ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERIA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"ANÁLISIS DE PRESTACIONES DE LOS PROTOCOLOS DE AUTENTICACIÓN REMOTA RADIUS Y TACACS+ EN INFRAESTRUCTURA DE COMUNICACIONES CORPORATIVAS"

TRABAJO DE TITULACIÓN

TIPO: PROYECTO TÉCNICO

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

AUTOR: GABRIELA ANABELL ANDRADE TUBUN

DIRECTOR: ING. ALBERTO LEOPOLDO ARELLANO AUCANCELA

Riobamba – Ecuador

2019

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

El tribunal del trabajo de titulación certifica que el proyecto técnico: ANÁLISIS DE PRESTACIONES DE LOS PROTOCOLOS DE AUTENTICACIÓN REMOTA RADIUS Y TACACS+ EN INFRAESTRUCTURA DE COMUNICACIONES CORPORATIVAS de responsabilidad del señor Francisco Javier Shagñay Iguasnia, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

NOMBRE	**FIRMA**	**FECHA**
Ing. Washington Luna **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Patricio Romero **DIRECTOR DE LA ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Alberto Arellano **DIRECTOR DEL TRABAJO DE TITULACIÓN**	_____	_____
Ing. Oswaldo Martínez **MIEMBRO DEL TRIBUNAL**	_____	_____

Yo, Gabriela Anabell Andrade Tubun soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis y el patrimonio intelectual del Trabajo de Titulación pertenece a la Escuela Superior Politécnica de Chimborazo.

_____

Gabriela Anabell Andrade Tubun

DEDICATORIA

A Dios que guio mi camino al triunfo.

A mis padres Duver y Silvia que me enseñaron a ser una mujer de bien y ser el pilar fundamental de mi vida.

A mis hermanas Dairis y Vianka por enseñarme el amor de familia y ser una inspiración para su futuro.

A toda mi familia en general que siempre me brindo apoyo para seguir adelante, así como también a los amigos que velaron por mí al estar lejos de casa.

Gabriela Andrade

AGRADECIMIENTO

Agradezco a Dios por la sabiduría la inteligencia y la perseverancia de seguir adelante sobre todas las cosas.

A mis padres que siempre me impulsaron por el buen camino para aprovechar su esfuerzo para alcanzar la meta tan anhelada.

A mis hermanas por ser la fuente de inspiración para no rendirme y cumplir mis objetivos.

A las autoridades de la ESPOCH sobre todo a los docentes que formaron parte de mi enseñanza y encaminaron a culminar la carrera, en especial al director y miembros del tribunal.

A todos mis familiares y amigos por el gran apoyo brindado.

TABLA DE CONTENIDO

CAPITULO II

CAPITULO III

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

La presente investigación tuvo como objetivo analizar las prestaciones de los protocolos de autenticación remota RADIUS y TACACS+ en infraestructura de comunicaciones corporativas, la infraestructura corporativa posee problemas con el manejo de sus redes debido a que existe un desconocimiento y brechas de inseguridad, principalmente en redes WLAN por lo que se pretende realizar estudios de las características y prestaciones de los protocolos RADIUS y TACACS+, diseñar el ambiente de prueba para validar la prestación de cada protocolo utilizando un ambiente Open Source, evaluar y verificar el adecuado funcionamiento de los protocolos seleccionados para establecer parámetros de comparación y elaborar una propuesta de guía técnica para la implementación de autenticación remota en infraestructuras corporativas, por cualquier vía, se puede mejorar y precautelar la integridad y seguridad de los clientes. Para confirmar la necesidad de implementar mecanismos de autenticación en las redes inalámbricas, se realizó una encuesta a los administradores de varias empresas públicas de Riobamba tales como: CNT-EP (Riobamba), Consejo Provincial de Chimborazo y la Municipalidad de Riobamba, para verificar si los administradores conocen sobre la existencia de los protocolos RADIUS o TACACS+ se obtuvo como resultados que tan solo CNT-EP Riobamba tiene conocimiento y utilizan protocolos de autenticación remota y control de acceso en su infraestructura. Llegando a la conclusión que la mejor característica posee TACACS+ debido a que brinda mejores beneficios de seguridad.

PALABRAS CLAVE: <TECNOLOGIA> <CIENCIAS DE LA INGENIERIA>, <TELECOMUNICACIONES>, <PROTOCOLOS DE AUTENTICACIÓN>, <RADIUS>, <TACACS+>, <REDES DE FUNCIONAMIENTO>, <SEGURIDAD INFORMÁTICA>.

SUMMARY

The objective of this research was to analyze the features of authentication protocols RADIUS AND TACACS+ in corporate communication infrastructure, The corporate infraestrucutre has problems with the management of this networks because there is a lack of knowledge and insecurity gaps, mainly in WLAN networks so it is intended to carry out studies of the characteristics and performance of the Protocols Radius and Tacacs+, design the test environment to validate the performance of each protocol using an Open Source environment, evaluate and verify the proper functioning of the protocols selected to establish comparison parameters and to develop a technical guide proposal for the implementation of remote authentication in corporate infrastructure, by any means, it is possible to improve and precaution the integrity and security of the clients. To confirm the need to implement authentication mechanisms in wireless networks, a survey was conducted to the administrators of several public companies of Riobamba such as: CNT-EP (Riobamba), Provincial Council of Chimborazo and the Municipality of Riobamba, to verify if the administrators know about the existence of the protocols RADIUS or TACACS+ was obtained as results that only CNT-EP Riobamba has knowledge and use protocols of remote authentication and access control in its infrastructure.Concluding that the best features have TACACS+ because it provides better security benefits.

KEY WORDS: <TECHNOLOGY>, <ENGINEERING SCIENCES>, <TELECOMMUNICATIONS>, <AUTHENTICATION PROTOCOLS>, <RADIUS>, <TACACS+>, <OPERATING NETWORKS>, <TECHNOLOGY SECURITY>

INTRODUCCIÓN

La mayoría de las instituciones y empresas cuentan con redes ya sea cableada o inalámbrica lo que significa que transporta información que es valiosa para las empresas. Si tomamos en cuenta un correcto manejo de las redes y de la información que se transporta por cualquier vía, se puede mejorar y precautelar la integridad y seguridad de los clientes.

En la actualidad es muy común escuchar sobre términos de hackeo, virus, robo de la información en general, lo que nos da a entender que habido un constante crecimiento de crímenes cibernéticos a los que diariamente empresas y personas en general están expuestas. Por estas razones ha sido indispensable investigaciones e implementación de sistemas de seguridad para protección de la información.

La mayoría de las redes por no decir todas presentan inconvenientes de vulnerabilidad, siendo esta el causal de determinar parámetros para salvaguardar la información, debido a esto existen varios protocolos a los que se pueden regir, para dar mayor seguridad a las redes y en un entorno globalizado de transmisión de información se puede estipular la prevención y ahorro de recursos sabiendo administrar de una manera correcta el manejo de la red.

La infraestructura corporativa posee problemas con el manejo de sus redes ya sea por desconocimiento o brechas de inseguridad, pero esta problemática puede ser resuelta con estudios, seguimiento y herramientas de control que permita mejorar la confiabilidad en la red de dicha infraestructura dentro de los parámetros designados.

Basado en la comparación y la seguridad de datos es fundamental el conocimiento de nuevas técnicas de seguridad y comportamiento de las redes para mantener a salvo los datos de los clientes de toda empresa que hace uso de nuevas tecnologías. Por este motivo el desarrollo de la presente tesis está basado en sistemas de control de acceso mejor conocido como AAA (Autenticación, Autorización y Administración), en especial con servidores que manejan estos protocolos como son RADIUS y TACACS+ que serán detallados y comparados para verificar cuáles son sus beneficios.

JUSTIFICACIÓN TEÓRICA

En la actualidad existe la necesidad de controlar el acceso de los usuarios a la infraestructura corporativa para tener el control en la seguridad de la información. Los servicios AAA hoy en día

son utilizados dentro del lineamiento de seguridad de redes de telecomunicaciones para cumplir con los requerimientos de protección de la información y tener un control centralizado del acceso y administración de los equipos.

El desarrollo del protocolo AAA ha sido primordial durante los últimos años; debido a esto se ha presentado al mercado múltiples soluciones que permitan contar con servicios de control de acceso y administración de una manera más confiable. Para estos aspectos los protocolos más utilizados en el mercado RADIUS y TACACS+ (Hoyos, 2013).

Uno de los aspectos más importantes que debemos tomar en cuenta para realizar una implementación de servicios AAA, es realizar un estudio previo que permita describir la definición para verificar cuál sería la mejor infraestructura, diseño y protocolo a utilizar de acuerdo a la necesidad. Para cubrir todas las necesidades de protección de la información, es necesario conocer a fondo el funcionamiento, requerimientos, ventajas y desventajas; para de esta forma realizar la elección más adecuada.

Uno de los protocolos utilizados ampliamente es RADIUS para controlar el acceso a servicios a la red. En particular, una solución de código abierto es Iron-Wifi y Tek-RADIUS Un caso real de utilización del protocolo RADIUS es la red (eduroam) como un método global de control de acceso a las redes inalámbricas de las principales instituciones académicas de Europa. (Glenhell, 2010).

TACACS+ es un protocolo propietario de Cisco donde existen algunos trabajos realizados a partir de este protocolo, tales como: punto de acceso Aironet para la autenticación de inicio de sesión con el uso del ejemplo de la Configuración del GUI además Cisco evaluó seriamente RADIUS como un (security protocol) antes de que desarrollara TACACS+. Muchas funciones fueron incluidas en el protocolo TACACS+ para que cumplan con las necesidades del mercado de seguridad en continuo crecimiento. (Cisco, 2011).

Para corroborar la necesidad de implementar mecanismos de autenticación en las redes inalámbricas, se realizó una encuesta a los administradores de varias empresas públicas de Riobamba tales como: CNT-EP (Riobamba), Empresa Eléctrica Riobamba S.A, Consejo Provincial de Chimborazo, Ecu 911 sede Riobamba y la Municipalidad de Riobamba. Para verificar si los administradores conocen sobre la existencia de estos protocolos ya sea (RADIUS o TACACS+) y sus ventajas; se obtuvo como resultados que tan solo CNT-EP Riobamba tiene conocimiento y utilizan protocolos de autenticación remota y control de acceso en su infraestructura.

JUSTIFICACÓN PRÁCTICA

Hoy en día la mayoría de las redes inalámbricas son vulnerables a ataques de seguridad. De acuerdo con el último Reporte Global de Cibercrimen Norton (2013) al menos 378 millones de usuarios web fueron víctimas de situaciones que van desde la recepción de virus, hackeado de cuentas, robos de identidad, etc. Evidenciando, los delitos vulneran a más de un millón de cibernautas cada día, lo que equivale a 12 cada segundo. Por eso la importancia de mantener la información de los usuarios protegida por protocolos para verificar quien tiene acceso a las redes corporativas.

Para verificar las prestaciones que nos proveen los protocolos RADIUS y TACACS+ presentaremos un escenario, donde probaremos el tiempo en que el usuario lograra conectarse con unos de los dos servidores RADIUS o TACACS+; pudiendo así determinar el tiempo de latencia, que procesos utilizarían para la autenticación, los códigos de seguridad, la longitud que tendrán las contraseñas para para evitar ataques de seguridad y finalmente verificar la mejor adaptación de capa de transporte ya sea UDP o TCP.

Por lo que es importante la realización de este trabajo de titulación que tiene como objetivo final realizar una propuesta de guía técnica de implementación de autenticación remota que permitirá mejorar la seguridad en instituciones tanto públicas o privadas.

FORMULACIÓN DEL PROBLEMA

¿El análisis de los protocolos de autenticación remota RADIUS y TACACS+ permitiría determinar el más adecuado para mejorar la seguridad de acceso en redes inalámbricas?

SISTEMATIZACIÓN DEL PROBLEMA

- ¿Cuál de los protocolos, RADIUS o TACACS+ ofrece las mejores características en cuanto a control de acceso y administración de la red?
- ¿Qué protocolos de la capa de transporte utiliza los mecanismos de Autenticación remota?
- ¿Qué protocolo de autenticación remota minimiza la latencia en este proceso?
- ¿Cuál es el tamaño adecuado de las contraseñas desde seguridad en cada uno de los protocolos de autenticación remota?

OBJETIVOS

OBJETIVO GENERAL

- Analizar las prestaciones de los protocolos de autenticación remota RADIUS y TACAS+ en infraestructura de comunicaciones corporativas.

OBJETIVOS ESPECIFICOS

- Estudiar las características y prestaciones de los protocolos RADIUS y TACACS+.
- Diseñar el ambiente de prueba para validar la prestación de cada protocolo utilizando un ambiente Open Source.
- Evaluar y verificar el adecuado funcionamiento de los protocolos seleccionados para establecer parámetros de comparación.
- Elaborar una propuesta de guía técnica para la implementación de autenticación remota en infraestructuras corporativas.

CAPÍTULO I

1. MARCO TEÓRICO

En este capítulo se detallan los conceptos fundamentales de la autenticación RADIUS y TACACS+ para la cual se realizará una investigación comparativa de sus características y los mecanismos que se utilizan para proporcionar seguridad y confiabilidad de datos en redes corporativas con accesos WLAN.

1.1. Seguridad en Redes Corporativas

La seguridad de los datos en las redes corporativas es un punto que resalta en la actualidad ya que en los últimos años se han realizado varios ataques a redes WLAN, incrementando el número de ataques informáticos a este tipo de infraestructura así lo demuestra la figura 1 que es un estudio desarrollado por Wifi Marketing Overview que resume el análisis de la conexión wifi realizada en países de potencia mundial donde nos demuestra que el 25% de hogares a nivel mundial posee una conexión wifi mientras que un 50% de hogares a nivel mundial prevé en los próximos años tener una conexión a internet por medio de wifi y un 44% de esta población utiliza conexiones wifi en otros lugares ya sea en el trabajo o lugares públicos.

Finalmente nos entrega el resultado que para el 2015 los puntos de acceso wifi público a nivel mundial crecieron más de cuatro veces (Huy, 2017)

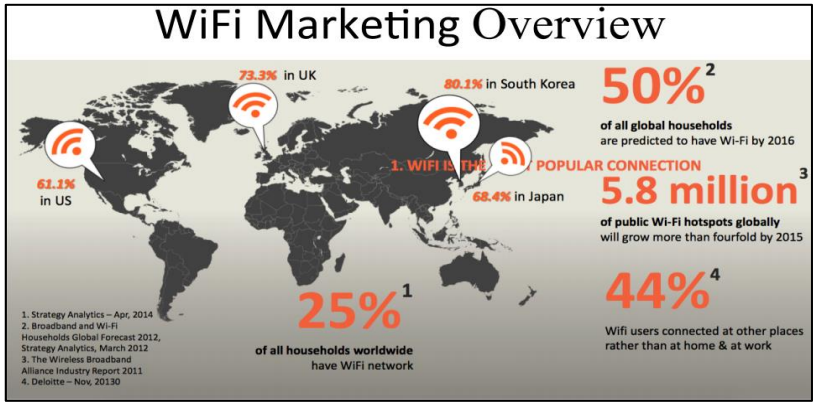


Figura 1-1: Análisis de conexiones Wifi

Fuente: (Huy, 2017)

Además, se ha evidenciado delitos que vulneran a más de un millón de cibernautas cada día, lo

que equivale a 12 delitos informáticos cada segundo así lo confirma la revista NORTON y Symantec. Un agravante a esto concluye al estudio, es el uso de conexiones WIFI inseguras para acceder a cuentas personales (bancarias, correo electrónico o redes sociales), un escenario extremadamente fácil para que quienes cometen cibercrímenes ganen acceso a la información personal.

El estudio realizado por Norton by Symantec realizó una encuesta en línea, donde consulta las percepciones y prácticas de conexiones WI-FI a los consumidores y revela así los problemas de seguridad encontrados en este tipo de conexiones. En mayo del 2017 Norton encuesto a 15,532 usuarios de dispositivos móviles que tenían conexiones inalámbricas para descubrir comportamientos mediante el uso de infraestructura inalámbrica en lugares públicos. Como resultado de la investigación realizada por la empresa Norton by Symantec

Como se muestra en el gráfico 1 la mayoría de los consumidores no pueden resistir a una conexión WI-FI gratuita es decir más de la mitad de las conexiones a nivel mundial (un 55%) no pensaría dos veces en intercambiar o incluso compartir una conexión WI-FI

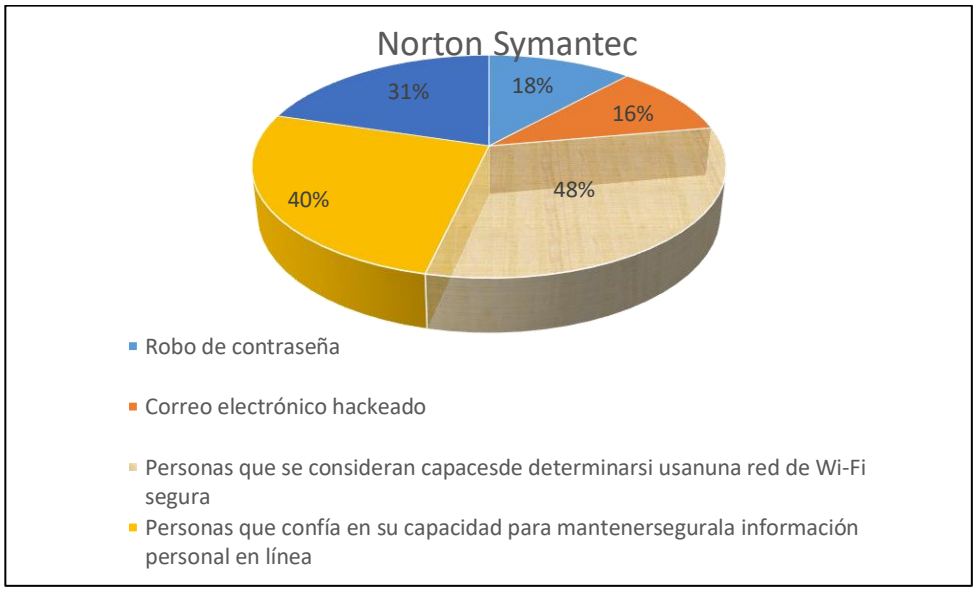


Gráfico 1-1: Delitos de cibercrimen según la empresa Norton Symantec

Realizado por: Gabriela Andrade, 2019

La dependencia de los consumidores a estar continuamente conectados a una red WIFI pública no consideran los riesgos que esto implica. Así Norton by Symantec según su estudio proporciona datos en la cual el 60% de usuarios de la red WI-FI pública siente que su información personal es segura, pero el 53% no puede distinguir entre una red WI-FI publica segura, el 75% de consumidores no usa una red privada virtual VPN para asegurar sus conexiones inalámbricas

seguras y un 87% de consumidores ha puesto potencialmente en riesgo su información mientras utiliza redes WI-FI públicas.

El gráfico 2 se detalla el uso de redes WI-FI públicas y la sensación de seguridad según sus consumidores. (Corporation [US])

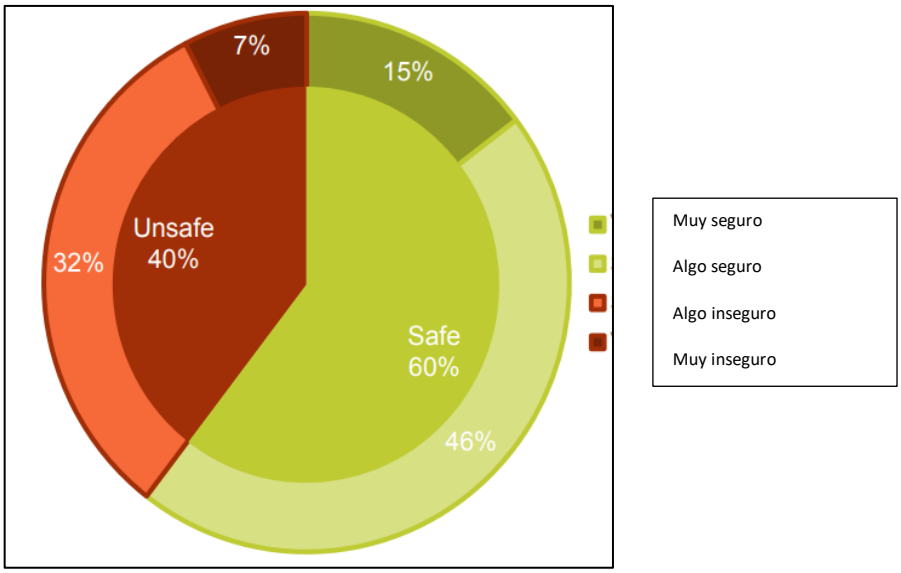


Gráfico 2-1: Tabulación de uso de la red WI-FI pública y seguridad que implica por consumidores

Fuente: (2017-norton-wifi-risk-report-global-results-summary)

Los datos entregados finalmente por Norton y Symantec son sorprendentes ya que un 87% de consumidores admite que toma riesgos al acceder a dichas redes porque desconocen qué tipo de información provee la red para ingresar a cuentas de correo, redes sociales, cuentas bancarias.

1.2. Protocolo AAA

Uno de los mecanismos que se utilizan para minimizar los riesgos de seguridad son los protocolos de Autenticación, Autorización y Auditoria o protocolos AAA, estos son protocolos de comunicación de redes, que limita a los usuarios al tipo de información que estos tienen acceso, especificando opciones y servicios que serán otorgados al usuario. Los servicios AAA prioriza el control de acceso de un dispositivo a la red. Ya que realiza una verificación y validación del usuario para que puedan coincidir las credenciales de autenticación y acceder a distintos servicios de la red. Los requisitos para acceder al modelo AAA se representa en la conexión de los usuarios a través de enrutadores y conmutadores (Ramirez, 2015).

En la Figura 2 el ítem 1 el suplicante envía la solicitud de autenticación al AAA Reuter l ítem 2

acepta o deniega el paso al servidor ACS el ítem 3 accede al servidor de autenticación y el ítem 4 autoriza y contabiliza los datos enviados.

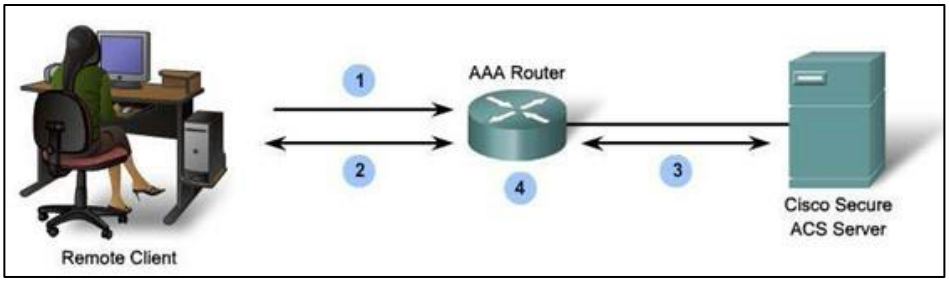


Figura 2-1: Protocolo AAA

Realizado por: Gabriela Andrade, 2018

1.2.1. Autenticación.

La autenticación es un proceso mediante el cual una entidad pueda probar su identidad ante otra, comúnmente una de las primeras entidades es un cliente, usuario o computador y la segunda es en este caso un servidor.

En la figura 3 se presenta un escenario donde un suplicante es autentificado por el servidor AAA y otro suplicante no es autentificado debido a que su contraseña y usuario no se encuentra en la base de datos o a su vez sus credenciales son incorrectas.

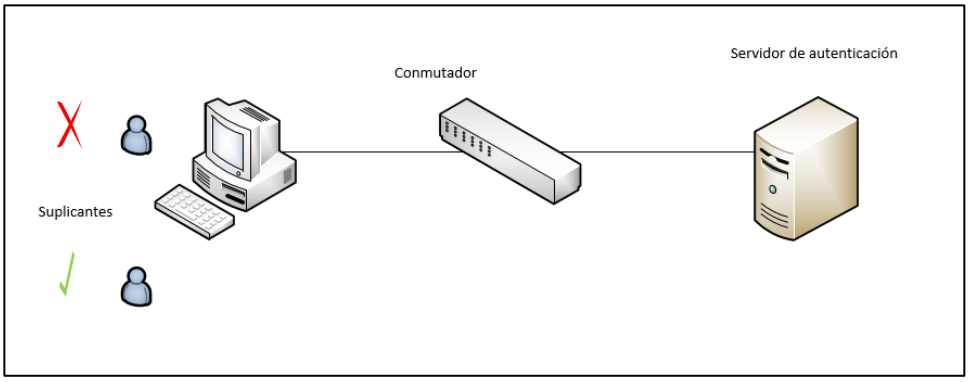


Figura 3-1: Autenticación

Realizado por: (ANDRADE Gabriela, 2018)

1.2.1.1. Proceso de Autenticación.

El proceso general de la autenticación consta de los siguientes pasos:

- El usuario solicita acceso a la red
- El sistema solicita que el usuario se autentique
- El usuario brinda las credenciales que lo identifican y permite verificar la autenticidad de su password.
- La red valida el acceso según las reglas y si las credenciales proporcionadas son suficientes para el acceso o no.

En la figura 4 se detalla el proceso de autenticación que es la solicitud enviada desde el interfaz del usuario la repuesta que envia el servidor si es aceptada o rechazada y la solicitud que vuelve a enviar el usuario para el envio de datos y usuarios posteriores

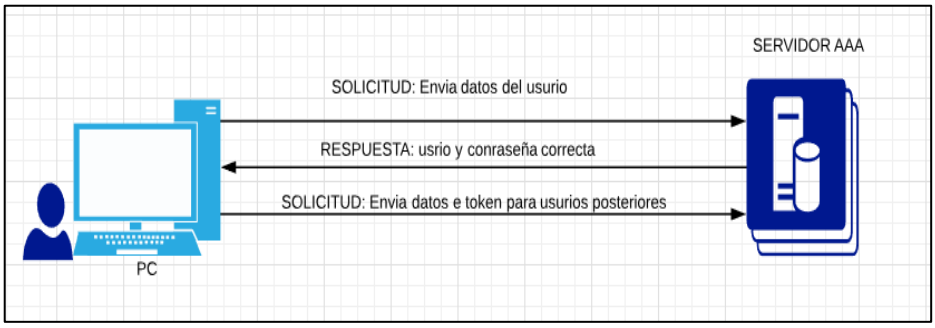


Gráfico 3-1: Proceso de Autenticación

Realizado por: Andrade Gabriela, 2018

1.2.2. Tipos de Autenticación

Para garantizar el control de acceso de los usuarios a la información que deseemos sea pública para ellos se controla la interacción de los recursos del sistema, por dicha razón hay soluciones como la implementación del protocolo AAA (autenticación, autorización y auditoria), estos estándares conllevan al control de acceso que se puede permitir a cada usuario.

1.2.3. Autenticación Estática

Los protocolos de autenticación estática más comunes son: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2).

Siendo el más utilizado la encriptación estática con el protocolo WPA2 considerado actualmente seguro, pero recientemente el núcleo de este protocolo presento errores dejando expuesto a la inseguridad de conexiones Wifi, ya que han desarrollado un Krack abreviatura de Key Reinstallation Attacks, y funciona explotando el "handshake de cuatro vías" de las WPA2,

(Saavedra, O, 2012).

1.2.3.1. Tipo de cifrado para la red

La mayor parte de los usuarios tiene un router Wi-Fi para conectarse a Internet de forma inalámbrica tanto desde un ordenador como desde los dispositivos móviles. Para evitar que usuarios no autorizados puedan conectarse de forma inalámbrica a nuestro router, robar nuestra conexión a Internet e incluso acceder al resto de ordenadores de nuestra red local, estos suelen protegerse con una contraseña de manera que, sin ella, el acceso no pueda ser posible.

Las contraseñas de los routers pueden conseguirse fácilmente ya que, por un lado, existen ataques de red especialmente diseñados para ello y, por otro, muchas aplicaciones cuentan con una serie de "diccionarios" que, según la MAC y el SSID nos pueden decir, al menos, la clave que viene por defecto y que, si no se ha cambiado, nos permitirá conectarnos a dicho router.

Los tipos de cifrado son:

- **Cifrado WEP:** Fue desarrollado para redes inalámbricas y aprobadas como estándar de seguridad Wi-Fi en septiembre de 1999. WEP tenía como objetivo ofrecer el mismo nivel de seguridad que las redes cableadas, sin embargo, hay un montón de problemas de seguridad. las aplicaciones desarrolladas para explotar este tipo de cifrado, finalmente se considera un cifrado "inseguro" y es posible obtener su clave en tan solo unos minutos capturando paquetes mediante falsas solicitudes de acceso. El cifrado WEP tiene dos niveles de seguridad, encriptación a 64 o 128 bit. La encriptación usa un sistema de claves. La clave de la tarjeta de red del ordenador debe coincidir con la clave del router. El cifrado WEP ofrece una protección insuficiente, por lo que no es recomendable su uso.

- **Cifrado WPA:** Se utilizó como una mejora de seguridad temporal para WEP. Se desarrolló para el estándar de seguridad inalámbrica 802.11i. La mayoría de las aplicaciones WPA modernas usan una clave previamente compartida (PSK), más a menudo conocida como WPA Personal, y el Protocolo de Integridad de Clave Temporal o TKIP (/ tiːkɪp /) para encriptación. WPA Enterprise utiliza un servidor de autenticación para la generación de claves y certificados. El cifrado WPA dos tiene tipos de seguridad, con servidor de seguridad y sin servidor. Este método se basa en tener una clave compartida de un mínimo de 8 caracteres alfanuméricos para todos los puestos de la red (Sin servidor) o disponer de un cambio dinámico de claves entre estos puestos (Con servidor). Este sistema de cifrado ofrece una serie de variantes según el uso que se le vaya

a dar

En la tabla 1 se compara las características de cifrado WPA con RADIUS.

Tabla 1-1: Cifrado WPA vs RADIUS

WPA	RADIUS
Utiliza un sistema de claves PSK o claves pre-compartidas donde el administrador especifica su propia contraseña y todos los usuarios se conectan a la red con ella, de manera que sea más fácil recordarla.	Enfocado a empresas, este sistema de seguridad se basa en un servidor en el que los usuarios deben autenticarse con un usuario y una contraseña diferente para cada uno en vez de conectarse todos con una contraseña global.

Realizado por: Gabriela Andrade, 2018

- Cifrado WPA2: El protocolo basado en estándares de seguridad inalámbrica 802.11i fue introducido en 2004. La mejoría más importante de WPA2 sobre WPA fue el uso del Estándar de cifrado avanzado (AES) para el cifrado. La posibilidad de ataques a través de Configuración de Wi-Fi Segura(WPS), sigue siendo alta en los actuales puntos de acceso capaces de WPA2, que es el problema con WPA también. AES (Advanced Encryption System) es un estándar de cifrado avanzado, que cifra en bloques simétricos de 128 bits

  Este sistema también cuenta con las variantes de claves personales PSK y sistemas RADIUS para la gestión de redes, aunque el cifrado es muy superior al de WPA.

1.2.4. Autenticación Dinámica

Uno de los servicios que usan autentificación de red es el de RPC "Remote Procedure Call – Llamada a Procedimiento Remoto" esto dificultaría al uso de este protocolo, el hecho de enviar las contraseñas encriptadas plantea otro problema de la comunicación de las claves. Para la autenticación dinámica, los nombres de usuarios y contraseñas de este esquema de autenticación existen en el servidor de autenticación y no en el cortafuegos.
Por lo tanto, el cortafuego dinámicamente (es decir, sobre una base "como es necesario") obtiene los nombres de usuario y contraseñas para la autenticación. La autenticación dinámica es compatible con ACE, defensor (SNK), RADIUS, CRYPTOCard, TACACS + y dominio NT (Gomez, C, 1996).

Este protocolo permite la movilidad y seguridad dinámica, ya que permite estrictamente el control del usuario y que tipo de información este está autorizado a llegar por eso viene este término

entrelazado con el termino AAA. Actualmente la mayoría de los dispositivos están conectados de esta forma debido al requerimiento de movilidad y dinamismo que ofrece este protocolo (AAA) como también el constante crecimiento de las redes sobre todo inalámbricas, (Garcia, A, 2015)

1.3. RADIUS

RADIUS es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP utiliza los puertos 1812 y 1813 UDP para así establecer sus conexiones, para autentificar, autorizar y contabilizar, respectivamente. (NetSpot, 2019)

RADIUS, para verificar que la información es correcta utiliza esquemas de autentificación como PAP, CHAP o EAP, por lo tanto, si es aceptado, el servidor autorizara el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP.

RADIUS está definido varios RFC los más importantes lo detallamos en la tabla 3:

Tabla 2-1: RFC publicados por RADIUS

RFC	ATRIBUTO
RFC 2548	Atributos RADIUS específicos del proveedor de Microsoft
RFC 2809	Implementation of L2TP Compulsory Tunneling via RADIUS
RFC 2865 (El más conocido y utilizado en este trabajo de titulación)	Authentication Remote Dial In User Service (RADIUS)
RFC 2866	Contabilidad RADIUS
RFC 2867	Modificaciones contables para el soporte del protocolo de túnel RADIUS
RFC 2868	Atributos de RADIUS para Tunnel Protocol Support
RFC 2869	Extensiones RADIUS
RFC 2882	Requisitos de los servidores de acceso a la red: Prácticas extendidas de RADIUS
RFC 3162	RADIUS e Ipv6
RFC 3576	Extensiones dinámicas de autorización para el servicio de usuario de marcado remoto de autenticación (RADIUS)
RFC 3579	(Servicio de usuario de acceso telefónico de autenticación remota) Compatibilidad con el protocolo de autenticación extensible (EAP)
RFC 3580	IEEE 802.1X Autenticación remota Marcación en el servicio de usuario (RADIUS) Usage Guidelines
RFC 4675	RADIUS Atributos para LAN virtual y soporte de prioridad
RFC 4679	Atributos de RADIUS específicos DSL Forum Vendor-Specific
RFC 4590	Extensión RADIUS para la Autenticación Digest
RFC 4818	RADIUS Atributo de prefijo Ipv6 delegado
RFC 4849	RADIUS Atributo de regla de filtro
RFC 5080	Problemas comunes de implementación del servicio de usuario de marcación remota de autenticación (RADIUS) y soluciones sugeridas
RFC 5997	Uso de paquetes de servidor de estado en el protocolo de autenticación remota en el servicio de usuario (RADIUS)

Realizado por: Gabriela Andrade, 2019

1.3.1. Formato del paquete RADIUS

Los paquetes que se envían a través de la red manejan un formato propio del protocolo RADIUS

el cual se detalla en la siguiente gráfica:

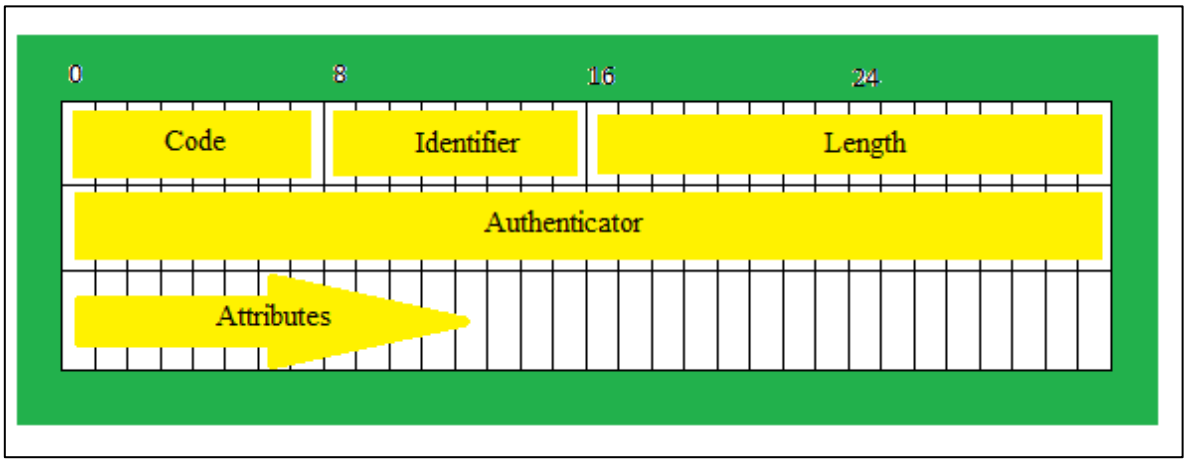


Figura 4-1: Formato de paquete RADIUS.

Fuente: (INFO, 2008)

El paquete RADIUS posee cinco campos denominados: código, identificador, longitud autentificado y atributos

1.3.1.1. Campo Código (Code)

El campo denominado código, tiene un octeto, que sirve para indicar el tipo de paquetes RADIUS.

Los principales valores del campo Código se demuestran en la siguiente tabla.

Tabla 3-1: Tipo de paquete que envía en el campo Código

Código	Tipo de Paquete	Descripción
1	Solicitud de acceso	Desde el cliente al servidor. Un paquete de este tipo lleva la información del usuario para el servidor para autenticar el usuario. Debe contener el nombre de usuario y el atributo puede contener opcionalmente los atributos de la NAS-IP-dirección, usuario-contraseña y NAS-Port.
2	Acceso-Aceptar	Desde el servidor al cliente. Si cualquier valor de atributo que se transporta en el acceso es una solicitud aceptable, es decir, la autenticación correctamente, el servidor envía un acceso –aceptar la respuesta.
3	Acceso-Rechazar	Desde el servidor al cliente. Si cualquier valor de atributo que se transporta en el acceso es una solicitud inaceptable, el servidor rechaza al usuario y envía un acceso –respuesta rechazar.
4	Solicitud de contabilidad	Desde el cliente al servidor. Un paquete de este tipo lleva la información del usuario para el servidor para iniciar la contabilidad en el usuario. Contiene el estado de cuenta de tipo atributo que indica si el servidor solicito el inicio o fin de la contabilidad.
5	Contabilidad-Respuesta	Desde el servidor al cliente. El servidor envía al cliente un paquete de este tipo de notificar que ha recibido la solicitud de contabilidad y ha grabado correctamente la información contable

Fuente: (INFO, 2008)

1.3.1.2. Identificador(Identifier)

El identificador posee un octeto que permite al cliente RADIUS relacionar una respuesta RADIUS con la solicitud correspondiente.

1.3.1.3. Longitud (Lenght)

La longitud del paquete consta con una total de 16 bits, incluyendo campos como el código hasta los atributos que posee. Además, indica la duración de todo el paquete, incluido el Código, Identificador, Longitud, Autentificador, y campos de atributo. Si la longitud de un paquete es

menor que a los dos octetos indicados por el campo de longitud, el paquete es eliminado.

1.3.1.4. Verificador (Authenticator)

Este campo posee 32 bits para autenticar la respuesta del servidor RADIUS y para encriptar la clave. Existen dos tipos de verificaciones: Solicitud y respuesta.

1.3.1.5. Atributos (Attributes)

Este campo transporta datos en la solicitud y respuesta para la autenticación, autorización y contabilización. El campo longitud del paquete sirve para determinar cuál es el final de los atributos El campo atributo lleva la información acerca de los detalles de la configuración está representado por: tipo, longitud, y el valor.

- **Tipo:** Un byte, en el rango de 1 a 255. Es para indicar el tipo de atributo. Comúnmente se utilizan atributos para la autenticación y autorización del RADIUS.
- **Duración:** Un byte para indicar la longitud del atributo en bytes, incluyendo el tipo, longitud, y el campo de valor.
- **Valor:** valor del atributo, hasta a 253 bytes. Su formato y contenido dependen del tipo y campos de longitud.

En la siguiente tabla se define el tipo de atributo que posee RADIUS para la autenticación por octeto.

Tabla 4-1: Tipos de Atributos del Paquete RADIUS

Tipo	Tipo de Atributo	Tipo	Tipo de Atributo
1	Nombre de usuario	**23**	Enmarcado-IPX-red
2	Usuario-contraseña	**24**	Estado
3	CHAP-contraseña	**25**	Clase
4	NAS-IP-dirección	**26**	Específicas de su proveedor
5	NAS-port	**27**	Periodo de sesiones-tiempo
6	Tipo de servicio	**28**	Tiempo de reposo
7	Enmarcado protocolo	**29**	La terminación –acción
8	Enmarcado-IP-dirección	**30**	Llamado estación-Id
9	Enmarcado-IP-mascara de red	**31**	Llamando a la estación-Id
10	Enmarcado-Routing	**32**	NAS-Identificador
11	Filtro-ID	**33**	Proxy-estado
12	Enmarcado-MTU	**34**	Login-LAT-Service
13	Enmarcado-compresión	**35**	Login-LAT-Nodo
14	Login-IP-host	**36**	Login-grupo de LAT
15	Servicio de inicio de sesión	**37**	Enmarcado-Apple-Talk-link
16	Login-TCP-Port	**38**	Enmarcado-Apple-Talk-red
17	(Sin asignar)	**39**	Enmarcado-zona Apple talk
18	Reply_Message	**40**	(Reservado para la contabilidad)
19	Numero de llamada	**41**	CHAP-Challenge
20	Identificación de llamada	**42**	NAS-port-tipo
21	(Sin asignar)	**43**	Puerto-limit
22	Enmarcado ruta	**44**	Login-LAT-Port

Fuente: (INFO, 2008)

1.3.2. Mensaje RADIUS

Ya establecido el acceso a la red por parte del usuario y accedido a sus recursos, será capaz de transmitir información y comenzará el proceso de la auditoria o contabilización del uso de los servicios asignados al usuario. En dicho proceso se van a registrar datos del usuario tales como: la identificación del usuario, dirección IP, punto de conexión y un identificador de sesión único. Estos datos serán actualizados periódicamente mientras se mantenga una sesión activa. De esta misma manera al momento de que la sesión sea terminada.

El mensaje RADIUS consta de una cabecera con sus respectivos atributos. Cada atributo especifica un fragmento de información acerca del intento de conexión.

El servidor RADIUS comprueba que la información sea correcta utilizando mensajes de autenticación que se muestran en la Figura 8: el acceso aceptado (Access-accept), reto de acceso

(acces-challenge) y el acceso rechazado (Access-reject).

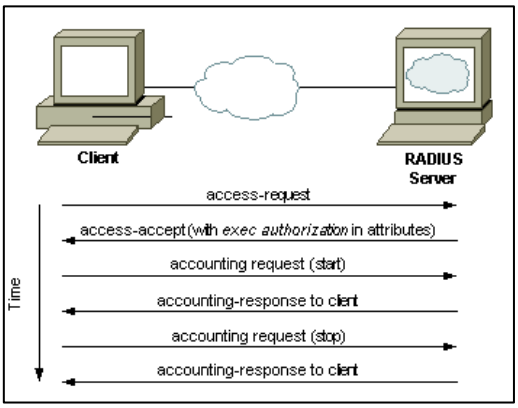


Figura 5-1: Mensajes RADIUS

Fuente: (Cisco)

- Access-accept o acceso aceptado se refiere a que el usuario tiene acceso, una vez que este se ha autenticado el servidor RADIUS asigna recursos de red como la dirección IP además de otros parámetros. De esta manera comprueba que el usuario está autorizado a utilizar algún servicio de la red que ha solicitado.

- Access- Challenge o reto de acceso es denominado de esta manera porque se solicita información adicional al usuario por ejemplo el PIN, una contraseña secundaria además de la implementación de diálogos de autenticación entre el usuario y el servidor RADIUS mediante túneles seguros entre ellos. Todo esto para que las credenciales y accesos tengan más seguridad además de estar ocultos para el servidor de acceso a la red llamado NAS.

- Access- reject o acceso rechazado nos quiere decir que el acceso al usuario es rechazado por distintos motivos como, que la cuneta del usuario esta desactivada o sea desconocida o a su vez proporcionar una prueba inválida de identificación.

1.3.3. Esquema de autenticación del protocolo RADIUS

RADIUS está basado en un modelo cliente-servidor, ya que escucha y espera de forma pasiva las solicitudes de sus clientes a las que responderá de una manera inmediata, en este modelo el cliente, en este caso es el responsable del envió y de la correcta recepción de las solicitudes de acceso y es el servidor RADIUS de verificar las credenciales del usuario y de ser correctas, de enviar al Network Access server, los parámetros de conexión necesarios para prestar el servicio (Sanchez, G, 2012).

Para configurar el protocolo RADIUS debemos tener en cuenta que hay varias maneras de configuración, en el método de autenticación podemos encontrar condiciones de protocolo que soporta PPP tales como EAP (Extensible Authentication Protocol), PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol) y para su origen de información puede soportar: una base de datos del sistema o una base de datos interna del propio servidor RADIUS, mecanismos PAM y otros como Active Directory, LDAP y Kerberos.

Todo protocolo Radius cuenta con configuraciones de autenticación y autorización por lo cual tiene que pasar por el proceso antes mencionado de un cifrado de la contraseña conocido únicamente por ellos además de que esta contraseña será encriptada a través de un algoritmo basado en RSA (Message Digest Algorithm MD5) esas medidas de seguridad, el método de autenticación y autorización consta de otros atributos como: el nombre del usuario, la ID del cliente y el puerto por la cual el cliente desea acceder. (Alonso, 2013 pág. 47)

Una vez que se verifica que todos los atributos del protocolo se hayan cumplido, el servidor ya puede responder al usuario con una prueba de acceso o (Access-Challenge), este proceso se realizará mediante mensajes donde dará la notificación al usuario para completar el proceso de la autorización. La respuesta a la prueba de acceso debe ser de 0 o 1 y si el usuario desea otra solicitud, el servidor responderá con un Acces-Accept, o un Access-Reject, Si el proceso se cumple satisfactoriamente y con todas sus fases correctas se habrá realizado el proceso de autenticación y autorización completamente, (NETGEAR, 2005).

Si todas las solicitudes fueron correctas y completado este responde con un Acces-Accept, por otra parte, si la autenticación se realiza mediante una prueba de acceso se denomina Acces-challenge y así este le asigna un código único para la identificación y manejo únicamente del servidor y el usuario.

El proceso de autorización el usuario genera una solicitud que es procesada por la NAS y dirigida hacia el servidor local y quien emite la información a un servidor remoto. Una vez recibida y procesada la información, el servidor envía la respuesta la cual puede ser aceptada o rechazada al servidor y quien envía este mensaje a la NAS.

En el caso de que no se cumpla con los debidos procesos y el usuario no cumpla con los atributos de su autenticación el servidor enviara un mensaje de rechazo que le indicara al usuario que su solicitud no es válida.

1.3.3.1. Modelo Cliente-Servidor RADIUS

El protocolo RADIUS sigue un modelo cliente/servidor donde el papel el papel de servidor es desempeñado por RADIUS y es el que contiene información de todos los usuarios, así como el contenido, sus contraseñas y perfiles además del elemento de red llamado NAS que es en este caso el que toma la función de cliente de RADIUS. La NAS tiene la responsabilidad de servir como un mediador entre los mensajes entrantes y salientes desde y hacia el servidor, es decir se encarga de transmitir las solicitudes de conexión, así como las de autenticación, autorización y auditoria y en general toda la información requerida por el usuario. (INFO, 2008)

Manejo de sesiones: Son las notificaciones de inicio/cierre de la conexión; esto es lo que permite que el usuario pueda determinar el consumo y facturación en consecuencia de su uso lo que constituye las principales características de este protocolo.

El usuario envía una solicitud al servidor de acceso a la red denominado NAS para poder tener acceso a un recurso de la red en particular, este envía información que usualmente es una contraseña o el ID del usuario, esta información se transfiere al dispositivo NAS a través de los protocolos de la capa de enlace y de esta manera realiza la petición al servidor Radius solicitando el acceso a la red.

En la siguiente figura se demuestra el modelo cliente servidor donde el usuario solicita la autenticación a través de un punto de acceso convirtiéndose en el cliente RADIUS y realizando la solicitud al servidor Radius.

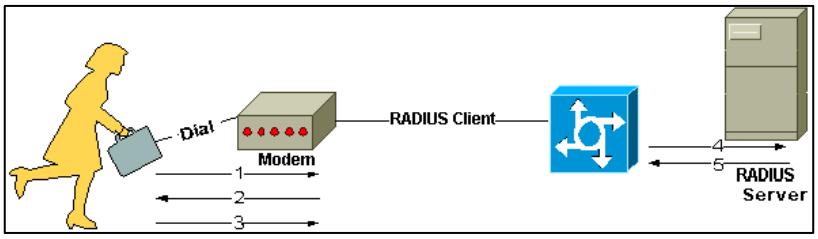


Figura 6-1: Modelo cliente servidor RADIUS

Fuente: (cisco.com)

Toda la información que emite Radius lo envía como datagramas de usuario. Usa el protocolo UDP ya que tiene que ser una comunicación rápida contra el servidor, el puerto que utiliza para la autenticación es el 1812, y para la administración de cuentas y de Radius usa el puerto 1813. (Francesc Perez, 2012)

1.3.3.2. Bases de datos del Servidor RADIUS

El servidor Radius contiene tres bases de datos las cuales son:

Usuarios: Es el que almacena la información del usuario tales como, el nombre de usuario, la contraseña, la dirección IP y finalmente aplica a los protocolos.

Clientes: Es el que almacena la información sobre los clientes Radius es decir su clave compartida.

Diccionario: Es el que almacena la información, pero esta vez para la interpretación de atributos y valores del protocolo Radius.

En el gráfico 4 se detalla mediante un diagrama la base de datos que posee el servidor de Radius para verificar los datos de los usuarios y realizar la autenticación

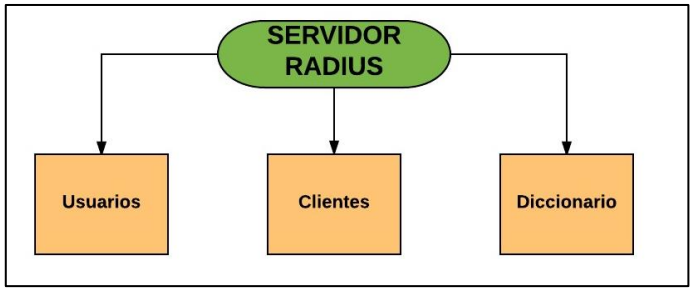


Gráfico 4-1: Bases de datos de Radius

Realizado por: Gabriela Andrade, 2018

Las características del nivel de seguridad se encuentran en los servidores de autenticación, en este caso RADIUS que se denominara como el servicio de usuario de acceso telefónico de autenticación remota. Para cumplir este parámetro se necesitará la correcta instalación y configuración de dicho servidor de autenticación. Pero todo este procedimiento claramente necesitara de una inversión extra y contratación de personal calificado para la instalación y configuración y administración.

El punto de acceso o AP es realizado mediante un login y un password para cada usuario. El servidor de autenticación verificará y validará la información que envía el usuario y según estos datos dará acceso al punto de acceso AP.

1.3.3.3. Cliente RADIUS

En este caso el cliente RADIUS envía credenciales de usuario e información sobre los parámetros de conexión en forma de un mensaje RADIUS al servidor. Este procederá a la autenticación y autoriza la solicitud del cliente y finalmente envía de regreso un mensaje de respuesta. Los clientes RADIUS de la misma manera envían un mensaje de cuentas a los servidores RADIUS (INFO, 2008).

El protocolo RADIUS se ha mantenido como estándar para el control de acceso AAA, autenticación, autorización y auditoria, más sin embargo con el avance de la tecnología se han desarrollado nuevos protocolos con mejores características de esta manera proporcionando escalabilidad y mejor arquitectura por esta razón se realizará un estudio del protocolo TACACS+.

1.4. TACACS+

Para comprender el protocolo TACACS+ debemos saber que antes de este protocolo hay versiones anteriores como TACACS que fue el primer protocolo AAA y que en la actualidad ya es inutilizado ya que siendo CISCO su creador ya no brinda soporte a este protocolo y se ha vuelto casi nulo. TACACS + es un protocolo estándar desarrollado por el Departamento de Defensa de EE. UU., y luego mejorado por Cisco Systems.

TACACS+ (Terminal Access Controller Acces Control System Plus) es un protocolo que ofrece mejores soluciones de control de acceso además se destaca una mejoría en las funciones AAA. Entre las principales características de este protocolo es que funciona con el protocolo de transporte TCP, varias ventajas del protocolo de transporte de TACACS+ está orientado a la conexión logrando así cifrar el tráfico entre servidores.

TACACS+ es un protocolo que funciona bajo el modelo de cliente/servidor y para su transporte utiliza el protocolo TCP por el puerto 49 y utiliza encriptación de credenciales y datos mediante el algoritmo de encriptación MD5 lo que lo hace más seguro y confiable de otros protocolos. Además, que para tener menos carga en el servidor y una mejor detección de caídas en la comunicación puede ser establecida en una sola sesión de cliente/servidor mientras que el servidor o dispositivo de red se encuentren en forma operacional.

Los RFC que tratan sobre TACACS+ son el RFC 1492 de 1993 “Un protocolo de control de acceso, TACACS”, RFC 927 “Opción de Telnet para TACACS” y RFC 2975 de 2000 “Introducción a la gestión de contabilidad o arqueo”. (Mazzei, 2014)

En la siguiente figura se visualiza la validación del usuario para la autenticación mediante un router o un switch que permita realizar la petición al servidor TACACS+

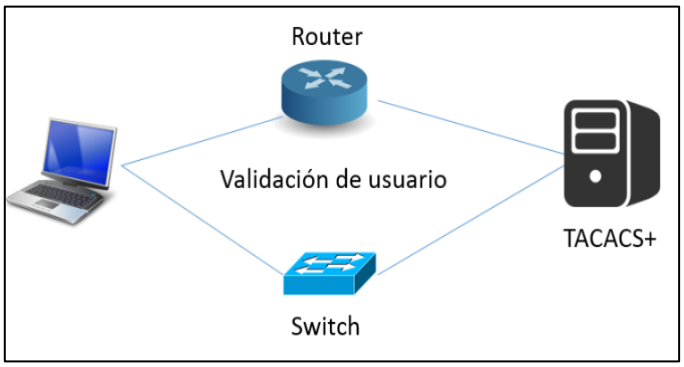


Figura 7-1: Protocolo TACACS+

Fuente: (Soto, 2015)

1.4.1. Operación de TACACS+

TACACS+ realiza los siguientes procesos cuando un usuario intenta acceder hacia su servidor:

Autenticación

El proceso de autenticación del protocolo TACACS+ es manejado por el servidor con su mismo nombre este se da mediante la comunicación que se recopila con la información para poder autenticar al usuario. Usualmente la información recopilada del usuario es el nombre del usuario y la contraseña además de incluir varios ítems proporcionados por el mismo usuario y a petición del servidor como pasatiempos y similares

Aunque el proceso de autenticación puede ser de diferentes maneras una de ellas y la más antigua se compone de un usuario y una contraseña asociada a su nombre relacionándola de forma permanente. La mayoría de los sistemas de autenticación funcionan de esta manera incluido el protocolo TACACS+ sin embargo al permanecer de forma fija este tipo de autenticación existen limitaciones en lo que se refiere a la seguridad. Por lo que los procesos de autenticación actuales permiten el uso de contraseñas con proceso de preguntas y respuestas para que este pueda mejorar significativamente en cuanto a la seguridad de la información además que TACACS+ posee una fortaleza en su seguridad ya que es capaz de soportar estos tipos de autenticación y modelos que aún se encuentran en desarrollo con un poco más de robustez en su seguridad.

Debemos tener en cuenta que en el protocolo TACACS+ no es obligatoria la autenticación, pero

se constituye una opción en su configuración de acuerdo a las necesidades del usuario. En tanto para otras implementaciones es necesario para diversos servicios o condiciones especiales como la relación de inicio de sesión o para permitir la entrada y acceso a una red especifica o si el usuario desea obtener privilegios especiales debe identificarse y darse a conocer al sistema o a otros usuarios que contiene la información requerida.

De igual manera que el protocolo Radius, TACACS+ realiza la comunicación entre el servidor y el usuario por medio de un cliente TACACS+ en este caso el cual brindara el acceso o negara el acceso dependiendo la respuesta del servidor.

En la siguiente figura, se detalla la secuencia que realiza el protocolo TACACS+, en la autenticación y autorización. En primer lugar, un usuario realiza una solicitud a un servidor de acceso (NAS), que requiere autenticación al TACACS+, esta a su vez va a solicitar a través de la (NAS) un usuario y una contraseña, que previamente dichos usuarios deben estar creados en el servidor AAA. Una vez que dichas credenciales sean las correctas, el servidor responde aceptando el ingreso a la información al usuario.

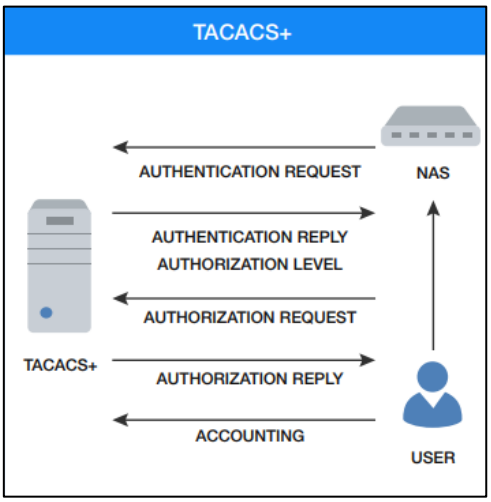


Figura 8-1: Mensajes de autenticación TACACS+

Fuente: (tacacs.net)

La siguiente tabla se detalla los mensajes para la autenticación con el protocolo TACACS+.

Tabla 5-1: Operación de Autenticación de TACACS+

ACCEPT	Acepta la autenticación, si el cliente está configurado para solicitar la autorización
REJECT	Rechaza la autenticación ya que algún ítem está mal proporcionado
ERROR	Informa que ocurrió un error durante la autenticación ya sea en la conexión entre el servidor y el usuario. Después de este mensaje el cliente debe utilizar un método alternativo para realiza la autenticación
CONTINUE	Encomienda al usuario realice autenticaciones adicionales

Realizado por: Gabriela Andrade, 2018

Autorización

La autorización es el proceso que está relacionado a las acciones que realice determinado usuario después de haberse autenticado. Concretamente la autenticación es un proceso que se realiza previamente al proceso de autorización, pero esta condición no es el de el cumplimento obligatorio ya que una petición de autorización se puede realizar sin haberse autenticado es decir no sabe quién es el usuario que va a acceder a la red es decir no podrá acceder a servicio determinados o privilegiados.

"Proporciona un control preciso sobre las capacidades del administrador durante el tiempo sesión del administrador, que incluye, pero no se limita a la configuración de auto comandos, control de acceso, sesión duración o soporte de protocolo. También puede aplicar restricciones a los comandos que el administrador puede ejecutar con la función de autorización TACACS +" (CISCO SYSTEM, 2008)

En TACACS+ el proceso de autorización no se limita a una respuesta de aprobación o rechazo de una solicitud ya que cada usuario puede modificar el servicio y su funcionamiento de una forma concreta.

En este proceso el cliente se contacta con el servidor y recibe la respuesta que en este pueden ser dos el ACCEPT o REJECT.

Tabla 6-1: Operación de Autorización de TACACS+

ACCEPT	En este caso es el que acepta la autorización y posee la información en forma de atributos y determinan a los servicios que tendría acceso el usuario
REJECT	En caso de que la autorización es negada

Realizado por: Gabriela Andrade, 2018

El mensaje ACCEPT contiene atributos como: parámetros de conexión, dirección IP, time-outs para el usuario, ACL, etc. Para el control de acceso a los servicios de la red en cuanto a la

seguridad debe contar con comandos de configuración que restringe de manera correcta los ataques internos. La autorización con comandos se realizará cada vez que el usuario inserte el comando, para que el servidor determine si este es aceptado o rechazado de acuerdo a los datos proporcionados por el usuario.

En la Figura podemos definir la autorización del usuario por medio de la NAS hacia el servidor TACACS+

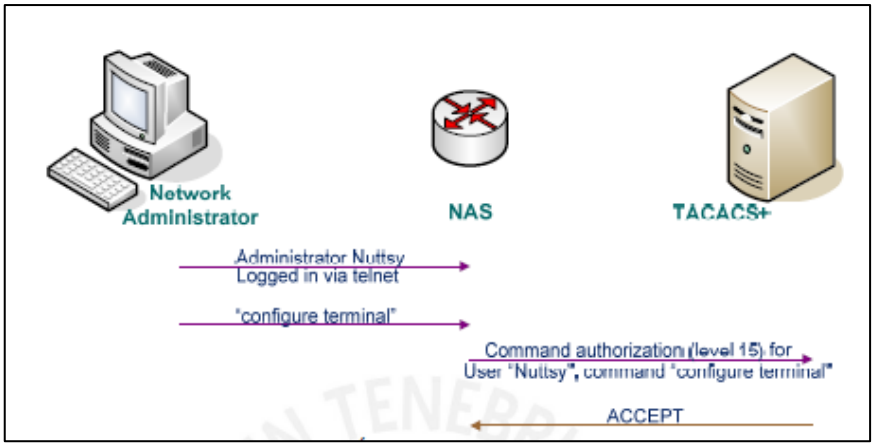


Figura 9-1: Autorización para TACACS+ por medio de comandos

Fuente: "Servidor TACACS+" (CISCO SYSTEM, 2009)

Auditoría

La auditoría es el proceso donde se recopila y envía la información utilizada para facturar, auditar e informar al servidor TACACS+. Los administradores de red pueden usar la función de contabilidad para rastrear la actividad del administrador para una auditoría de seguridad o para proporcionar información del usuario. Los registros de auditoria incluyen las identidades de administrador, tiempos de inicio y finalización, comandos ejecutados como PPP, numero de paquetes y numero de bytes (CISCO SYSTEM, 2008).

Para cumplir el proceso de auditoria en TACACS+ soporta tres tipos de procesos como: el registro de inicio que indican que el servicio está a punto de iniciar, dejar los registros que informa la finalización de un servicio, los registros intermedios que representan los avisos de que un servicio está en proceso de ejecución.

1.4.2. Paquetes TACACS+

En la siguiente figura se muestra el formato de paquete que posee el protocolo TACACS+ y los

bits que contiene cada paquete del protocolo.

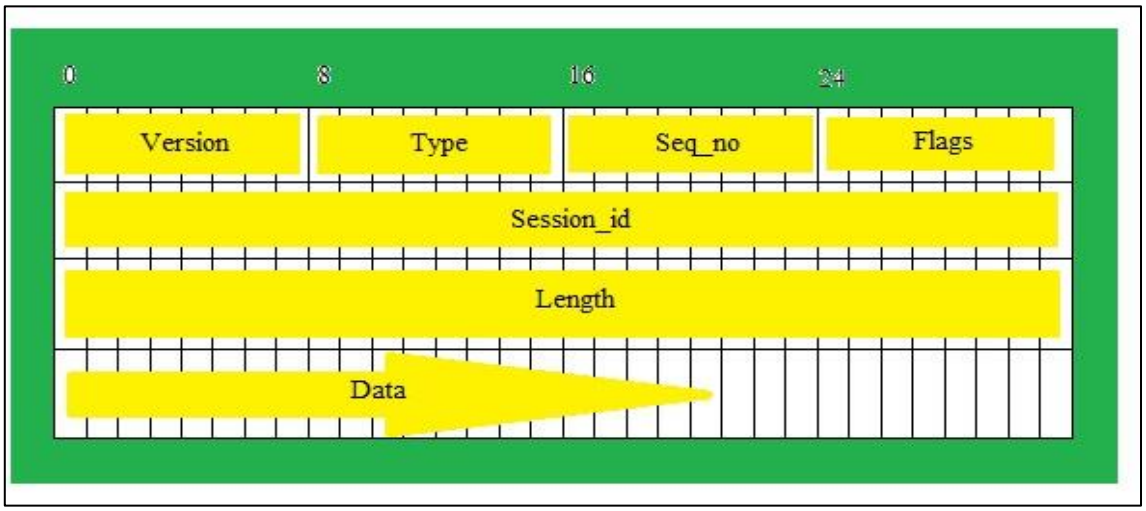


Figura 10-1: Formato de paquetes TACACS+

Fuente: (INFO, 2008)

En el protocolo TACACS+ se intercambian mensajes entre el cliente y el servidor teniendo este un formato específico para realizar este intercambio de mensajes, siendo el siguiente:

Tabla 7-1: Paquetes TACACS+

PAQUETE	**ATRIBUTO**
Versión (Version)	Es el primer octeto y sirve para indicar el número de versión
Typo (Tipo)	Consta de 8 bits para indicar un tipo de mensaje dependiendo de la acción ya sea de autenticación, autorización o auditoria
Seq_no (Numero de secuencia)	Consta de 1 octeto que indica el número de secuencia de paquetes que posee la sesión actual
Flags (Banderas)	Consta de 1 octeto e indica si se encuentras o no datos encriptados
Session_id (identificador de 27ccess)	Consta de cuatro octetos para identificar la sesión de paquetes en respuesta al servidor
Length (Longitud)	Identifica a la longitud del paquete

Realizado por: Gabriela Andrade, 2018

1.4.3. Ventajas de TACACS+

Dentro de las principales ventajas de usar el protocolo TACACS+ son:

- Las credenciales proporcionadas por el usuario no son guardadas en los dispositivos de red
- La contraseña que se provee para ingresar a la red es cifrada por el servidor TACACS+
- Los dispositivos ingresados a la red apuntan a un servidor central, esto es ayuda al

momento de la administración de redes corporativas donde tenemos un gran número de dispositivos de red

- Una mejor protección en contra los ataques de fuerza bruta.

CAPITULO II

2. MARCO METODOLÓGICO

2.1. Comparación de protocolos RADIUS y TACACS+

En la tabla 9 destacamos las diferencias entre el protocolo RADIUS y TACACS+ detallando cada característica que posee cada protocolo así posteriormente poder llegar a elegir el mejor protocolo de seguridad para implementar en una red corporativa según las exigencias que esta requiera.

La principal diferencia funcional entre RADIUS y TACACS + es que TACACS + separa la funcionalidad de autorización y RADIUS combina autenticación y autorización en un solo paquete. Aunque esto puede parecer un pequeño detalle, se refleja una diferencia al implementar el administrador AAA en un entorno de red.

Tabla 1-2: Comparación RADIUS vs TACACS+

	RADIUS	**TACACS+**
Protocolo de transporte	El protocolo RADIUS usa UDP, este protocolo brinda el mejor esfuerzo para entrega de paquetes tiene la necesidad de administrar variables y tiempos de espera para la compensación del transporte y por ende carece del nivel de soporte.	TACACS+ usa TCP este protocolo garantiza un transporte que es dirigido por conexión. TCP garantiza una mayor ampliación el cual se adapta a las redes en crecimiento y congestionadas.
Cifrado de Paquetes	Las características de RADIUS, permite cifrar la contraseña dentro del paquete de solicitud de acceso del modo cliente/servidor, cabe destacar que el resto del paquete no está cifrado, tal como el nombre de usuario.	TACACS+ tiene la capacidad de cifrar todo el cuerpo del paquete y a su vez deja un encabezado estándar de TACACS+, lo que se encuentra dentro del encabezado se puede observar como un campo que indica si se ha cifrado o no. Para la facilitación del debugging, es posible la observar la utilidad que los cuerpos de los paquetes no estén cifrados, sin embargo, durante su funcionamiento normal el paquete puede ser cifrado de manera completa para tener comunicaciones más seguras.
Autenticación y autorización	RADIUS tiene la habilidad de combinar la autenticación y autorización, es por	TACACS+ tiene la capacidad de usar la arquitectura AAA, que separa la autenticación,

	ello por lo que los paquetes 30ccess-accept enviados por el servidor de RADIUS al cliente contienen la información de la autorización, lo que dificulta la tarea de separar lo que es la autenticación y autorización.	autorización y auditoria. En medio de una sesión es necesario una verificación previa a la autorización, el servidor de acceso tiene la función de verificar con un servidor TACACS+ y a su vez determinar si el usuario cuenta con el permiso para usar un comando determinado, con ello tiene un mayor control de comandos determinados y así ejecutarse en el servidor de acceso.
Soporte Multiprotocolo	El componente RADIUS no admite los siguientes protocolos: ● Protocol AppleTalk Remote Access (ARA) ● Protocolo NetBIOS Frame Protocol Control ● Novell Asynchronous Services Interface (NASI) ● Conexión X.25 PAD	TACACS+ ofrece soporte multiprotocolo.
Administración del Router	El protocolo RADIUS por su parte no les permite a los usuarios controlar los tipos de comandos que pueden y no pueden ejecutarse en un router, de tal forma RADIUS no se considera tan útil para ejercer la administración del router y a su vez no es tan flexible para los servicios de terminal.	TACACS+ garantiza dos métodos, en primer lugar, para el control previo a la autorización de los comandos del router por usuario o por grupo, de esta forma su función es asignarle los niveles de privilegio a los comandos y por ende hacer que el router pueda verificar con el servidor TACACS+
Interoperabilidad	RADIUS (RFC) 2865, no garantiza la interoperabilidad, es decir ya que ciertos vendedores adquieren más clientes RADIUS, lo que significa que son interoperables. Por su parte Cisco implementa en su mayoría los atributos de RADIUS.	TACACS+ cuenta con dos métodos distintos para el control de privilegios de usuarios a través del proceso de autorización de comandos permitidos en el enrutador, que puede establecer por usuario o por grupo (Alonso, 2013).

Complejidad y RFC	Los servidores RADIUS son comúnmente licenciados por los usuarios o conexiones del módem, que pueden hacer que el software sea libre. Esto se evidencia por el hecho de que hay más de 40 RFC escritos en RADIUS.	La complejidad en TACACS+ es más visual y sus comandos nos generan la opción de considerar privilegios de administrador TACACS + solo tiene un RFC (927)
Seguridad	La seguridad del protocolo RADIUS entre cliente y servidor es autenticar mediante una clave compartida, que es creada por el administrador, y que debe ser la igual en ambos casos extremos, la cual nunca es enviada a través de la red	El protocolo de autenticación TACACS+ fue desarrollado a partir de la experiencia Cisco con RADIUS. Los mecanismos más robustos fueron creados para manejar los nuevos niveles de seguridad que demandaban las redes modernas. Además, TACACS+ encripta el nombre de usuario y otros datos asociados, es escalable

Realizado por: Gabriela Andrade, 2019

2.2. Cifrado asimétrico para el protocolo RADIUS

En el tipo de cifrado existe una autoridad que maneja las claves públicas del cliente como del servidor, por lo que se realiza es enviar dentro del texto la clave en forma cifrada para el solicitante de la misma, el cual teniendo conocimiento de la clave pública puede descifrar de forma privada este mensaje es reenviado al servidor RADIUS para repetir el procedimiento, si este proceso no tiene errores se da acceso a la red y sus recursos, una aplicación de este tipo es EAP-TLS Transport Layer Security, que utiliza el algoritmo de cifrado asimétrico RSA, de forma bidireccional, a partir de allí se crea el cifrado EAP-TTLS el mismo que establece un túnel encriptado por el que se manejan el transporte de los datos de autenticación.

También se conoce un cifrado PEAP que significa protección EAP que usa el túnel de encriptado descrito anteriormente los cuales los certificados del se5rvidor que funcionan como autenticador son necesarios no así los EAP-TTLS y EAP-PEA, por último, se conoce el cifrado EAP-MSCHAPv2, el cual funciona como usuario y contraseña y se encapsulan en EAP.

El estándar 802.1x con autenticación EAP también funciona para redes inalámbricas para ello se usa el cifrado conocido como WPA para ello existe el tipo de administración donde las claves funcionan juntamente con el estándar 802x/EAP para permitir la autenticación acceso a la red en conjunto con el servidor RADIUS.

En el siguiente gráfico vamos a ver como la trama generada por el estándar 802.1x y el análisis de cada uno de los campos.

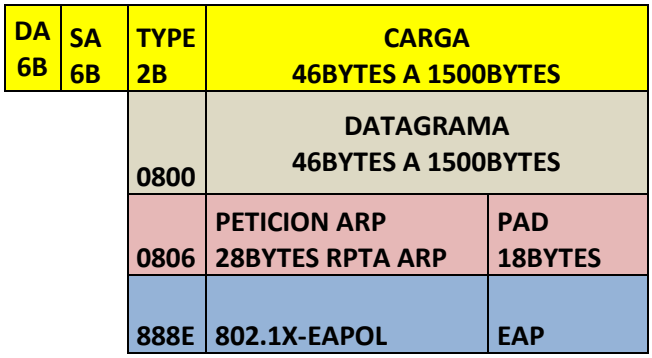


Gráfico 1-2: Trama estándar para 802.1x

Realizado por: Gabriela Andrade, 2019

DA: en este campo tiene la dirección MAC del destino, es decir la dirección del dispositivo que va a finalizar la conexión.

SA: En este campo posee la dirección la dirección MAC de origen

TYPE: Este campo puede variar ya que indica el tipo de conexión que se realiza dónde puede variar y e indica en la siguiente tabla:

Tabla 2-2: Tipo y nombre de atributos

TIPO	NOMBRE
0800	Datagram IP
8006	ARP
8035	RARP
888E	802.1X
8863	Trama DA

Realizado por: Gabriela Andrade, 2019

2.3. Cabecera de claves compartidas EAPOL/EAP

Las claves compartidas entre el usuario y el servidor, donde el servidor usa esta clave para comparar la contraseña del suplicante para permitir el acceso a los servicios. La cabecera EAPPOL/EAP es la aplicación más utilizada para el servidor RADIUS.

Versión de Protocolo: Es el tipo de versión usada por EAPOL la cual es tomada según el que envía datos el valor por defecto es 0000 0001 es decir el tamaño de este campo es de 1 byte.

Longitud del paquete: En este campo tiene el cuerpo en si del paquete y su tamaño es de 2 Bytes

Tipo de paquete: Existen 4 parámetros en este campo los cuales podemos ver el cuadro.

En la siguiente tabla vamos a ver los campos que tiene el protocolo EAP:

Tabla 3-2: Campo tipo de paquete de la trama

TIPO	NOMBRE
Paquete EAPOL	0000 0000
Inicio EAPOL	0000 0001
LogOff EAPOL	0000 0010
Clave EAPOL	0000 0011

Realizado por: Gabriela Andrade, 2019

2.3.1. Cabecera EAP

La cabecera de las claves EAP tiene tres campos que son código, identificador y longitud.

Código: El tamaño de este campo es de 1 Byte en la siguiente tabla se muestra el código y las acciones en el protocolo EAP.

Tabla 4-2: Campo de código EAP

CÓDIGO	**ACCIÓN**
CÓDIGO 1	PETICIÓN
CÓDIGO 2	RESPUESTA
CÓDIGO 3	EAP EXITOSO
CÓDIGO 4	EAP NO EXITOSO

Realizado por: Gabriela Andrade, 2019

Identificador: Es el campo que asocia la respuesta con las peticiones que llegan y su tamaño es de 1 byte.

Longitud: Es el tamaño de todo el paquete EAP y su tamaño es de 2 bytes.

2.4. Escenario de prueba RADIUS

Para el análisis del desempeño de los diferentes protocolos, se implementó un prototipo. El escenario de prueba para la configuración del protocolo RADIUS consta de:

- Switch capa 3 Catalyst 3560

- Router Mikrotik modelo RB951G-2HnD
- Computadoras y smartphones
- Servidor IRON-Wifi
- Servidor Tek-Radius

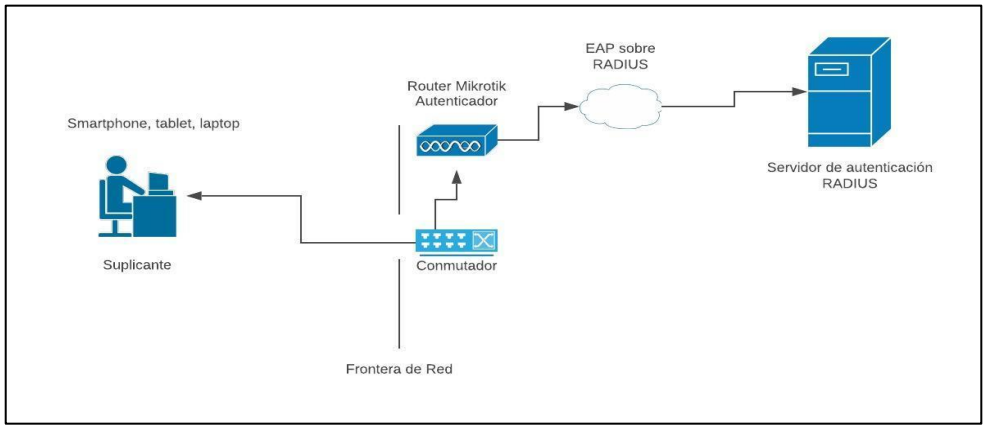


Gráfico 2-2: Topología 802.1x Escenario implementado para pruebas Radius

Realizado por: Gabriela Andrade, 2018

Se presenta en la siguiente figura la implementación del escenario para la configuración de RADIUS donde cada dispositivo procederá su función: el router Mikrotik será el cliente Radius el switch será el NAS (Network Attached Storage) y una laptop en este caso como el dispositivo suplicante para autenticarse.

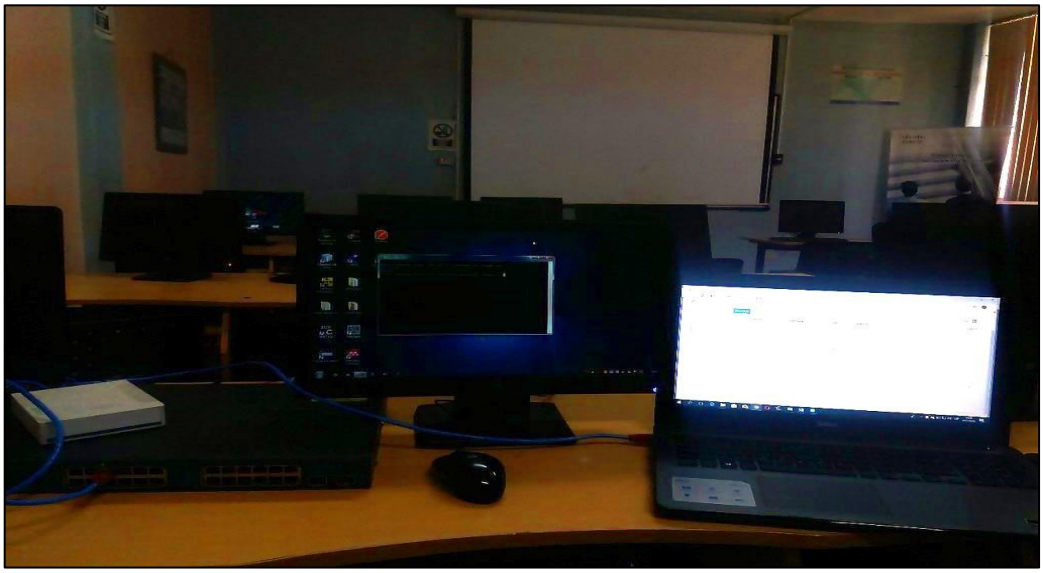


Figura 1-2: Escenario de implementación RADIUS

Realizado por: Gabriela Andrade, 2019

Se realiza un mecanismo específico para la demostración de un escenario para una red la cual

consta de un servidor en este caso gratuito y dado desde la nube y un servidor adicional para el sistema operativo Windows, un switch que cumple la función de NAS (Network Attached Storage) o almacenamiento conectado a la red y un router mikrotik que tiene como función ser el cliente radius con encriptación EAP para poder acceder a la red de esta manera llegando al usuario final o suplicante.

Montar un sistema de seguridad para redes inalámbricas con el fin de restringir el acceso a usuarios finales que no están autorizados para operar en un entorno específico de cualquier red corporativa es primordial para la seguridad de la información.

Se realiza un mecanismo específico para a demostración y levantamiento de un escenario de simulación para una red la cual consta de un servidor en este caso gratuito y dado desde la nube IRON-WIFI, un switch que distribuye por medio de vlans el redireccionamiento de red y un router mikrotik que tiene como función ser el suplicante para poder acceder a la red esta manera llegando al usuario final.

- Dirección del servidor radius
- Servidor Radius (authentication server) = 10.10.1.37
- Ap (authenticator) = 10.10.0.102

2.4.1. Servidor AAA Autenticación RADIUS

El servidor de autenticación Radius será el encargado de autenticar al usuario ya que nos permite ingresar los campos necesarios para que los usuarios puedan acceder a la red. Para ello se ha realizado dos pruebas con diferentes servidores. Uno llamados Iron-Wifi que nos proporciona automáticamente la dirección y puertos que utilizara dicho servidor que lo encontramos en la nube y otro servidor denominado TekRADIUS que es un servidor creado para el sistema operativo Windows que se utiliza de manera local.

2.4.1.1. Servidor Iron-Wifi

IRONWIFI ofrece una solución cloud de Hosted RADIUS servers y Portales Cautivos para la autenticación de redes inalámbricas y puntos de acceso de Internet.

La siguiente figura muestra el icono del servidor en la nube RADIUS Iron-Wifi

Figura 2-2: Servidor IronWfi.

Realizado por: Gabriela Andrade, 2018

- RADIUS como un servicio diseñado para clientes de cualquier tamaño.
- Portal cautivo con soporte para redes sociales.
- SAML, facturación, vales, SMS y más.
- Soporte nativo para dispositivos de más de más de 25 proveedores.
- Conectores a Proveedores de Identidad externos como Google Apps.
- Informes completos y la interfaz de la API REST.
- Listo para ser utilizado con WiFi4EU y Eduroam.

IronWiFi está utilizando la plataforma Google Cloud para atender a clientes en más de 190 países. Están ampliando constantemente la infraestructura global para ayudar a sus clientes a lograr una menor latencia y un mayor rendimiento y para asegurar que sus datos residan sólo en la Región que especifican. A medida que nuestros clientes crecen sus negocios, IronWiFi continuará proporcionando la infraestructura que satisfaga sus requerimientos globales. (bammtech)

2.4.1.2. TEK – RADIUS

TekRadius es un servidor RADIUS para Windows con un servidor DHCP incorporado. TekRADIUS se ha probado en servidores de Microsoft Windows Vista, Windows 7-10 y Windows 2003-2016.

Dicho servidor posee dos ediciones; TekRADIUS (Primera edición; compatible con Microsoft SQL Server) y TekRADIUS LT (Segunda edición; compatible con SQLite) que es la cual con la que realizaremos las pruebas. Este se ejecuta como un servicio de Windows y viene con una interfaz de administración de Windows.

2.4.2. Comparación entre servidores IRON-WIFI vs TEK-RADIUS

Existen algunas diferencias entre los servidores Iron-wifi y Tek-Radius que fueron utilizados en el presente trabajo de titulación.

Tabla 5-2: Comparación de los dos servidores RADIUS

IRON-WIFI	TEK-RADIUS
Posee una plataforma i-cloud	Software gratuito para Windows
Cobertura en 190 países	No tiene restricciones ya que tiene diccionarios de idiomas siempre y cuando sea solo para el sistema operativo Windows
Provee sus propios puertos de autenticación y designa una dirección IP según el país que se encuentra	Cumple especificaciones RFC 2865 Y 2866
Obligatoriamente conectado a el internet	Se puede crear usuario y grupos dentro de una red interna y servidor DHCP
Utilización global, pero por determinado tiempo	Posee una base de datos propia y administración de interfaz

Realizado por: (Andrade Gabriela, 2019)

2.5. Implementación Escenario de Pruebas TACACS+

La presentación del escenario para realizar pruebas del protocolo TACACS+ se representa en el siguiente gráfico.

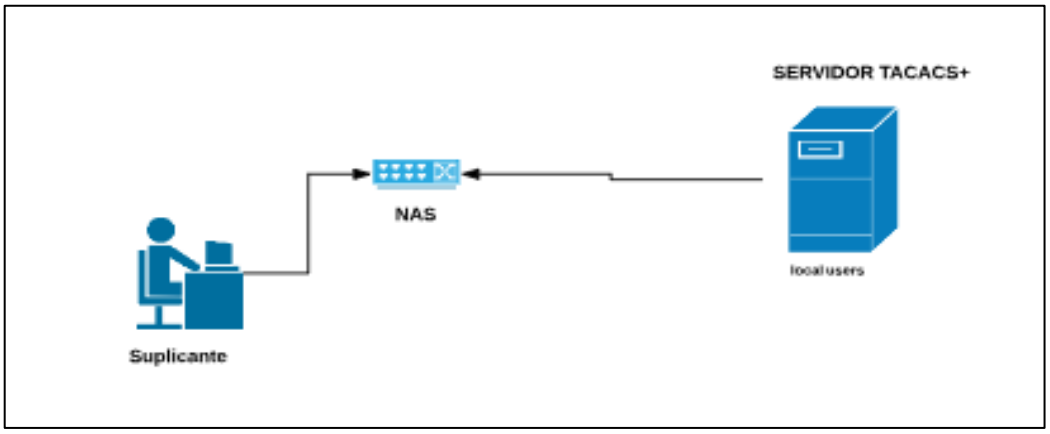


Gráfico 3-2: Topología del escenario de prueba TACACS+

Realizado por: Gabriela Andrade, 2019

En la siguiente figura se muestra el escenario que se utilizó para implementar el protocolo TACACS+ ya que se realizó varias pruebas con switches catalyts y 3560 y routers Cisco donde se configuro todos los comandos para administración del protocolo, es decir se le dio privilegios para que los usuarios puedan autenticarse mediante este protocolo.

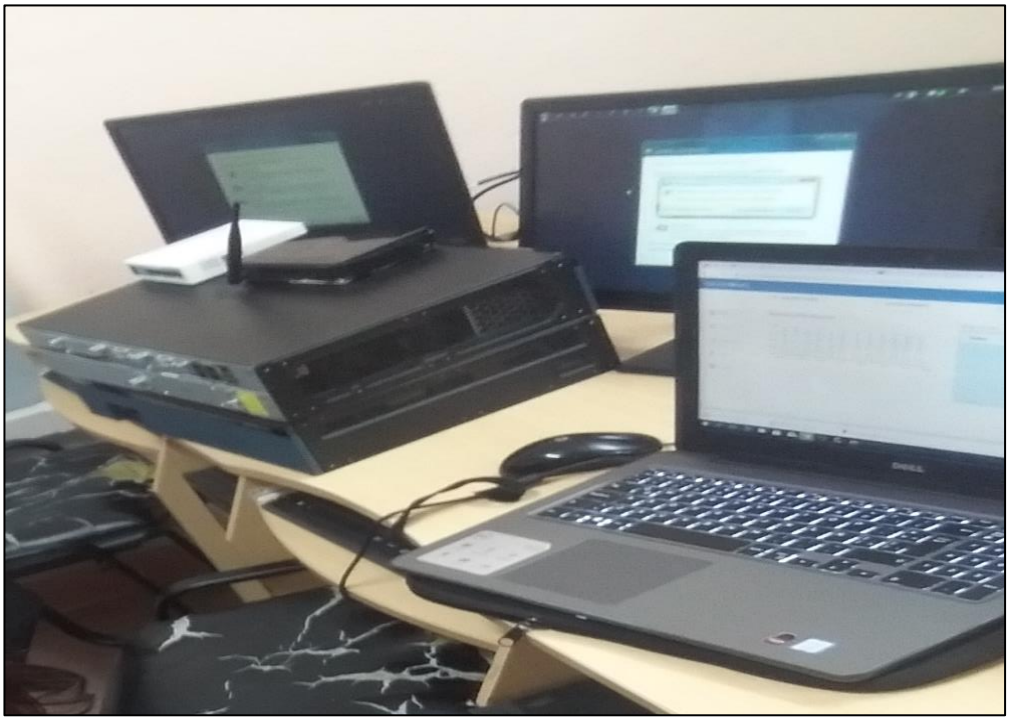


Figura 3-2: Escenario de implementación TACACS+

Realizado por: Gabriela Andrade, 2019

El software que se utilizara para implementar el servidor TACACS+ llamado Tacacs.net que es implementado e instalado en el sistema operativo Windows como un framework propio del sistema.

Una vez instalado este servidor propio del sistema operativo Windows se verificará las carpetas creadas dentro del folder Windows system32 donde están ubicados los frameworks de Windows tomando el nombre de tacac.net que es el propietario de este servidor.

Cuando finaliza la instalación de Tacacs.setup se crearán aplicaciones en los archivos de programas de Windows tales como:

- **Tacdes:** Aplicación tacacs.net que nos da una descripción de la configuración del tacacs.net.
- **Tacplus:** aplicación de arranque del servidor.
- **Tactest:** aplicación para recibir información sobre paquetes Tacacs+ aceptados y rechazados.
- **Tacverify:** aplicación para verificar si las configuraciones de los archivos están modificadas correctamente para que pueda arrancar sin errores la aplicación tacplus

CAPITULO III

3. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En este capítulo se muestra los resultados obtenidos de la investigación realizada en este proyecto. En la cual esta detallado en el capítulo II, presentando los resultados de conexión encriptación y seguridad obtenidos de la implantación del protocolo RADIUS y TACACS+. Considerando el grado de seguridad y accesibilidad para implementar este proyecto en redes corporativas.

A continuación, se representa los resultados de la comparación del desempeño del protocolo RADIUS y TACACS+ y la implementación de sus respectivos servidores

3.1. Escala de Likert para comparación de RADIUS y TACACS+

La principal diferencia funcional entre RADIUS y TACACS + es que TACACS + separa la funcionalidad de autorización y RADIUS combina autenticación y autorización en un solo paquete. Aunque esto puede parecer un pequeño detalle, se refleja una diferencia al implementar el administrador AAA en un entorno de red. Otras diferencias importante entre RADIUS y TACACS+ está en que RADIUS sólo cifra la contraseña en la petición de acceso hasta un máximo de 16 bytes TACACS +, por otra parte, cifra todo el cuerpo del paquete, pero dejará la cabecera TACACS+ intacta. Por ello podemos decir que el cifrado que maneja el protocolo TACACS+ es más robusta que el cifrado usado por el protocolo RADIUS.

A continuación, se presentan las comparaciones según varias características del TACACS+ y RADIUS tomando como referencia la herramienta la escala de Likert para diferenciar y verificar cuál de los dos protocolos es el más conveniente al momento de realizar el levantamiento en una red corporativa.

Tomando como referencia para realizar la escala de Likert se detalla en la siguiente tabla el valor cuantitativo por nivel de seguridad, interoperabilidad, cifrado, autenticación de paquetes administración y complejidad entre los protocolos RADIUS y TACACS+.

Tabla 1-3: Denominación de valores para escala de Likert

DENOMINACION	VALOR CUANTITATIVO
MUY ALTA	5
BUENA	4
MEDIA	3
BAJA	2
MUY BAJA	1

Realizado por: Gabriela Andrade, 2019

En la siguiente tabla se evalúa según la descripción y características que presenta el protocolo Radius y Tacacs+

Los valores se ha proporcionado tomando en cuenta los valores de tiempo de autenticación entre Radius y Tacacs+ que son los de las cabeceras de contraseñas ya que se verifica protocolos de transporte, nivel de seguridad, interoperabilidad, cuantos RFC existen por protocolo separación del protocolo AAA así lo demuestra el un documento registrado como "Análisis del desempeño del protocolo RADIUS en redes inalámbricas" y el valor de la implementación de prueba que se realizó para cada protocolo RADIUS y TACACS+ llevando al final a una numeración subjetiva. (Alejandra Mendoza Carreón, 2010)

Tabla 2-3: Escala de Likert

DESCRIPCION	RADIUS	TACACS+
Protocolo de transporte	2	5
Cifrado de Paquetes	2	4
Autenticación y autorización	4	2
Soporte Multiprotocolo	1	4
Administración del Router	2	4
Interoperabilidad	5	3
Complejidad y RFC	5	2
Seguridad	4	5
Total	25	29

Realizado por: Gabriela Andrade, 2019

Como podemos verificar según la tabla 16 donde se presenta la escala de Likert se determina que Tacacs+ posee mejores ventajas sobre Radius tales como el protocolo de transporte TCP que es más seguro, el cifrado de paquetes en Tacacs+ es total es decir cifre toda la información requerida, Tacacs+ además puede ser administrador del router y es multiprotocolo y finalmente englobando a todo lo antes mencionado Tacacs+ nos ofrece mejores beneficios en cuanto a la seguridad.

Otras diferencias importantes entre RADIUS y TACACS+ está en que RADIUS sólo cifra la contraseña en la petición de acceso hasta un máximo de 16 bytes TACACS +, por otra parte, cifra todo el cuerpo del paquete, pero dejará la cabecera TACACS+ intacta. Por ello podemos decir que el cifrado que maneja el protocolo TACACS+ es más robusta que el cifrado usado por el protocolo RADIUS.

3.2. Guía de implementación de RADIUS y TACACS+

Como objetivo para la implementación del proyecto de titulación se propuso realizar una guía técnica para el levantamiento de los protocolos RADIUS y TACACS+ la cual se detallará paso a paso en los siguientes ítems de la misma manera se presentare gráficos y figuras donde se visualizará las configuraciones respectivas.

3.2.1. Configuración servidor Iron-Wifi

En la especificación 802.1X el solicitante y el autentificador son considerandos Entidades de Autentificación por Puerto (PAEs),en este caso el servidor IRON-WIFI nos proporciona la dirección 35.198.25.46 con los puertos 12013 y 1204 para ala autenticación y autorización respectivamente los puertos no autorizados evitan que el usuario pueda acceder a la red, restringiendo únicamente al envío de marcos de autenticación EAPOL (EAP over LAN) inicializando este proceso antes de permitir paso de tráfico de datos.

En la figura 14 muestra la configuración del servidor y los campos que son necesarios para la conexión con el cliente Radius en este caso con el router mikrotik, como nos muestra campos muy importantes como la IP que será la misma que deberemos configurar en el router, los puertos y la contraseña compartida entre el servidor y el cliente.

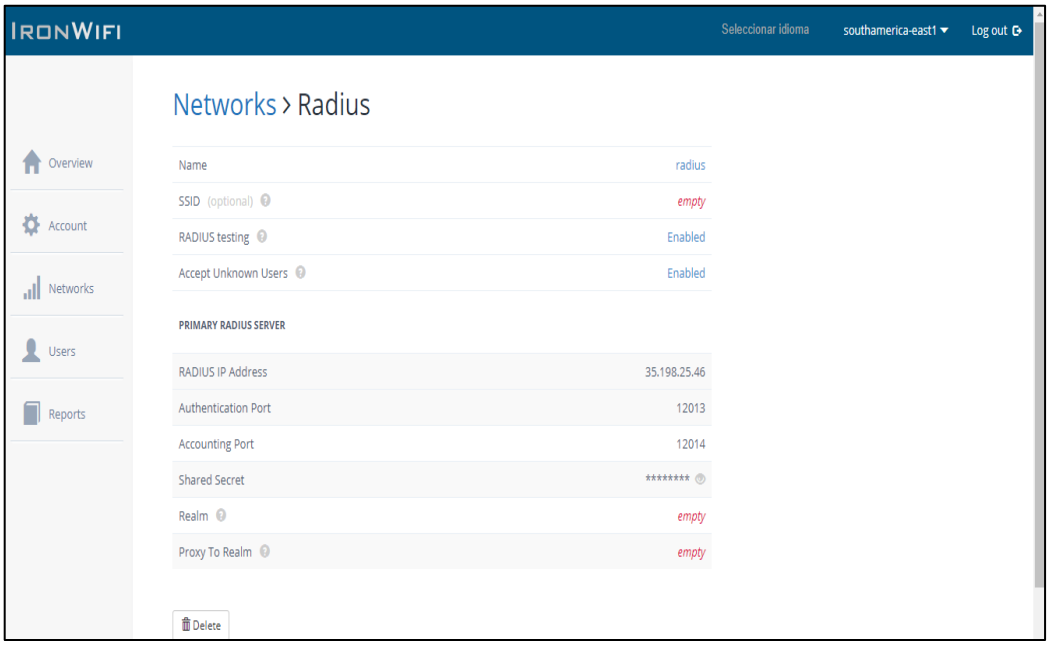


Figura 1-3: Configuración del servidor RADIUS

Realizado por: Gabriela Andrade, 2019

Configurados ya los campos correctamente en el servidor Iron-Wifi (Radius) e identificados puertos contraseña de comunicación con el cliente se procede a crear los usuarios para crear el acceso a la red. En la figura 15 muestra 8 usuarios creados para realizar todas las pruebas de autenticación.

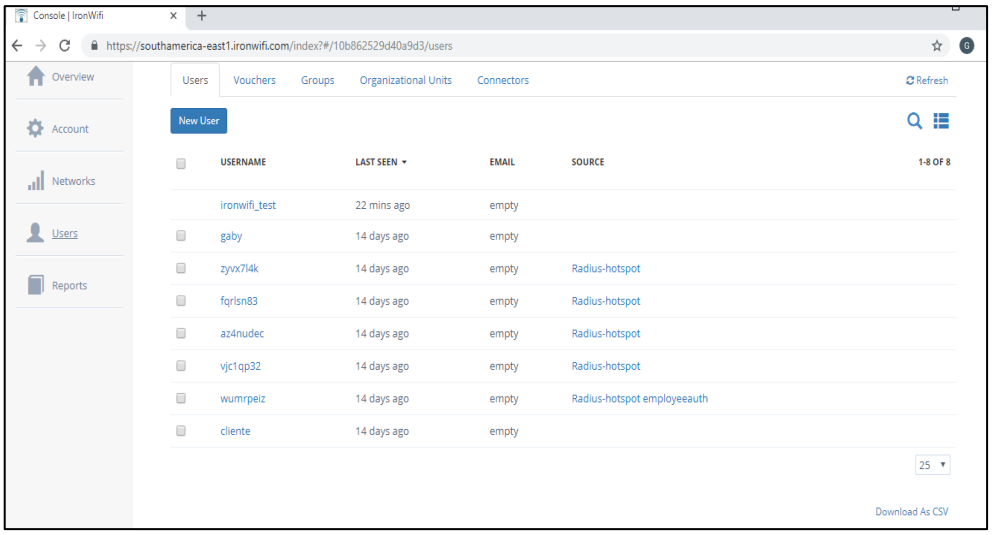


Figura 2-3: Creación de varios usuarios

Realizado por: Gabriela Andrade, 2019

Todo en cuanto a las configuraciones del servidor en la nube denominado Iron-Wifi procedemos a la configuración del cliente que en este caso será nuestro router mikrotik modelo RB951G-2HnD. Visualizamos en la figura 13 como está configurado el mikrotik con la dirección, contraseña compartida entre el servidor y el cliente y los puertos de autenticación.

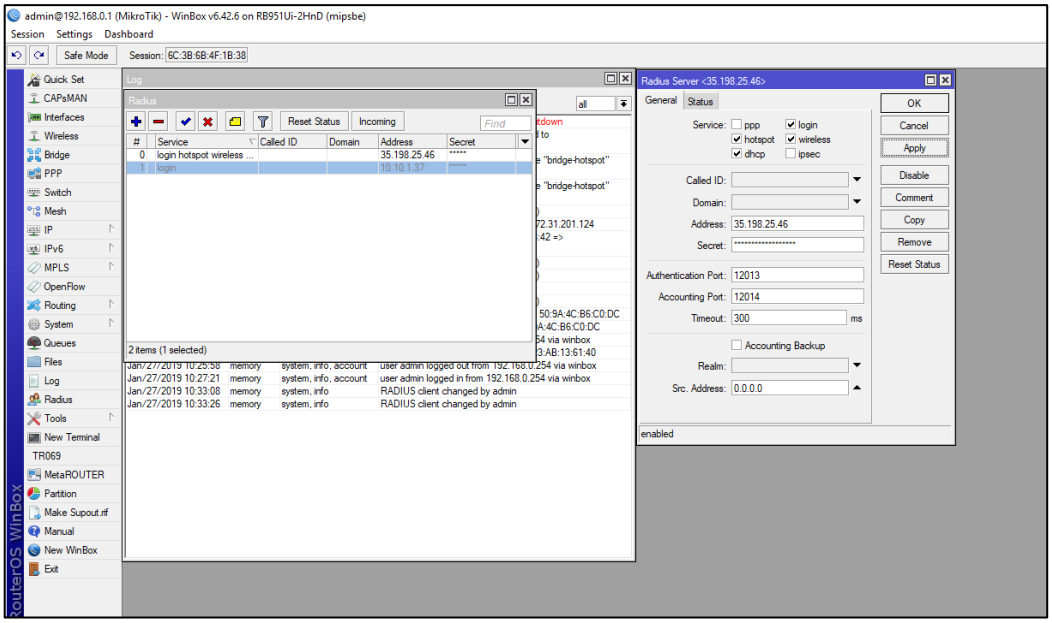


Figura 3-3: Configuración de router mikrotik

Realizado por: (ANDRADE, Gabriela 2019)

El switch cisco 3560 capa 3 realizara su función de frontera de red en la cual utilizaremos las siguientes configuraciones

Para realizar las configuraciones entramos en modo consola al switch donde utilizamos los comandos de dot1x y AAA- new model para activar el protocolo radius y que cumpla la función de frontera de red.

Switch (config)#interface fastEthernet 0/5
Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan 1
Switch (config-if)#spanning-tree portfast
Switch (config-if)#exit
Switch (config)#interface range fastEthernet 0/1 , fastEthernet 0/7
Switch (config-if-range)#switchport mode access
Switch (config-if-range)#switchport voice vlan 1
Switch (config-if-range)#dot1x port-control auto
Switch (config-if-range)#dot1x host-mode multi-domain
Switch (config-if-range)#dot1x guest-vlan 1
Switch (config-if-range)#dot1x auth-fail vlan 1
Switch (config-if-range)#dot1x reauthentication
Switch (config-if-range)#dot1x timeout reauth-period 60
Switch (config-if-range)#dot1x auth-fail max-attempts 2
Switch (config)# aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch (config)# aaa authorization network default group radius
Switch (config)# radius-server host 35.198.25.46 port-acc 12013 port-rej 12014 key**********

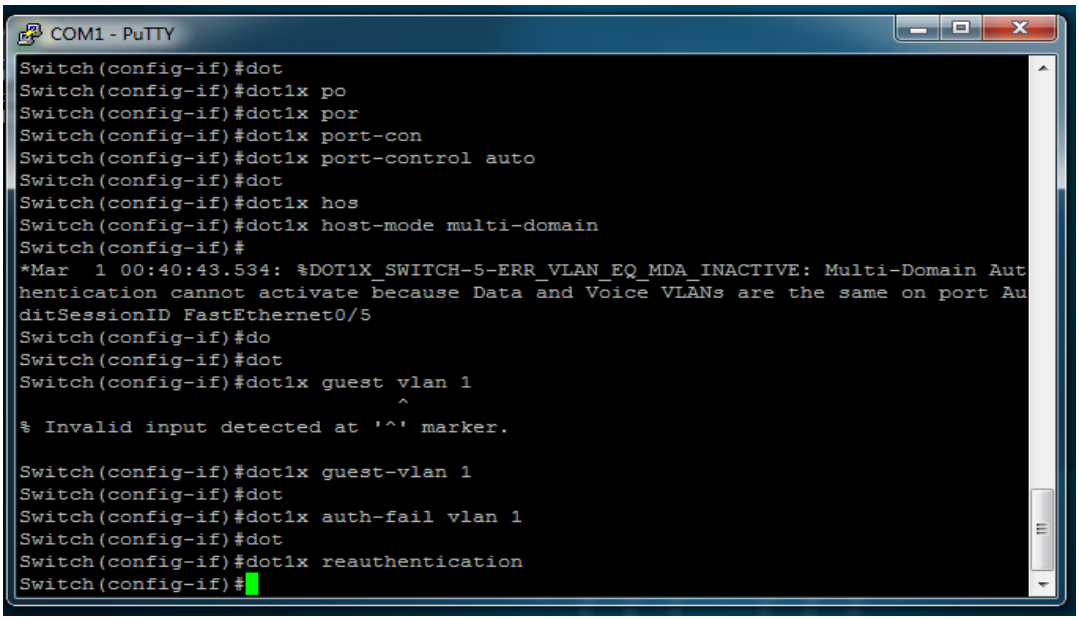


Figura 4-3: Configuraciones de red.

Realizado por: Gabriela Andrade, 2019

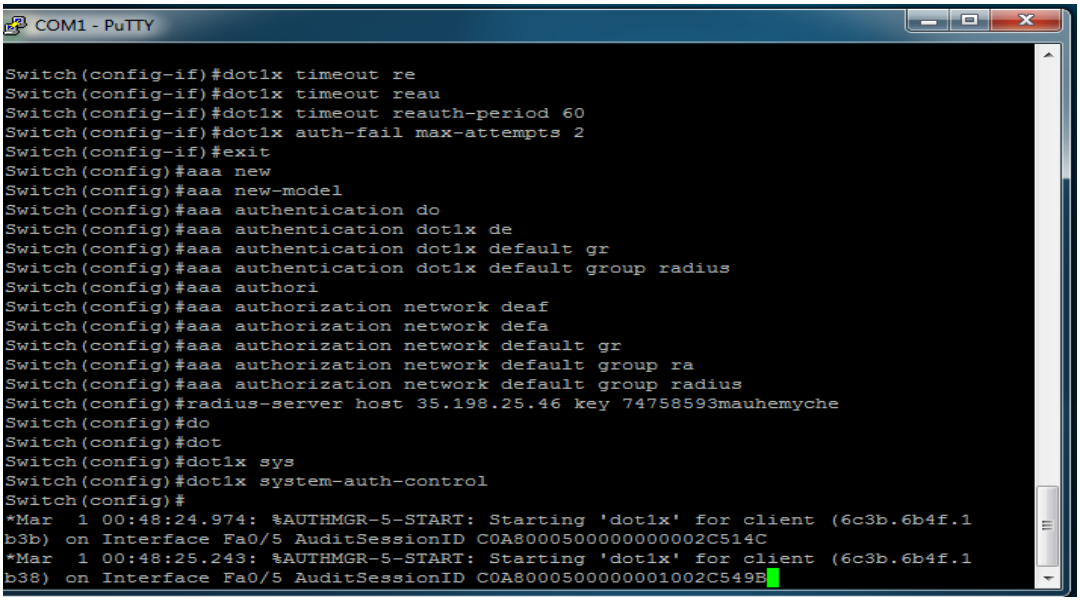


Figura 5-3: Configuraciones de red

Realizado por: Gabriela Andrade, 2019

Una vez realizado esto para una computadora con sistema operativo Windows deberemos activar el modo autenticación 802.1x demostrado en la figura 19.

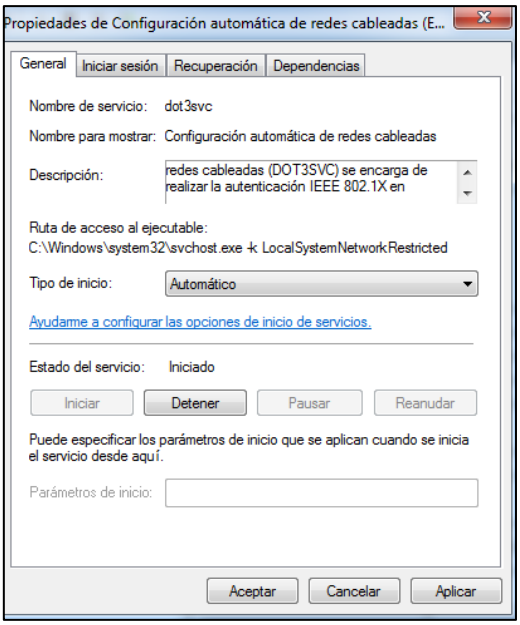


Figura 6-3: Activando modo autenticación 802.1x

Realizado por: Gabriela Andrade, 2019

Finalmente una vez realizado los cambios y configuraciones respectivas se realizan las pruebas de autenticación, de parte del suplicante en este caso una laptop con conexión inalámbrica también pruebas en smartphones con los usuarios creados en el servidor radius Iron-Wifi . Visualizamos en la siguiente imagen que para conectarnos a la red nos solicita nuestro usuario y contraseña mismas que deben coincidir los creadas anteriormente en la siguiente figura.

En la siguiente figura demostramos la validacion del usuario creado con el nombre de “gaby” con su respectiva contraseña, realizada esta prueba con los 10 usuarios que se ha creado en el servidor Iron-wifi con éxito en la autenticacion.

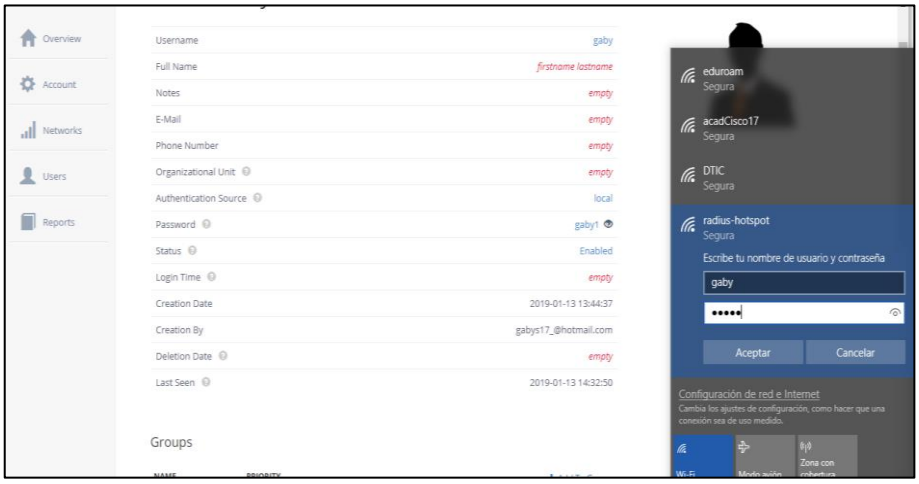


Figura 7-3: Autenticación del usuario y acceso a la red

Realizado por: Gabriela Andrade, 2019

Se realizo varias pruebas una de ellas consta en introducir erróneamente la contraseña o el usuario para que no se pueda autenticar de y pruebas introduciendo los datos del usuario designado correctamente se autentique y tenga acceso a la red en este proceso el router mikrotik tiene la característica de verificar el estado en que el usuario intento autenticarse y si fallo o lo logro demostrándolo en los paquetes REJECT- ACCEPT – PENDING- y REQUEST.

Así se ha demostrado en la siguiente figura, contabilizando cuantas veces ha sido autenticado algún usuario de la misma manera existe contador de cuantas veces el usuario fue rechazado o transmitió paquetes RADIUS

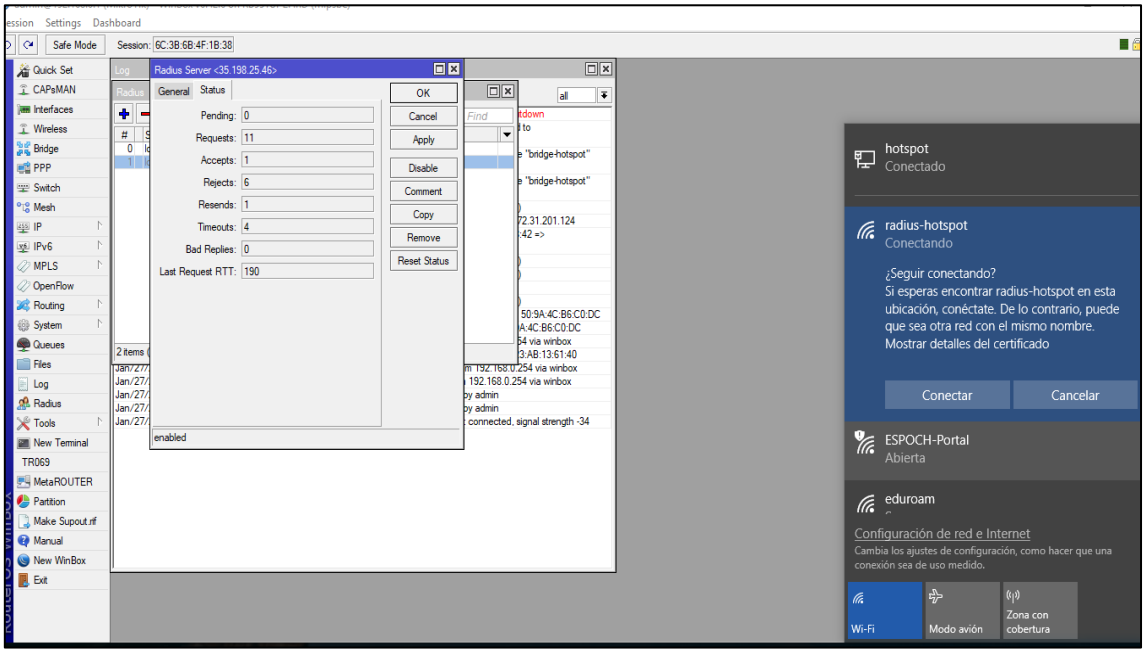


Figura 8-3: Paquetes RADIUS pendientes rechazados aceptados

Realizado por: Gabriela Andrade, 2019

3.2.2. Configuración servidor TekRadius

Los mismos procedimientos se realizo con el servidor Tek-Radius que utilizamos de la misma manera para realizar las pruebas la diferencia entre el servidor Iron-wifi y Tek radius son que iron-wifi es un servidor en la nube que permite directamente la conexión a la internet mientras que tek-radius es un servidor propio y estable para l sistema Windows y se detalla a continuacion las configuraciones del servidor.

En la siguiente figura se muestra las consfiguraciones del servidor Tek-Radius y de la misma manera la configuracion del router mikrotik.

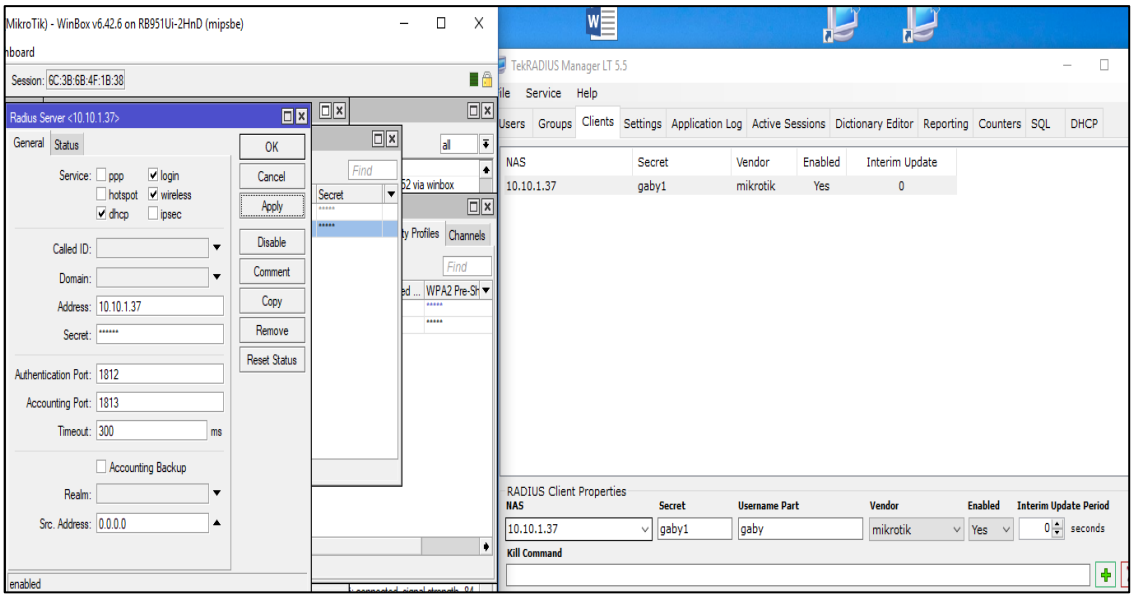


Figura 9-3: Configuraciones del servidor

Realizado por: Gabriela Andrade, 2019

En la siguiente figura se muestra el usuario creado en el servidor Tek-Radius ya que como en el anterior caso se creó vario usuarios en este servidor nos da la opción de crear todo un grupo que tendrá los mismos privilegios de autenticación.

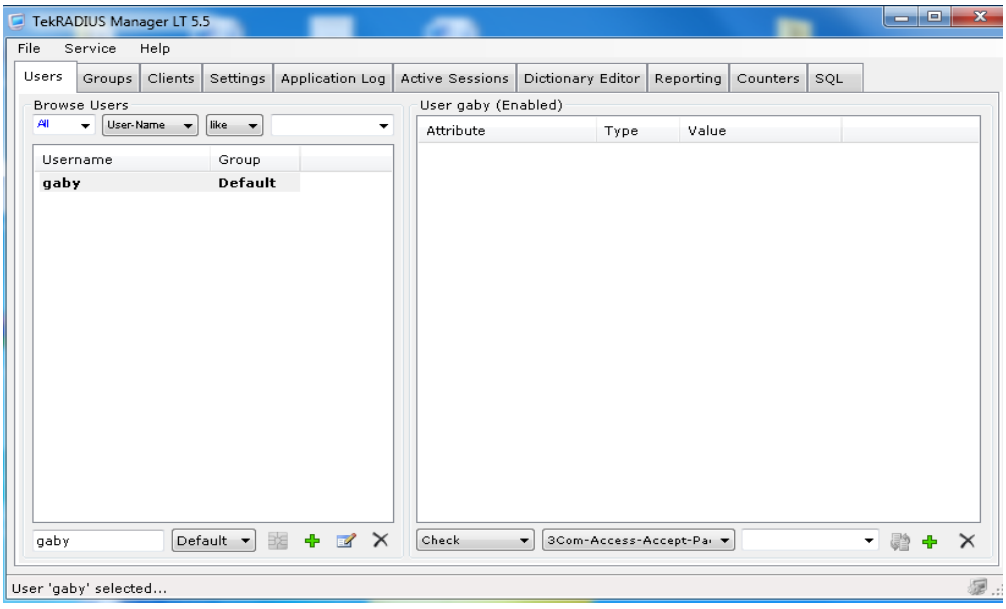


Figura 10-3: Configuración Tek-Radius

Realizado por: Gabriela Andrade, 2019

En la siguiente figura se muestra las veces que los usuarios creados en el servidor Radius fueron aceptados, rechazados o estan pedientes

Asi lo detalla que se encuentra 0 usuarios pendientes a que se autentiquen, el servidor ha dado 11 respuestas de autenticacion, 1 paquete fue aceptado por el servidor Radius, 6 veces dio un mensaje de rechazo o se introdujeron mal las claves de autenticacion, 1 vez fue reenviada una clave de autenticacion, 4 usuarios estan a la espera de ser autenticados y finalmente que se ha realizado 190 peticiones de autenticacion

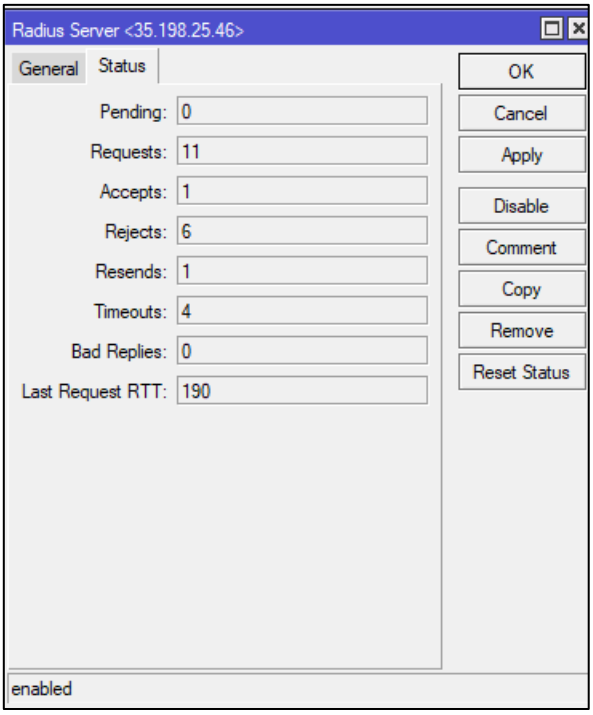
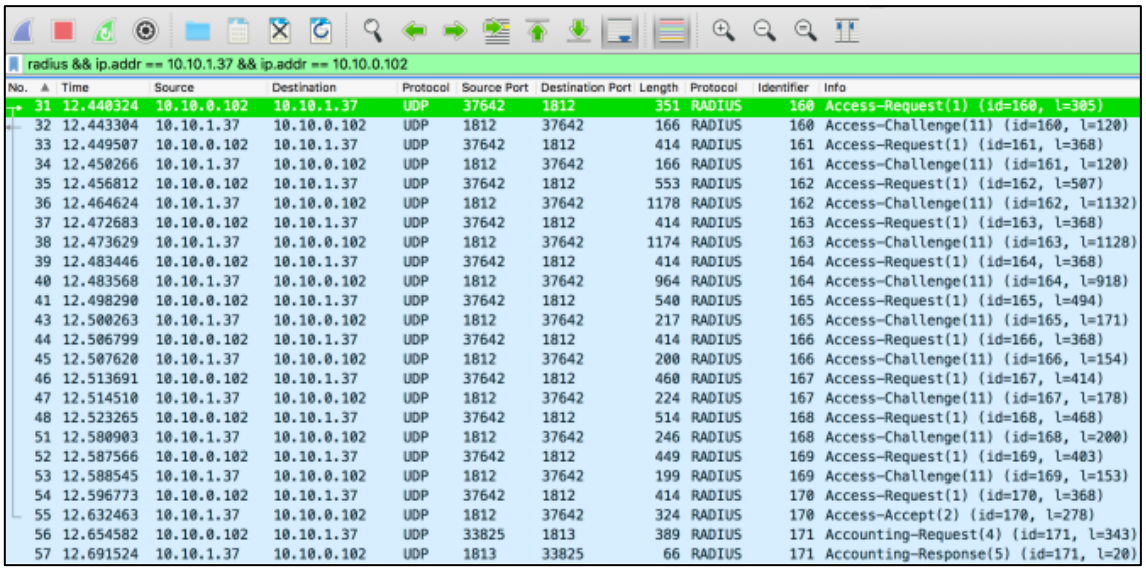


Figura 11-3: Pruebas de aceptación y rechazo de RADIUS

Realizado por: Gabriela Andrade, 2019

Al momento de iniciar el funcionamiento del servicio, en la PC en la que se tiene configurado, Tek-RADIUS entra en marcha como servidor de autentificación, detectando al enrutador como el servidor de acceso a la red, y comienzan a intercambiar paquetes para reconocerse dentro de la red. Esperando el momento en que un usuario realice una solicitud de servicios, en ese momento comienza la transferencia de paquetes RADIUS figura 23, que en el capítulo anterior se mencionan, con el fin de realizar una conexión a la red y obtener los servicios de ésta, se podrán capturar los paquetes que viajan entre el servidor y el control de acceso.

Si se quisiera extraer alguna información de éstos, para realizar una suplantación de usuarios, en principio no se comprendería nada, porque la información que proporciona una entidad certificante en este caso realiza una encriptación MD5, así como también sobre EAP y puede incluirse una clave de tipo WEB.



radius && ip.addr == 10.10.1.37 && ip.addr == 10.10.0.102

No.	Time	Source	Destination	Protocol	Source Port	Destination Port	Length	Protocol	Identifier	Info
31	12.440324	10.10.0.102	10.10.1.37	UDP	37642	1812	351	RADIUS	160	Access-Request(1) (id=160, l=305)
32	12.443304	10.10.1.37	10.10.0.102	UDP	1812	37642	166	RADIUS	160	Access-Challenge(11) (id=160, l=120)
33	12.449507	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	161	Access-Request(1) (id=161, l=368)
34	12.450266	10.10.1.37	10.10.0.102	UDP	1812	37642	166	RADIUS	161	Access-Challenge(11) (id=161, l=120)
35	12.456812	10.10.0.102	10.10.1.37	UDP	37642	1812	553	RADIUS	162	Access-Request(1) (id=162, l=507)
36	12.464624	10.10.1.37	10.10.0.102	UDP	1812	37642	1178	RADIUS	162	Access-Challenge(11) (id=162, l=1132)
37	12.472683	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	163	Access-Request(1) (id=163, l=368)
38	12.473629	10.10.1.37	10.10.0.102	UDP	1812	37642	1174	RADIUS	163	Access-Challenge(11) (id=163, l=1128)
39	12.483446	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	164	Access-Request(1) (id=164, l=368)
40	12.483568	10.10.1.37	10.10.0.102	UDP	1812	37642	964	RADIUS	164	Access-Challenge(11) (id=164, l=918)
41	12.498290	10.10.0.102	10.10.1.37	UDP	37642	1812	540	RADIUS	165	Access-Request(1) (id=165, l=494)
43	12.500263	10.10.1.37	10.10.0.102	UDP	1812	37642	217	RADIUS	165	Access-Challenge(11) (id=165, l=171)
44	12.506799	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	166	Access-Request(1) (id=166, l=368)
45	12.507620	10.10.1.37	10.10.0.102	UDP	1812	37642	200	RADIUS	166	Access-Challenge(11) (id=166, l=154)
46	12.513691	10.10.0.102	10.10.1.37	UDP	37642	1812	460	RADIUS	167	Access-Request(1) (id=167, l=414)
47	12.514510	10.10.1.37	10.10.0.102	UDP	1812	37642	224	RADIUS	167	Access-Challenge(11) (id=167, l=178)
48	12.523265	10.10.0.102	10.10.1.37	UDP	37642	1812	514	RADIUS	168	Access-Request(1) (id=168, l=468)
51	12.580903	10.10.1.37	10.10.0.102	UDP	1812	37642	246	RADIUS	168	Access-Challenge(11) (id=168, l=200)
52	12.587566	10.10.0.102	10.10.1.37	UDP	37642	1812	449	RADIUS	169	Access-Request(1) (id=169, l=403)
53	12.588545	10.10.1.37	10.10.0.102	UDP	1812	37642	199	RADIUS	169	Access-Challenge(11) (id=169, l=153)
54	12.596773	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	170	Access-Request(1) (id=170, l=368)
55	12.632463	10.10.1.37	10.10.0.102	UDP	1812	37642	324	RADIUS	170	Access-Accept(2) (id=170, l=278)
56	12.654582	10.10.0.102	10.10.1.37	UDP	33825	1813	389	RADIUS	171	Accounting-Request(4) (id=171, l=343)
57	12.691524	10.10.1.37	10.10.0.102	UDP	1813	33825	66	RADIUS	171	Accounting-Response(5) (id=171, l=20)

Figura 12-3: Transmisión de paquetes radius Protocolo UDP

Realizado por: Gabriela Andrade, 2019

3.3. Configuración del Servidor TACACS+

En el término de la instalación al igual que el Servidor Radius nos pide una contraseña compartida entre el servidor y el cliente para posteriormente utilizar esta misma contraseña para configurar en el switch 3560 catalyst capa 3.

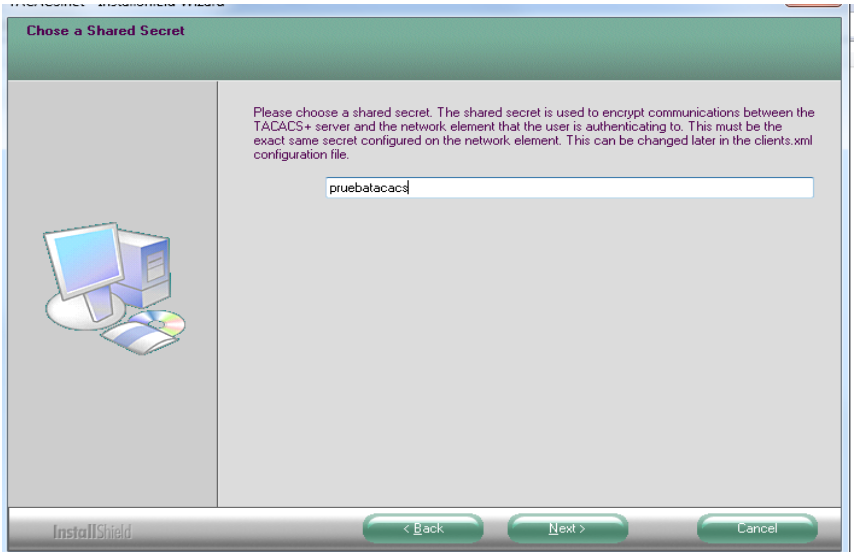


Figura 13-3: Contraseña compartida TACACS+

Realizado por: Gabriela Andrade, 2019

Ahora se puede acceder a los archivos de configuración desde el menú Programas en Inicio>

Todos los programas> TACACS.net> Configuración. Estos archivos están en formato XML y son fáciles de modificar con cualquier editor de texto como Bloc de notas o Wordpad o un editor de XML. Todos los archivos son leídos por el software de forma lineal (de arriba a abajo), así que, si hay un conflicto, la primera entrada tendrá prioridad.

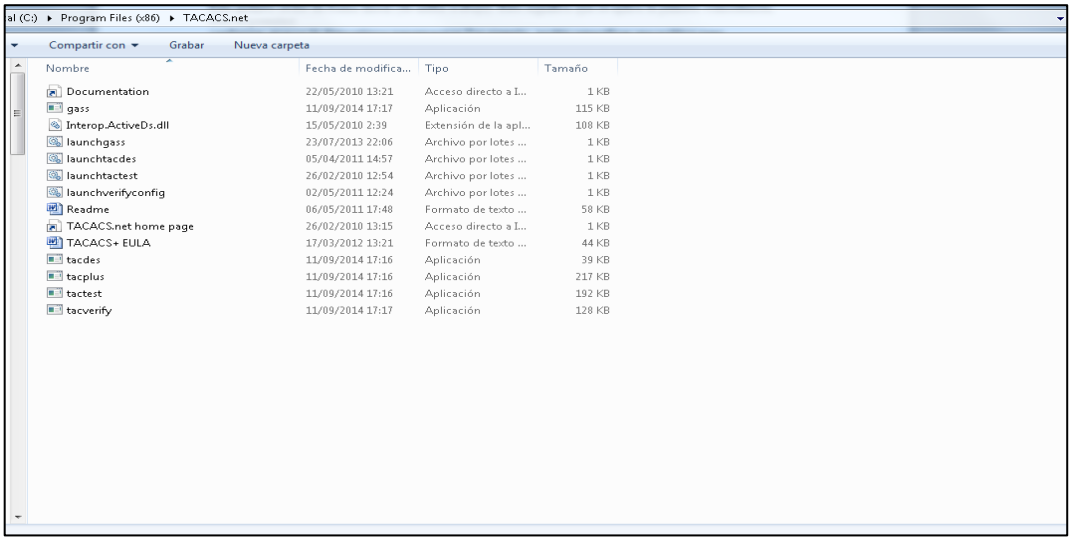


Figura 14-3: Aplicaciones de tacacs.net

Realizado por: Gabriela Andrade, 2019

3.3.1. Configuración de la autenticación utilizando usuarios Localhost

Adicionalmente se modifica también los archivos .xml que se crean en la instalación ya que ahí se modifica la dirección del servidor contraseñas y clientes TACACS+.

Los usuarios de localhost son usuarios configurados dentro de Usuarios y grupos de Windows en la computadora local. Estos son las cuentas de usuario que están autorizadas para iniciar sesión en este equipo local desde el inicio de sesión estándar de Windows pantalla. Esto no se aplica a los usuarios configurados dentro de Active Directory en un controlador de dominio. Esto es un escenario común si TACACS + se ejecutará desde una computadora en un entorno de laboratorio.

El ejemplo proporcionado (Administradores de sistemas locales) está habilitado de forma predeterminada para permitir la prueba y la verificación. Hacer modificaciones a este ejemplo para satisfacer las necesidades de su instalación. Por ejemplo, modifique el <Nombre> para que coincida con el nombre que le gustaría usar para este grupo Modifique el <LocalhostGroupName> para que coincida con el nombre del Grupo de usuarios en Usuarios y grupos de Windows que le gustaría usar para la autenticación.

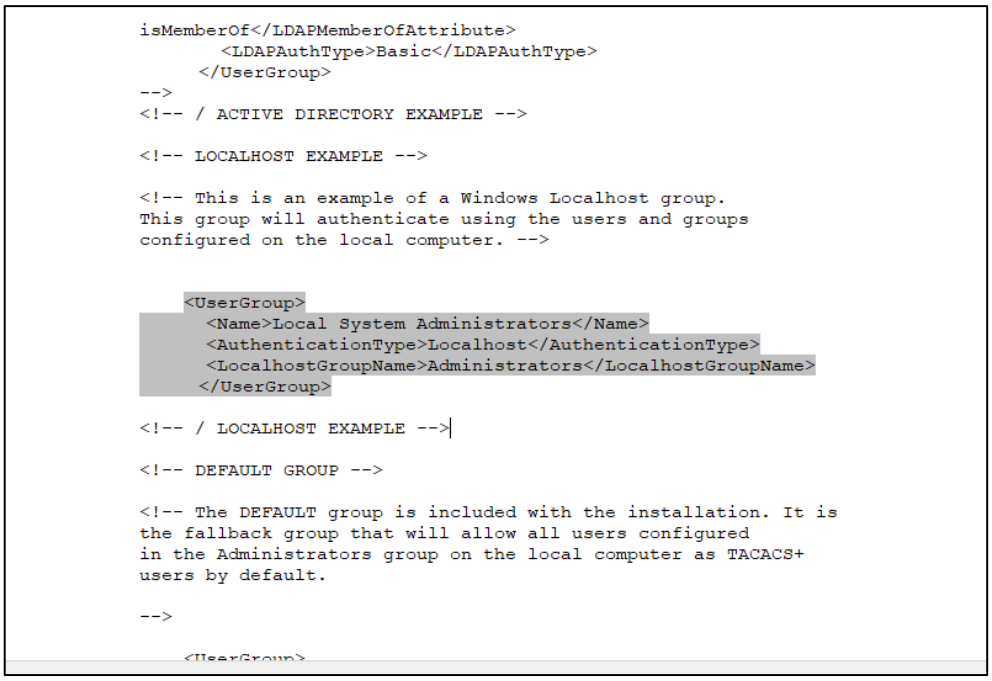


Figura 15-3: Aplicaciones de tacacs.net

Realizado por: Gabriela Andrade, 2019

3.3.2. Configuración Clientes TACACS+

Un cliente TACACS + es un enrutador, conmutador, firewall u otro dispositivo de red que enviará la autenticación de solicitudes al servidor TACACS +. Los clientes también se denominan a veces NAS (Servidor de acceso a la red). Para que un cliente trabaje con TACACS +, el servidor necesita saber que un cliente específico es autorizado para enviar solicitudes. Estas configuraciones están en un archivo llamado clientes.xml. Los clientes también pueden ser utilizados con la configuración de autorización para especificar políticas por cliente o tipo de cliente.

Este archivo de configuración admite expresiones regulares. Esto le da al administrador flexibilidad adicional en la creación de clientes. Las expresiones regulares pueden ser útiles cuando desea establecer una política basada en nombres de host en lugar de direcciones IP.

```
the TACTest test tool. -->
          <ClientGroup Name="LOCALHOST">
               <Secret ClearText="12345" DES=""></Secret>
               <Clients>
                    <Client>127.0.0.1</Client>
               </Clients>
          </ClientGroup>
          <!-- INTERNAL GROUP

The INTERNAL Group is added by default. This group will
 enable all non-routeable IP addresses to be TACACS+
 clients without having to explicitly define them.
This is useful in an internal NAT or lab network.-->
          <ClientGroup Name="INTERNAL">
               <Secret ClearText="12345" DES=""></Secret>
               <Clients>
                    <Client>10.0.0.0/8</Client>
                    <Client>172.16.0.0/12</Client>
                    <Client>192.168.0.0/16</Client>
               </Clients>
          </ClientGroup>
          <!-- DEFAULT GROUP

The DEFAULT group is added by default and is used as a
 catch-all group to verify operations of the server.
This group will permit ANY network element to use TACACS+.
This group should be removed or commented out
 before deploying the server in a production environment.-->
          <ClientGroup Name="DEFAULT">
               <Secret ClearText="12345" DES=""></Secret>
               <Clients>
```

Figura 16-3: Clientes Tacacs.net

Realizado por: Gabriela Andrade, 2019

3.3.3. Configuración dirección servidor Tacacs.net

Finalmente, en el archivo tacplus.xml se modifica la dirección del servidor para la autenticación de los suplicantes. La comunicación de TACACS + está cifrada de forma predeterminada, por lo que he incluido la clave TACACS + para que pueda ver la información descifrada

```
If you have multiple physical or virtual NICs, you will need to
manually hard code the IP address in <LocalIP>,
disconnect any open sessions, and restart the service. You will
also need to use the -s switch in TACTest.

The following logging levels are available: Alert, Critical,
Error, Warning, Notice, Information, and Debug.
Debug generates the most information, and Alert generates the
least amount of logging information.
-->
<Server xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>49</Port>
  <LocalIP>10.10.1.10</LocalIP>
  <DisabledPrompt>This account has been
disabled</DisabledPrompt>
  <PasswordPrompt>Password: </PasswordPrompt>
  <UserNamePrompt>Username: </UserNamePrompt>
  <ExpiredPasswordPrompt>The password for this account has
expired</ExpiredPasswordPrompt>
  <IncorrectPasswordPrompt>Incorrect
Password</IncorrectPasswordPrompt>
  <IncorrectUserOrPasswordPrompt>Invalid username or incorrect
password</IncorrectUserOrPasswordPrompt>
  <SocketTimeoutSecs>30</SocketTimeoutSecs>
  <AccountingLog RolloverDays="30" RolloverMB="10"
DeleteDays="90" LoggingLevel="Information">  </AccountingLog>
  <DebugLog RolloverDays="30" RolloverMB="10" DeleteDays="90"
LoggingLevel="Debug">  </DebugLog>
  <SystemLog RolloverDays="30" RolloverMB="10" DeleteDays="90"
```

Figura 17-3: Configuración archivo tacplus.xml

Realizado por: Gabriela Andrade, 2019

3.3.4. Configuración de equipos suplicantes

El dispositivo 10.1.1.10 envía un mensaje de recibo y luego envía un paquete TACACS + a 10.1.1.1. Una vez que se descifra este mensaje TACACS +, podemos ver que el servidor TACACS + ahora ha solicitado una contraseña para el usuario: synack.

Una vez configurado todos los campos respectivos para el levantamiento del servidor de Tacacs+ hay configuraciones propias en los equipos donde vayamos a utilizar el protocolo Tacacs+ lo cual se realiza desde el módulo de servicios de Windows ya que como se mencionó anteriormente este servidor se instala en forma de un Update de Windows se procede a realizar la activación. Así se demuestra en la figura 28.

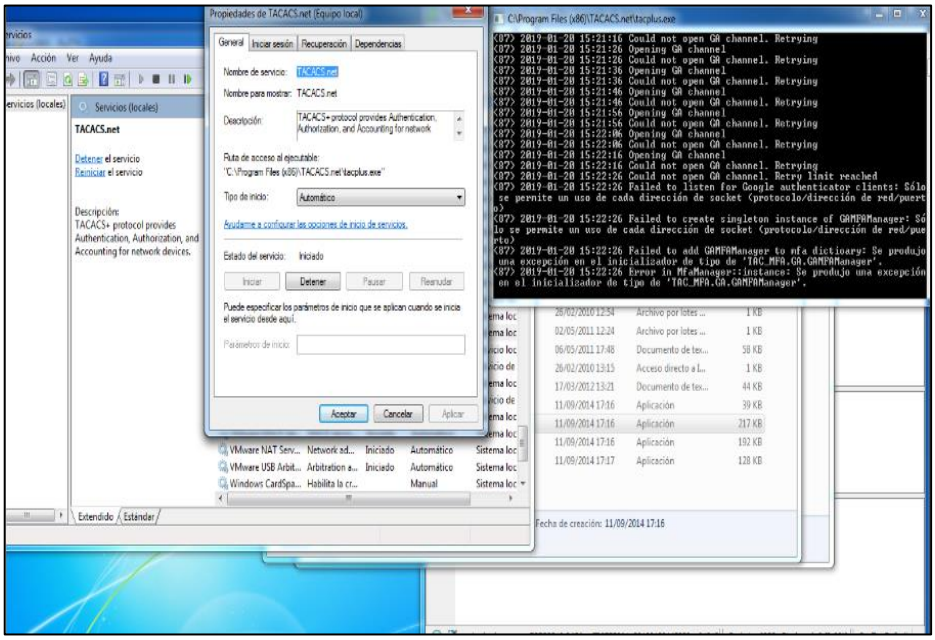


Figura 18-3: Configuración de TACACS+ en equipo suplicante

Realizado por: Gabriela Andrade, 2019

3.3.5. Configuración switch capa 3

El ejemplo de configuración del protocolo TACACS+ en un switch Catalyst capa 3 IOS3560 es muy sencilla así lo presentamos en los siguientes comandos utilizados en el equipo para su respectiva configuración:

Switch (config)# aaa new-model
Switch (config-if)# aaa authentication login DEFAULT group tacacs+ line
Switch (config-if)# aaa authorization console aaa authorization config-commands

Switch (config-if)# aaa authorization exec DEFAULT group tacacs+ none
Switch (config-if)# aaa authorization commands 0 DEFAULT group tacacs+ none
Switch (config)# aaa authorization commands 1 DEFAULT group tacacs+ none
Switch (config-if)# aaa authorization commands 15 DEFAULT group tacacs+ none
Switch (config-if)# aaa accounting commands 0 default start-stop group tacacs+
Switch (config-if)# aaa accounting commands 1 default start-stop group tacacs+
Switch (config-if)# aaa accounting commands 15 default start-stop group tacacs+
Switch (config-if)# tacacs-server host 10.226.72.222
Switch (config-if)# tacacs-server key <SHARED KEY>

3.4. Transmisión de paquetes TACACS+

Podemos ver que el protocolo de enlace de 3 vías TCP inicial se produce desde una fuente de 10.1.1.1 con un puerto de destino de 49 (TACACS +). El dispositivo comienza enviando una solicitud de autenticación a la dirección 10.1.1.10.

El dispositivo 10.1.1.10 responde con un puerto de origen de 49 al destino 10.1.1.1 por medio del protocolo TCP En esta etapa, puede utilizar la clave para descifrar y analizar la comunicación TACACS +. Podemos ver que un usuario: synack ha enviado una solicitud de autenticación de inicio de sesión al 10.1.1.10.

El dispositivo 10.1.1.10 envía un mensaje de recibo y luego envía un paquete TACACS + a 10.1.1.1. Una vez que se descifra este mensaje TACACS +, podemos ver que el servidor TACACS + ahora ha solicitado una contraseña para el usuario: synack. El dispositivo 10.1.1.1 envía un acuse de recibo para indicar que se ha recibido la solicitud de la contraseña.

El dispositivo 10.1.1.1 luego envía la contraseña: Contraseña1 al servidor TACACS + El servidor TACACS + responde con una autenticación aprobada. Esto significa que el usuario: synack ahora ha sido autenticado La sesión TCP ahora se arranca con el dispositivo 10.1.1.1

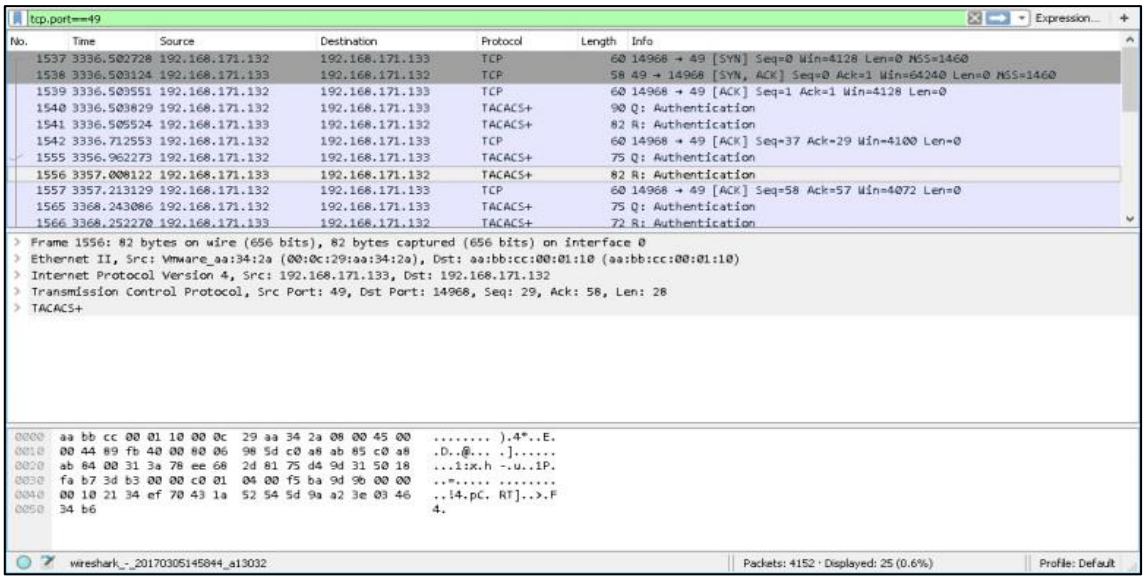


Figura 19-3: Paquetes Tacacs+ aceptados y rechazados

Realizado por: Gabriela Andrade, 2019

3.5. Tiempo de Autenticación de la red

Para realizar el cálculo del tiempo que se toma en autenticar un usuario el protocolo RADIUS fue necesario capturar paquetes EAPOL/EAP tomando en cuenta la diferencia de tiempo entre el momento en que envió la petición y el momento en que el cliente recibe la respuesta a dicha petición.

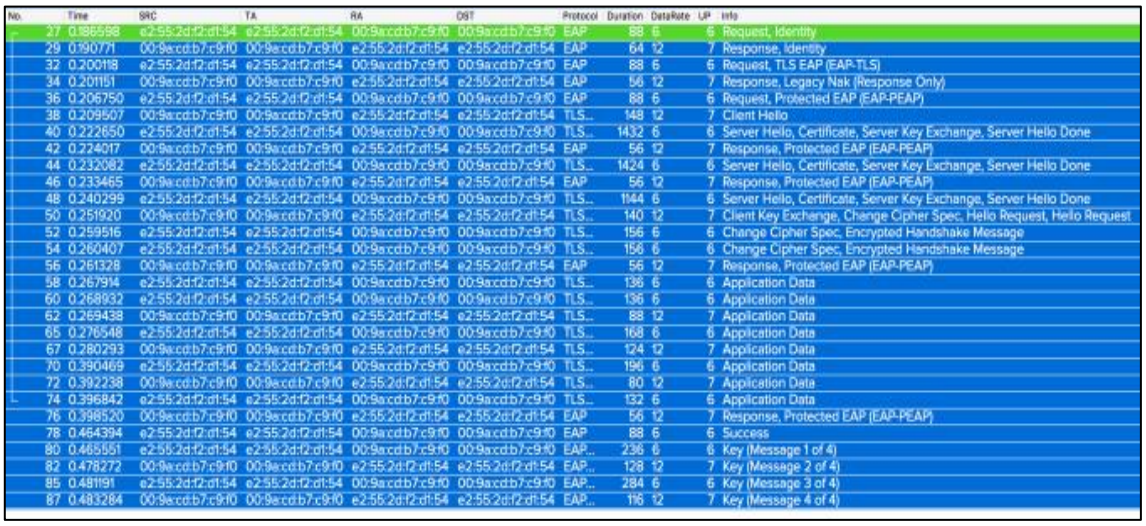


Figura 20-3: Acceso requerido

Realizado por: Gabriela Andrade, 2019

EAP Success (cableado e inalámbrico) y 4 Way Handshake (cuando el cliente es inalámbrico)

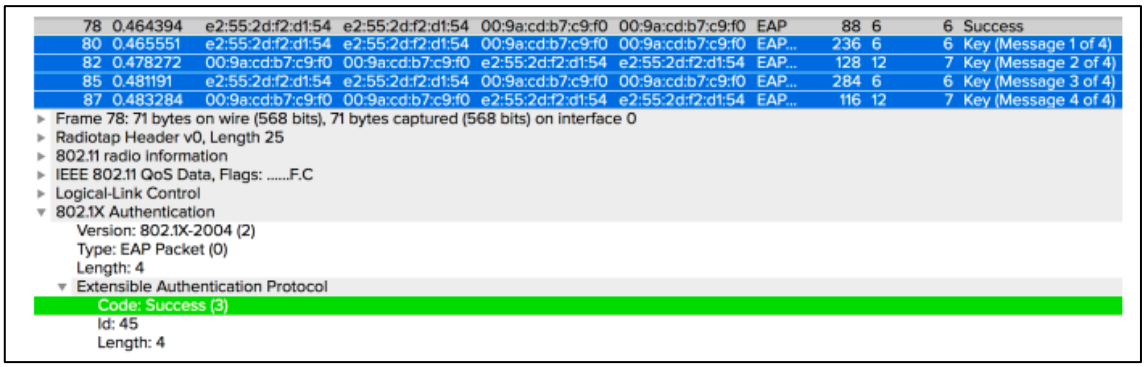


Figura 21-3: EAP de una red inalámbrica

Realizado por: Gabriela Andrade, 2019

La forma en que opera el protocolo EAP se basa en el uso de un controlador de acceso llamado autentificador, que le otorga o deniega a un usuario el acceso a la red. El usuario en este sistema se llama solicitante. Cuando se trata de una red inalámbrica, el punto de acceso actúa como autentificador.

En la siguiente grafica se muestra el tiempo que toma en autenticarse un usuario para determinar el tiempo que este se demora en acceder a la red se ha utilizado un software denominado PRTG de licencia gratuita para Windows donde detalla el protocolo por el cual se autentica el código de Radius y el tiempo de respuesta del servidor en el cual autentica al usuario.

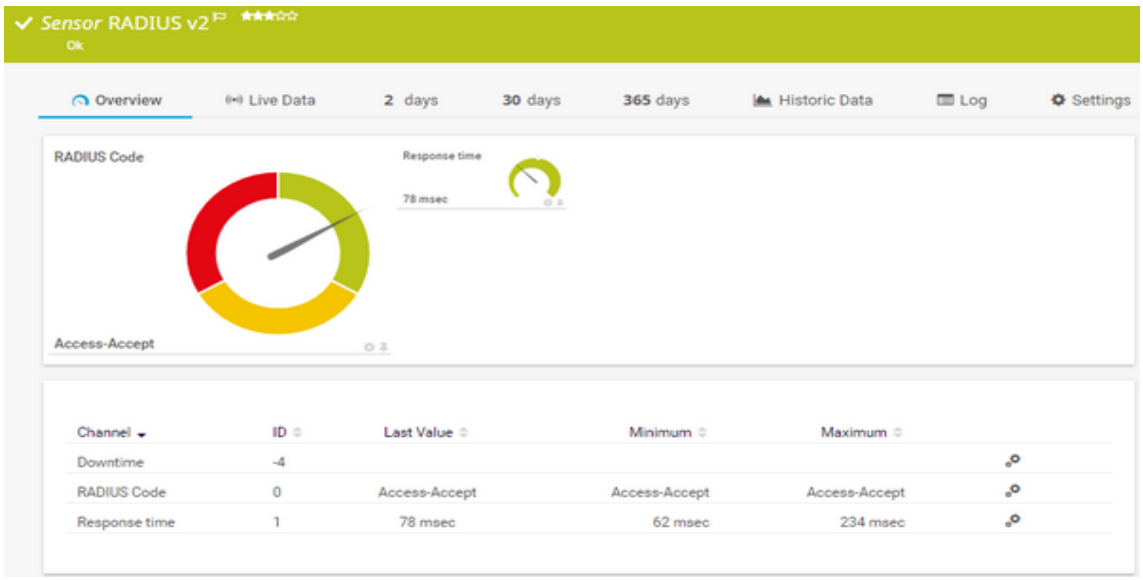


Gráfico 1-3: Tiempo de autenticación con PRTG software

Realizado por: Gabriela Andrade, 2019

En la siguiente gráfica se observa que al implementar algún protocolo de seguridad como lo son

WEP y WPA con sus respectivos tipos de cifrado no les toma más de 0.4 segundos en poder ser autentificados a la red ya que solamente están bajo sus propios parámetros de seguridad, mientras que al implementarse estos protocolos de seguridad en conjunto con RADIUS el tiempo de autenticación se eleva alrededor de 0.6 segundos en promedio, que representa hasta cuatro veces el tiempo de autenticación sin incluir RADIUS.

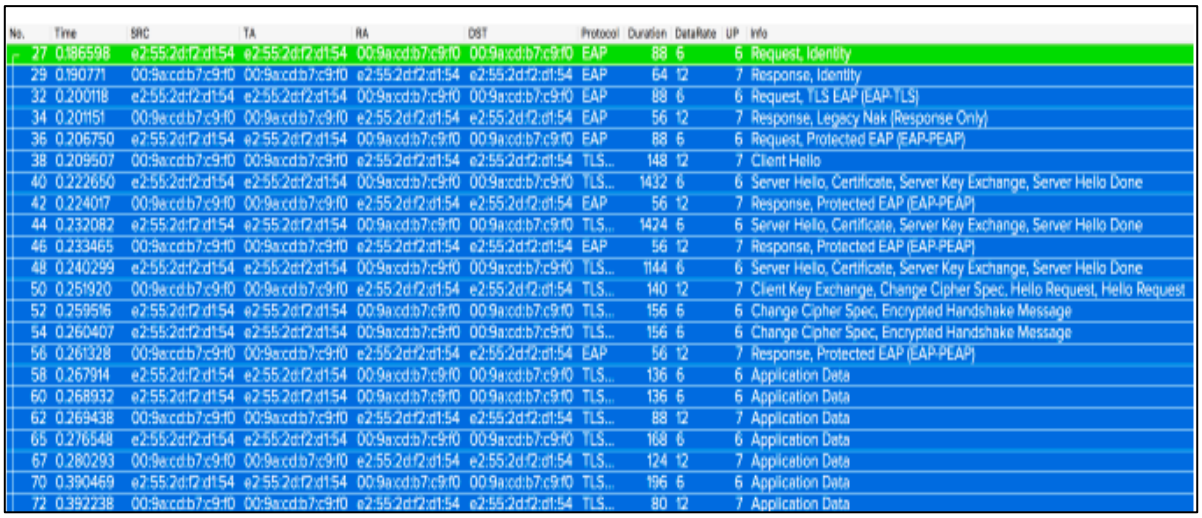
Lo anterior debido a que se tiene que tomar en cuenta el tiempo que tarda el punto de acceso en mandar la petición del cliente al servidor RADIUS para que éste pueda verificar las credenciales del cliente.

Gráfico 2-3: Tiempo de Autenticación con RADIUS

Realizado por: Gabriela Andrade, 2019

Esta prueba se realizó con todos los usuarios creados en los dos servidores Radius de lo cual se tomó el tiempo óptimo para representar el aproximado más cercano a todas las pruebas realizadas salió el valor de tiempo de autenticación entre 70mseg y 120mseg

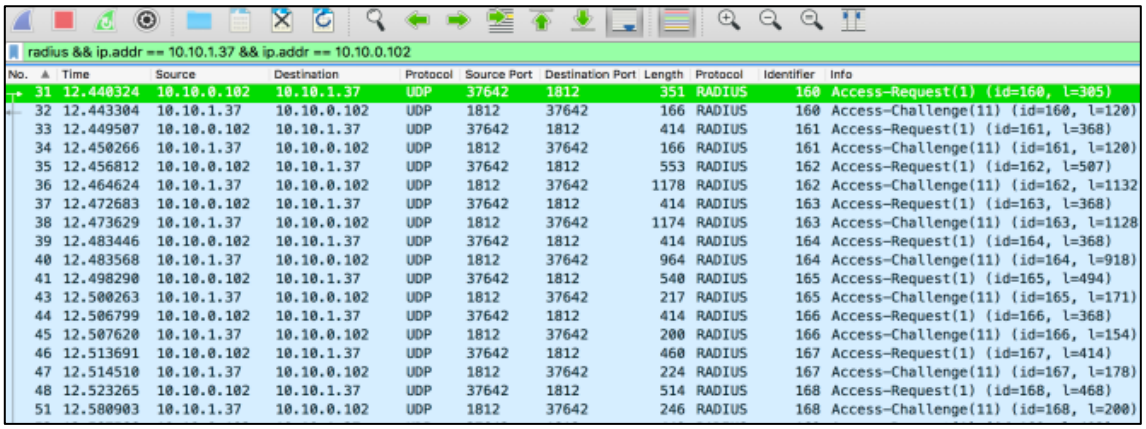
Negociación del método de autenticación EAP e intercambio de credenciales:



No.	Time	SRC	TA	RA	DST	Protocol	Duration	DataRate	UP	Info
27	0.186598	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	EAP	88	6	6	Request, Identity
29	0.190771	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	EAP	64	12	7	Response, Identity
32	0.200118	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	EAP	88	6	6	Request, TLS EAP (EAP-TLS)
34	0.201151	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	EAP	56	12	7	Response, Legacy Nak (Response Only)
36	0.206750	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	EAP	88	6	6	Request, Protected EAP (EAP-PEAP)
38	0.209507	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	TLS...	148	12	7	Client Hello
40	0.222650	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	1432	6	6	Server Hello, Certificate, Server Key Exchange, Server Hello Done
42	0.224017	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	EAP	56	12	7	Response, Protected EAP (EAP-PEAP)
44	0.232082	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	1424	6	6	Server Hello, Certificate, Server Key Exchange, Server Hello Done
46	0.233465	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	EAP	56	12	7	Response, Protected EAP (EAP-PEAP)
48	0.240299	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	1144	6	6	Server Hello, Certificate, Server Key Exchange, Server Hello Done
50	0.251920	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	TLS...	140	12	7	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
52	0.259516	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	156	6	6	Change Cipher Spec, Encrypted Handshake Message
54	0.260407	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	156	6	6	Change Cipher Spec, Encrypted Handshake Message
56	0.261328	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	EAP	56	12	7	Response, Protected EAP (EAP-PEAP)
58	0.267914	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	136	6	6	Application Data
60	0.268932	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	136	6	6	Application Data
62	0.269438	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	TLS...	88	12	7	Application Data
65	0.276548	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	168	6	6	Application Data
67	0.280293	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	TLS...	124	12	7	Application Data
70	0.390469	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	TLS...	196	6	6	Application Data
72	0.392238	00:9a:cd:b7:c9:f0	00:9a:cd:b7:c9:f0	e2:55:2d:f2:d1:54	e2:55:2d:f2:d1:54	TLS...	80	12	7	Application Data

Figura 22-3: Negociación de autenticación EAP.

Realizado por: Gabriela Andrade, 2019



radius && ip.addr == 10.10.1.37 && ip.addr == 10.10.0.102

No.	Time	Source	Destination	Protocol	Source Port	Destination Port	Length	Protocol	Identifier	Info
31	12.440324	10.10.0.102	10.10.1.37	UDP	37642	1812	351	RADIUS	160	Access-Request(1) (id=160, l=305)
32	12.443304	10.10.1.37	10.10.0.102	UDP	1812	37642	166	RADIUS	160	Access-Challenge(11) (id=160, l=120)
33	12.449507	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	161	Access-Request(1) (id=161, l=368)
34	12.450266	10.10.1.37	10.10.0.102	UDP	1812	37642	166	RADIUS	161	Access-Challenge(11) (id=161, l=120)
35	12.456812	10.10.0.102	10.10.1.37	UDP	37642	1812	553	RADIUS	162	Access-Request(1) (id=162, l=507)
36	12.464624	10.10.1.37	10.10.0.102	UDP	1812	37642	1178	RADIUS	162	Access-Challenge(11) (id=162, l=1132
37	12.472683	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	163	Access-Request(1) (id=163, l=368)
38	12.473629	10.10.1.37	10.10.0.102	UDP	1812	37642	1174	RADIUS	163	Access-Challenge(11) (id=163, l=1128
39	12.483446	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	164	Access-Request(1) (id=164, l=368)
40	12.483568	10.10.1.37	10.10.0.102	UDP	1812	37642	964	RADIUS	164	Access-Challenge(11) (id=164, l=918)
41	12.498290	10.10.0.102	10.10.1.37	UDP	37642	1812	540	RADIUS	165	Access-Request(1) (id=165, l=494)
43	12.500263	10.10.1.37	10.10.0.102	UDP	1812	37642	217	RADIUS	165	Access-Challenge(11) (id=165, l=171)
44	12.506799	10.10.0.102	10.10.1.37	UDP	37642	1812	414	RADIUS	166	Access-Request(1) (id=166, l=368)
45	12.507620	10.10.1.37	10.10.0.102	UDP	1812	37642	200	RADIUS	166	Access-Challenge(11) (id=166, l=154)
46	12.513691	10.10.0.102	10.10.1.37	UDP	37642	1812	460	RADIUS	167	Access-Request(1) (id=167, l=414)
47	12.514510	10.10.1.37	10.10.0.102	UDP	1812	37642	224	RADIUS	167	Access-Challenge(11) (id=167, l=178)
48	12.523265	10.10.0.102	10.10.1.37	UDP	37642	1812	514	RADIUS	168	Access-Request(1) (id=168, l=468)
51	12.580903	10.10.1.37	10.10.0.102	UDP	1812	37642	246	RADIUS	168	Access-Challenge(11) (id=168, l=200)

Figura 23-3: Resultado de las pruebas RADIUS protocolo UDP

Realizado por: Gabriela Andrade, 2019

3.6. Respuesta de TACACS+

Al realizar pruebas con el servidor TACACS+ y enviar paquetes notamos la manera que opera al enviar y recibir el protocolo TACACS+

En la siguiente secuencia de captura de wireshark se puede identificar, la IP del servidor es 10.226.72.222 y la IP del suplicante es 10.208.50.37, la solicitud de autenticación se reenvía al nodo: 10.208.50.37

Así lo demostramos en la siguiente figura:

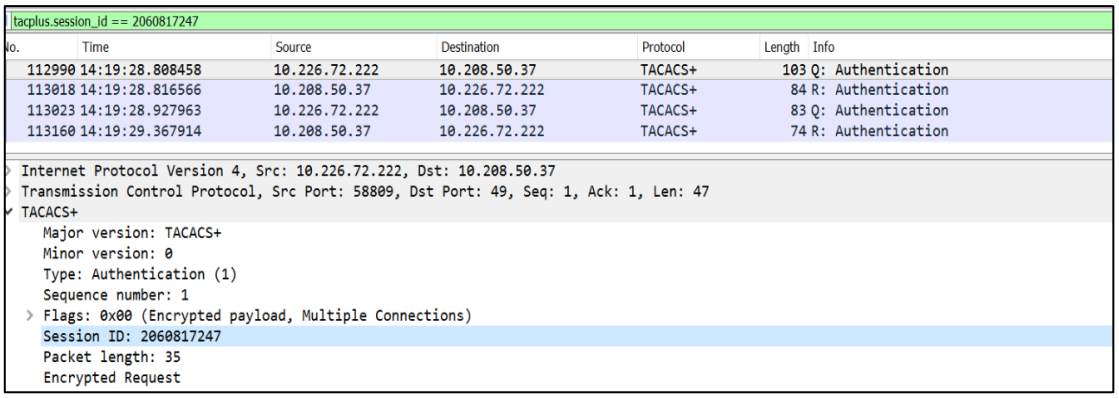


Figura 24-3: Resultado de las pruebas RADIUS protocolo UDP

Realizado por: Gabriela Andrade, 2019

Se utilizó de igual manera el software PRTG para identificar el tiempo que le lleva a los usuarios autentificarse por medio del protocolo Tacacs+, debido a que este software es de libre licencia no posee un sensor específico para tacacs+ pero se logra identificar mediante el puerto en el que el usuario se logra identificar que es el puerto 49 que utiliza Tacacs+ para autenticarse así lo demuestra en el siguiente gráfico.

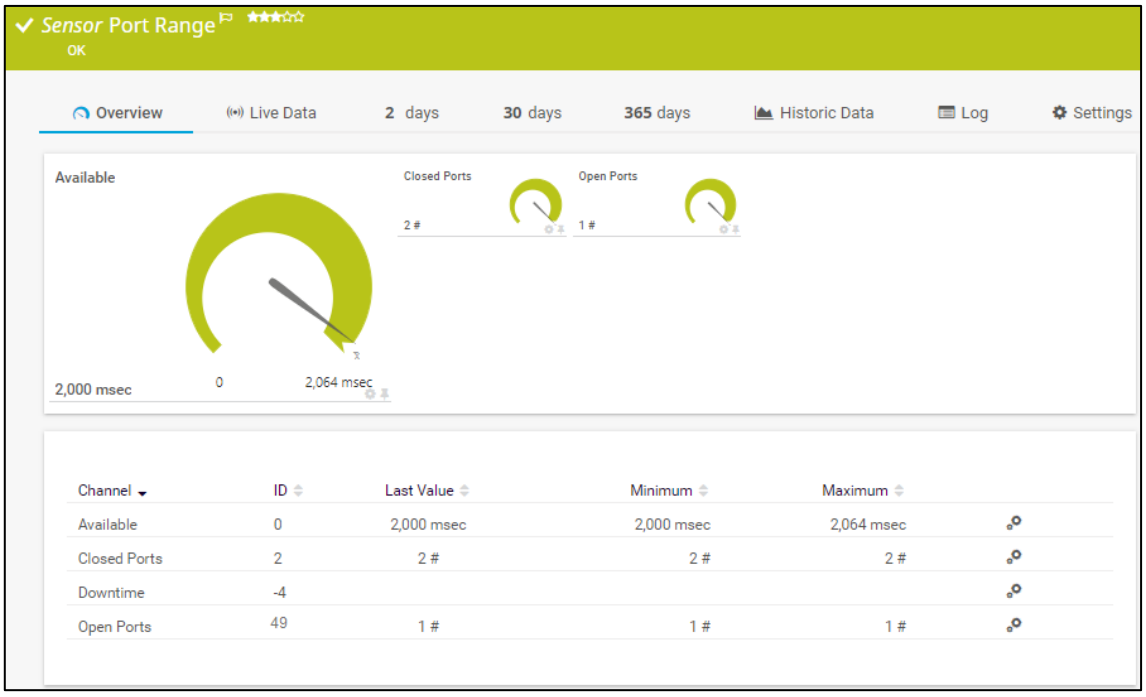


Gráfico 3-3: Tiempo de autenticación Tacacs+ por medio del protocolo de transporte

Realizado por: Gabriela Andrade, 2019

Después de que la autenticación se realiza correctamente, se envía una solicitud de autorización.

En el siguiente ejemplo, el dispositivo NAD es un switch Cisco catalyst 3560 a la cual la solicitud

de autorización es enviada a un nodo diferente. así dándonos como resultado la captura de tráfico wireshark.

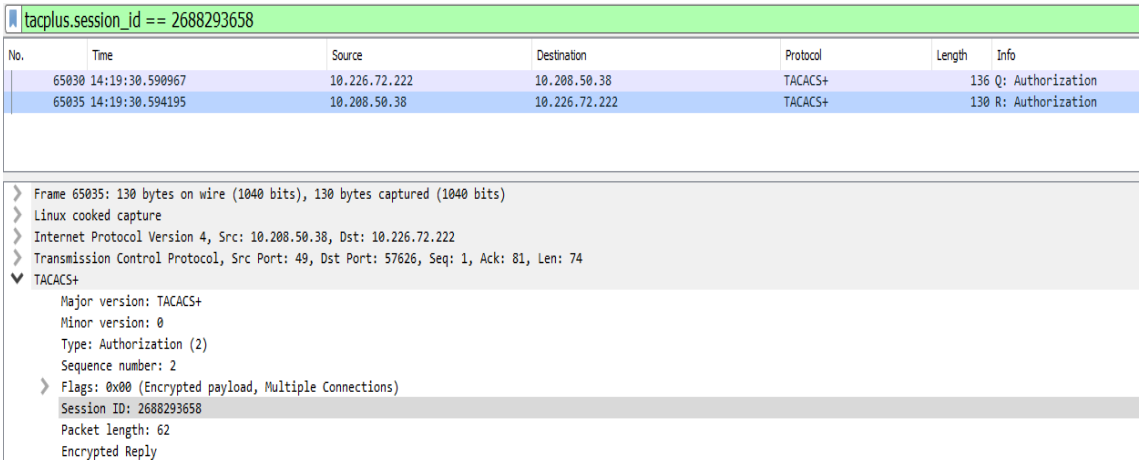


Figura 25-3: Resultado de las pruebas TACACS+ Autenticación correcta

Realizado por: Gabriela Andrade, 2019

Con el equilibrio de carga de las solicitudes, podemos garantizar que la autenticación de TACACS+ y la solicitud de autorización de TACACS lleguen al mismo nodo habilitando la persistencia de la sesión.

De este modo podemos identificar como realiza la autorización de paquetes con el protocolo TACACS+

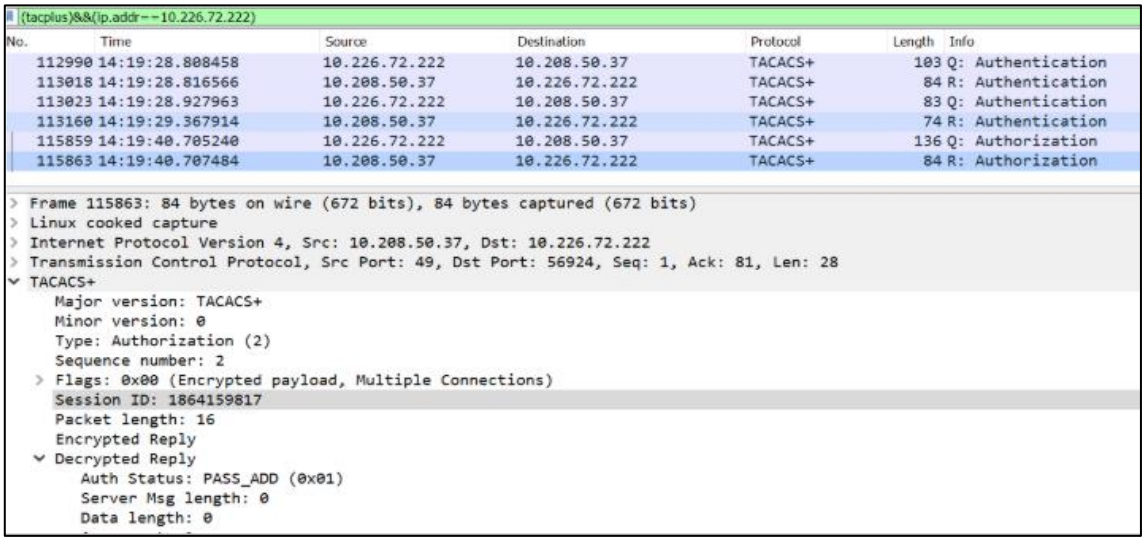


Figura 26-3: Autorización y tiempo de respuesta de TACACS+

Realizado por: Gabriela Andrade, 2019

Finalmente, en el siguiente gráfico comparamos el tiempo de autenticación entre Radius y

Tacacs+ comparando el tiempo en que se demora cada usuario en mandar la petición de autenticación a su respectivo servidor. Como se muestra en las distintas pruebas el servidor Radius se demora en promedio entre 0.2 y 0.7 milisegundos en autenticarse mientras que el servidor Tacacs+ tarda en promedio entre 0.2 y 2 milisegundos en autenticar al usuario debido a que cifra todo el paquete de autenticación y ahí la diferencia entre Radius ya que este protocolo solo encripta la contraseña del usuario.

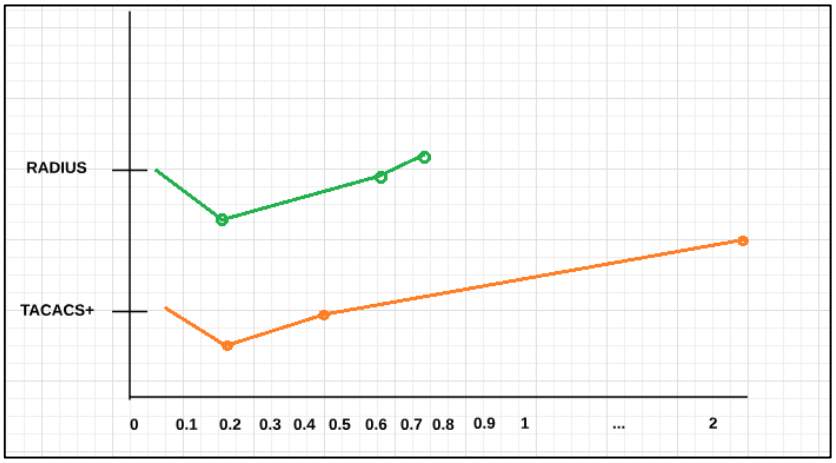


Gráfico 4-3: Comparación de tiempo de autenticación entre Radius y Tacacs+

Realizado por: Gabriela Andrade, 2019

CONCLUSIONES

Se analizó las prestaciones de los protocolos de autenticación remota Radius y Tacacs+ en infraestructura de comunicaciones corporativas

Se estudió detalladamente cada característica entre RADIUS y TACACS+ además de las prestaciones que brinda cada protocolo llegando a la conclusión de que Tacacs+ posee mejores características en entornos de seguridad corporativos, ´pero Radius ofrece ms prestaciones ya que posee varios códigos abiertos para que este pueda ser implementado en cualquier tipo de ambiente.

Se diseñó un ambiente de prueba para validar las prestaciones de cada uno de los protocolos estudiados donde se utilizó un ambiente Open Source ya que Radius posee la mayoría de sus servidores y RFC están en código abierto, así mismo Tacacs+ a pesar de ser compatible con la mayoría de equipos CISCO este también libero su versión en un estándar abierto definido por RFC 1492 y el borrador de IETF así lo demostramos en este trabajo de titulación ya que se utilizó un software abierto para Windows denominado Tacacs.net.

Se evaluó y se verifico el adecuado funcionamiento de los protocolos seleccionados, verificando el tiempo de autenticación, cifrados seguros para el protocolo RADIUS, longitud , códigos e identificadores de los paquetes radius y tacacs+ además de parámetros de comparación por medio de una tabla de Likert para llegar a la conclusión de que en tiempo de autenticación Radius es más óptimo que Tacacs+ pero que por el contrario en cuestión de seguridad TACACS+ es el más adecuado por protocolos d transporte, interoperabilidad, soporte multiprotocolo además que permite la administración del router.

Se elaboró una propuesta de guía técnica que se dedujo paso a paso la implementación de RADIUS y TACACS+, según el escenario al que vaya a ser implementado en este caso se utilizó dos servidores Radius de la misma manera realizando un análisis comparativo entre los servidores se opta por el más adecuado según los requerimientos de la red a la que vayan a ser implementado, de la misma manera TACACS+ se especifica paso a paso una guía de implementación para redes corporativas con equipamiento de preferencia CISCO.

RECOMENDACIONES

RADIUS normalmente tiene licencias mayormente gratuitas y de software libre a diferencia de TACACS + que en cierta medida es exclusivo para dispositivos CISCO por lo cual se toma en consideración a la hora de priorizar costos e implementación viéndolo desde un plano económico sería más factible implementación de servidores RADIUS. Una de las principales limitaciones que he encontrado durante el estudio fue la incapacidad de los dispositivos compatibles para implementar el protocolo Tacacs+ ya que esta función se basa a dispositivos Cisco y software que soporte este protocolo.

En complejidad de la misma manera RADIUS es mucho más grafico incluso información muy espontanea para las configuraciones de los diferentes servidores a prueba evidenciando así por el hecho de que hay más de 40 RFC escritos en RADIUS, mientras que TACACS + solo tiene uno (versión liberada).

El servidor RADIUS es un servicio muy sensible, que debe estar disponible en cualquier momento. Indicando que señalaría que es muy importante implementar el segundo servidor de copia de seguridad conmutación por error o equilibrio de carga de RADIUS. Esta característica asegurará la presencia constante del servicio en la red.

En la parte práctica de este proyecto de titulación, se ha encontrado con algunos problemas relacionados con el soporte insuficiente del software TekRADIUS, se ha creado una red independiente con el servidor RADIUS como servidor de autenticación, que otorga a los usuarios autorizados servicios adicionales.

Esta tesis aún se puede mejorar de varias maneras. En primer lugar, es una red privada y no tiene acceso a internet en el caso de utilizar el servidor TekRadius por el contrario el servidor en la nube ICloud tenía obligatoriamente acceso al internet. Lo que concluye que Radius nos da varias maneras de implementar sus servidores tanto en la nube como un servidor interno que trabaja en el modo cliente/servidor. Tacacs+ demostró menos accesibilidad para su implementación. Desde un rango de comparación según la tabla 10 TCACS+ ofrece mejores prestaciones en cuanto a seguridad, pero Radius es mucho más accesible a su utilización.

Se recomienda de igual manera no implementar los dos protocolos Radius y Tacacs+ en el mismo servidor ya que el sistema de autenticación va a presentar varios errores ya que no sabrá a que base datos dirigirse para autenticar al usuario además se haría muy pesado para el servidor.

BIBLIOGRAFIA

ALVARADO, José, *Principios Seguridad Informática* [en línea]. Quetzaltenango, 2008. [Consulta: 7 de mayo 2018]. Disponible en: https://es.scribd.com/doc/55774691/nociones-seguridad-principios

APCD - PÁGINA WEB DE SERVICIOS METEOROLÓGICOS, *APCD - Variables - Presión barométrica.* [en línea]. 2018. [Consulta: 24 May 2018]. Disponible en: http://apcd-spv.org/index.php?lang=es&secc=variables&type=pressio_barometrica

AIRHEADS COMMUNITY, *Tutorial de Open Authentication Role Initial* [en línea]. 2018**.** Disponible en: https://community.arubanetworks.com/t5/Foro-en-Espa%C3%B1ol/Tutorial-Open-Authentication-Role-Initial-Authentication-Role-y/td-p/436372.

ALONSO, Ivan Dario. [en línea]. 2013 [Consulta: Mayo de 2013]. Disponible en: https://www.perlesystems.es/supportfiles/aaa-security.shtml.

ARIAS, Luis & SARMIENTO, German, *Protocolos del control de acceso RADIUS.* 2012.

BAMMTECH. *IRON-WIFI.* [en línea] Disponible en: https://www.bammtech.cl/iron-wifi.html.

BAUER, Michael D, *Seguridad en servidores Linux.* Madrid: Anaya Multimedia, 2001.

CEVALLOS, Y, *Investigacion del servidor radius para la seguridad en redes lan inalambricas.* Riobamba. 2011

CISCO SYSTEM, *Seguridad utilizando RADIUS y TACACs* [en línea]. 2009. Disponible en: https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.pdf.

CORPORATION [US], *Norton by Symantec*. [en línea]. 2017. Disponible en: https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf.

COIMBRA, Edison, *Propagacion de onda en el espacio libre.* [en línea], 2011. [Consulta: 4 de mayo 2018]. Disponible en: https://es.slideshare.net/edisoncoimbra/63-propagacion-en-el-espacio-libre

CUELLAR, A. 2006. *Concepto universal de auditoria.* 2006. [en línea], 2012. [Consulta: 3 de mayo 2018]. Disponible en: https://www.bammtech.cl/iron-wifi.html.

GARCIA, A. *Documental y narrativa transmedia.* [en línea], 2014. Cartagena: Universidad Politécnica de Cartagena. [Consulta: 17de mayo de 2018]. ISBN 9788416325030. Disponible en: https://ebookcentral.proquest.com/lib/espochsp/detail.action?docID=4794898&query=docnarr

GOMEZ, C. *Autenticacion de red* [en línea], 2011. [Consulta: 9 de mayo 2018]. Disponible en: https://ebookcentral.proquest.com/lib/espochsp/reader.action?docID=3202559&query=network auth

HERNANDEZ, Ara, *Familia de Protocolos AAA descripción y servicios* [en línea], 2015. Disponible en: http://aracelibarrerahdz10.blogspot.com/2015/11/familia-aaa-descripcion-y-servicios.html.

HUY, Quoc, *MIKROTIK HOTSPOT EXTERNAL SERVER*. [en línea], 2017. Disponible en: https://mum.mikrotik.com/presentations/VN17/presentation_4370_1493373796.pdf.

MAZZEI, Giovanni Domenico, *Seguridad y Servidor RADIUS* [en línea], 2014. Disponible en: http://digibuo.uniovi.es/dspace/bitstream/10651/27812/1/TFM_UNIVERSIDAD%20DE%20OVIEDO_GiovanniMazzei.pdf.

MEJIAS, D, *Redes de Computadores* [en línea], 2015. Disponible en: https://slideplayer.es/slide/10627907/

RAMIREZ, Erika, *Protocolo AAA* [en línea]. 2015. Disponible en: http://calidadsoftwaretics.blogspot.com/2015/11/protocolo-aaa.html.

SAAVEDRA, O, *Implementacion de un diseño de puente inalambrico punto multi punto para la mejora de la interconexion de las areas de la empresa plasticos Rimac* .[en linea]. 2012. Chiclayo. Universidad Católica Santo Toribio de Mogrovejo. Disponible en: http://tesis.usat.edu.pe/handle/usat/517

Zambrano, E. *La importancia de la autenticacion en el internet de todas las cosas.* [en línea]. 2016. Quito. Escuela Politécnica Nacional. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/15087