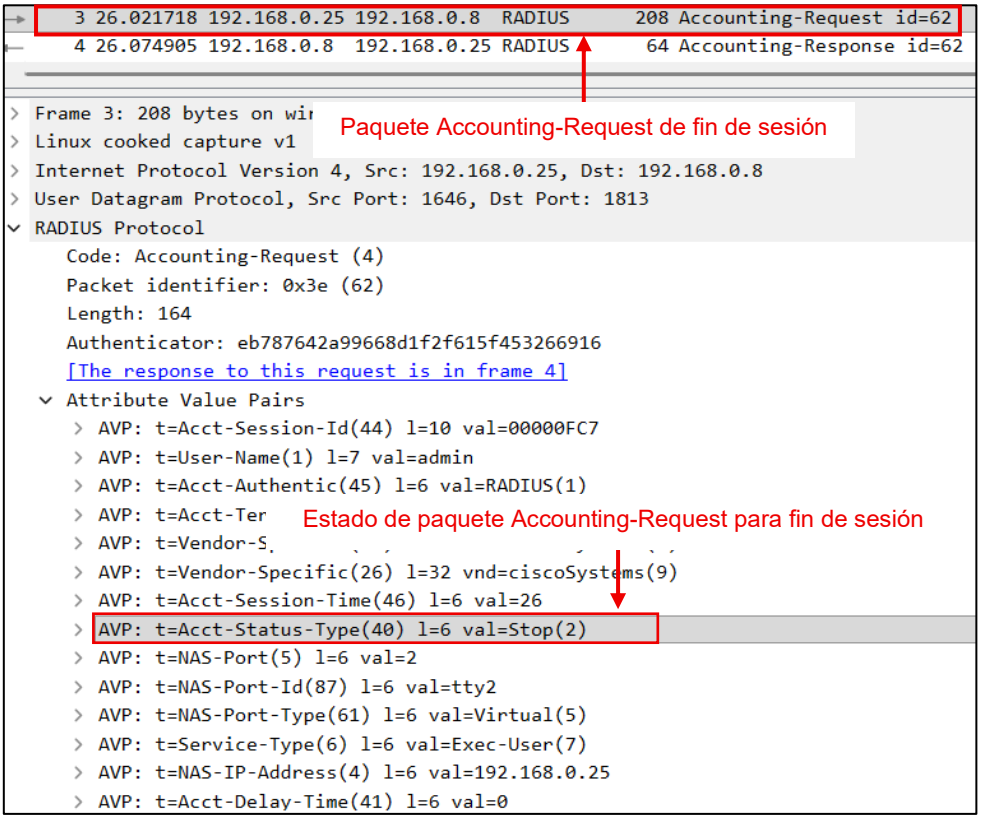
Contenido del paquete Accounting-Request de inicio de sesión.



Nota. Elaboración propia.

Figura 123.

Contenido del paquete Accounting-Request de fin de sesión.



Nota. Elaboración propia.

La Tabla 8 describe cada paquete RADIUS intercambiado durante la auditoría.

Tabla 8.

Intercambio de paquetes durante el proceso de auditoría con RADIUS.

Item	N° Paquete	Paquete	Descripción
1	1	Accounting-Request	Inicio de sesión del usuario.
2	2	Accounting-Response	Respuesta al paquete Accounting-Response de inicio de sesión.
3	3	Accounting-Request	Inicio de sesión del usuario.
4	4	Accounting-Response	Respuesta al paquete Accounting-Response de fin de sesión.

Nota. Elaboración propia.

Por otro lado, el protocolo TACACS+ generan un total de 10 paquetes de tipo *Accounting* durante la sesión del usuario. Ver Figura 124.

Figura 124.

Paquetes Accounting TACACS+ capturados con Wireshark.

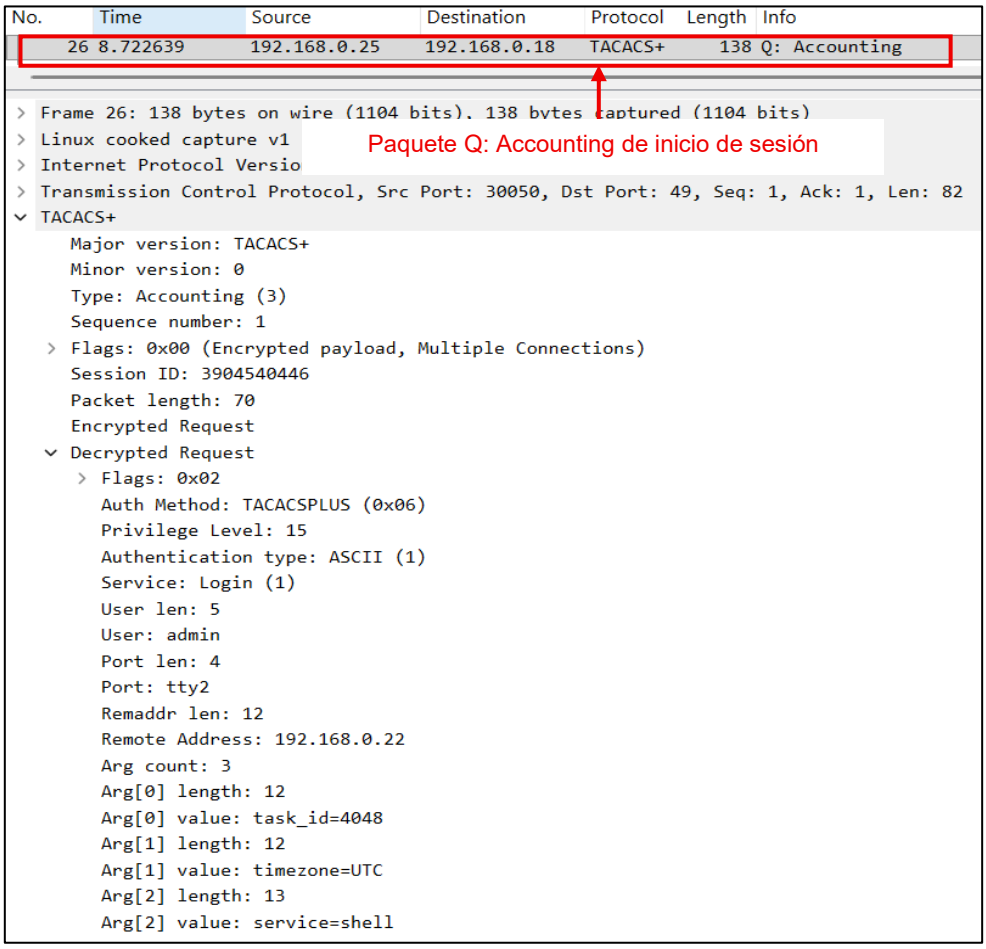
No.	Time	Source	Destination	Protocol	Length	Info
26	8.722639	192.168.0.25	192.168.0.18	TACACS+	138	Q: Accounting
28	8.723365	192.168.0.18	192.168.0.25	TACACS+	73	R: Accounting
35	42.605598	192.168.0.25	192.168.0.18	TACACS+	176	Q: Accounting
37	42.608093	192.168.0.18	192.168.0.25	TACACS+	73	R: Accounting
44	59.939142	192.168.0.25	192.168.0.18	TACACS+	174	Q: Accounting
46	59.947343	192.168.0.18	192.168.0.25	TACACS+	73	R: Accounting
53	69.445256	192.168.0.25	192.168.0.18	TACACS+	178	Q: Accounting
55	69.449143	192.168.0.18	192.168.0.25	TACACS+	73	R: Accounting
62	79.622104	192.168.0.25	192.168.0.18	TACACS+	224	Q: Accounting
64	79.625140	192.168.0.18	192.168.0.25	TACACS+	73	R: Accounting

Nota. Elaboración propia.

Como se observa en las Figuras 125 a 128, estos paquetes TACACS+ registran tanto el inicio y fin de la sesión del usuario, como los comandos ejecutados por el usuario en la CLI del switch, con excepción de los comandos *end* y *exit*, los cuales se omiten por carecer de relevancia para efectos de auditoría.

Figura 125.

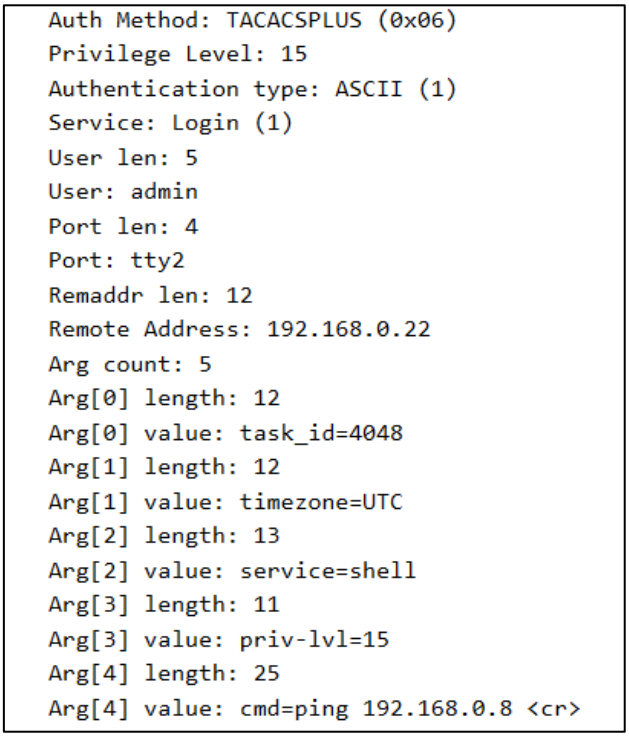
Contenido del paquete Q: Accounting de inicio de sesión.



Nota. Elaboración propia.

Figura 126.

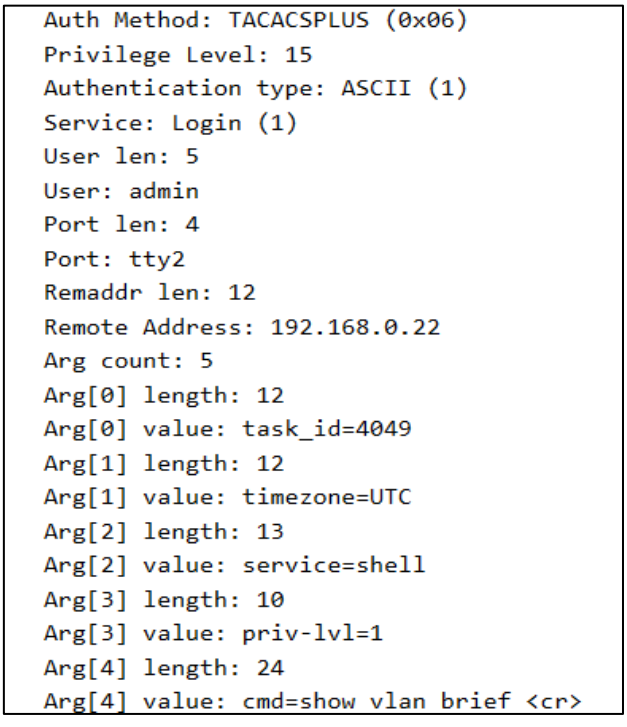
Contenido del paquete Q: Accounting que registra la ejecución del comando ping 192.168.0.8.



Nota. Elaboración propia.

Figura 127.

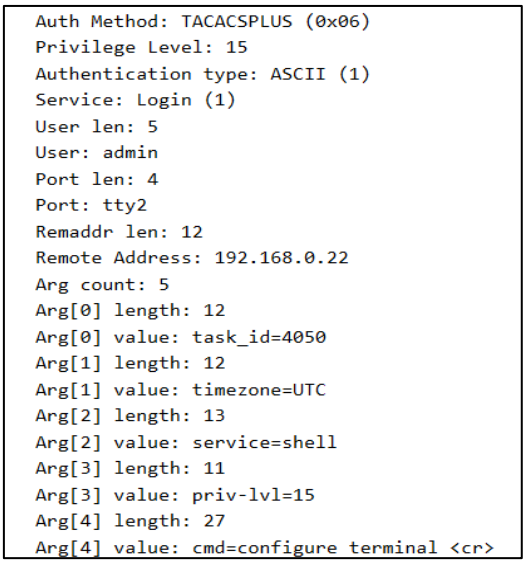
Contenido del paquete Q: Accounting que registra la ejecución del comando show vlan brief.



Nota. Elaboración propia.

Figura 128.

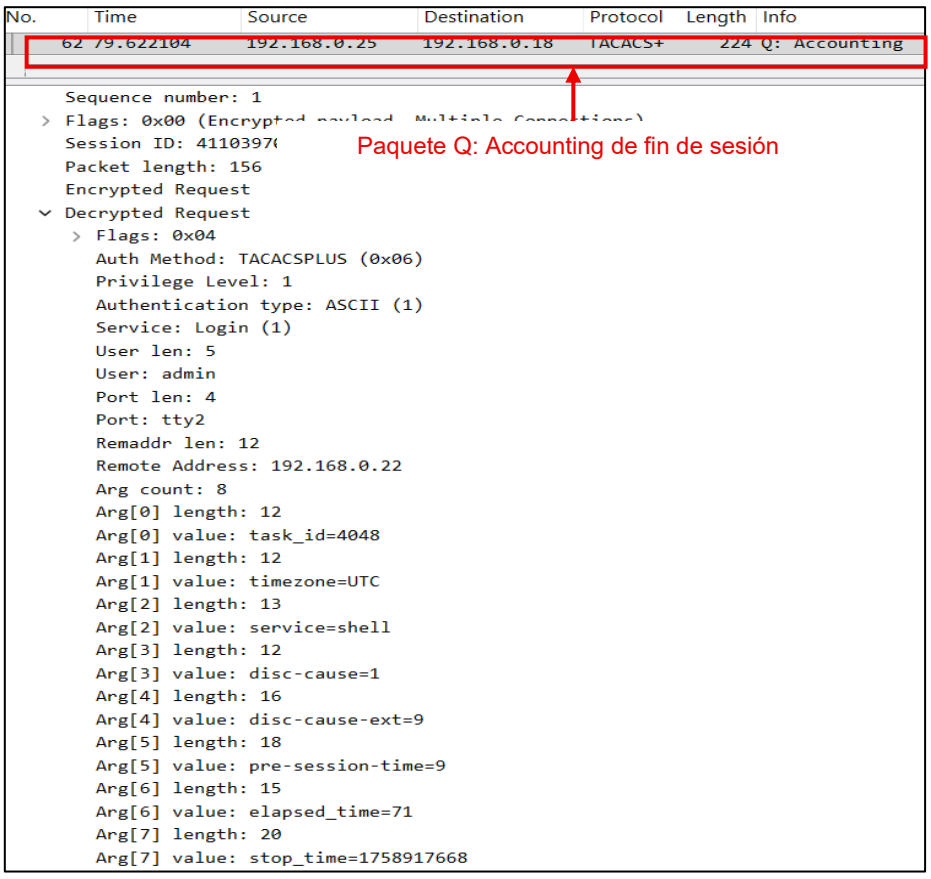
Contenido del paquete Q: Accounting que registra la ejecución del comando configure terminal.



Nota. Elaboración propia.

Figura 129.

Contenido del paquete Q: Accounting de fin de sesión.



Nota. Elaboración propia.

La Tabla 9 describe cada paquete TACACS+ intercambiado durante la auditoría.

Tabla 9.

Intercambio de paquetes durante el proceso de auditoría con TACAS+.

Item	N° Paquete	Paquete	Descripción
1	26	Q: Accounting	Inicio de sesión del usuario.
2	28	R: Accounting	Respuesta al primer paquete Q: Accounting de inicio de sesión.
3	35	Q: Accounting	Registro de comando ping 192.168.0.8
4	37	R: Accounting	Respuesta al segundo paquete Q: Accounting.
5	44	Q: Accounting	Registro de comando show vlan brief.
6	46	R: Accounting	Respuesta al tercer paquete Q: Accounting.
7	53	Q: Accounting	Registro de comando configure terminal.
8	55	R: Accounting	Respuesta al cuarto paquete Q: Accounting.
9	62	Q: Accounting	Fin de sesión del usuario.
10	64	R: Accounting	Respuesta al último paquete Q: Accounting de fin de sesión.

Nota. Elaboración propia.

Con esto se refleja que TACACS+ posee una capacidad de auditoría mucho más detallada que RADIUS. Mientras este último solo documenta los eventos de conexión y desconexión, TACACS+ ofrece un registro completo de la actividad del usuario, lo que facilita la trazabilidad, el análisis forense y la detección de posibles incidentes. Esta funcionalidad incrementa significativamente la visibilidad y el control sobre las acciones realizadas en los dispositivos de red.

Considerando los resultados obtenidos, se demuestra que, desde la perspectiva de la seguridad, el protocolo TACACS+ ofrece un mayor nivel de cifrado de datos en los procesos de autenticación, autorización y auditoria. Además, permite un control más granular del nivel de privilegio asignado a los usuarios, lo que reduce la posibilidad de ejecuciones no autorizadas sobre la configuración del switch. Del mismo modo, su capacidad de auditoría posibilita un registro exhaustivo de las acciones realizadas por los usuarios legítimos durante toda la sesión frente a RADIUS. De esta manera, se cumple con el segundo objetivo de esta investigación.

4.1.3. Disponibilidad

Se evalúa la disponibilidad de los protocolos RADIUS y TACACS+ considerando el tiempo promedio de fail-over entre servidores AAA. Este indicador permite determinar la capacidad de tolerancia a fallos de cada protocolo ante la caída o inaccesibilidad del servidor principal.

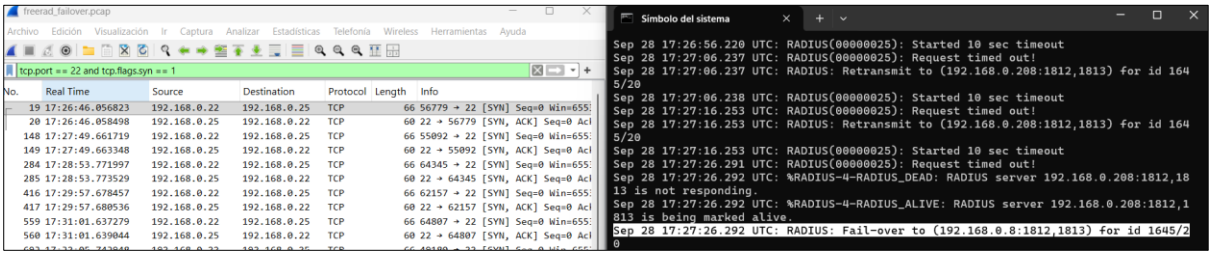
4.1.3.1. Tiempo promedio de fail-over

Se configuran servidores AAA redundantes con el propósito de simular escenarios de falla. Para el protocolo RADIUS, se utilizaron las direcciones 192.168.0.208 y 192.168.0.8, mientras que para TACACS+ se emplearon 192.168.0.228 y 192.168.0.18. En ambos casos, los servidores con direcciones terminadas en .208 y .228 actuaron como servidores primarios no disponibles, de modo que el switch debía detectar la falla y redirigir automáticamente las solicitudes hacia el servidor secundario operativo.

En el caso de RADIUS, tal como se muestra en la Figura 130, el switch realiza la conmutación desde el servidor no disponible 192.168.0.208 hacia el servidor funcional 192.168.0.8.

Figura 130.

Fail-over de servidor RADIUS.

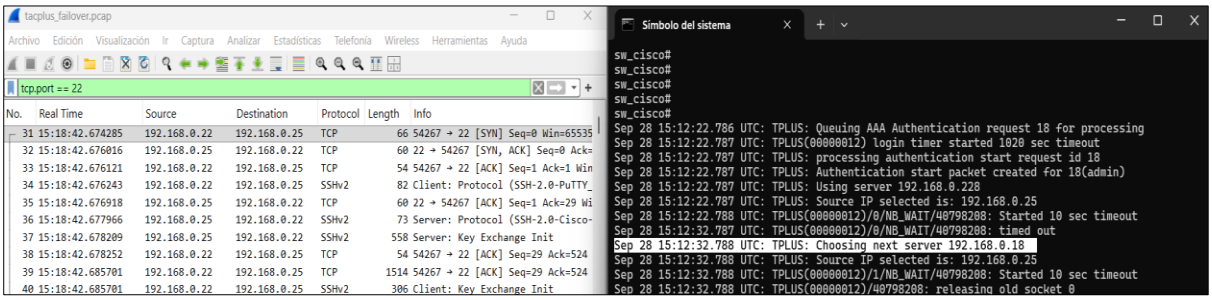


Nota. Elaboración propia.

Para TACACS+, la conmutación desde el servidor no disponible 192.168.0.228 hacia el servidor operativo 192.168.0.18 se realiza en menos tiempo, como se aprecia en la Figura 131.

Figura 131.

Fail-over de servidor TACACS+.



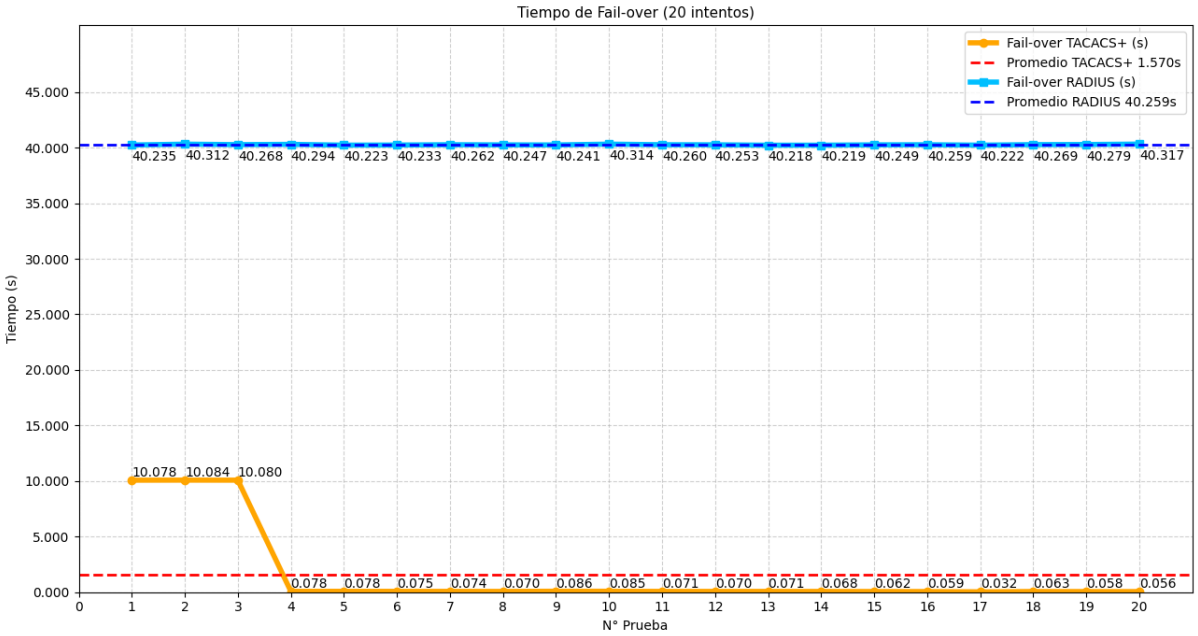
Nota. Elaboración propia.

Como se observa en la Figura 132, durante veinte 20 intentos consecutivos de conexión mediante RADIUS, el tiempo promedio requerido por el switch para detectar la falla y restablecer comunicación con el servidor disponible es de aproximadamente 40 segundos. Considerando todos los intentos de prueba, el tiempo promedio de fail-over con RADIUS es de 40.259 segundos.

Con TACACS+ el tiempo de detección y conmutación es de aproximadamente 10 segundos durante los tres 3 primeros intentos de conexión. A partir del cuarto intento, el switch establece contacto directo con el servidor disponible en menos de un segundo. Considerando todos los intentos de prueba, el tiempo promedio de fail-over con TACACS+ es de 1.57 segundos.

Figura 132.

Resultados de tiempo de fail-over para RADIUS y TACACS+.



Nota. Elaboración propia.

Los resultados evidencian que TACACS+ presenta un tiempo de fail-over significativamente menor que RADIUS. Esta diferencia se debe principalmente a que TACACS+ utiliza el protocolo de transporte TCP, que establece una conexión orientada y confiable. Por otro lado, RADIUS utiliza UDP, que carece de mecanismos de retransmisión y verificación del estado de enlace.

Considerando los resultados obtenidos, se demuestra que, desde la perspectiva de la disponibilidad, el protocolo TACACS+ ofrece una mayor tolerancia a fallos en la comunicación, al detectar la inactividad de un servidor AAA y conmutar hacia el servidor secundario en un tiempo considerablemente menor que RADIUS. De este modo, se da cumplimiento al tercer objetivo específico de la presente investigación.

4.2. Contrastación de Hipótesis

A partir de los resultados experimentales se acepta parcialmente la hipótesis general: “La comparación de los protocolos RADIUS y TACACS+ determinará que TACACS+ ofrece mejor desempeño, seguridad y disponibilidad en el acceso a la configuración de un switch”, debido a que los hallazgos demuestran que TACACS+ no supera a RADIUS en todos los

indicadores evaluados. En cuanto al desempeño, el protocolo RADIUS evidenció mayor eficiencia operacional. Sin embargo, en términos de seguridad y disponibilidad, TACACS+ sí superó a RADIUS.

La hipótesis específica: “La evaluación del tráfico de red que genera un usuario al solicitar y obtener acceso de forma centralizada a la configuración de un switch cuando se utilizan los protocolos RADIUS y TACACS+ determinará que el protocolo TACACS+ tiene mejor desempeño operacional” se rechaza, dado que las mediciones demostraron que el protocolo RADIUS genera menor número de paquetes, volumen de datos y latencia en la red al otorgar acceso a un usuario legítimo. El número de paquetes generados durante la autenticación y autorización para RADIUS fueron 2 paquetes y para TACACS+ fueron 22 paquetes. El tamaño total de datos transmitidos alcanzó 226 bytes para RADIUS y 1517 bytes para TACACS+. La latencia promedio desde la solicitud de conexión del usuario hasta su autorización fue de 0.137 segundos para RADIUS y de 0.169 segundos para TACACS+.

La hipótesis específica “La comparación del nivel de cifrado y granularidad que se puede lograr con RADIUS y TACACS+, establecerá que protocolo TACACS+ ofrecerá mayor nivel de seguridad” se confirma, ya que los resultados evidencian que el protocolo TACACS+ presenta un mayor porcentaje de cifrado en los paquetes de autenticación, autorización y auditoría. En TACACS+, los primeros paquetes Q: Authentication y R: Authentication registraron un 70.731% y 70.778% de cifrado del payload TCP. En el siguiente intercambio, los porcentajes fueron 53.846% y 33.333%. Para los paquetes Q: Authorization y R: Authorization, los niveles de cifrado alcanzaron el 80% y 60%, mientras que en Q: Accounting y R: Accounting los valores fueron 87.5% y 29.412%, incrementándose en el siguiente intercambio a 92.857% y 29.412%.

En contraste, en RADIUS, los paquetes Access-Request y Access-Accept presentaron solo un 26% y 0% de cifrado del payload UDP, y en Accounting-Request y Accounting-Response no se registró cifrado alguno. Además, TACACS+ demostró un mayor control granular de privilegios, al permitir denegar comandos específicos según el nivel asignado al usuario, característica no disponible en RADIUS. De los 42 comandos que un

usuario con nivel de privilegio 1 puede ejecutar en la CLI del switch, 40 fueron denegados con TACACS+, lo que equivale al 95.2% de comandos restringidos. En cambio, con RADIUS no fue posible denegar ninguno, manteniéndose en 0%.

Asimismo, TACACS+ generó 10 paquetes de auditoría con información detallada sobre el inicio y fin de sesión, así como los comandos ejecutados por el usuario, mientras que RADIUS solo registró el inicio y cierre de sesión, con 4 paquetes en total.

Finalmente, la hipótesis específica “El análisis del impacto sobre el acceso de un usuario debido a fallas en la comunicación entre el cliente y el servidor AAA al utilizar RADIUS y TACACS+, identificará a TACACS+ como el protocolo que garantiza mayor disponibilidad del servicio AAA” se acepta, dado que el tiempo promedio de conmutación (fail-over) de TACACS+ fue de 1.570 segundos, mientras que el de RADIUS fue de 40.259 segundos.

4.3. Discusión de Resultados

Los resultados obtenidos en esta investigación permiten establecer una discusión comparativa con los antecedentes revisados, evidenciando coincidencias, divergencias y aportes sustanciales al conocimiento sobre la evaluación y selección de los protocolos RADIUS y TACACS+ para el acceso centralizado a la configuración de switches.

El trabajo de Navarro (2020) se enfocó en el diseño de una infraestructura segura con TACACS+ bajo simulación, concluyendo la viabilidad técnica y económica del diseño propuesto. Sin embargo, su investigación no abordó comparativamente la eficiencia ni la disponibilidad frente a otros protocolos AAA. En contraste, la presente investigación trasciende el nivel de simulación al implementar los protocolos RADIUS y TACACS+ en un entorno real, validando su comportamiento operativo y seguridad mediante captura y análisis de tráfico.

El trabajo de Chinchay & Peña (2021) compara los protocolos RADIUS, TACACS+, DIAMETER y KERBEROS mediante una matriz de ponderación teórica, concluyendo que RADIUS es el protocolo más competente para la autenticación de usuarios. Sin embargo, su investigación se basó en un enfoque cualitativo y subjetivo, sin mediciones experimentales

de tráfico. Los resultados del presente estudio discrepan parcialmente con los resultados de estos autores, ya que RADIUS efectivamente presenta mejor desempeño operacional, pero TACACS+ supera a RADIUS en los indicadores de seguridad y disponibilidad, aspectos no evaluados en profundidad por Chinchay & Peña. Por tanto, esta investigación amplía y refina las conclusiones de estos autores, incorporando evidencia cuantitativa y experimental.

El trabajo de Ramos y Torres (2021) estudia la influencia del servidor RADIUS en el control de acceso a redes inalámbricas, concluyendo que su implementación mejora la autenticación, el control de acceso y la confidencialidad. Los resultados de su estudio coinciden con esta investigación en que RADIUS mantiene un rendimiento superior en la fase de autenticación. No obstante, las limitaciones en cuanto al nivel de seguridad y la disponibilidad que ofrece RADIUS no fueron analizadas por dichos autores. Este trabajo, por tanto, profundiza en los aspectos de seguridad y disponibilidad que Ramos y Torres no consideraron, evidenciando que la elección del protocolo AAA debe responder a los requisitos de seguridad y disponibilidad específicos de la infraestructura, más allá de la eficiencia en la autenticación.

El trabajo de Huamán et al. (2022) propone el uso de Cisco ISE con TACACS+ y RADIUS para la gestión centralizada de políticas de seguridad, recomendando su implementación por su capacidad de integración y control. Sin embargo, su estudio fue de tipo cualitativo y se basó en encuestas a expertos, sin validar empíricamente el comportamiento técnico de los protocolos. En cambio, la presente investigación valida experimentalmente las capacidades de ambos protocolos.

El trabajo de Andrade (2019) coincide con la presente investigación en que TACACS+ ofrece mejores ventajas en cuanto a seguridad, pero RADIUS es más optimo en la autenticación. Sin embargo, la comparación de estos protocolos no se obtiene a partir de resultados experimentales si no del análisis de información teórica. Por lo tanto, la presente investigación aporta una visión más precisa y equilibrada del comportamiento real de los protocolos RADIUS y TACACS+.

El trabajo de Pozo & Solís (2024) compara las tecnologías FreeRADIUS y Cisco ISE

utilizando una escala de Likert, concluyendo que Cisco ISE ofrece mayor seguridad, facilidad de uso e integración. Aunque su investigación valida la superioridad de Cisco ISE como plataforma AAA, no analiza directamente el comportamiento técnico de los protocolos RADIUS y TACACS+ que estas tecnologías implementan. En ese sentido, la presente investigación complementa sus hallazgos al demostrar con evidencia experimental que TACACS+ mantiene sus ventajas en seguridad y disponibilidad y RADIUS sus ventajas de desempeño, independientemente de la tecnología que se utilice.

Finalmente, el trabajo de Alimatov (2025) señala que TACACS+ proporciona mayor seguridad y granularidad, mientras que RADIUS destaca por su compatibilidad y ligereza. Los resultados de la presente investigación coinciden plenamente con su análisis, al evidenciar que TACACS+ logra un cifrado más robusto, un mejor control de privilegios y mayor tolerancia a fallos, mientras que RADIUS presenta un rendimiento más eficiente. No obstante, la presente investigación añade valor empírico al trabajo de Alimatov, al realizar pruebas de campo en un entorno de red real, y no únicamente un análisis técnico.

CONCLUSIONES

- Si bien el protocolo RADIUS presenta un mejor desempeño operativo, el protocolo TACACS+ ofrece mayores niveles de seguridad y disponibilidad en el acceso centralizado a la configuración de los switches, por lo que la elección del protocolo de debe responder al nivel de criticidad del entorno de red, siendo TACACS+ la opción más adecuada en escenarios donde la protección de las credenciales, el control de privilegios y la tolerancia a fallos son prioritarios.
- Al evaluar el tráfico de red generado durante el acceso centralizado a la configuración de un switch, se concluye que el protocolo RADIUS evidencia mejor desempeño operacional, al intercambiar un menor número de paquetes, menor volumen de datos y reducir el tiempo de respuesta promedio. Estos resultados demuestran que RADIUS presenta un mejor desempeño en términos de velocidad y consumo de recursos de red durante el proceso de autenticación y autorización de usuarios legítimos.
- Al comparar el nivel de cifrado y la granularidad del control de acceso, se concluye que el protocolo TACACS+ ofrece mayor nivel de seguridad al cifrar completamente el contenido de los paquetes de autenticación, autorización y auditoría, mientras que RADIUS únicamente cifra el campo de contraseña, exponiendo información sensible en texto plano. Asimismo, TACACS+ permite definir privilegios específicos para cada usuario y registrar en detalle las acciones ejecutadas durante la sesión, lo que mejora significativamente la trazabilidad y el cumplimiento de políticas de seguridad.
- El análisis del impacto de fallas en la comunicación entre el cliente y el servidor AAA evidencia que TACACS+ garantiza mayor disponibilidad del servicio, al presentar un tiempo de fail-over promedio significativamente menor que el de RADIUS gracias al uso del protocolo TCP que contribuye a una detección y recuperación más eficiente ante interrupciones en la comunicación, garantizando la continuidad del servicio AAA.

RECOMENDACIONES

- Dado que el protocolo TACACS+ demostró mayores niveles de seguridad y disponibilidad, se recomienda su implementación en infraestructuras críticas donde el control granular de privilegios, la trazabilidad de comandos y la protección de credenciales sean prioritarios, especialmente en dispositivos de red que administran tráfico sensible.
- Debido a su mayor eficiencia operativa y menor consumo de recursos, RADIUS puede mantenerse como protocolo de autenticación para servicios de red menos críticos, como conexiones Wi-Fi corporativas o VPN de usuarios, donde el rendimiento prime sobre la granularidad del control.
- Para mejorar la disponibilidad del servicio AAA, se recomienda implementar configuraciones de alta disponibilidad (HA) con servidores AAA redundantes y enlaces de respaldo, asegurando conmutación automática en caso de fallos.
- Se sugiere integrar el protocolo TACACS+ con servicios como Active Directory y herramientas de doble factor de autenticación para garantizar una gestión eficaz y segura del acceso a la CLI de un switch.
- Para futuras investigaciones, sería valioso comparar TACACS+ y RADIUS en distintos entornos de red (por ejemplo, firewalls, routers, controladores inalámbricos).

REFERENCIAS

Amazon Web Services. (2024). *¿Qué es el RTT en redes? Explicación del tiempo de ida y vuelta*. Retrieved from AWS: https://aws.amazon.com/es/what-is/rtt-in-networking/

Amazon Web Services. (2025). *¿Cuál es la diferencia entre HTTP y HTTPS?* Retrieved from AWS: https://aws.amazon.com/es/compare/the-difference-between-https-and-http/

Amazon Web Services. (2025). *¿Cuál es la diferencia entre LAN y WAN?* Retrieved from https://aws.amazon.com/es/compare/the-difference-between-lan-and-wan/

Cisco. (2011). *Configuring Authentication, Authorization, and Accounting*. Retrieved from Cisco Support: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/security/503_u2_2/Cisco_n3k_security_cg_503_u2_2_chapter3.html

Dahm, T., Ota, A., Gash, M., C., D., Carrel, D., & & Grant, L. (2020). *The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol.* IETF. Retrieved from IETF: https://datatracker.ietf.org/doc/html/rfc8907

Fortinet. (2024). *¿Qué es el control de acceso?* Retrieved from https://www.fortinet.com/lat/resources/cyberglossary/access-control

Fortinet. (2025). *¿Qué es la seguridad de autenticación, autorización y contabilidad (AAA)?* Retrieved from https://www.fortinet.com/lat/resources/cyberglossary/aaa-security

Fortinet. (2025). *Diferencia clave entre el modelo TCP/IP y OSI*. Retrieved from https://www.fortinet.com/lat/resources/cyberglossary/tcp-ip-model-vs-osi-model

FreeRADIUS. (2025). *¿Qué es FreeRADIUS?* Retrieved from https://www.freeradius.org/documentation/freeradius-server/3.2.9/concepts/freeradius.html

FS. (2022). *How to Log into a Network Switch: 3 Methods*. Retrieved from https://www.fs.com/eu-en/blog/three-approaches-to-log-in-to-your-network-switch-1256.html

García, F. (2025). *SSH: qué es y cómo funciona este protocolo*. Retrieved from Arsys:

http://arsys.es/blog/ssh#tree-2

Geeksforgeeks. (2025). *Differences between TCP and UDP*. Retrieved from https://www.geeksforgeeks.org/computer-networks/differences-between-tcp-and-udp/

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación.*

Huawei. (2025). *What Is RADIUS?* Retrieved from Info-Finder: https://info.support.huawei.com/info-finder/encyclopedia/en/RADIUS.html

Huawei Technologies. (2023). *What Is AAA?* Retrieved from https://info.support.huawei.com/info-finder/encyclopedia/en/AAA.html

Huber, M. (2025). *TACACS+ NG.* Retrieved from https://projects.pro-bono-publico.de/event-driven-servers/doc/tac_plus-ng.pdf?utm_source=chatgpt.com

IBM. (2021). *Protocolos a nivel de transporte de Internet*. Retrieved from https://www.ibm.com/docs/es/aix/7.1.0?topic=protocols-internet-transport-level

Jacobs, D. (2022). *Intro to encapsulation and decapsulation in networking*. Retrieved from https://www.techtarget.com/searchnetworking/tip/Intro-to-encapsulation-and-decapsulation-in-networking

Juniper Networks. (2025). *User Access and Authentication Administration Guide for Junos OS*. Retrieved from Juniper: https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/topic-map/junos-os-user-authentication-overview.html

Kaspersky. (2025). *¿Qué es el cifrado de datos? Definición y explicación*. Retrieved from https://latam.kaspersky.com/resource-center/definitions/encryption

Linares, K. (2017). *Componentes de la red - CCNA V6.0*. Retrieved from https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-LAN-WAN-e-Internet-Componentes-de-la-red.html

Lowe, D. (2005). *Networking All-in-One Desk Reference For Dummies.* Wiley Publishing, Inc.

Microsoft. (2024). *Tutorial: SSH en Windows Terminal*. Retrieved from Microsoft Learn: https://learn.microsoft.com/es-es/windows/terminal/tutorials/ssh

Mikac, E. (2024). *Network Device Management Access Methods to Know for CCNA*. Retrieved from https://www.cbtnuggets.com/blog/technology/networking/network-device-management-access-methods-to-know-for-ccna?utm_source=chatgpt.com

Palo Alto Networks. (2025). *¿Qué es el principio del mínimo privilegio?* Retrieved from https://www.paloaltonetworks.es/cyberpedia/what-is-the-principle-of-least-privilege

Postel, J., & Reynolds, J. (2013). *Telnet Protocol Specification.* RFC 854, IETF. Retrieved from https://datatracker.ietf.org/doc/rfc854/

Rigney, C. (2000). *RADIUS Accounting.* IETF. Retrieved from IETF: https://datatracker.ietf.org/doc/html/rfc2866

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2000). *Remote Authentication Dial In User Service (RADIUS).* IETF. Retrieved from IETF: https://datatracker.ietf.org/doc/html/rfc2865

Wireshark. (2025). *What is Wireshark?* Retrieved from Wireshark: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs

Ylonen, T., & Lonvick, C. (2015). *The Secure Shell (SSH) Protocol Architecture.* IETF. Retrieved from https://datatracker.ietf.org/doc/rfc4251/

ANEXOS

ANEXO A: Matriz de Consistencia.

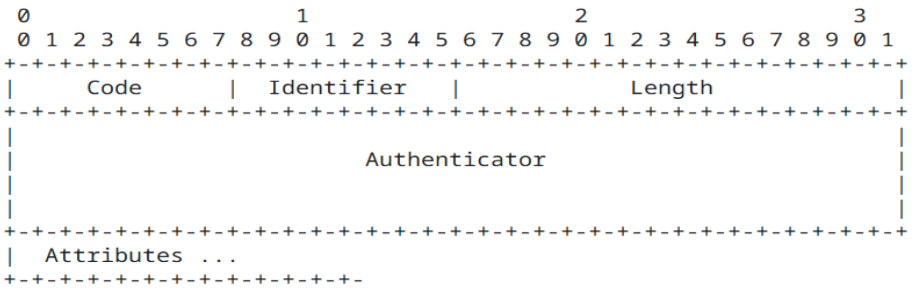
Título	Análisis Comparativo de los Protocolos RADIUS y TACACS+ en el Control de Acceso Centralizado a la Configuración de Switches.			
PROBLEMAS	**OBJETIVOS**	**HIPÓTESIS**	**VARIABLES**	**METODOLOGÍA**
Problema general: ¿Cuál protocolo proporciona mejor desempeño, seguridad y disponibilidad en el control de acceso centralizado a la configuración de un switch entre RADIUS y TACACS+?	**Objetivo general:** Comparar los protocolos RADIUS y TACACS+, para determinar cuál ofrece mejor desempeño, seguridad y disponibilidad en el acceso de forma centralizada a la configuración de un switch.	**Hipótesis general:** La comparación de los protocolos RADIUS y TACACS+, determinará que TACACS+ ofrece mejor desempeño, seguridad y disponibilidad en el acceso a la configuración de un switch.		**Tipo de investigación:** Aplicada **Enfoque:** Cuantitativo **Nivel de Investigación:** Descriptivo **Diseño:** Cuasi-experimental
Problemas específicos: a) ¿Cómo difiere el tráfico de red que genera un usuario al solicitar y obtener acceso de forma centralizada a la configuración de un switch cuando se utilizan los protocolos RADIUS y TACACS+? a) ¿Qué nivel de cifrado de datos y granularidad se puede lograr con RADIUS y TACACS+ durante los procesos de autenticación, autorización y auditoría? c) ¿Cuál es el impacto sobre el acceso de un usuario debido a fallas en la comunicación entre el cliente y el servidor AAA al utilizar RADIUS y TACACS+?	**Objetivos específicos:** a) Evaluar el tráfico de red que genera un usuario al solicitar y obtener acceso de forma centralizada a la configuración de un switch cuando se utilizan los protocolos RADIUS y TACACS+, para determinar el protocolo que tiene mejor desempeño operacional. b) Comparar el nivel de cifrado y granularidad que se puede lograr con RADIUS y TACACS+ durante los procesos de autenticación, autorización y auditoría, para establecer el protocolo que ofrece mayor nivel de seguridad. c) Analizar el impacto sobre el acceso de un usuario debido a fallas en la comunicación entre el cliente y el servidor AAA al utilizar RADIUS y TACACS+, para identificar el protocolo que garantiza mayor disponibilidad del servicio AAA.	**Hipótesis específicas:** a) La evaluación del tráfico de red que genera un usuario al solicitar y obtener acceso de forma centralizada a la configuración de un switch cuanto se utilizan los protocolos RADIUS determinará que el protocolo TACACS+ que tiene mejor desempeño operacional. b) La comparación del nivel de cifrado y granularidad que se puede lograr con RADIUS y TACACS+, establecerá que protocolo TACACS+ ofrecerá mayor nivel de seguridad. c) El análisis del impacto sobre el acceso de un usuario debido a fallas en la comunicación entre el cliente y el servidor AAA al utilizar RADIUS y TACACS+, identificará a TACACS+ como el protocolo que garantiza mayor disponibilidad del servicio AAA.	**Variable independiente:** Protocolo AAA **Variable dependiente:** • Desempeño • Seguridad • Disponibilidad	**Técnicas e instrumentos de recolección de datos:** Técnica experimental. **Técnicas e instrumentos de análisis y procesamiento de datos:** Comparación de métricas asociadas al desempeño, seguridad y disponibilidad de los protocolos AAA.

ANEXO B: Especificaciones del Protocolo RADIUS

B.1. Formato del Paquete de Autenticación y Autorización RADIUS

El paquete autenticación y autorización RADIUS se encapsula en el campo de datos UDP, donde el campo puerto de destino UDP indica 1812.

Formato del paquete RADIUS para la autenticación y autorización.



Nota. Adaptado de “Remote Authentication Dial In User Service (RADIUS)”, por C. Rigney, S. Willens, A. Rubens, & W. Simpson, 2000, IETF (https://datatracker.ietf.org/doc/html/rfc2865).

Se detallan los campos que conforman el paquete RADIUS, los cuales permiten identificar y controlar el intercambio de mensajes entre el cliente y el servidor durante la autenticación y autorización.

Campos del paquete RADIUS.

Campo	Descripción	Valor
Code	Identifica el tipo de paquete RADIUS que se está enviando o recibiendo.	Access-Request := 0x01 Access-Accept := 0x02 Access-Reject := 0x03 Access-Challenge := 0x0B Reservado := 0xFF
Identifier	ID del paquete que facilita la correspondencia entre solicitudes y respuestas.	0x00 … 0xFF
Length	Indica la longitud total del paquete RADIUS.	0x0014 ... 0x1000
Authenticator	Campo de verificación criptográfica.	Access-Request := 16 bytes aleatorios Access-Accept/Reject/Chalenge := Valor MD5 calculado sobre el contenido del paquete y el shared secret.
Attributes	Tiene una longitud variable y contienen datos específicos de autenticación, autorización o configuración entre el cliente y el servidor RADIUS.	Cada atributo dentro de este campo incluye los campos type, length y value.

Nota. Elaboración propia.

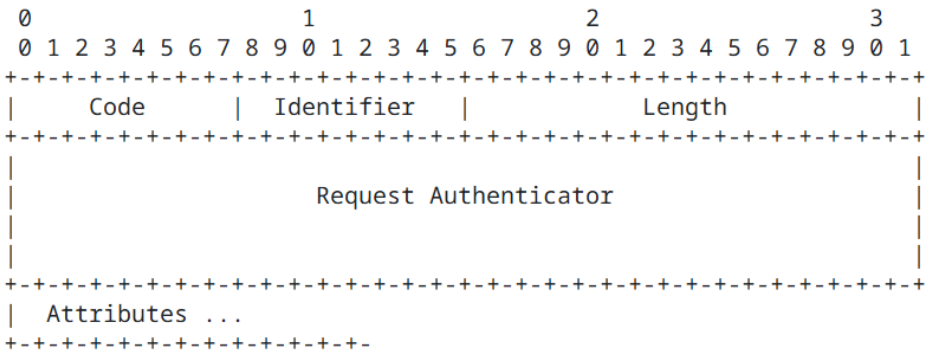
B.2. Tipos de Paquetes de Autenticación y Autorización RADIUS

El tipo de paquete RADIUS para la autenticación y autorización está determinado por el campo Code en el primer octeto del paquete.

B.2.1. Paquete Access-Request

Los paquetes Access-Request se envían a un servidor RADIUS y transmiten información utilizada para determinar si a un usuario se le permite el acceso a un NAS específico y cualquier servicio especial solicitado para el usuario.

Formato del paquete Access-Request.



Nota. Adaptado de “Remote Authentication Dial In User Service (RADIUS)”, por C. Rigney, S. Willens, A. Rubens, & W. Simpson, 2000, IETF (https://datatracker.ietf.org/doc/html/rfc2865).

Se presentan los campos que conforman el paquete Access-Request del protocolo RADIUS.

Campos del paquete Access-Request.

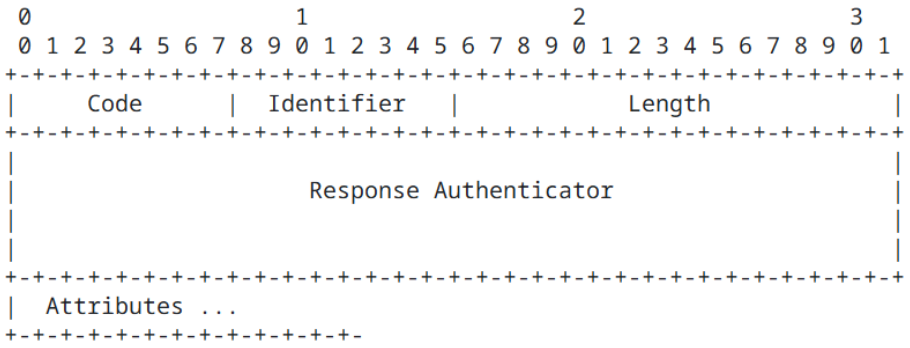
Campo	Descripción	Valor
Code	Identifica el tipo de paquete Access-Request.	0x01
Identifier	ID del paquete. Debe cambiarse siempre que cambie el contenido del campo Attributes y siempre que se haya recibido una respuesta válida para una solicitud anterior. Para las retransmisiones, este campo debe permanecer sin cambios.	0x00 … 0xFF
Length	Indica la longitud total del paquete Access-Request	0x0014 ... 0x1000
Request Authenticator	Campo de verificación criptográfica.	16 bytes aleatorios
Attributes	Tiene longitud variable y contiene la lista de atributos que son requeridos para el tipo de servicio, así como cualquier atributo opcional que se desee incluir.	Cada atributo dentro de este campo incluye los campos type, length y value.

Nota. Elaboración propia.

B.2.2. Paquete Access-Accept

Los paquetes Access-Accept son enviados por el servidor RADIUS y proporcionan información de configuración específica necesaria para comenzar la prestación del servicio al usuario.

Formato del paquete Access-Accept.



Nota. Adaptado de “Remote Authentication Dial In User Service (RADIUS)”, por C. Rigney, S. Willens, A. Rubens, & W. Simpson, 2000, IETF (https://datatracker.ietf.org/doc/html/rfc2865).

Se detallan los campos que conforman el paquete Access-Accept del protocolo RADIUS.

Campos del paquete Access-Accept.

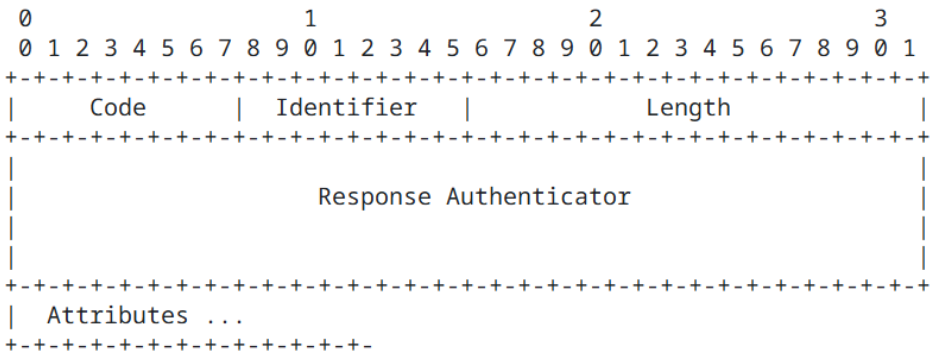
Campo	Descripción	Valor
Code	Identifica el tipo de paquete Access-Accept.	0x02
Identifier	ID del paquete. Coincide con el valor del campo Identifier en el paquete Access-Request que originó el paquete Access-Accept.	0x00 … 0xFF
Length	Indica la longitud total del paquete Access-Accept.	0x0014 ... 0x1000
Response Authenticator	Campo de verificación criptográfica.	Valor MD5 calculado sobre el contenido del paquete Access-Accept y el shared secret.
Attributes	Tiene una longitud variable y contiene una lista de cero o más atributos.	Cada atributo dentro de este campo incluye los campos type, length y value.

Nota. Elaboración propia.

B.2.3. Paquete Access-Reject

Si algún valor de los Atributos recibidos no es aceptable, el servidor RADIUS debe transmitir un paquete Access-Reject. Este puede incluir un mensaje de texto que el NAS puede mostrar al usuario.

. *Formato del paquete Access-Reject.*



Nota. Adaptado de “Remote Authentication Dial In User Service (RADIUS)”, por C. Rigney, S. Willens, A. Rubens, & W. Simpson, 2000, IETF (https://datatracker.ietf.org/doc/html/rfc2865).

Se presentan los campos que conforman el paquete Access-Reject del protocolo RADIUS.

Campos del paquete Access-Reject.

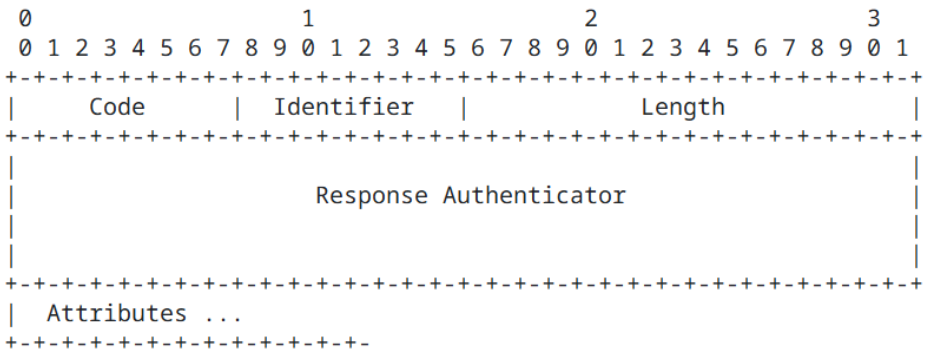
Campo	Descripción	Valor
Code	Identifica el tipo de paquete Access-Reject.	0x03
Identifier	ID del paquete. Coincide con el valor del campo Identifier en el paquete Access-Request que originó el paquete Access-Reject.	0x00 … 0xFF
Length	Indica la longitud total del paquete Access-Reject.	0x0014 ... 0x1000
Response Authenticator	Campo de verificación criptográfica.	Valor MD5 calculado sobre el contenido del paquete Access-Reject y el shared secret.
Attributes	Tiene una longitud variable y contiene una lista de cero o más atributos.	Cada atributo dentro de este campo incluye los campos type, length y value.

Nota. Elaboración propia.

B.2.4. Paquete Access-Challenge

Si el servidor RADIUS desea enviar al usuario un desafío que requiere una respuesta, entonces el servidor RADIUS debe responder a la Access-Request transmitiendo un paquete Access-Challenge.

Formato del paquete Access-Challenge.



Nota. Adaptado de “Remote Authentication Dial In User Service (RADIUS)”, por C. Rigney, S. Willens, A. Rubens, & W. Simpson, 2000, IETF (https://datatracker.ietf.org/doc/html/rfc2865).

Se especifican los campos que conforman el paquete Access-Challenge del protocolo RADIUS.

Campos del paquete Access-Challenge.

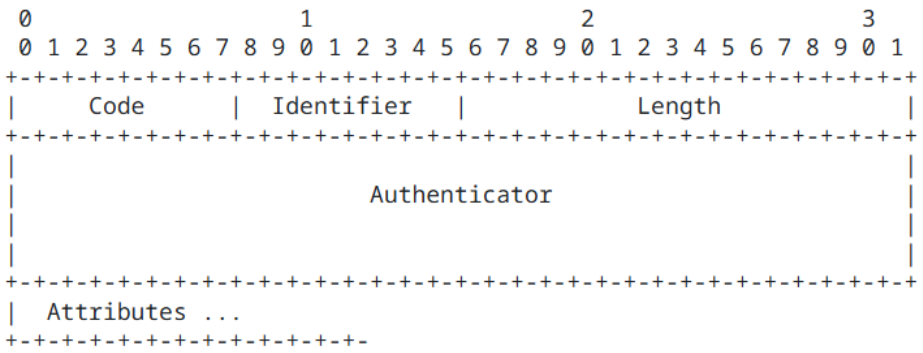
Campo	Descripción	Valor
Code	Identifica el tipo de paquete Access-Challenge.	0x0B
Identifier	ID del paquete. Coincide con el valor del campo Identifier en el paquete Access-Request que originó el paquete Access-Challenge.	0x00 … 0xFF
Length	Indica la longitud total del paquete Access-Challenge.	0x0014 ... 0x1000
Response Authenticator	Campo de verificación criptográfica.	Valor MD5 calculado sobre el contenido del paquete Access-Challenge y el shared secret.
Attributes	Tiene una longitud variable y contiene una lista de cero o más atributos.	Cada atributo dentro de este campo incluye los campos type, length y value.

Nota. Elaboración propia.

B.3. Formato del Paquete de Auditoría RADIUS

El paquete de auditoría RADIUS se encapsula en el campo de datos UDP, donde el campo puerto de destino UDP indica 1813.

Formato del paquete RADIUS para la auditoría.



Nota. Adaptado de “Remote Authentication Dial In User Service (RADIUS)”, por C. Rigney, 2000, IETF (https://datatracker.ietf.org/doc/html/rfc2866).

Se detallan los campos que conforman el paquete RADIUS, los cuales permiten identificar y controlar el intercambio de mensajes entre el cliente y el servidor durante la auditoría.

Campos del paquete RADIUS para la auditoría.

Campo	Descripción	Valor
Code	Identifica el tipo de paquete RADIUS que se está enviando o recibiendo.	Accounting-Request := 0x04 Accounting-Response := 0x05 Reservado := 0xFF
Identifier	ID del paquete que facilita la correspondencia entre solicitudes y respuestas.	0x00 … 0xFF
Length	Indica la longitud total del paquete RADIUS.	0x0014 ... 0x1000
Authenticator	Campo de verificación criptográfica.	Accounting-Request/Response := Valor MD5 calculado sobre el contenido del paquete y el shared secret.
Attributes	Tiene una longitud variable y contiene los detalles específicos de auditoría, información y configuración para la solicitud y la respuesta.	Cada atributo dentro de este campo incluye los campos type, length y value.

Nota. Elaboración propia.

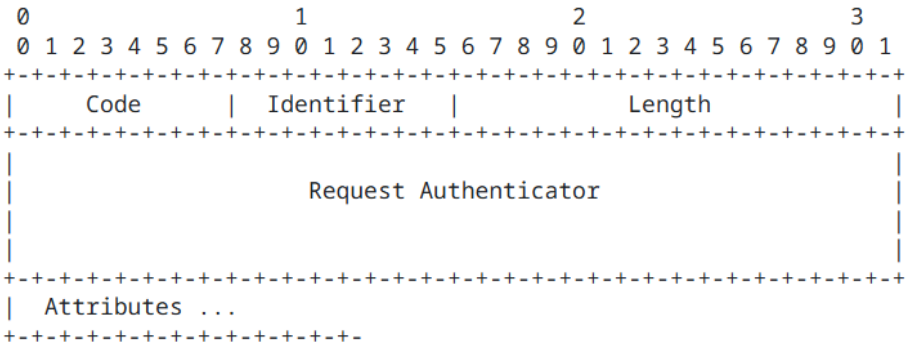
B.4. Tipos de Paquetes de Auditoría RADIUS

El tipo de paquete RADIUS para la auditoría está determinado por el campo Code en el primer octeto del paquete.

B.4.1. Accounting-Request

Los paquetes Accounting-Request se envían desde un cliente (normalmente un NAS o su proxy) a un servidor de auditoría RADIUS, y transmiten información para auditoría de un servicio prestado a un usuario.

Formato del paquete Accounting-Request.



Nota. Adaptado de “Remote Authentication Dial In User Service (RADIUS)”, por C. Rigney, 2000, IETF (https://datatracker.ietf.org/doc/html/rfc2866).

Se especifican los campos que conforman el paquete Accounting-Request del protocolo RADIUS.

Campos del paquete Accounting-Request.

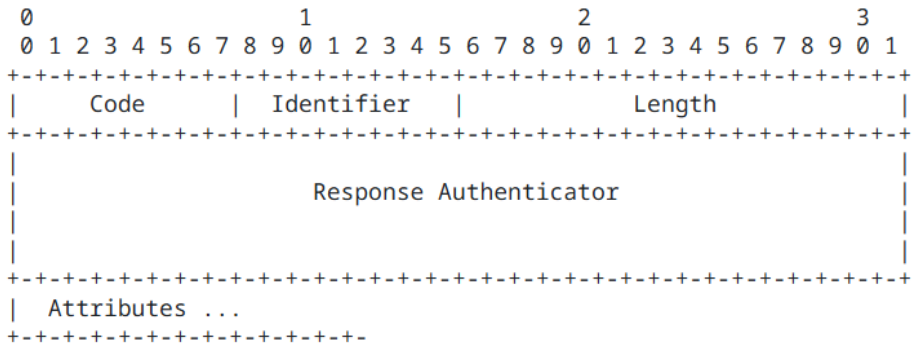
Campo	Descripción	Valor
Code	Identifica el tipo de paquete Accounting-Request.	0x04
Identifier	ID del paquete. Debe cambiarse siempre que cambie el contenido del campo Attributes y siempre que se haya recibido una respuesta válida para una solicitud anterior. Para las retransmisiones, este campo debe permanecer sin cambios.	0x00 … 0xFF
Length	Indica la longitud total del paquete RADIUS.	0x0014 ... 0x1000
Response Authenticator	Campo de verificación criptográfica.	Valor MD5 calculado sobre el contenido del paquete y el shared secret.
Attributes	Tiene una longitud variable y contiene una lista de atributos.	Cada atributo dentro de este campo incluye los campos type, length y value.

Nota. Elaboración propia.

B.4.2. Accounting-Response

El servidor de contabilidad RADIUS envía paquetes Accounting-Response al cliente para confirmar que la Accounting-Request se recibió y registró correctamente.

Formato del paquete Accounting-Response.



Nota. Adaptado de “Remote Authentication Dial In User Service (RADIUS)”, por C. Rigney, 2000, IETF (https://datatracker.ietf.org/doc/html/rfc2866).

Se detallan los campos que conforman el paquete Accounting-Response del protocolo RADIUS.

Campos del paquete Accounting-Response.

Campo	Descripción	Valor
Code	Identifica el tipo de paquete Accounting-Response.	0x05
Identifier	ID del paquete. Coincide con el valor del campo Identifier en el paquete Accounting-Request que originó el paquete Accounting-Response.	0x00 … 0xFF
Length	Indica la longitud total del paquete RADIUS.	0x0014 ... 0x1000
Response Authenticator	Campo de verificación criptográfica.	Valor MD5 calculado sobre el contenido del paquete y el shared secret.
Attributes	Tiene una longitud variable y contiene una lista de cero o más atributos.	Cada atributo dentro de este campo incluye los campos type, length y value.

Nota. Elaboración propia.

B.5. Proceso de Autenticación y Autorización RADIUS

Cuando un cliente está configurado para utilizar RADIUS, cualquier usuario del cliente presenta información de autenticación ante este. Esto puede realizarse mediante un mensaje de inicio de sesión personalizable, donde se espera que el usuario ingrese su nombre de usuario y contraseña. Alternativamente, el usuario podría emplear un protocolo de enlace de nivel de enlace, como el Protocolo Punto a Punto (PPP), que incluye paquetes de autenticación que transportan esta información.

Una vez que el cliente ha obtenido dicha información, puede optar por autenticarse

utilizando RADIUS. Para hacerlo, el cliente crea un paquete Access-Request que contiene atributos tales como el nombre del usuario, la contraseña del usuario, el identificador del cliente (Client ID) y el identificador del puerto (Port ID) al que el usuario está accediendo. Cuando se incluye una contraseña, esta se oculta utilizando un método basado en el algoritmo de resumen de mensaje RSA MD5.

El paquete Access-Request se envía al servidor RADIUS a través de la red. Si no se recibe respuesta dentro de un período determinado, la solicitud se reenvía varias veces. El cliente también puede reenviar las solicitudes a uno o más servidores alternos en caso de que el servidor principal no esté disponible o sea inaccesible. Un servidor alterno puede usarse después de varios intentos fallidos con el servidor principal, o mediante un mecanismo de rotación (round-robin).

Una vez que el servidor RADIUS recibe la solicitud, valida al cliente que la envía. Cualquier solicitud proveniente de un cliente para el cual el servidor RADIUS no tenga una clave compartida (shared secret) debe ser descartada silenciosamente. Si el cliente es válido, el servidor RADIUS consulta una base de datos de usuarios para encontrar al usuario cuyo nombre coincida con el de la solicitud. La entrada del usuario en la base de datos contiene una lista de requisitos que deben cumplirse para permitir el acceso. Esto siempre incluye la verificación de la contraseña, pero también puede especificar los clientes o puertos a los que el usuario tiene permitido acceder.

El servidor RADIUS puede realizar solicitudes a otros servidores para satisfacer la autenticación, actuando en ese caso como cliente.

Si algún atributo Proxy-State está presente en el paquete Access-Request, debe ser copiado sin modificaciones y en el mismo orden dentro del paquete de respuesta. Otros atributos pueden colocarse antes, después o incluso entre los atributos Proxy-State.

Si alguna condición no se cumple, el servidor RADIUS envía una respuesta Access-Reject, indicando que la solicitud del usuario es inválida. Si se desea, el servidor puede incluir un mensaje de texto dentro del Access-Reject, el cual puede ser mostrado por el cliente al usuario.

No se permite incluir otros atributos (excepto Proxy-State) en un Access-Reject.

Si todas las condiciones se cumplen y el servidor RADIUS desea emitir un desafío al usuario, el servidor envía una respuesta Access-Challenge. Esta puede incluir un mensaje de texto para que el cliente lo muestre al usuario, solicitando una respuesta al desafío, y puede incluir además un atributo State.

Si el cliente recibe un Access-Challenge y admite el mecanismo de desafío/respuesta, puede mostrar el mensaje de texto (si existe) al usuario y solicitar su respuesta. Luego, el cliente reenvía su Access-Request original, con un nuevo identificador de solicitud (Request ID), reemplazando el atributo User-Password por la respuesta (cifrada) e incluyendo el atributo State recibido en el Access-Challenge (si corresponde). Solo debe haber cero o una instancia del atributo State en una solicitud. El servidor puede responder a este nuevo Access-Request con un Access-Accept, Access-Reject o con otro Access-Challenge.

Si todas las condiciones se cumplen, la lista de valores de configuración para el usuario se coloca en una respuesta Access-Accept. Estos valores incluyen el tipo de servicio (por ejemplo: SLIP, PPP o Login User) y todos los parámetros necesarios para proveer el servicio deseado. Para SLIP y PPP, esto puede incluir valores como dirección IP, máscara de subred, MTU, compresión deseada e identificadores de filtro de paquetes. Para usuarios en modo carácter, puede incluir valores como el protocolo y el host deseado.

B.6. Proceso de Auditoría RADIUS

Cuando un cliente está configurado para utilizar RADIUS Accounting, al inicio de la prestación del servicio generará un paquete Accounting-Start que describe el tipo de servicio que se está proporcionando y el usuario al que se le entrega. Luego, enviará dicho paquete al servidor de auditoría RADIUS, el cual responderá con un acuse de recibo indicando que el paquete ha sido recibido. Al finalizar la prestación del servicio, el cliente generará un paquete Accounting-Stop que describe el tipo de servicio que fue entregado y, de manera opcional, incluirá estadísticas como el tiempo transcurrido, los octetos de entrada y salida, o los paquetes de entrada y salida. Este paquete será enviado al servidor de auditoría RADIUS,

que también responderá con un acuse de recibo indicando que el paquete ha sido recibido.

El Accounting-Request (ya sea de inicio o de fin) se envía al servidor de auditoría RADIUS a través de la red. Se recomienda que el cliente continúe intentando enviar el paquete Accounting-Request hasta recibir un acuse de recibo, utilizando algún tipo de mecanismo de reintento progresivo (backoff). Si no se recibe respuesta dentro de un período de tiempo determinado, la solicitud se retransmite varias veces. El cliente también puede reenviar las solicitudes a uno o más servidores alternativos en caso de que el servidor principal esté inactivo o no sea accesible. Un servidor alternativo puede utilizarse después de varios intentos fallidos al servidor principal o de manera rotativa (round-robin).

El servidor de auditoría RADIUS puede realizar solicitudes a otros servidores para satisfacer la petición, en cuyo caso actúa como cliente.

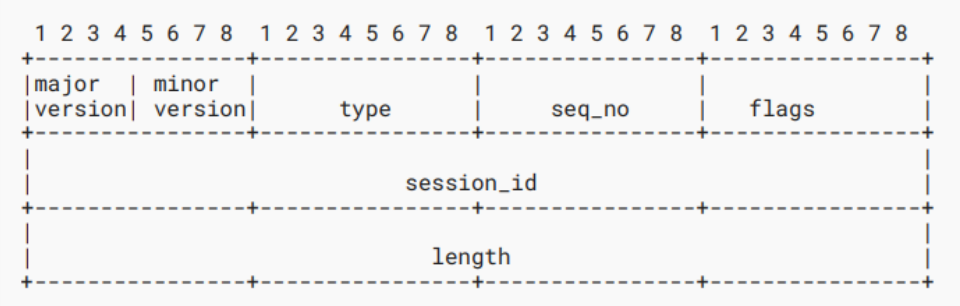
Si el servidor de auditoría RADIUS no puede registrar correctamente el paquete de auditoría, no debe enviar una respuesta de acuse de recibo Accounting-Response al cliente.

ANEXO C: Especificaciones del Protocolo TACACS+

C.1. Encabezado del Paquete TACACS+

El paquete TACACS+ comienzan con un encabezado de 12-bytes que incluye varios campos. La imagen ilustra la estructura del encabezado. Se puede observar la disposición y el tamaño de tiene cada campo en el paquete.

Encabezado del paquete TACACS+.



Nota. Adaptado de “The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol”, por T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, & L. Grant, 2020, IETF (https://datatracker.ietf.org/doc/html/rfc8907).

En adición, se proporciona una descripción detallada de cada uno de estos campos, explicando su función y valor específico.

Campos del encabezado del paquete TACACS+.

Campo	Descripción	Valor
major version	Número de versión mayor de TACACS+.	TAC_PLUS_MAJOR_VER:= 0x0C
minor version	Número de versión menor de TACACS+.	TAC_PLUS_MINOR_VER_DEFAULT:= 0x00 TAC_PLUS_MINOR_VER_ONE := 0x01
type	Tipo de paquete.	TAC_PLUS_AUTHEN:= 0x01 TAC_PLUS_AUTHOR:= 0x02 TAC_PLUS_ACCT:= 0x03
seq_no	Número de secuencia actual del paquete.	0x01 ... 0xFF
flags	Banderas que indican si el cuerpo del paquete está cifrado o si la conexión entre el cliente y un servidor es "Modo de conexión única".	TAC_PLUS_ENCRYPTED_FLAG:= 0x00 TAC_PLUS_UNENCRYPTED_FLAG:= 0x01 TAC_PLUS_SINGLE_CONNECT_FLAG:= 0x04
session_id	ID de la sesión TACACS+. Es un número aleatorio y no cambia durante la sesión.	0x00000001 … 0xFFFFFFFF
length	Longitud total del cuerpo del paquete, en bytes.	0x00000001 … 0xFFFFFFFF

Nota. Elaboración propia.

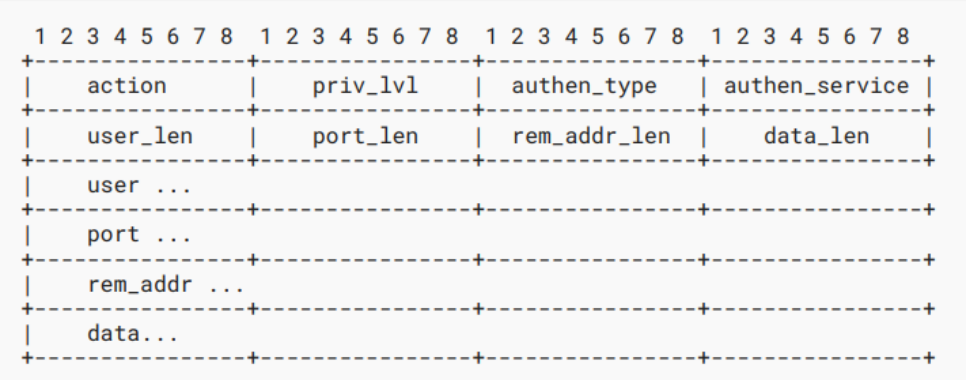
C.2. Cuerpo del Paquete TACACS+

El cuerpo del paquete TACACS+ contiene datos específicos para cada tipo de paquete, cuya naturaleza se define en el encabezado del paquete. Estos datos pueden incluir información sobre la autenticación, autorización o auditoría según el tipo de solicitud realizada. La estructura y contenido del cuerpo del paquete varían dependiendo del tipo de operación que se está llevando a cabo en el protocolo TACACS+.

C.2.1. Cuerpo del Paquete de Autenticación START

El proceso de autenticación comienza con el paquete START, que inicia la comunicación entre el cliente y el servidor. Este paquete contiene información clave que es utilizada para establecer la identidad del usuario. La imagen muestra la estructura del cuerpo del paquete START, destacando los campos relevantes para iniciar el proceso de autenticación.

Cuerpo del paquete START en la autenticación TACACS+.



Nota. Adaptado de “The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol”, por T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, & L. Grant, 2020, IETF (https://datatracker.ietf.org/doc/html/rfc8907)

Se detalla los campos presentes en el cuerpo del paquete START durante la autenticación TACACS+, proporcionando la función y valor de cada uno.

Campos en el cuerpo del paquete START en la autenticación TACACS+.

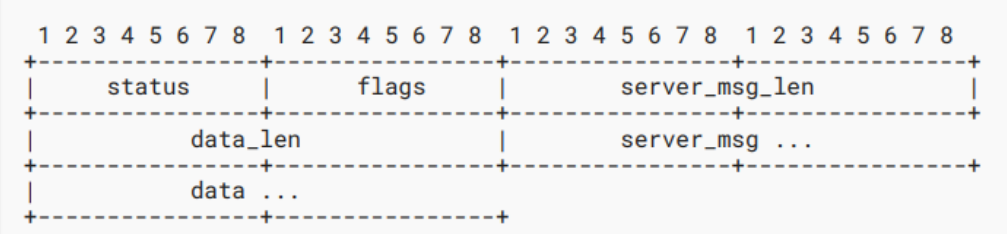
Campo	Descripción	Valor
action	Acción de la autenticación.	TAC_PLUS_AUTHEN_LOGIN := 0x01 TAC_PLUS_AUTHEN_CHPASS := 0x02 TAC_PLUS_AUTHEN_SENDAUTH := 0x04
priv_lvl	Nivel de privilegio con el que se autentica el usuario.	TAC_PLUS_PRIV_LVL_MIN := 0x00 TAC_PLUS_PRIV_LVL_USER := 0x01 TAC_PLUS_PRIV_LVL_ROOT := 0x0F TAC_PLUS_PRIV_LVL_MAX := 0x0F
authen_type	Tipo de autenticación.	TAC_PLUS_AUTHEN_TYPE_ASCII := 0x01 TAC_PLUS_AUTHEN_TYPE_PAP := 0x02 TAC_PLUS_AUTHEN_TYPE_CHAP := 0x03 TAC_PLUS_AUTHEN_TYPE_MSCHAP := 0x05 TAC_PLUS_AUTHEN_TYPE_MSCHAPV2 := 0x06
authen_service	Servicio que está solicitando la autenticación.	TAC_PLUS_AUTHEN_SVC_NONE := 0x00 TAC_PLUS_AUTHEN_SVC_LOGIN := 0x01 TAC_PLUS_AUTHEN_SVC_ENABLE := 0x02 TAC_PLUS_AUTHEN_SVC_PPP := 0x03 TAC_PLUS_AUTHEN_SVC_PT := 0x05 TAC_PLUS_AUTHEN_SVC_RCMD := 0x06 TAC_PLUS_AUTHEN_SVC_X25 := 0x07 TAC_PLUS_AUTHEN_SVC_NASI := 0x08 TAC_PLUS_AUTHEN_SVC_FWPROXY := 0x09
user_len	Longitud, en bytes, del campo “user”.	0x00 … 0xFF
port_len	Longitud, en bytes, del campo “port”.	0x00 … 0xFF
rem_addr_len	Longitud, en bytes, del campo “rem_add”.	0x00 … 0xFF
data_len	Longitud, en bytes, del campo “data”.	0x00 … 0xFF
user	Nombre de usuario (opcional).	Cadena de caracteres ASCII en hexadecimal (máx. 4 bytes)
port	Nombre del puerto del cliente con el que se realiza la autenticación.	Cadena de caracteres ASCII en hexadecimal (máx. 4 bytes)
rem_addr	Cadena que indica la dirección IP desde la que el usuario se ha conectado al cliente.	Cadena de caracteres ASCII en hexadecimal (máx. 4 bytes)
data	Datos que forman parte del intercambio de autenticación.	Cadena de caracteres ASCII en hexadecimal (máx. 4 bytes)

Nota. Elaboración propia.

C.2.2. Cuerpo del Paquete de Autenticación REPLY

El servidor TACACS+ envía solo un único paquete de autenticación, un paquete REPLY, que contiene la respuesta del servidor a una solicitud de autenticación del cliente, incluyendo datos que pueden afectar la autorización y el acceso del usuario. La imagen muestra la estructura del cuerpo del paquete REPLY en el protocolo TACACS+. Para una descripción detallada del cuerpo, se proporciona una lista completa de los campos presentes.

Cuerpo del paquete REPLY en la autenticación TACACS+.



Nota. Adaptado de "The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol", por T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, & L. Grant, 2020, IETF (https://datatracker.ietf.org/doc/html/rfc8907).

A continuación, se presenta una descripción detallada de los campos que se encuentran en el cuerpo del paquete.

Campos en el cuerpo del paquete REPLY en la autenticación TACACS+.

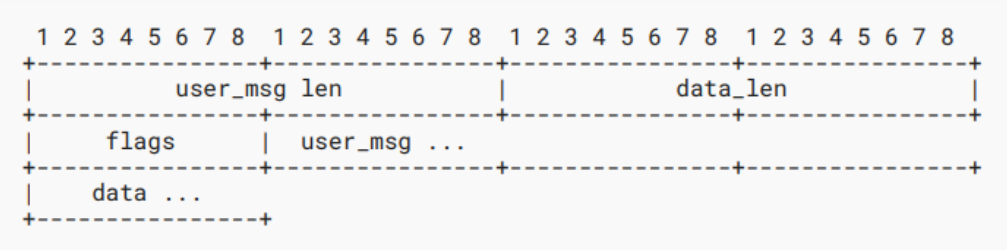
Campo	Descripción	Valor
status	Estado actual de la autenticación.	TAC_PLUS_AUTHEN_STATUS_PASS := 0x01 TAC_PLUS_AUTHEN_STATUS_FAIL := 0x02 TAC_PLUS_AUTHEN_STATUS_GETDATA := 0x03 TAC_PLUS_AUTHEN_STATUS_GETUSER := 0x04 TAC_PLUS_AUTHEN_STATUS_GETPASS := 0x05 TAC_PLUS_AUTHEN_STATUS_RESTART := 0x06 TAC_PLUS_AUTHEN_STATUS_ERROR := 0x07 TAC_PLUS_AUTHEN_STATUS_FOLLOW := 0x21
flags	Banderas en mapa de bits que modifican la acción a realizar.	TAC_PLUS_REPLY_FLAG_NOECHO := 0x01
server_msg_len	Longitud, en bytes, del campo "server_msg".	0x0000 … 0xFFFF
data_len	Longitud, en bytes, del campo "data".	0x0000 … 0xFFFF
server_msg	Mensaje que se muestra al usuario (opcional).	Cadena de caracteres ASCII en hexadecimal (máx. 2 bytes)
data	Datos que forman parte del intercambio de autenticación.	Cadena de caracteres ASCII en hexadecimal (máx. 2 bytes)

Nota. Elaboración propia.

C.2.3. Cuerpo del Paquete de Autenticación CONTINUE

El paquete CONTINUE es utilizado para enviar información adicional requerida para completar el proceso de autenticación. La imagen presenta la estructura detallada del cuerpo del paquete CONTINUE.

Cuerpo del paquete CONTINUE en la autenticación TACACS+.



Nota. Adaptado de “The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol”, por T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, & L. Grant, 2020, IETF (https://datatracker.ietf.org/doc/html/rfc8907).

Se proporciona una descripción detallada de los campos que se encuentran en el cuerpo del paquete.

Campos en el cuerpo del paquete CONTINUE en la autenticación TACACS+.

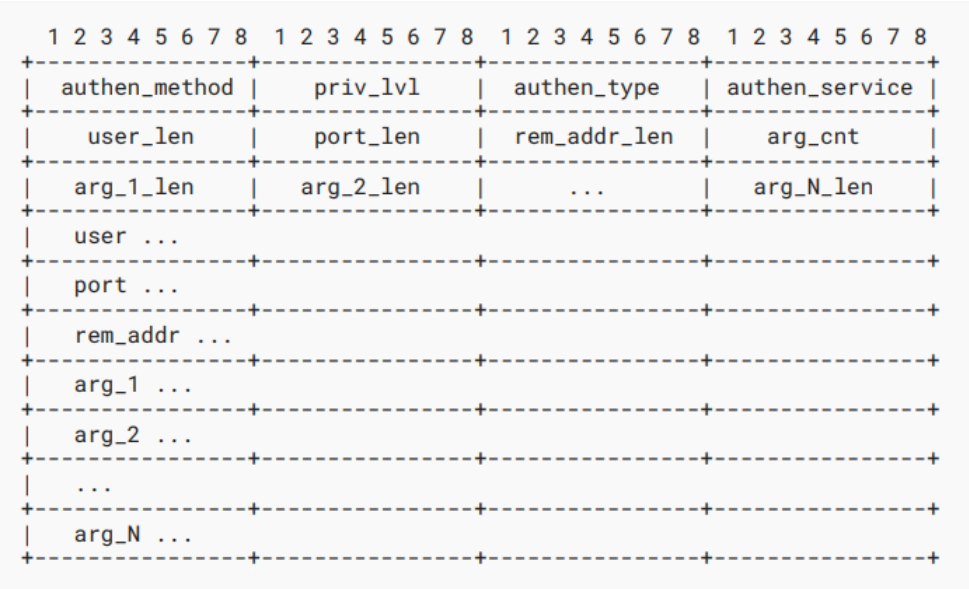
Campo	Descripción	Valor
user_msg len	Longitud, en bytes, del campo “user_msg”.	0x0000 … 0xFFFF
data_len	Longitud, en bytes, del campo “data”.	0x0000 … 0xFFFF
flags	Banderas que modifican la acción a realizar.	TAC_PLUS_CONTINUE_FLAG_ABORT := 0x01
user_msg	Cadena que el usuario ingresó o que el cliente proporcionó en nombre de usuario como respuesta a “server_msg” de un paquete REPLY.	Cadena de caracteres ASCII en hexadecimal (máx. 3 bytes)
data	Datos que forman parte del intercambio de autenticación.	Cadena de caracteres ASCII en hexadecimal (máx. 1 byte)

Nota. Elaboración propia.

C.2.4. Cuerpo del Paquete de Autorización REQUEST

Este paquete contiene los datos necesarios para que el servidor evalúe y determine los permisos del usuario. La imagen muestra la estructura del cuerpo del paquete.

Cuerpo del paquete REQUEST en la autorización TACACS+.



Nota. Adaptado de “The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol”, por T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, & L. Grant, 2020, IETF (https://datatracker.ietf.org/doc/html/rfc8907).

Se proporciona una descripción detallada de los campos que se encuentran en el cuerpo del paquete.

Campos en el cuerpo del paquete REQUEST en la autorización TACACS+.

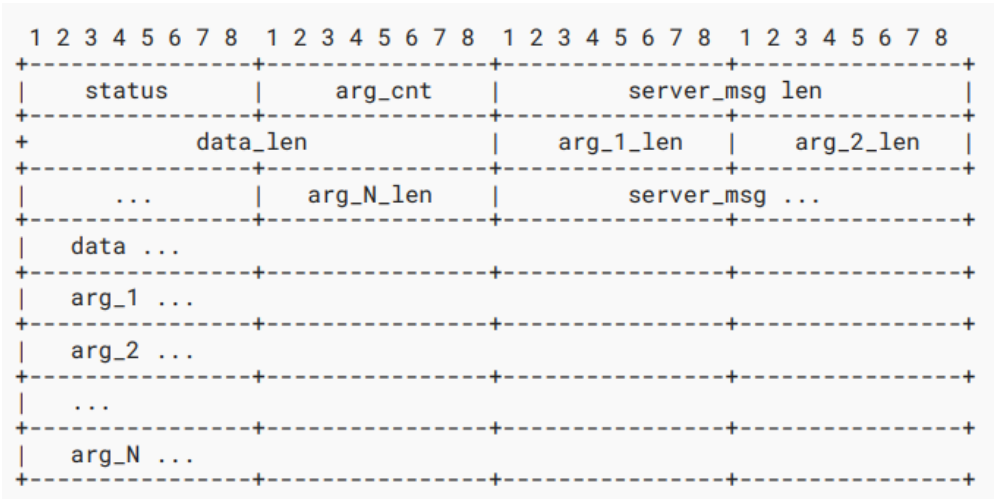
Campo	Descripción	Valor
authen_method	Método de autenticación utilizado por el cliente para adquirir información del usuario	TAC_PLUS_AUTHEN_METH_NOT_SET := 0x00 TAC_PLUS_AUTHEN_METH_NONE := 0x01 TAC_PLUS_AUTHEN_METH_KRB5 := 0x02 TAC_PLUS_AUTHEN_METH_LINE := 0x03 TAC_PLUS_AUTHEN_METH_ENABLE := 0x04 TAC_PLUS_AUTHEN_METH_LOCAL := 0x05 TAC_PLUS_AUTHEN_METH_TACACSPLUS := 0x06 TAC_PLUS_AUTHEN_METH_GUEST := 0x08 TAC_PLUS_AUTHEN_METH_RADIUS := 0x10 TAC_PLUS_AUTHEN_METH_KRB4 := 0x11 TAC_PLUS_AUTHEN_METH_RCMD := 0x20
priv_lvl	Indica, igual que el campo "priv_lvl" en la autenticación, el nivel de privilegio actual del usuario.	TAC_PLUS_PRIV_LVL_MIN := 0x00 TAC_PLUS_PRIV_LVL_USER := 0x01 TAC_PLUS_PRIV_LVL_ROOT := 0x0F TAC_PLUS_PRIV_LVL_MAX := 0x0F
authen_type	Este campo corresponde al campo “authen_type” en la autenticación.	TAC_PLUS_AUTHEN_TYPE_ASCII := 0x01 TAC_PLUS_AUTHEN_TYPE_PAP := 0x02 TAC_PLUS_AUTHEN_TYPE_CHAP := 0x03 TAC_PLUS_AUTHEN_TYPE_MSCHAP := 0x05 TAC_PLUS_AUTHEN_TYPE_MSCHAPV2 := 0x06
authen_service	Este campo es el mismo que el campo “authen_service” en la autenticación.	TAC_PLUS_AUTHEN_SVC_NONE := 0x00 TAC_PLUS_AUTHEN_SVC_LOGIN := 0x01 TAC_PLUS_AUTHEN_SVC_ENABLE := 0x02 TAC_PLUS_AUTHEN_SVC_PPP := 0x03 TAC_PLUS_AUTHEN_SVC_PT := 0x05 TAC_PLUS_AUTHEN_SVC_RCMD := 0x06 TAC_PLUS_AUTHEN_SVC_X25 := 0x07 TAC_PLUS_AUTHEN_SVC_NASI := 0x08 TAC_PLUS_AUTHEN_SVC_FWPROXY := 0x09
user_len	Longitud, en bytes, del campo “user”.	0x00 … 0xFF
port_len	Longitud, en bytes, del campo “port”.	0x00 … 0xFF
rem_addr_len	Longitud, en bytes, del campo “rem_addr”.	0x00 … 0xFF
arg_cnt	Número de argumentos de autorización a seguir.	0x00 … 0xFF
arg_1_len, …, arg_N_len	Longitud, en bytes, de los argumentos.	0x00 … 0xFF
user	Nombre de la cuenta del usuario.	Cadena de caracteres ASCII en hexadecimal (máx. 4 bytes)
port	Este campo coincide con el campo “port” en la autenticación.	Cadena de caracteres ASCII en hexadecimal (máx. 4 bytes)
rem_addr	Este campo coincide con el campo “rem_addr” en la autenticación.	Cadena de caracteres ASCII en hexadecimal (máx. 4 bytes)
arg_1, …, arg_N	Argumentos de la interacción de autorización.	Máximo 4 bytes por argumentos.

Nota. Elaboración propia.

C.2.5. Cuerpo del Paquete de Autorización REPLY

El paquete REPLY, cuya estructura se muestra en la Figura, contiene la información necesaria para determinar si una solicitud de acceso será permitida o denegada, y juega un papel vital en la gestión de seguridad y control de acceso. Para detalles específicos sobre los campos incluidos en este cuerpo, se describe cada campo y su posible valor durante la etapa de autorización TACACS+.

Cuerpo del paquete REPLY en la autorización TACACS+.



Nota. Adaptado de “The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol”, por T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, & L. Grant, 2020, IETF (https://datatracker.ietf.org/doc/html/rfc8907).

Campos en el cuerpo de paquete REPLY en la autorización TACACS+.

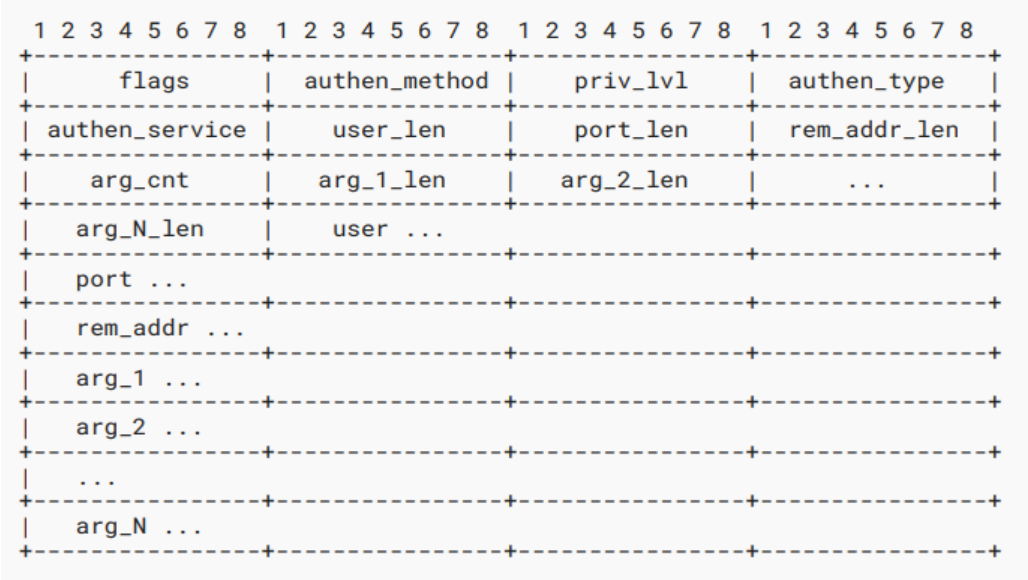
Campo	Descripción	Valor
status	Indica el estado de la autorización.	TAC_PLUS_AUTHOR_STATUS_PASS_ADD := 0x01 TAC_PLUS_AUTHOR_STATUS_PASS_REPL := 0x02 TAC_PLUS_AUTHOR_STATUS_FAIL := 0x10 TAC_PLUS_AUTHOR_STATUS_ERROR := 0x11
arg_cnt	Número de argumentos de autorización a seguir.	0x00 … 0xFF
server_msg len	Longitud, en bytes, del campo “server_msg”.	0x0000 … 0xFFFF
data_len	Longitud, en bytes, del campo “data”.	0x0000 … 0xFFFF
arg_1_len, …, arg_N_len	Longitud, en bytes, de los argumentos.	0x00 … 0xFF
server_msg	Mensaje que se muestra al usuario (opcional).	Cadena de caracteres ASCII en hexadecimal (máx. 2 bytes)
data	Cadena que puede presentarse en una pantalla, consola o registro administrativo (opcional).	Cadena de caracteres ASCII en hexadecimal (máx. 4 bytes)
arg_1, …, arg_N	Argumentos que describen los detalles de la autorización que se solicita.	Máximo 4 bytes por argumento.

Nota. Elaboración propia.

C.2.6. Cuerpo del Paquete de Auditoría REQUEST

El paquete REQUEST inicia la recolección de datos sobre las actividades de los usuarios, solicitando al servidor la información necesaria para registrar y auditar las acciones realizadas. La figura ilustra la estructura detallada del cuerpo del paquete REQUEST.

Cuerpo del paquete REQUEST en la auditoría TACACS+.



Nota. Adaptado de “The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol”, por T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, & L. Grant, 2020, IETF (https://datatracker.ietf.org/doc/html/rfc8907).

Se proporciona una descripción detallada de los campos presentes en el cuerpo del paquete REQUEST durante el proceso de auditoría TACACS+.

Campos en el cuerpo del paquete REQUEST en la auditoría TACACS+.

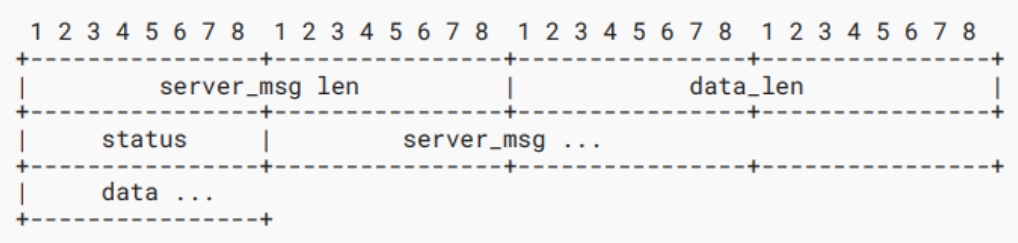
Campo	Descripción	Valor
flags	Banderas de mapa de bits.	TAC_PLUS_ACCT_FLAG_START := 0x02 TAC_PLUS_ACCT_FLAG_STOP := 0x04 TAC_PLUS_ACCT_FLAG_WATCHDOG := 0x08
authen_method	Definido en "authen_method" en la autenticación.	Igual a "authen_method" en la autenticación.
priv_lvl	Definido en "priv_lvl" en la autenticación y autorización.	Igual a "priv_lvl" en la autenticación y autorización.
authen_type	Definido en "authen_type" en la autenticación.	Igual a "authen_type" en la autenticación.
authen_service	Definido en "authen_service" en la autenticación.	Igual a "authen_service" en la autenticación.
user_len	Definido en "user_len" en la autenticación y autorización.	Igual a "user_len" en la autenticación y autorización.
port_len	Definido en "port_len" en la autenticación y autorización.	Igual a "port_len" en la autenticación y autorización.
rem_addr_len	Definido en "rem_addr_len" en la autenticación y autorización.	Igual a "rem_addr_len" en la autenticación y autorización.
arg_cnt	Número de argumentos de autorización a seguir.	0x00 … 0xFF
arg_1_len, …, arg_N_len	Longitud, en bytes, de los argumentos.	0x00 … 0xFF
user	Definido en "user" en la autenticación y autorización.	Igual a "user" en la autenticación y autorización.
port	Definido en "port" en la autenticación y autorización.	Igual a "port" en la autenticación y autorización.
rem_addr	Definido en "rem_addr" en la autenticación y autorización.	Igual a "rem_addr" en la autenticación y autorización.
arg_1, …, arg_N	Argumentos que describen los detalles de la autorización que se solicita.	Máximo 4 bytes por argumento.

Nota. Elaboración propia.

C.2.7. Cuerpo del Paquete de Auditoría REPLY

El paquete REPLY es utilizado por el servidor para enviar la respuesta al cliente después de procesar la solicitud de auditoría. La respuesta contiene información del estado de la solicitud y detalles relacionados con el registro de las actividades del usuario. La figura presenta la estructura del cuerpo del paquete REPLY y la Tabla los campos que contiene.

Cuerpo del paquete REPLY en la auditoría TACACS+.



Nota. Adaptado de “The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol”, por T. Dahm, A. Ota, D.C. Medway Gash, D. Carrel, & L. Grant, 2020, IETF (https://datatracker.ietf.org/doc/html/rfc8907).

Campos en el cuerpo del paquete REPLY en la auditoría TACACS+.

Campo	Descripción	Valor
server_msg len	Longitud, en bytes, de campo “server_msg”.	0x0000 ... 0xFFFF
data_len	Longitud, en bytes, de campo “data”.	0x0000 ... 0xFFFF
status	Estado de la auditoría.	TAC_PLUS_ACCT_STATUS_SUCCESS := 0x01 TAC_PLUS_ACCT_STATUS_ERROR := 0x02 TAC_PLUS_ACCT_STATUS_FOLLOW := 0x21
server_msg	Cadena que se presenta al usuario (opcional).	Máximo 3 bytes.
data	Cadena que puede presentarse en una pantalla, consola o registro administrativo (opcional).	Máximo 1 byte.

Nota. Elaboración propia.

C.3. Proceso de Autenticación TACACS+

Los campos “action”, “authen_type” y “authen_service” se combinan para indicar el tipo de autenticación que se va a realizar. Cada paquete de autenticación START, REPLY y CONTINUE incluye el campo “data”. El uso de este campo depende del tipo de autenticación.

Todo proceso de autenticación consta de un paquete START. El servidor responde con un paquete REPLY solicitando más información con GETDATA, GETUSER o GETPASS, o finaliza con PASS, FAIL, ERROR o RESTART.

Cuando el campo “status” de un paquete REPLY es igual a TAC_PLUS_AUTHEN_STATUS_GETDATA, TAC_PLUS_AUTHEN_STATUS_GETUSER o TAC_PLUS_AUTHEN_STATUS_GETPASS, la autenticación continua y el servidor proporciona un mensaje contenido en el campo “server_msg” para que el cliente solicite al usuario más información. Luego el cliente devuelve un paquete CONTINUE que contiene la información solicitada en el campo “user_msg”.

El cliente debe interpretar TAC_PLUS_AUTHEN_STATUS_GETUSER como una solicitud de nombre de usuario y TAC_PLUS_AUTHEN_STATUS_GETPASS como solicitud de contraseña. El campo “status” igual a TAC_PLUS_AUTHEN_STATUS_GETDATA es la solicitud genérica de más información para respaldar de manera flexible los requisitos futuros del protocolo TACACS+.

Si la información que el servidor solicita al cliente es confidencial, entonces el servidor debe establecer el flag TAC_PLUS_REPLY_FLAG_NOECHO.

Cuando el cliente solicita información al usuario, la respuesta se reflejará en la interfaz de usuario mientras interactúa con la interfaz del cliente.

C.4. Cierre de una Sesión de Autenticación TACACS+

El cliente puede terminar prematuramente una sesión configurando el flag TAC_PLUS_CONTINUE_FLAG_ABORT en el paquete CONTINUE.

Se definió un mecanismo para dirigir las solicitudes de autenticación a un servidor alternativo. Sin embargo, se considera inseguro por lo que está en desuso. El cliente debe interpretar el campo “status” TAC_PLUS_AUTHEN_STATUS_FOLLOW como

TAC_PLUS_AUTHEN_STATUS_FAIL.

Si el campo “status” del paquete REPLY es igual a TAC_PLUS_AUTHEN_STATUS_ERROR, entonces el host indica que está experimentando un error irrecuperable y la autenticación continuará como si ese host no pudiera ser contactado.

Si el campo “status” del paquete REPLY es igual a TAC_PLUS_AUTHEN_STATUS_RESTART, entonces la secuencia de autenticación se reinicia con un nuevo paquete START del cliente, con una nueva ID de sesión y “seq_no” establecido en 1. Este paquete REPLY indica que el valor actual de “authen_type” (como se especifica en el paquete START) no es aceptable para esta sesión y el cliente puede probar un “authen_type” alternativo.

Si un cliente no implementa la opción TAC_PLUS_AUTHEN_STATUS_RESTART, entonces procesa la respuesta como si “status” fuera TAC_PLUS_AUTHEN_STATUS_FAIL.

C.5. Proceso de Autorización TACACS+

Generalmente, la autenticación precede a la autorización, aunque no es obligatorio que un cliente utilice el mismo servicio de autenticación que utilizará para la autorización. Una solicitud de autorización puede indicar que el usuario no está autenticado. En este caso, corresponde al servidor determinar, según su configuración, si a un usuario no autenticado se le permite los servicios que solicita.

En el protocolo TACACS+, la autorización utiliza un único par de mensajes: un paquete REQUEST del cliente seguido de un paquete REPLY del servidor. El paquete de autorización REQUEST contiene un conjunto fijo de campos que indican cómo se autenticó el usuario y un conjunto variable de argumentos que describen los servicios y opciones para los cuales se solicita autorización. El paquete de autorización REPLY contiene un conjunto variable de argumentos de respuesta (pares argumento-valor) que pueden restringir o modificar las acciones del cliente.

C.6. Proceso de Auditoría TACACS+

La auditoría en TACACS+ puede tener dos propósitos: puede usarse como herramienta de auditoría para servicios de seguridad y también puede usarse para contabilizar servicios utilizados. Para esto último, TACACS+ soporta tres tipos de registros de auditoría: Los registros de inicio indican que un servicio está a punto de comenzar (TAC_PLUS_ACCT_FLAG_START := 0x02), los registros de parada indican que un servicio acaba de finalizar (TAC_PLUS_ACCT_FLAG_STOP := 0x04) y los registros de actualización (TAC_PLUS_ACCT_FLAG_WATCHDOG := 0x08) son avisos intermedios que indican que un servicio aún se está ejecutando.

El servidor responde en el paquete REPLY con TAC_PLUS_ACCT_STATUS_SUCCESS := 0x01 sólo cuando se ha registrado la solicitud de auditoría. Si el servidor no registró la solicitud de auditoría, responde con TAC_PLUS_ACCT_STATUS_ERROR := 0x02.