UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA ELECTRÓNICA Y REDES DE COMUNICACIÓN

"CONTROL DE ACCESO Y ADMINISTRACIÓN DE RECURSOS DE RED MEDIANTE UN SERVIDOR AAA EN EL GAD MUNICIPAL DE URCUQUI USANDO SOFTWARE LIBRE"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: WILLIAM EDUARDO VACA AGUIRRE

DIRECTOR: ING. CARLOS VÁSQUEZ

Ibarra, 2014

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de identidad	1002949822
Nombres y apellidos	Vaca Aguirre William Eduardo
Dirección	Caranqui, Vía a San Cristóbal
Email	william_889@hotmail.com
Teléfono móvil	0986260191

DATOS DE LA OBRA	
Título	"CONTROL DE ACCESO Y ADMINISTRACIÓN DE RECURSOS DE RED MEDIANTE UN SERVIDOR AAA EN EL GAD MUNICIPAL DE URCUQUI USANDO SOFTWARE LIBRE"
Autor	Vaca Aguirre William Eduardo
Fecha	2014/11/10
Programa	Pregrado
Título por el que se aspira	Ingeniero en Electrónica y Redes de Comunicación
Director	Ing. Carlos Vásquez

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, **William Eduardo Vaca Aguirre**, con cédula de identidad Nro. 1002949822, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

.....
Firma
Nombre: William Eduardo Vaca Aguirre
Cédula: 1002949822
Ibarra a los 10 días del mes de noviembre del 2014

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **William Eduardo Vaca Aguirre**, con cédula de identidad Nro. 1002949822, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4. 5 y 6, en calidad de autor de la obra o trabajo de grado denominado **"CONTROL DE ACCESO Y ADMINISTRACIÓN DE RECURSOS DE RED MEDIANTE UN SERVIDOR AAA EN EL GAD MUNICIPAL DE URCUQUI USANDO SOFTWARE LIBRE"** que ha sido desarrollado para optar por el título de: **Ingeniero en Electrónica y Redes de Comunicación** en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Firma

Nombre: William Eduardo Vaca Aguirre

Cédula: 1002949822

Ibarra a los 10 días del mes de noviembre del 2014

DECLARACIÓN

Ante las autoridades de la Universidad Técnica del Norte declaro que el contenido del proyecto denominado: **"CONTROL DE ACCESO Y ADMINISTRACIÓN DE RECURSOS DE RED MEDIANTE UN SERVIDOR AAA EN EL GAD MUNICIPAL DE URCUQUI USANDO SOFTWARE LIBRE",** presentado como requisito de graduación para obtener el título de: **Ingeniero en Electrónica y Redes de Comunicación**, es de mi autoría y total responsabilidad.

Atentamente,

William Eduardo Vaca Aguirre
AUTOR TRABAJO DE GRADO
C.I. 100294982-2

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación **"CONTROL DE ACCESO Y ADMINISTRACIÓN DE RECURSOS DE RED MEDIANTE UN SERVIDOR AAA EN EL GAD MUNICIPAL DE URCUQUI USANDO SOFTWARE LIBRE"** fue desarrollado en su totalidad por el Sr. William Eduardo Vaca Aguirre, bajo mi supervisión.

Ing. Carlos Vásquez

DIRECTOR DE PROYECTO

CERTIFICACIÓN

Urcuquí, 07 de noviembre de 2014

Señores
UNIVERSIDAD TÉCNICA DEL NORTE
Presente.-

De mis consideraciones.

Siendo auspiciantes del proyecto de tesis del egresado WILLIAM EDUARDO VACA AGUIRRE con CI: 1002949822, quien desarrolló su trabajo con el tema "CONTROL DE ACCESO Y ADMINISTRACIÓN DE RECURSOS DE RED MEDIANTE UN SERVIDOR AAA EN EL GAD MUNICIPAL DE URCUQUI USANDO SOFTWARE LIBRE ", me es grato informar que se ha cumplido el proceso con satisfacción, por lo que se recibe el proyecto como culminado y realizado en su totalidad por parte del egresado. Una vez que hemos recibido la documentación respectiva, nos comprometemos a continuar utilizando el mencionado aplicativo en beneficio de nuestra institución.

Es todo lo que puedo certificar en honor a la verdad, el interesado puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente,

G.A.D. MUNICIPAL "SAN MIGUEL DE URCUQUÍ"
UNIDAD DE SISTEMAS

Ing. Mario Farinango
Administrador Unidad de Sistemas
GAD Municipal San Miguel de Urcuquí

DEDICATORIA

A mi familia quienes me han apoyado en cada etapa de mi vida y han sido pilares importantes en mi constante deseo de superación.

William Vaca Aguirre

AGRADECIMIENTOS

Al GAD Municipal San Miguel de Urcuqui e Ing. Mario Farinango, administrador de la Unidad de Sistemas, quienes gentilmente me abrieron las puertas de la Institución.

Al Ing. Carlos Vásquez, director de tesis, quien fue una guía fundamental para desarrollar el proyecto.

William Vaca Aguirre

CONTENIDO

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

ANEXO A

ANEXO B

ÍNDICE DE TABLAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

ANEXO C

RESUMEN

El proyecto planteado consiste en el diseño e implementación de un esquema de red que proporcione el servicio de Autenticación, Autorización y Auditoria (AAA) en el GAD Municipal San Miguel de Urcuquí, para el control de acceso y administración de recursos de red, empleando soluciones basadas en software libre. El fundamento teórico requerido para el desarrollo del sistema AAA inicia con el estudio de los principales métodos de autenticación EAP (TLS, TTLS y PEAP) soportados por el estándar IEEE 802.1x, el protocolo LDAP y RADIUS. En el segundo capítulo se identifican los perfiles de acceso de los usuarios a cada una de las aplicaciones y servicios de red del GAD Municipal San Miguel de Urcuquí, se crea además la política de seguridad para el sistema AAA. El tercer capítulo contiene el diseño de la infraestructura de red con servicio AAA (Autenticación, Autorización y Contabilidad), tomando en cuenta cada uno de los requerimientos establecidos en base al estudio y la política de seguridad desarrollada. En el cuarto capítulo se procede con la configuración de los equipos de red, la implementación del servidor AAA en el entorno virtual PROXMOX y las pruebas de aplicación ejecutadas en posibles escenarios que pudieran presentarse al momento de acceder al sistema. Finalmente, el quinto capítulo contiene el análisis Costo – Beneficio que determina la factibilidad económica del proyecto.

ABSTRACT

The proposed project involves the design and implementation of a network diagram that provides Authentication, Authorization, and Auditing (AAA) service on the "GAD Municipal San Miguel de Urcuqui" for the access control and network resources administration using open-software based solutions. The theoretical foundation required for the AAA system development starts with the study of the main methods of authentication EAP (TLS, TTLS and PEAP) supported by the standard IEEE 802.1x, RADIUS and LDAP protocol. In the second chapter, user- access profiles are identified in each application and each network service for the "GAD Municipal San Miguel de Urcuqui". As a result, the AAA system security policy is created. The third chapter contains the design of the network infrastructure with AAA service (Authentication, Authorization and Accounting), taking into account each of the requirements set based on the study and the security policy developed. In the fourth chapter, we proceed to configure the network's hardware; we implement the AAA server using the PROXMOX virtual environment, then testing of applications executed in possible different settings is done to prove that conflicts might be encountered when accessing the system. Finally, the fifth chapter contains the Cost-Benefit analysis that determines the economic feasibility of the project.

PRESENTACIÓN

Las redes de información son esenciales para el crecimiento y desarrollo de las empresas, proporcionan además la capacidad de soportar nuevas tecnologías evolucionando fácilmente a la par de los cambios y nuevas aplicaciones que día a día se desarrollan.

Actualmente, las empresas se enfrentan a muchos riesgos en la seguridad de sus redes que van desde técnicas de ingeniería social informática, ataques de negación de servicio a servidores, uso indebido de aplicaciones, hasta la sustracción de datos, amenazas que pueden originarse desde fuera de la empresa o de empleados que intencionalmente o por falta de conocimientos puedan comprometer la operatividad de toda la red.

La implementación del proyecto permitirá un proceso seguro de acceso a la red, suministrará los servicios necesarios de acuerdo a las políticas del administrador a quienes hayan cumplido con el proceso de autenticación, como también registrará el uso de recursos de todos aquellos que se encuentren conectados a la red del GAD Municipal de Urcuquí.

Proporcionando así un servicio AAA a la intranet, para que la información y los servicios de red estén disponibles exclusivamente para los usuarios autorizados, de esta manera los trabajadores del GAD Municipal de Urcuquí realizarán sus actividades en un ambiente más seguro, ofreciendo a los ciudadanos servicios públicos de calidad.

CAPÍTULO I

ANÁLISIS DEL ESTÁNDAR IEEE 802.1X, PROTOCOLO RADIUS Y EL SERVIDOR DE DIRECTORIO LDAP

1.1 SISTEMAS AAA

El estándar AAA[1] se utiliza en el diseño de sistemas de control de acceso a redes de datos, proporcionando los servicios de autenticación, autorización y contabilidad de forma centralizada.

1.1.1 AUTENTICACIÓN

La Autenticación es el proceso de mayor relevancia en los sistemas AAA, sirve de base a todo el sistema completo, debido a su directa relación con los procesos de autorización y contabilidad. Los primeros sistemas de seguridad para control de acceso usaban una infraestructura de autenticación simple basada en nombre de usuario y contraseña en texto plano, quedando expuestos a posibles intercepciones y sustracciones por otra persona.

Actualmente, los sistemas de autenticación han aumentado el nivel de seguridad con la aplicación de métodos criptográficos que evitan el transporte de la contraseña en texto plano. Existen diversos mecanismos de autenticación, por ejemplo: tarjetas de acceso, sistemas biométricos, hasta los sistemas más seguros basados en certificados digitales PKI[2].

[1] Authentication, Authorization, and Accounting, Autenticación, Autorización y Contabilidad.
[2] Public key infrastructure, Infraestructura de clave pública.

En general la autenticación permite comprobar la identidad de un usuario a través de los siguientes elementos: Algo que se conoce, como un número de identificación personal (PIN[3]) o contraseña; algo que se tiene, como una tarjeta ATM[4] o una tarjeta inteligente; algo que identifique físicamente al usuario de forma única, como una huella dactilar, el reconocimiento de voz, escaneo de la retina ocular, etc. Utilizar más de un factor para identificar al usuario añade credibilidad al proceso de autenticación.

En los sistemas AAA cuando el usuario se autentica para acceder a una red, no establece un canal directo con el servidor de autenticación, si no que el usuario se comunica con un intermediario o equipo autenticador que puede ser un conmutador[5] de red o un punto de acceso inalámbrico, quien traduce y encamina los paquetes hacia el servidor de autenticación. Es decir no existe un camino abierto con el servidor AAA que lo exponga a un ataque directo, cualquier usuario de la LAN que no posea las credenciales de autenticación legítimas para su acceso queda aislado de la infraestructura de red, garantizando así la seguridad del servidor y consecuentemente de todo el sistema AAA.

El proceso de autenticación inicia con un mensaje de solicitud de acceso (Access - Request) desde el equipo NAS[6] al servidor de autenticación. El usuario o suplicante[7] que intenta acceder a la red envía el nombre de usuario y la contraseña cifrada de acuerdo al método de autenticación establecido, hacia el equipo NAS. Éste reenvía entonces el mensaje al servidor de autenticación solicitando la habilitación del puerto de acceso para que el suplicante pueda acceder a los recursos o servicios de red permitidos.

[3] Personal Identification Number, Número de identificación Personal.
[4] Tarjetas ATM (Automatic Teller Machine), tarjeta de cajero automático.
[5] Dispositivo digital lógico de interconexión de redes de computadoras.
[6] Network Access Server, opera como un cliente de un servidor RADIUS.
[7] Software requerido para iniciar el proceso de autenticación.

El formato de un paquete Access - Request se muestra en la Figura 1.

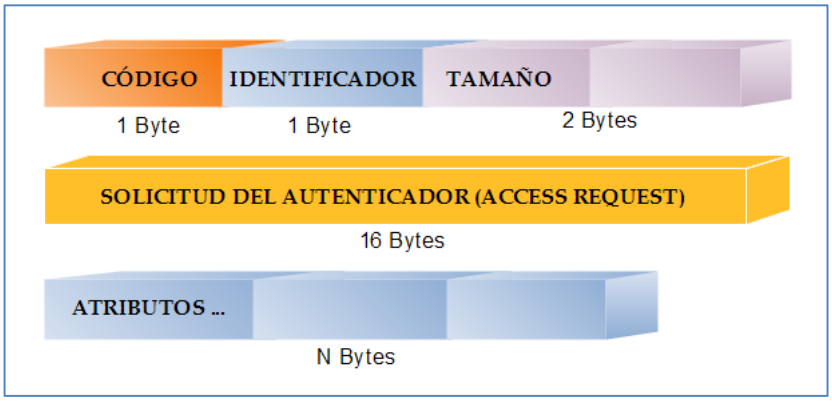


Figura 1. Formato de un paquete Access – Request.
Nota. Fuente: Adaptado de Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS) (p. 18)*. Recuperado de http://tools.ietf.org/pdf/rfc2865.pdf

El paquete Access – Request se identifica mediante la asignación del valor uno en el campo código.

1.1.2 AUTORIZACIÓN

La autorización es el proceso mediante el cual a un usuario se le asigna una determinada cantidad de recursos o servicios de red, en base a las actividades que realice y las políticas[8] de acceso establecidas por el administrador. Está obligatoriamente relacionado con el proceso de autenticación, si un usuario no se autentica correctamente los siguientes procesos se descartan.

Para cumplir con el proceso de autorización los sistemas AAA utilizan soluciones como bases de datos o directorios que permiten almacenar las políticas de acceso de cada usuario.

[8] Conjunto de reglas que indican los privilegios de cada uno de los usuarios de red.

Una vez enviadas las credenciales de autenticación se produce la consulta del servidor a la base de datos[9] de usuarios, para verificar la información del usuario que solicita el acceso.

En los registros se pueden realizar consultas de las políticas relacionados con el usuario que intenta acceder a la red. Se puede crear una variedad de políticas de acceso en base a las necesidades de cada organización, de esta manera el servidor conocerá detalles como: horario de acceso a la red, dirección IP que se debe asignar, parámetros específicos para su conexión, asignación de un ancho de banda determinado, si debe solicitar otro tipo de credenciales, o simplemente si denegar el acceso. Todas estas reglas son definidas para cada usuario en particular o para un grupo de usuarios.

Para el caso de usuarios que no se encuentren registrados en ninguno de los directorios y bases de datos se denegará el acceso, sin embargo existe la posibilidad de crear un perfil dedicado a los usuarios no autenticados, aquellos que acceden al servicio de internet a través de un enlace inalámbrico.

Toda la comunicación en un sistema AAA se basa en la configuración de campos o parámetros que se conocen como atributos o AVP[10] (Attribute Value Pair), el estándar es totalmente configurable, debido a que el intercambio de paquetes entre los equipos se basa en estos atributos.

[9] Aplicación informática para almacenamiento de información de forma organizada.
[10] Método de encapsulación de información usado en una comunicación RADIUS

Algunos atributos están definidos en los RFCs[11] comunes y otros son específicos de cada fabricante de equipos, para el caso de una comunicación AAA utilizando RADIUS los atributos se definen en el RFC 2924[12], se considera atributo a parámetros como: la contraseña de un usuario, nombre de usuario, número de puerto NAS, tipo de autenticación, dirección IP, etc.

Fabricantes como Cisco[13], 3COM[14], etc. disponen de sus diccionarios de atributos para configurar sus equipos NAS, gran parte del intercambio de estos atributos se produce en la fase de autorización.

En la fase de autorización, el servidor luego de conocer los atributos que se deben asignar al solicitante, responderá a la solicitud de autenticación con un mensaje enviado al equipo NAS para permitir, denegar o reintentar la conexión.

Los paquetes que se usan para llevar a cabo este proceso son los siguientes:

- **Access – Accept (Aceptación del acceso).** El objetivo de este paquete es la aceptación del acceso. Si el proceso de autenticación ha sido correcto, se le envía este mensaje al NAS con los atributos necesarios para controlar el acceso del usuario de forma personificada.

  El paquete Access – Accept se identifica mediante la asignación del valor dos en el campo código.

[11] Request for Comments, documento que explica en detalle un protocolo de internet.
[12] Accounting Attributes and Record Formats.
[13] Empresa multinacional dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.
[14] Fabricante de equipos para infraestructuras de Redes Informáticas.

El formato de un paquete Access - Accept se muestra en la Figura 2.

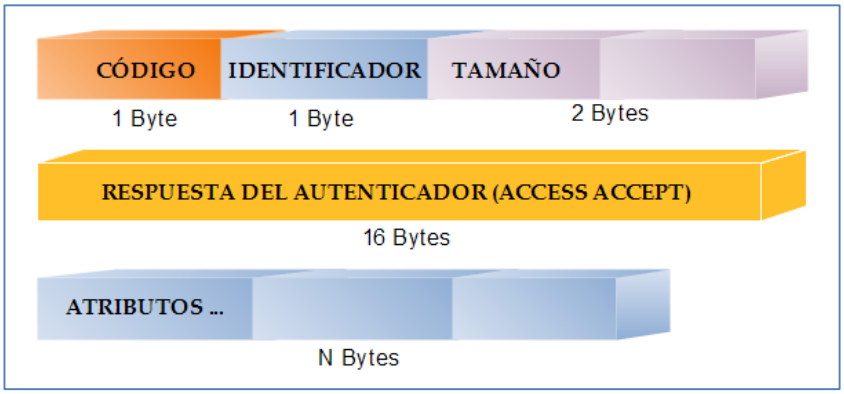


Figura 2. Formato de un paquete Access – Accept.
Nota. Fuente: Adaptado de Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS) (p. 19).* Recuperado de http://tools.ietf.org/pdf/rfc2865.pdf

- **Access – Reject (Denegación del acceso).** Este mensaje se envía cuando a un usuario no se le permite el acceso a la red por diversas circunstancias como: usuario inexistente, contraseña incorrecta, conexión fuera de horario, etc. Se puede incluir en este mensaje la razón por la que se ha denegado el servicio. El NAS que recibe este mensaje no permite el acceso al suplicante, enviando un mensaje de conexión rechazada. El formato de un paquete Access - Reject se muestra en la Figura 3.

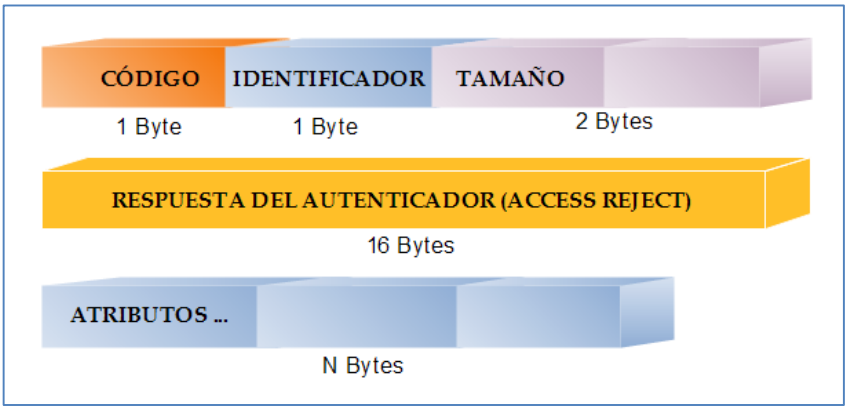


Figura 3. Formato de un paquete Access – Reject.
Nota. Fuente: Adaptado de Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS) (p. 20).* Recuperado de http://tools.ietf.org/pdf/rfc2865.pdf

El paquete Access – Reject se identifica mediante la asignación del valor tres en el campo código.

- **Access – Challenge (Información adicional para el acceso).** Se le solicita al suplicante información adicional, como clave, tarjeta de acceso, PIN de acceso, o cualquier otro método alternativo de acceso. Este tipo de mensajes puede ser intercambiado en múltiples ocasiones dependiendo de la información que se requiera.

  El paquete Access – Challenge se identifica mediante la asignación del valor once en el campo código. El formato se muestra en la Figura 4.

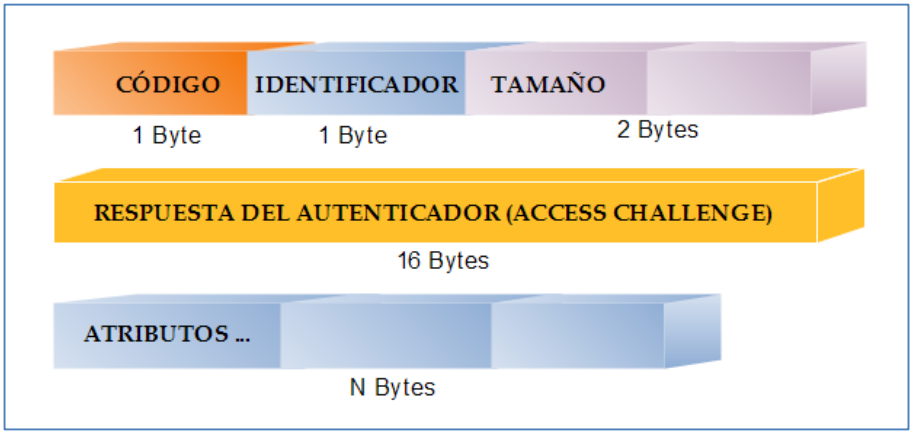


Figura 4. Formato de un paquete Access – Challenge.
Nota. Fuente: Adaptado de Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS) (p. 22).* Recuperado de http://tools.ietf.org/pdf/rfc2865.pdf

Una vez realizado el intercambio de mensajes el usuario estará autorizado o no a usar los recursos de la red a la cual desea acceder. En caso de estarlo sería controlado por las políticas de acceso fijadas durante el proceso de autorización, que describen las

características de la conexión para el usuario autenticado como duración máxima de la sesión, máximo flujo de datos, VLANs[15] de acceso, etc.

1.1.3 CONTABILIDAD

Finalmente una vez realizado el proceso de autenticación y autorización se produce la fase de contabilidad o "Acconunting". Ésta inicia cuando el equipo autenticador o NAS autoriza al suplicante acceder a los servicios de red. La contabilidad es el proceso estadístico y de recolección de datos sobre la conexión.

Estos valores se almacenan generalmente en bases de datos SQL[16] relacionadas con el usuario o en ficheros tipo log. Esta información manejada y procesada correctamente permite tomar decisiones en cuanto al uso de los recursos por parte de los usuarios, con el fin de gestionar de manera eficiente todos los servicios de red.

El buen tratamiento de los datos recolectados durante los procesos de autenticación y autorización permiten al administrador de la red gestionar la futura demanda de sus sistemas para planificar su crecimiento. Algunos sistemas de seguridad generan avisos por intentos reiterados o denegados de conexiones fallidas para tomar decisiones que mejoren la seguridad, lamentablemente la mayor parte de equipos y servidores no proveen el soporte para este servicio.

[15] Virtual LAN, red de área local virtual.
[16] Structured Query Language, Lenguaje de consulta estructurado.

En una comunicación RADIUS[17] el tipo de paquetes que se transmiten durante el proceso de contabilidad son los siguientes:

- **Accounting-Request (Solicitud para Contabilidad).** Generalmente este tipo de paquetes son enviados desde un cliente NAS hacia un servidor, para indicar que ha comenzado la fase de contabilidad y registrar los datos de la sesión del usuario. Para señalar que se trata de un paquete Accountig-Request el cliente asigna el código cuatro en el campo correspondiente de la trama.

  Una vez recibido el paquete, el servidor transmite un mensaje Accouting-Response indicando que el proceso de contabilidad ha iniciado con éxito, caso contrario no se envía ninguna respuesta.

  EL formato de un paquete Accouting-Request se muestra en la Figura 5.

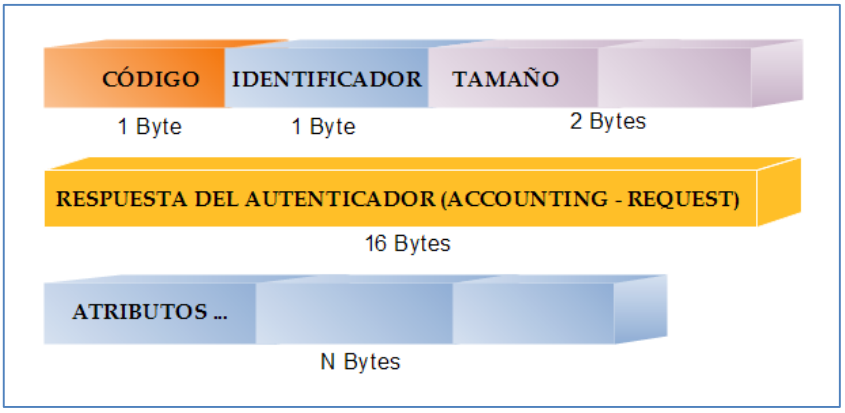


Figura 5. Formato de un paquete Accouting – Request.
Nota. Fuente: Adaptado de Rigney, C. (Junio de 2000). *RADIUS Accounting (p. 8).* Recuperado de http://tools.ietf.org/pdf/rfc2866.pdf

El paquete Accouting-Request se identifica mediante la asignación del valor cuatro en el campo código.

[17] Remote Authentication Dial In User Service

- **Accounting-Response (Respuesta para Contabilidad).** Los paquetes de respuesta son transmitidos por el servidor RADIUS hacia el cliente, indicando que la solicitud de contabilidad se ha recibido y registrado con éxito. Si esto sucede el servidor envía un paquete con el código cinco en el campo de la trama Accounting-Response.

El paquete Accouting-Response se identifica mediante la asignación del valor cinco en el campo código.

El formato de un paquete Accouting-Response se muestra en la Figura 6:

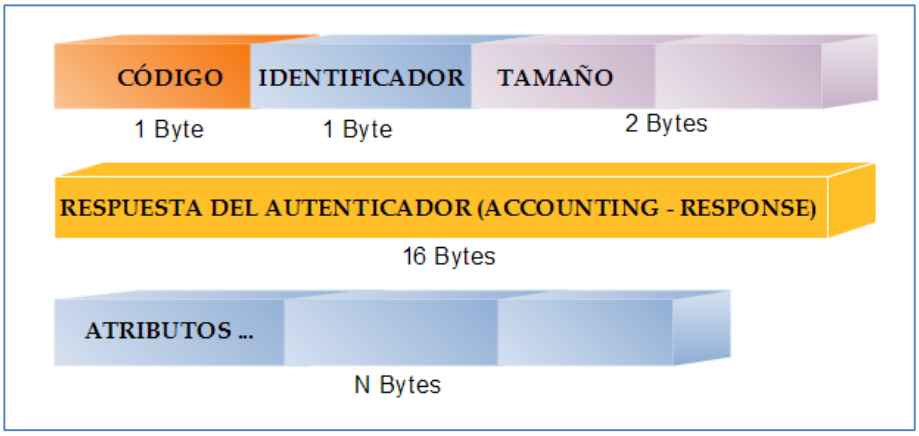


Figura 6. Formato de un paquete Accouting-Response.
Nota. Fuente: Adaptado de Rigney, C. (Junio de 2000). *RADIUS Accounting (p. 10).* Recuperado de http://tools.ietf.org/pdf/rfc2866.pdf

1.2 RADIUS

RADIUS son las siglas de Remote Authentication Dial In User Service, que significa Autenticación Remota para usuarios de Servicio Telefónico. Es un protocolo AAA (Autenticación, Autorización y Contabilidad) utilizado en aplicaciones de acceso a redes.

1.2.1 INTRODUCCIÓN A RADIUS

RADIUS es una solución que se puede implementar sobre diversas plataformas (Windows, GNU/Linux, Unix, Solaris, etc…) para permitir servicios de acceso a la red mediante el manejo de diversos mecanismos de autenticación soportados. Los números de puerto UDP[18] asignados oficialmente para las comunicaciones RADIUS son el 1812 en la autenticación y 1813 en la contabilidad.

El protocolo RADIUS ha evolucionado desde su creación lo que ha permitido solventar muchos fallos de seguridad que se han descubierto con el paso del tiempo, a pesar de sus limitaciones ha ido adoptando una serie de mejoras que han hecho de este protocolo una solución fiable y segura para su implementación.

1.2.2 PROTOCOLO RADIUS

RADIUS es un protocolo cuya infraestructura de red se basa en un modelo cliente-servidor, donde los servicios de autenticación, autorización y contabilidad son administrados por un equipo proveedor de recursos, en este caso el servidor RADIUS, y los clientes son aquellos que acceden a los servicios ofrecidos. De esta manera se tiene una gestión centralizada que permite mejorar el nivel de seguridad de la red.

Un equipo de acceso a la red NAS opera como un cliente de RADIUS. El cliente es el responsable de transmitir la información al servidor RADIUS y luego actuar de acuerdo a la respuesta entregada por el servidor.

[18] User Datagram Protocol, Protocolo de transporte basado en el intercambio de datagramas.

El servidor RADIUS se encarga de recibir las solicitudes de acceso de los usuarios que intentan conectarse a la red, verificar las credenciales en base a los registros que se utilicen para almacenar las políticas de acceso, y finalmente enviar toda la información de configuración necesaria al equipo autenticador para que este entregue el servicio al usuario.

La seguridad en una comunicación RADIUS es garantizada, los paquetes que se transmiten entre el cliente y el servidor son encriptados mediante el uso de un shared secret[19] (secreto compartido) el cual nunca se envía a través de la red para evitar posibles intercepciones. El secreto compartido es una contraseña con formato alfanumérico que se establecen en los extremos de un canal de comunicación, usada para encriptar las comunicaciones entre el cliente y el servidor RADIUS.

El protocolo RADIUS soporta varios mecanismos para autenticar a los usuarios que quieren acceder a la red, esto permite implementar sistemas AAA con diversos niveles de seguridad de acuerdo a los requerimientos de la red en la cual se va a implantar la solución.

1.2.3 FORMATO DEL PAQUETE RADIUS

RADIUS utiliza UDP como protocolo de transporte, razón por la cual no otorga garantías en la entrega de sus mensajes. El formato del paquete UDP que se muestra en la figura 7 se encuentra definido en el RFC 768.

[19] Contraseña secreta conocida solo por las partes involucradas en una comunicación segura.

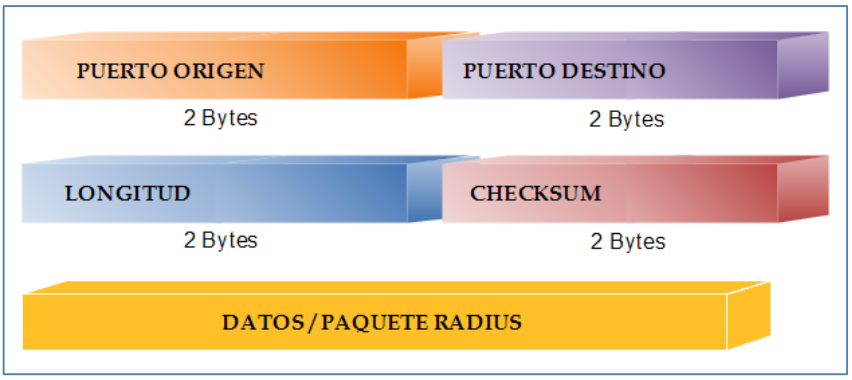


Figura 7. Formato del paquete UDP
Nota. Fuente: Adaptado de Postel, J. (28 de Agosto de 1980). *User Datagram Protocol (p. 1)*. Recuperado de http://tools.ietf.org/pdf/rfc768.pdf

El paquete RADIUS se inserta en el campo datos UDP cuando el valor del puerto destino es 1812 (decimal).

La estructura de un paquete RADIUS se encuentra definido en el RFC 2865, véase la Figura 8.

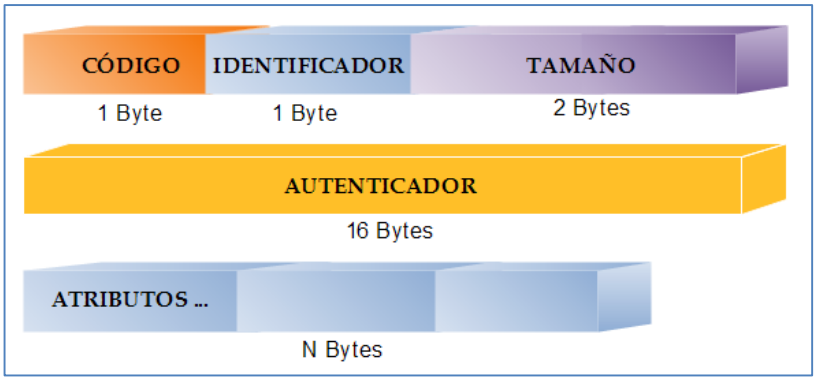


Figura 8. Estructura de un paquete RADIUS
Nota. Fuente: Adaptado de Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS) (p. 14)*. Recuperado de http://tools.ietf.org/pdf/rfc2865.pdf

CÓDIGO. El campo código tiene una longitud de ocho bits e identifica el tipo de paquete RADIUS. Cuando un paquete se recepta con un código inválido este se descarta. Los códigos comúnmente usados por RADIUS se muestran en la Tabla 1:

Tabla 1. Códigos de los tipos de paquetes RADIUS

CÓDIGO (DECIMAL)	TIPO DE PAQUETE RADIUS
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Nota. Fuente: Adaptado de Fernández, Y., Ramos, A., & García, J. (2008). *RADIUS / AAA / 802.1X : Sistemas basados en la autenticación en Windows y GNU/Linux (pp.77-78).* Madrid: RA-MA Editorial.

IDENTIFICADOR. El campo Identificador tiene una longitud de ocho bits y permite relacionar los paquetes que conforman una conversación (solicitud – respuesta), cada cliente cuando solicita un servicio lo hace con un número diferente. El servidor RADIUS puede detectar solicitudes duplicadas si el valor del campo identificador es el mismo.

LONGITUD. Este campo es de dos bytes, e indica el tamaño total del paquete incluyendo el código, identificador, tamaño, autenticador, y el campo atributos. Los octetos que se encuentren fuera de este valor son considerados como relleno y se ignoran en la recepción. Si el tamaño del paquete es inferior al indicado este se descarta. El tamaño mínimo del paquete es 20 y el máximo 4096.

AUTENTICADOR. El campo autenticador tiene un tamaño de 16 Bytes. El octeto más significativo se transmite primero, este valor es usado para autenticar las respuestas del servidor RADIUS y se utiliza como elemento en un algoritmo para encriptar la comunicación.

- **Solicitud del Autenticador**. En las solicitudes de acceso el valor para el campo Autenticador es un número aleatorio de 16 Bytes. Este valor es un número único e irrepetible que brinda seguridad en una comunicación. La clave secreta (shared secret) que comparte el NAS y el servidor RADIUS junto a este valor aleatorio se usan para generar un nuevo de 16 bytes, luego se aplica el cifrado XOR[20] entre el ultimo valor obtenido y la contraseña introducida por el usuario, generándose así el atributo contraseña de usuario requerido en el paquete solicitud de acceso.

- **Respuesta del Autenticador**. El valor del campo Autenticador en los paquetes Access-Accept, Access-Reject, y Access-Challenge contiene un número MD5[21] calculado de la cadena de bytes de los campos: código + longitud + solicitud de autenticación + atributos + clave secreta.

ATRIBUTOS. Son variables a las que se les asigna una función, un tipo de dato o un valor enviados en las solicitudes y respuestas de los sistemas AAA, por ejemplo el nombre de usuario, contraseña, número de puerto, método de autenticación, etc. Existen hasta 256 atributos, estos están definidos en los RFCs que establecen las normas de las comunicaciones RADIUS.

[20] Operador lógico.
[21] Message-Digest Algorithm 5, es un algoritmo de reducción criptográfico de 128 bits.

La trama de un atributo estándar se muestra en la Figura 9:

Figura 9. Formato del campo ATRIBUTO en RADIUS
Nota. Fuente: Adaptado de Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS) (p. 23).* Recuperado de http://tools.ietf.org/pdf/rfc2865.pdf

- TIPO. El campo tipo tiene una longitud de 1 Byte, representa el código del atributo ya que no se utiliza el nombre real del atributo. El rango de valores 192-223 está restringido para usos experimentales, el rango 224-240 para implementaciones específicas, y el rango 241-255 está reservado y no debe ser usado. Si este campo toma algún valor desconocido, el cliente y servidor ignoraran el paquete.

Los tipos de atributos se definen en el RFC 1700 (Asignación de números), algunos ejemplos se muestran en la Tabla 2.

Tabla 2. Tipo de Atributos RADIUS

CÓDIGO	TIPO DE ATRIBUTO	CÓDIGO	TIPO DE ATRIBUTO
1	User-Name	**21**	(unassigned)
2	User-Password	**22**	Framed-Route
3	CHAP-Password	**23**	Framed-IPX-Network
4	NAS-IP-Address	**24**	State
5	NAS-Port	**25**	Class
6	Service-Type	**26**	Vendor-Specific
7	Framed-Protocol	**27**	Session-Timeout
8	Framed-IP-Address	**28**	Idle-Timeout

9	Framed-IP-Netmask	**29**	Termination-Action
10	Framed-Routing	**30**	Called-Station-Id
11	Filter-Id	**31**	Calling-Station-Id
12	Framed-MTU	**32**	NAS-Identifier
13	Framed-Compression	**33**	Proxy-State
14	Login-IP-Host	**34**	Login-LAT-Service
15	Login-Service	**35**	Login-LAT-Node
16	Login-TCP-Port	**36**	Login-LAT-Group
17	(unassigned)	**37**	Framed-AppleTalk-Link
18	Reply-Message	**38**	Framed-AppleTalk-Network
19	Callback-Number	**39**	Framed-AppleTalk-Zone
20	Callback-Id	**40 - 59**	(reserved for accounting)

Nota. Fuente: Adaptado de Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS) (p. 24).* Recuperado de http://tools.ietf.org/pdf/rfc2865.pdf

- **LONGITUD.** El tamaño de este campo es un Byte, e indica el tamaño del paquete incluyendo los tres campos tipo, longitud y valor. Si en una solicitud de acceso se recibe un paquete con una longitud inválida, se responde con una denegación de acceso.

- **VALOR.** El campo valor puede o no contener datos. En este campo se inserta información específica de cada atributo. La longitud y formato de este campo dependerá del tipo de atributo que se envíe.

1.2.4 PROCESO AAA DE RADIUS

Cuando un usuario accede a una red mediante un Sistema AAA RADIUS ocurre un proceso de intercambio de paquetes que garantizan un elevado nivel de seguridad para todos los elementos de la red.

El estándar de autenticación IEEE[22] 802.1x[23] define tres elementos que intervienen en un proceso de autenticación: el usuario o suplicante, el cliente o NAS, y el servidor de autenticación. La secuencia de comunicación AAA de RADIUS se muestra en la Figura 10.

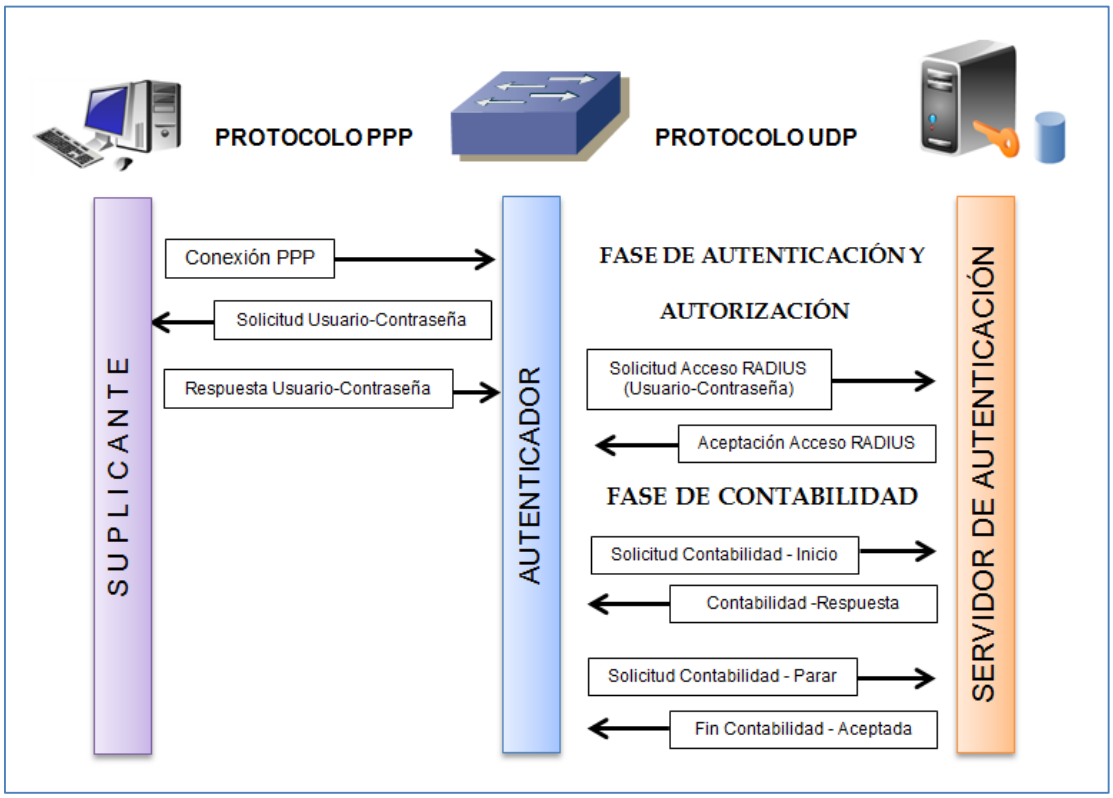


Figura 10. Secuencia de comunicación AAA RADIUS
Nota. Fuente: Adaptado de Fernández, Y., Ramos, A., & García, J. (2008). *RADIUS / AAA / 802.1X : Sistemas basados en la autenticación en Windows y GNU/Linux (p. 80).* Madrid: RA-MA Editorial.

Cuando un cliente, por ejemplo un switch, se configura para usar un servidor RADIUS, cualquier usuario que intente acceder a la red a través de él debe autenticarse para poder hacerlo. Existen muchos métodos de autenticación, el que comúnmente usamos a diario es mediante un usuario y contraseña. Por razones de seguridad se utilizan diversos mecanismos de encriptación que permiten transportar estos datos de manera segura.

[22] Institute of Electrical and Electronics Engineers.
[23] Norma del IEEE para el control de acceso a la red basada en puertos.

Una vez obtenida la información, se autentica al usuario mediante un servidor RADIUS. Para esto, el NAS crea un paquete Access-Request que contenga los atributos del usuario que intenta acceder a la red, por ejemplo: nombre de usuario, contraseña de usuario, identificador del cliente, número de puerto a través del cual está accediendo, etc. Por seguridad las contraseñas nunca se envían en texto plano, se codifican usando el algoritmo MD5.

El paquete solicitud de acceso se envía al servidor RADIUS a través de la red. En caso de no haber respuesta por parte del servidor en un determinado tiempo se reenvía el paquete. El cliente puede enviar la solicitud de acceso a un servidor secundario si existiera, un servidor alternativo se puede utilizar después de un determinado número de intentos de conexión fallidos con el servidor principal.

Una vez que el servidor RADIUS recibe la solicitud, lo valida enviando una respuesta al cliente. En las comunicaciones RADIUS tanto el cliente como el servidor conocen una contraseña secreta, si la solicitud de autenticación no contiene esta clave el paquete se descarta inmediatamente.

Si el cliente es válido, el servidor RADIUS consulta en la base de datos de usuarios para encontrar al usuario cuyo nombre coincide con la solicitud. La base de datos contiene una lista de requisitos que se deben cumplir para permitir el acceso al usuario, así como los recursos y servicios que puede usar. El servidor RADIUS puede hacer solicitudes de acceso a otros servidores con el fin de garantizar la autenticidad del usuario, en este caso el servidor actúa como un cliente.

Si alguna condición no se cumple el servidor responde con un paquete rechazando a la solicitud de acceso, se puede configurar al servidor para que añada un mensaje de texto indicando las razones del fallo. Caso contrario si tras verificar las credenciales y los servicios autorizados para el usuario se decide aceptar el acceso, el servidor envía una respuesta al NAS con los atributos necesarios para permitir el servicio.

Tras haber superado el proceso de autenticación y autorización, el NAS abrirá el puerto solicitado con los atributos designados para proveer el servicio al usuario. Al mismo tiempo envía un mensaje al servidor RADIUS indicando que ha comenzado a registrar los datos de sesión de usuario mediante un paquete tipo Accounting-Request [Start]. Si el equipo NAS no soporta este servicio se omite este proceso.

El servidor RADIUS una vez recibida esta solicitud almacena en su base de datos la información de inicio de sesión del usuario, y responde con un mensaje Accounting-Response [Start] al NAS indicando el correcto inicio del proceso de contabilidad.

Cuando el usuario termina la sesión por cualquier razón, el NAS informa al servidor con un mensaje Accounting-Request [Stop], enviando toda la información referente al consumo de recursos del usuario. El servidor RADIUS informa la correcta recepción de estos datos al NAS mediante un mensaje Accounting-Response [Stop].

1.3 MÉTODOS DE AUTENTICACIÓN

Los métodos de autenticación son paquetes de software programados para soportar un protocolo de autenticación específico con el fin de negociar el acceso de un usuario a la

red durante el establecimiento de la conexión. Este software es el encargado de realizar el cifrado, descifrado y empaquetado de todos los paquetes involucrados en el proceso de autenticación.

Los métodos de autenticación han evolucionado su seguridad a la par de las amenazas, vulnerabilidades y riesgos de seguridad que han surgido con el tiempo y la tecnología. Actualmente existen muchos métodos de autenticación utilizados para verificar las credenciales de los usuarios y controlar el acceso a la red, desde los más básicos como PAP[24], CHAP[25] hasta los más robustos y seguros como EAP.

Existe una variedad de métodos de autenticación que usan el Protocolo de Autenticación Extensible (EAP).

Métodos EAP

- EAP-MD5
- EAP-OTC
- EAP-GTC
- EAP-MS-CHAP
- EAP-MS-CHAPv2
- EAP-SIM

[24] Password Authentication Protocol, protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto mediante contraseña.
[25] Challenge-Handshake Authentication Protocol, protocolo de autenticación basado en un sistema desafío-respuesta.

Métodos EAP propietarios de Cisco

- EAP-LEAP
- EAP-FAST

Métodos EAP basados en Certificados

- EAP-TLS
- EAP-TTLS
- EAP-PEAP

1.3.1 PROTOCOLO DE AUTENTICACIÓN EXTENSIBLE EAP

El Protocolo de Autenticación Extensible (EAP) se creó inicialmente para permitir la autenticación de usuarios en sistemas que usaban el protocolo PPP[26], se encuentra establecido en el RFC 2284. Sin embargo su poca flexibilidad para soportar otros métodos de autenticación dio paso al nuevo estándar EAP definido en el RFC 3748, el cual detalla al Protocolo de Autenticación Extensible para el uso con el estándar IEEE 802.1x, que permite la implementación de una gran variedad de mecanismos de autenticación que pueden funcionar sobre cualquier capa de enlace.

EAP es un protocolo encargado del transporte, encapsulado y seguridad de la autenticación. Soporta múltiples mecanismos de autenticación, lo que lo hace muy versátil para cualquier tipo de implementación a cualquier escala. Al ser EAP un protocolo de transporte como PPP dispone de sus propios mecanismos de control para la conexión.

[26] Point-to-Point Protocol. permite establecer una comunicación a nivel de la capa de enlace TCP/IP.

El intercambio de mensajes en una autenticación EAP es simple y tiene la siguiente secuencia:

- El equipo autenticador envía un paquete al suplicante solicitando las credenciales o cualquier otro parámetro necesario para proceder con la autenticación.

- El usuario que realizó la petición responde con un mensaje al equipo autenticador, enviando la información requerida. Parámetros como nombre de usuario, contraseña de usuario, código de identidad, etc. son enviados en este paquete.
- El NAS o equipo autenticador no realiza el proceso de autenticación, simplemente direcciona el paquete de datos recibido hacia el servidor de autenticación, el trabajo del NAS es encapsular los paquetes tipo EAP en paquetes RADIUS. El resto del proceso se lleva a cabo entre el servidor y el equipo autenticador, en esta parte el intercambio de mensajes es manejado de forma transparente por el protocolo RADIUS.

1.3.1.1 EAP-TLS

El Protocolo de Autenticación Extensible (EAP) se encuentra definido en el RFC 3748 y permite múltiples métodos de autenticación, uno de ellos EAP-TLS. Transport Layer Security (TLS[27]), es el sucesor del protocolo SSL[28], permite una conexión segura mediante la creación de un canal cifrado entre el cliente y el servidor.

[27] Transport Layer Security, Seguridad en la Capa de Transporte.
[28] Secure Sockets Layer, Capa de conexión segura.

El método EAP-TLS se basa en una autenticación mutua, lo que significa, que tanto el suplicante debe autenticarse contra el servidor como el servidor contra el suplicante, de esta manera se evitan los ataques del tipo MiTM[29] (hombre en medio) que pueden provocar que un suplicante entregue sus credenciales a un falso servidor.

Cuando los certificados digitales se despliegan se deben instalar en todos los suplicantes de la red y en el servidor de autenticación. Una desventaja significativa de usar EAP-TLS en una red empresarial con una gran cantidad de usuarios, es la difícil tarea de administrar los certificados digitales.

El administrador de la red deberá instalar un nuevo certificado después de adquirir un nuevo ordenador o cualquier otro dispositivo que hará uso de la autenticación mediante EAP-TLS.

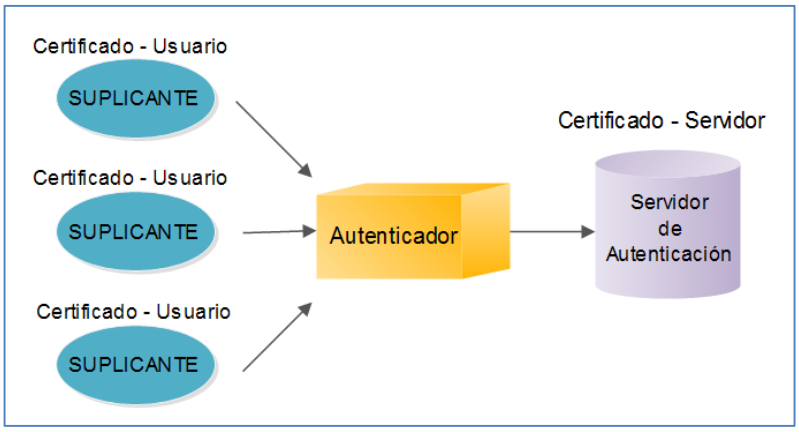


Figura 11. La autenticación EAP-TLS requiere certificados digitales en el servidor y todos los suplicantes.
Nota. Fuente: Adaptado de Geier, J. (2008). *Implementing 802.1X Security Solutions for Wired and Wireless Networks (p. 111).* Indianapolis: Wiley Publishing, Inc.

[29] Man-in-the-middle. es un ataque en el que el enemigo adquiere la capacidad de interceptar y modificar los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

El RFC 5216 establece la secuencia de una autenticación exitosa usando el método EAP-TLS, véase la Figura 12, cuyo proceso inicia con el envío de un paquete EAP-Request/Identity del equipo autenticador hacia cualquier suplicante una vez detectado una conexión activa, por ejemplo, cuando el sistema de un suplicante se ha asociado a un punto de acceso.

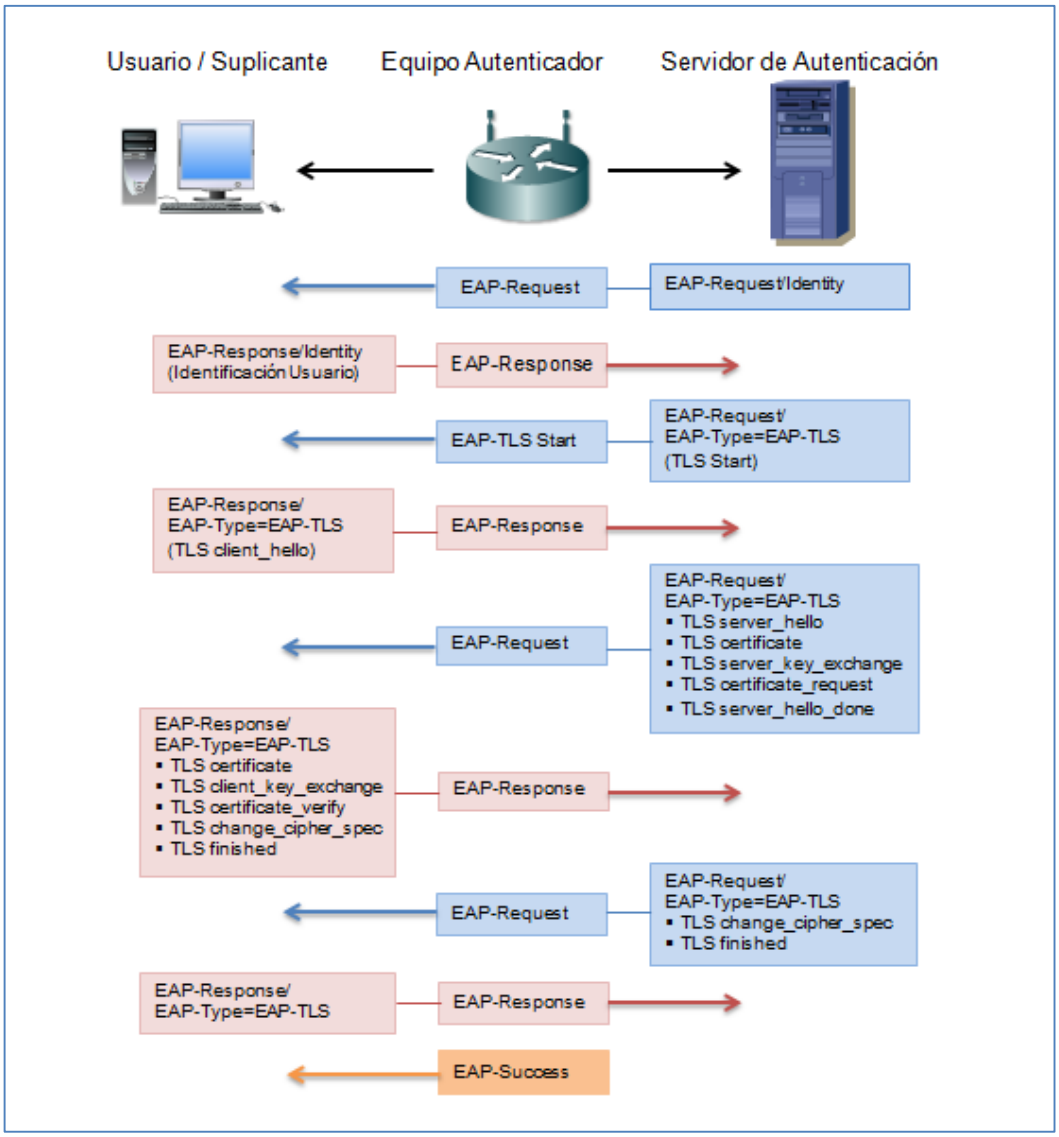


Figura 12. Secuencia de autenticación usando el método EAP-TLS
Nota. Fuente: Adaptado de Simon, D., Aboba, B., & Hurst, R. (Marzo de 2008). *The EAP-TLS Authentication Protocol (p. 6).* Recuperado de http://tools.ietf.org/pdf/rfc5216.pdf

Una conversación TLS normalmente comienza con la autenticación, intercambiando paquetes EAP entre los pares suplicante – autenticador. El autenticador envía un paquete EAP-Request/Identity al suplicante solicitando la identidad del usuario, el cual responderá con un mensaje EAP-Response/Identity con la información requerida. A partir de este punto, el equipo autenticador encapsula los paquetes recibidos para enviarlos hacia el servidor de autenticación, el cual se encarga de continuar con el proceso de autenticación.

Una vez recibida la identidad del usuario que intenta acceder a red, el servidor responde con un mensaje EAP-TLS/Start, el paquete contiene un campo [s] el cual indica el inicio del proceso, este paquete no contiene datos.

La conversación EAP-TLS inicia cuando el suplicante responde con un mensaje EAP-Type=EAP-TLS. El mensaje de respuesta contiene un saludo (client_hello) en el campo de datos, que transporta detalles como la versión TLS del suplicante, un identificador de sesión, un número aleatorio y los métodos de cifrado soportados por el usuario.

El servidor responderá con un paquete EAP-Request indicando el tipo de EAP utilizado para la comunicación. En el campo datos de este mensaje se insertarán un conjunto de atributos como: mensaje de saludo [server_hello], seguido de un certificado TLS, certificado de clave pública [server_key_exchange], solicitud del certificado [certificate_request], y un mensaje de finalización [server_hello_done]. El mensaje de finalización contiene el número de versión TLS, un número aleatorio, el identificador de la sesión, y los métodos de cifrado.

Si el usuario o suplicante soporta el método de autenticación EAP-TLS y está configurado correctamente para su uso, responde con un paquete EAP-Response enviando todos los parámetros solicitados en este mensaje. En caso de ser requerido un certificado, el usuario envía adicionalmente un paquete de verificación [certificate_verify].

De esta manera el servidor EAP verifica el certificado y firma digital para establecer un canal protegido mediante TLS, logrando así establecer una sesión segura de comunicaciones. Dentro de este canal se puede utilizar cualquier otro sistema de autenticación menos seguro como PAP, CHAP, u otros similares.

1.3.1.1.1 Descripción de los paquetes EAP-TLS Request y EAP-TLS Response

Los paquetes EAP-TLS Request y EAP-TLS Response se encuentran definidos en el RFC 5216, el formato se muestra en la Figura 13:

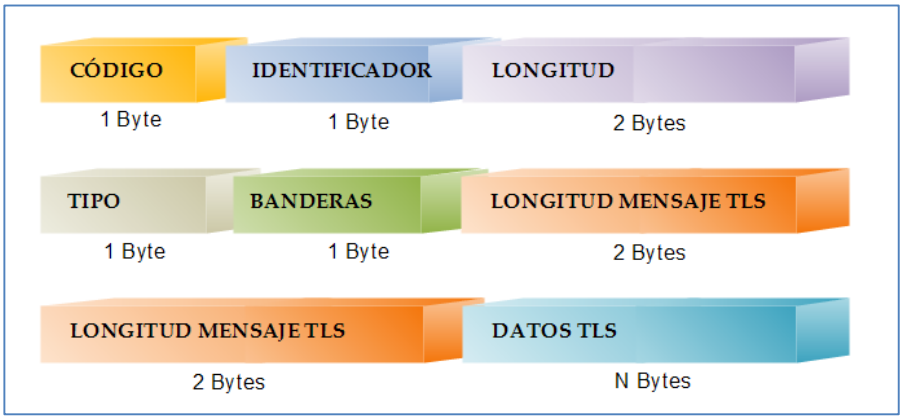


Figura 13. Formato del paquete EAP-TLS Request
Nota. Fuente: Adaptado de Simon, D., Aboba, B., & Hurst, R. (Marzo de 2008). *The EAP-TLS Authentication Protocol (pp 20-22).* Recuperado de http://tools.ietf.org/pdf/rfc5216.pdf

Código. Este campo tiene una longitud de un Byte. Para identificar un paquete EAP-TLS Request se asigna el código uno y para un EAP-TLS Response el código dos.

Identificador. El campo identificador tiene una longitud de un byte, y permite asociar las solicitudes con las respuestas, este campo se modifica con cada solicitud.

Longitud. El campo longitud es de 2 Bytes, e indica el tamaño del paquete EAP incluyendo los campos: código, identificador, longitud, tipo y datos. Los bytes que excedan el tamaño indicado se deben tratan como relleno y son ignorados en recepción.

Tipo. Al paquete EAP-TLS le corresponde el código 13.

Banderas. Este campo tiene 1 Byte de longitud y los bits que lo conforman indican diferentes estados:

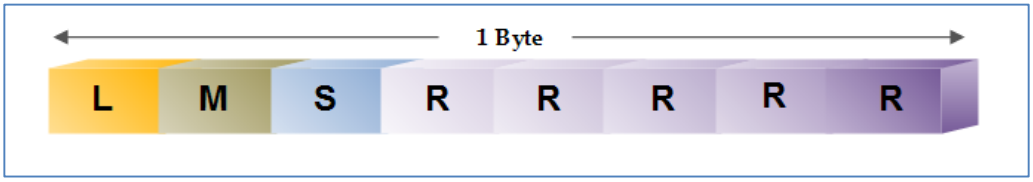


Figura 14. Banderas de un paquete EAP-TLS
Nota. Fuente: Adaptado de Simon, D., Aboba, B., & Hurst, R. (Marzo de 2008). *The EAP-TLS Authentication Protocol (p. 21).* Recuperado de http://tools.ietf.org/pdf/rfc5216.pdf

- L = [length included]. Este bit indica la inserción del campo Longitud del Mensaje TLS de cuatro bytes.
- M = [More fragments]. Este bit se incluye en todos los paquetes menos en el último, lo que permite saber cuándo se termina la transmisión.
- S = [EAP-TLS start]. Este bit indica el inicio de una comunicación EAP-TLS. Está presente únicamente en los paquetes EAP-TLS Request.
- R = [Reserved]. Estos bits son reservados y se envían como ceros.

Longitud del mensaje TLS. Este campo es de cuatro Bytes, y solo está presente cuando el bit L así lo indica. Este indica la longitud total del mensaje TLS o conjunto de mensajes que se está fragmentando.

Datos TLS. Este campo corresponde al paquete encapsulado con formato TLS.

1.3.1.2 EAP-TTLS

EAP-TTLS[30] fue desarrollado como una extensión de EAP-TLS, se basa en el sistema de autenticación mutua mediante certificados digitales, sin embargo EAP-TTLS requiere la instalación de un certificado sólo del lado del servidor.

Los usuarios pueden identificarse a través de una contraseña, en lugar de un certificado, reduciendo considerablemente la complejidad del sistema de autenticación debido a que no existe necesidad de instalar y gestionar los certificados de todos los dispositivos de la red.

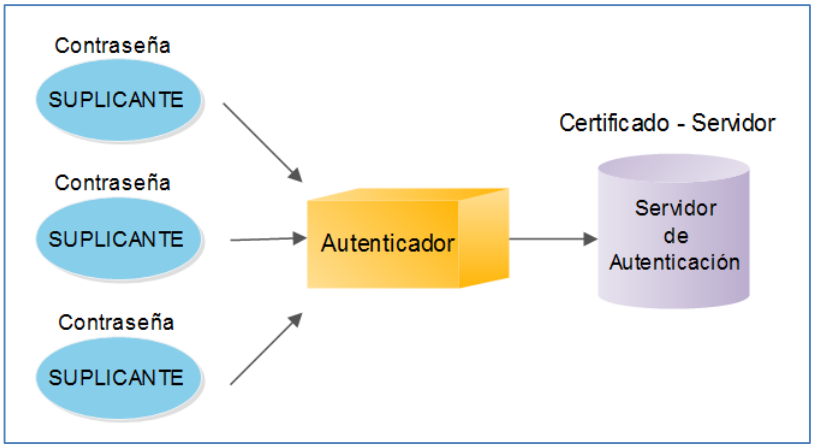


Figura 15. EAP-TTLS sólo requiere certificados digitales en el servidor de autenticación.
Nota. Fuente: Adaptado de Geier, J. (2008). *Implementing 802.1X Security Solutions for Wired and Wireless Networks (p. 112).* Indianapolis: Wiley Publishing, Inc.

[30] Túnel Transport Layer Security

EAP-TTLS es un método de autenticación que crea túneles TLS (Transport Layer Security) para enviar los paquetes de forma segura. La comunicación TTLS se establece en dos fases, el primer túnel TLS se crea para el intercambio de credenciales donde el cliente se autentica con el servidor o viceversa, esto permite crear un túnel seguro usando mecanismos criptográficos para el intercambio de información que procederá en la siguiente fase.

En la fase posterior, el cliente se autentica con el servidor utilizando cualquier mecanismo menos seguro como PAP, CHAP, MS-CHAP. De esta manera EAP-TTLS soporta conexiones con bases de datos de autenticación manteniendo en todo momento un medio seguro para el intercambio de datos. La fase dos no siempre es necesario realizarla ya que el usuario se ha autenticado de forma segura en la primera parte.

Fase 1: Saludo (Handshake). El servidor inicia el método EAP-TTLS enviando el paquete de inicio EAP-TTLS/Start, los paquetes EAP se siguen intercambiando entre el cliente y el servidor al igual que EAP-TLS descrito en la anterior sección, hasta completar el saludo.

Fase 2: Tunelamiento. En la fase dos, se utiliza el túnel para intercambiar información de seguridad entre las partes, esta información es encapsulada en secuencias atributo-valor AVP. Cualquier tipo de información puede ser intercambiada en la fase dos de acuerdo a los requerimientos del sistema. Una vez que el suplicante envía los datos, el servidor recupera esta información para procesarla, el intercambio de información continua hasta que el servidor acepta o rechaza la conexión con el cliente.

1.3.1.2.1 Formato del paquete EAP-TTLS

El paquete EAP-TTLS se encuentra definido en el RFC 5281, su formato se muestra en la Figura 16.

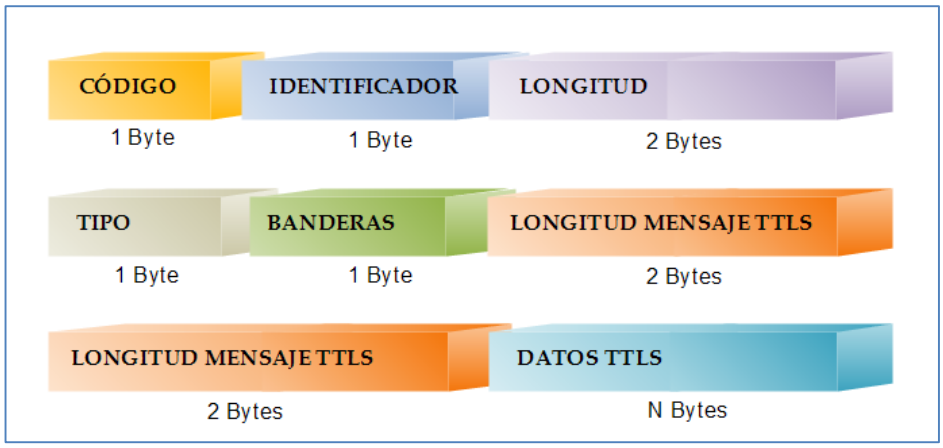


Figura 16. Estructura de un paquete EAP-TTLS
Nota. Fuente: Adaptado de Funk, P., & Blake, S. (Agosto de 2008). *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) (p. 20).* Recuperado de http://tools.ietf.org/pdf/rfc5281.pdf

Código. Este campo tiene una longitud de un Byte. Se asigna el código uno para los paquetes de solicitud y dos para las respuestas.

Identificador. El campo identificador tiene una longitud de un byte, y permite asociar las solicitudes con las respuestas, este campo se modifica con cada solicitud.

Longitud. El campo longitud es de 2 Bytes, e indica el tamaño del paquete EAP desde el código hasta los datos.

Tipo. Al paquete EAP-TTLS le corresponde el código 21.

Banderas. Este campo tiene 1 Byte de longitud y los bits que lo conforman indican diferentes estados o acciones:

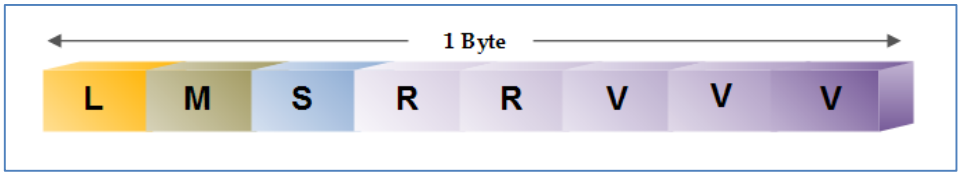


Figura 17. Banderas de un paquete EAP-TTLS
Nota. Fuente: Adaptado de Funk, P., & Blake, S. (Agosto de 2008). *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) (p. 21).* Recuperado de http://tools.ietf.org/pdf/rfc5281.pdf

- L = [length included]. Este bit indica la inserción del campo Longitud del Mensaje de cuatro bytes.
- M = [More fragments]. Este bit se incluye en todos los paquetes menos en el último, lo que permite saber cuándo se termina la transmisión.
- S = [EAP-TLS start]. Este bit indica el inicio de una comunicación EAP-TTLS. Está presente únicamente en los paquetes EAP-TTLS Request.
- R = [Reserved]. Estos 3 bits son reservados y se envían como ceros.
- V = Version (000 para EAP-TTLSv0)

Longitud del mensaje. Este campo es de cuatro Bytes, y solo está presente cuando el bit L así lo indica. Este indica la longitud total del mensaje TTL o conjunto de mensajes que se está fragmentando.

Datos. Este campo corresponde a la secuencia de mensajes encapsulados con formato TLS, en este se pueden incluir los pares atributo – valor AVP.

1.3.1.2.2 Formato de un paquete AVP

El formato de un paquete AVP está definido en el RFC 5281, véase la Figura 18.

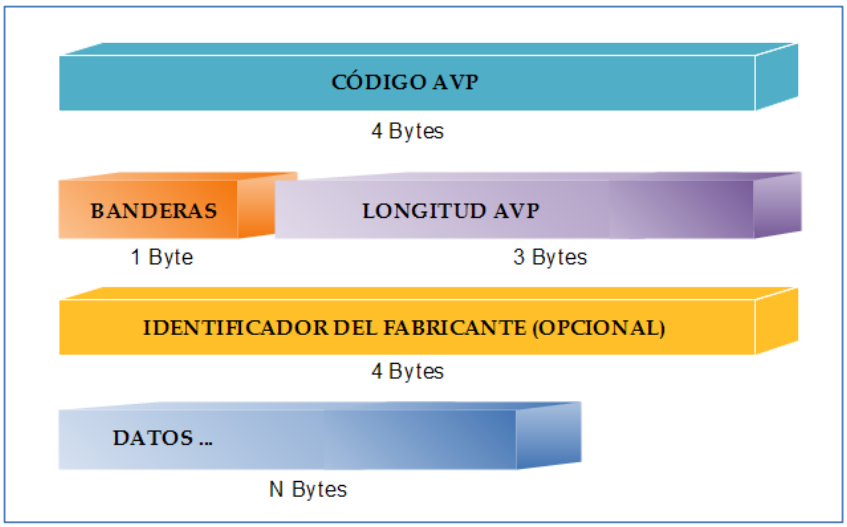


Figura 18. Formato de un paquete AVP
Nota. Fuente: Adaptado de Funk, P., & Blake, S. (Agosto de 2008). *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) (p. 24).* Recuperado de http://tools.ietf.org/pdf/rfc5281.pdf

Código AVP. Este campo está formado de 4 bytes, y combinado al ID del fabricante identifica al atributo de forma exclusiva. Los primero 256 atributos están definidos en el RFC 2865 para uso de RADIUS.

Banderas AVP. Este campo es de un Byte y proporciona la información necesaria para interpretar el paquete AVP receptado.

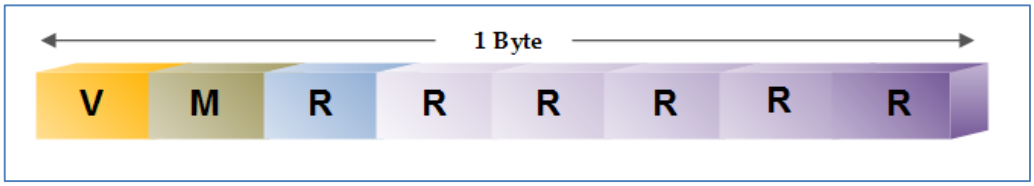


Figura 19. Formato del campo Bandera del mensaje AVP
Nota. Fuente: Adaptado de Funk, P., & Blake, S. (Agosto de 2008). *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) (p. 24).* Recuperado de http://tools.ietf.org/pdf/rfc5281.pdf

- V = El bit indica si el campo Identificador del vendedor está incluido en el paquete, para esto le asigna el código 1.
- M = El bit indica si la información del AVP es obligatoria u opcional. Si se asigna el valor 0 significa que el paquete puede ser ignorado con seguridad en recepción si existe algún error, de lo contrario si se asigna el valor 1 implica la terminación de la negociación por cualquier motivo o fallo en la recepción del mensaje.
- R = Los bits R son reservados, por tal razón se envían como ceros.

Longitud AVP. Este campo tiene una longitud de tres Bytes, indica el tamaño total del paquete AVP incluyendo los campos código, longitud, banderas y el identificador del fabricante.

Identificador del Fabricante. Es un campo de cuatro Bytes, contiene el número del fabricante asignado por la IANA[31] (Internet Assigned Numbers Authority). El valor de este campo en cero equivale la ausencia del proveedor.

1.3.1.3 EAP-PEAP

El protocolo EAP-PEAP (Protected Extensible Authentication Protocol) fue desarrollado por Cisco Systems, Microsoft[32] y RSA Security[33], es similar al EAP-TTLS. La única diferencia es que el protocolo EAP-TTLS puede usar cualquier método de autenticación (EAP, CHAP, MS-CHAP) en el túnel seguro, y el protocolo EAP-PEAP solo permite utilizar métodos de autenticación EAP dentro el túnel creado en la fase uno.

[31] Autoridad de Asignación de Números en Internet.
[32] Empresa multinacional de origen estadounidense, fundada el 4 de abril de 1975 por Bill Gates y Paul Allen. Dedicada al sector de la informática
[33] Empresa dedicada a la criptografía y al software de seguridad.

EAP-PEAP trabaja en dos fases:

Fase 1. El cliente se autentica con el servidor mediante el intercambio de paquetes TLS para crear un túnel encriptado.

Fase 2. El servidor autentica las credenciales de un usuario o equipo con un protocolo de autenticación EAP. La autenticación está protegida por el túnel cifrado creado en la primera fase.

Las implementaciones de EAP-PEAP tanto de Microsoft como Cisco utilizan diferentes métodos de autenticación para los clientes a través del túnel TLS. Microsoft requiere el uso del método MS-CHAPv2 para la autenticación del cliente y Cisco usa el método de autenticación EAP-GTC[34] basado en tarjetas de identificación.

Otra característica es que Microsoft envía las credenciales del usuario en texto plano durante la fase uno de la autenticación PEAP, lo que no sucede con Cisco, el cual permite ocultar la identidad del usuario hasta que el túnel codificado TLS se establece y la primera fase de autenticación termina.

El haber sido desarrollado en parte por Microsoft y Cisco representa una ventaja para aquellos administradores que utilizan esta marca de equipos en su red, por el soporte que tiene PEAP en ellos. Tanto TTLS como PEAP son productos con un nivel de seguridad muy adecuado para cualquier implementación actual.

[34] Generic Token Card. Permite el intercambio de credenciales de autenticación a través de la red.

1.3.2 COMPARACIÓN DE TIPOS EAP

Tabla 3. Comparación de los métodos de autenticación EAP

MÉTODO EAP	EAP - MD5	LEAP	EAP - TLS	EAP - TTLS	EAP-PEAP	EAP - FAST
Certificado de Servidor	No	Challenge	Si	Si	Si	No PKI Shared Secret
Certificado de Cliente	No (Usuario - contraseña)	No (Usuario - contraseña)	Obligatorio	Opcional	Opcional	PAC No PKI
Validación de Certificados	No	No	OCSP TLS	OCSP TLS	OCSP TLS	No
Credenciales Soportadas	MD5 hash	Hash similar a MS - CHAP	Certificados de Cliente	CHAP, PAP, MS-CHAP	EAP-MSCHAP, EAP-GTC	PAC
Soporta cambio de Contraseñas	No	No	No	Si	Si	Si
Autenticación Mutua	No (solo cliente)	Si (Challenge)	Si	Si	Si	Si
Tunelamiento	No	No	Si, TLS	Si, TLS	Si, TLS	Si, TLS
Entrega de claves dinámicas	No	Si	Si	Si	Si	Si
Reconexión Rápida	No	No	Si	Si	Si	Si
Bases de datos de Autenticación	SQL, en formato MD5	AD, NTLM	AD, NTLM, LDAP, OTP, Token	AD, NTLM, LDAP, Token	AD, NTLM, Novell NDS, Token	AD, NTLMM LDAP
Desarrollador	Estándar	Solo Cisco	Microsoft	Funk y Certicom	Microsoft, Cisco y RSA	Cisco
Suplicantes que lo soportan	Microsoft WPA Supplicant MacOs	Propietarios MacOs Linux	Microsoft MacOs Linux	Junip, MacOs Oddissey SecureW2 WPA Supplicant	Microsoft MacOs Linux	Cisco
Muestra nombres de usuario	Si	Si	Si	Anónimo en la fase 1	Anónimo en la fase 1	Si
Vulnerables MiTM	Si	Si	No	No	No	No
Vulnerable actualmente	Si (Diccionario)	Si	No	No	No	No
Usos recomendados	Solo redes cableadas 802.1x	No Recomendado	802.1x Alámbrica e inalámbrica	802.1x Alámbrica e inalámbrica	802.1x Alámbrica e inalámbrica	Redes con equipos Cisco

Nota. Fuente: Adaptado de Fernández, Y., Ramos, A., & García, J. (2008). *RADIUS / AAA / 802.1X : Sistemas basados en la autenticación en Windows y GNU/Linux (pp. 64-65).* Madrid: RA-MA Editorial.

A la hora de tomar una decisión sobre el método de autenticación EAP que se debe utilizar en una infraestructura de red para el control de acceso, es necesario analizar las características del entorno de red donde se lo va a implantar.

Un factor determinante es el medio de acceso, si se trata de una infraestructura de red cableada cuyos equipos de distribución soporten 802.1x, el nivel de seguridad en el método de autenticación puede pasar a segundo plano, teniendo en cuenta que cada puerto de conexión está físicamente controlado. En el caso de redes inalámbricas el nivel de privacidad en la autenticación y posterior funcionamiento debe brindar un mayor nivel de seguridad a todas las conexiones que se hayan realizado de forma exitosa, siendo imprescindible utilizar un método de autenticación que cumpla con dichos requerimientos.

De la tabla anterior que muestra en detalle las características principales de los métodos de autenticación, EAP-TLS, EAP-TTLS y EAP-PEAP son los métodos recomendados y que mejor se adaptan tanto a redes cableadas como inalámbricas.

Otro factor que se debe tomar en cuenta es la complejidad de la implantación del método de autenticación, por ejemplo en las infraestructuras que utilizan EAP-TLS (Infraestructura completa PKI) es indispensable implantar certificados en el servidor y en todos los usuarios de la red, convirtiéndose muchas veces en un problema para el administrador a la hora de gestionar los certificados.

En pequeñas o medianas empresas se puede optar por el uso de sistemas como EAP-TTLS o EAP-PEAP que permiten un alto nivel de seguridad similar al ofrecido por EAP-TLS, con la notable diferencia del número de certificados utilizados, siendo necesario la

instalación de un solo certificado en el servidor de autenticación evitando gran parte de la infraestructura PKI.

Las redes actuales permiten la interconexión de una extensa variedad de clientes que utilizan plataformas diferentes como Windows, Linux, MacOS, etc. Motivo por el cual es indispensable asegurarse que el suplicante que se elija sea compatible con el método de autenticación del sistema y además que las plataformas usadas por los usuarios soporten la instalación de este suplicante.

Algunos suplicantes se pueden obtener de forma gratuita debido a su programación en software libre, de ellos, los más populares por soportar una gran cantidad de métodos de autenticación EAP son wpa_supplicant y Xsupplicant.

1.4 EL ESTÁNDAR 802.1X

IEEE 802.1x es un estándar de autenticación, permite al administrador de la red controlar el acceso a los servicios de red a través de sus puertos. El estándar especifica la arquitectura, elementos y protocolos que se utilizan para permitir una comunicación segura de los dispositivos conectados a la red.

Fue originalmente diseñado para aplicaciones en rede cableadas, pero fue adaptándose para mitigar los problemas de seguridad de las redes inalámbricas debido a su infraestructura robusta, seguridad y potentes capacidades de autenticación y privacidad de los datos.

El estándar IEEE 802.1x opera en la capa dos del modelo OSI[35], asegura el intercambio de las credenciales de usuario o dispositivo evitando cualquier acceso no autorizado a la red.

La implementación de 802.1x en redes cableadas aumenta considerablemente la seguridad de la red, reduce los costos de movilidad y facilita la gestión de redes LAN[36] virtuales. Si bien es un estándar creado hace algunos años, se trata de una solución segura de control de acceso al medio, siendo un componente clave en las tecnologías más populares de red hoy en día.

1.4.1 ELEMENTOS DE UNA INFRAESTRUCTURA 802.1X

Una red 802.1x requiere de tres elementos para operar:

- **El suplicante**. Es un software que se instala en los clientes del equipo autenticador, utilizado en ambientes cableados e inalámbricos. El suplicante se carga en el dispositivo del usuario y se utiliza para solicitar acceso a la red.

- **Autenticador.** Es el componente a través del cual los usuarios acceden a los servicios de red, se encuentra entre el dispositivo que necesita ser autenticado y el servidor utilizado para realizar la autenticación. Ejemplos de Autenticador son conmutadores de red y puntos de acceso inalámbricos.

[35] Open System Interconnection. Modelo de interconexión de sistemas abiertos
[36] Local Area Network, Red de área local.

- **Servidor de Autenticación.** Es un equipo que recibe mensajes mediante una comunicación RADIUS y utiliza esa información para comprobar la autenticidad del usuario o del dispositivo que intenta acceder a la red, por lo general se emplean bases de datos para realizar este proceso tales como SQL, Microsoft Active Directory[37], LDAP[38], etc.

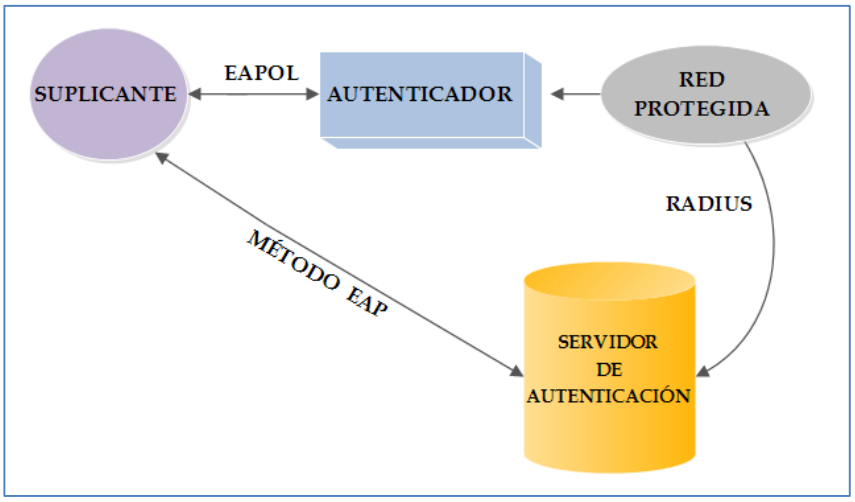


Figura 20. Elementos de un sistema de autenticación 802.1x basada en puertos: suplicante, autenticador y servidor de autenticación.
Nota. Fuente: Adaptado de Geier, J. (2008). *Implementing 802.1X Security Solutions for Wired and Wireless Networks (p. 38).* Indianapolis: Wiley Publishing, Inc.

Cuando un usuario intenta acceder a una red basada en 802.1X, antes de encaminar los datos hacia su destino, el puerto solicita a los usuarios las credenciales de identificación. Si el dispositivo del usuario no está configurado para acceder a la red basada en 802.1X, es decir, no es parte de la red, se rechaza la conexión del suplicante. Caso contrario, el Suplicante responderá la solicitud mediante un mensaje que contenga las credenciales autenticación.

[37] Implementación de servicio de directorio en una red distribuida de computadores
[38] Lightweight Directory Access Protocol - Protocolo Ligero de Acceso a Directorios.

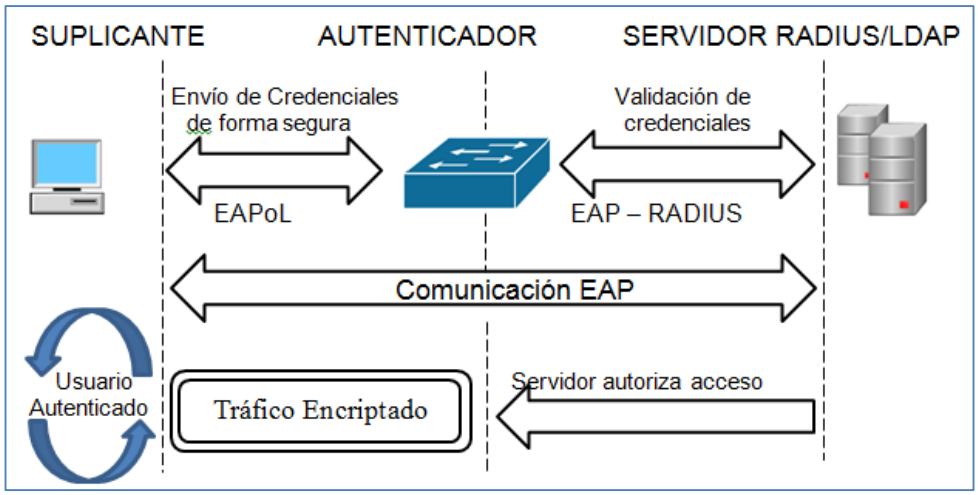


Figura 21. Infraestructura general de red 802.1x
Nota. Fuente: Adaptado de Juniper-Networks. (Septiembre de 2010). *802.1X: Port-Based Authentication standard for network access control (NAC) (p. 2).* Recuperado de http://www.juniper.net/us/en/local/pdf/whitepapers/2000216-en.pdf

El Suplicante envía las credenciales (nombre de usuario - información de identificación del dispositivo) hacia el equipo autenticador, que verifica la conexión a la red y pasa la información de identificación al servidor para que las valide.

En una red compatible con 802.1x, tanto el suplicante como el autenticador deben ser compatibles con el estándar 802.1x, y deben manejar el mismo protocolo del servidor de autenticación para completar la transacción de mensajes.

Las credenciales enviadas por el suplicante que intenta acceder a la red son re-direccionadas hacia el servidor de autenticación, quien se encarga de validarlas. Una vez ocurrido este proceso, el autenticador que puede ser un conmutador de red o punto de acceso inalámbrico configura el estado de los puertos para permitir o no el acceso del suplicante a la red. Si las credenciales del usuario están correctas el usuario puede acceder a la red, sin embargo, si las credenciales de red no son válidas o si el servicio para comprobar las credenciales no está disponible por cualquier razón, se negará el acceso del usuario a la red.

En organizaciones donde se tenga usuarios con privilegios limitados que solo acceden a una determinada cantidad de recursos o servicios de red, será necesario segmentar la red de acuerdo a los requerimientos de la empresa, esto se puede configurar usando las redes virtuales o VLANs.

1.4.2 802.1X – EAP

El estándar 802.1X trabaja en combinación con los métodos de autenticación soportados por el protocolo EAP, por ejemplo EAP-TTLS y EAP-PEAP descritos anteriormente, que proporcionan una canal seguro de comunicación mediante la creación de túneles cifrados que permiten usar otro método de autenticación a través de ellos.

Con la implementación de los métodos de Tunelamiento EAP, los administradores pueden estar seguros que la información que identifica a cada usuario de la red está totalmente protegida, manteniendo la privacidad de los datos en todo momento.

Una vez que un método EAP ha sido seleccionado, tanto el servidor de autenticación como el suplicante deben usarlo para establecer la comunicación. Los mensajes EAP que se transportan entre el suplicante y el autenticador usando la capa dos del modelo de referencia OSI se establece en el estándar IEEE 802.1X como EAPoL[39].

Un equipo autenticador que soporte el estándar 802.1x utiliza un sistema virtual que le permite dividir cada puerto físico LAN en dos puertos virtuales, un puerto controlado y otro no controlado. De manera que el puerto físico trabaja como una puerta lógica, mientras

[39] EAP over LAN – definido en el estándar IEEE 802.1x

el puerto lógico no controlado se abre para escuchar los paquetes EAPoL que llevan información para el proceso de autenticación de un suplicante, el puerto controlado permanece cerrado bloqueando el transporte de cualquier paquete.

Una vez que se produce la autenticación exitosa de un suplicante el puerto controlado se abre para permitir el paso de los paquetes de datos del usuario que en ese momento accede a los servicios de red.

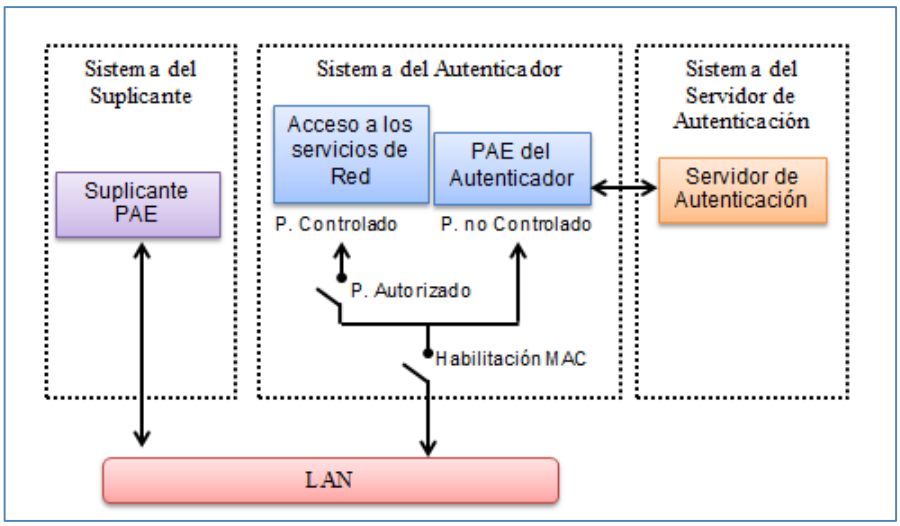


Figura 22. Principio de Operación de los puertos 802.1x
Nota. Fuente: Adaptado de Congdon, P., & Packard, H. (Marzo de 2000). *IEEE 802.1X Overview: Port Based Network Access*. Recuperado de http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF

1.4.3 SECUENCIA DE UNA COMUNICACIÓN 802.1X

En la Figura 23 se puede observar la secuencia de mensajes que se transmiten para establecer una comunicación exitosa entre el suplicante y un servidor RADIUS con el fin de acceder a los servicios de red a través de un equipo autenticador que soporte el estándar 802.1x.

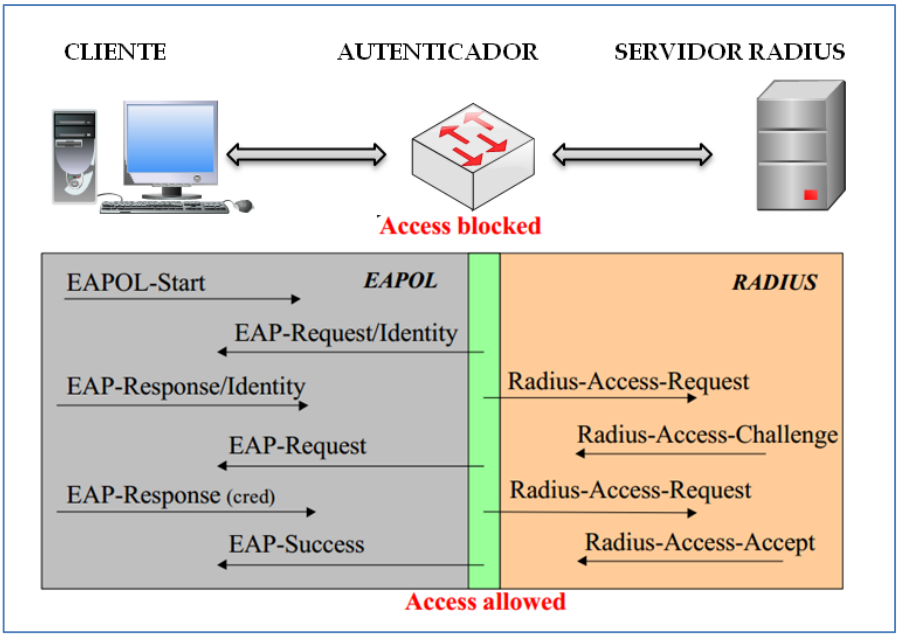


Figura 23. Secuencia de una comunicación 802.1X
Nota. Fuente: Adaptado de Congdon, P., & Packard, H. (Marzo de 2000). *IEEE 802.1X Overview: Port Based Network Access*. Recuperado de http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF

- El suplicante inicia el proceso de autenticación mediante el envío de un mensaje EAPoL-Start hacia el equipo autenticador solicitando el acceso a los servicios de red.

- En este momento el puerto no controlado está activo a la espera de alguna solicitud de acceso EAPoL, a la que responderá con un mensaje EAP-Request/Identity solicitando la identificación del suplicante o dispositivo.

- El suplicante envía la información requerida en un mensaje EAP-Response/Identity hacia el equipo autenticador.

- El servidor es el encargado de verificar las credenciales del suplicante que intenta acceder a la red, por tal motivo el autenticador le envía una solicitud de acceso Radius-Access-Request al servidor RADIUS para establecer la comunicación.

- El servidor de autenticación envía una respuesta mediante un paquete encapsulado Radius-Access-Challenge al autenticador, que contiene una solicitud indicando el método de autenticación EAP que el solicitante debe manejar para el establecimiento de un canal seguro para la comunicación.

- En esta parte del proceso, el autenticador encapsula la petición del servidor RADIUS en un mensaje EAPOL y lo transmite al suplicante, el cual responde mediante un paquete EAP-Response que contiene los datos solicitados, específicamente los métodos de autenticación EAP que soporta para el intercambio de las credenciales.

- Finalmente el servidor RADIUS analiza los mensajes recibidos y comprueba las credenciales del usuario a través de sus bases de datos que almacenan las políticas de acceso de cada uno de los elementos de red para determinar si puede o no acceder a los servicios.

- Si el servidor de autenticación y el suplicante están de acuerdo con el método EAP requerido para el establecimiento del canal y toda la información para el acceso es correcta, se envía un mensaje Radius-Access-Accept indicando que el proceso de autenticación se ha realizado exitosamente, por lo tanto el puerto del equipo autenticador cambia de un estado no controlado a uno autorizado a través del cual el usuario puede acceder a los servicios o recursos de red permitidos por el servidor.

1.4.4 PROTOCOLO DE AUTENTICACIÓN EXTENSIBLE SOBRE LAN EAPOL

EAPoL se define en el estándar 802.1X que detalla la aplicación de los métodos de autenticación EAP a través de redes cableadas. El protocolo EAPoL opera en la capa 2 del modelo OSI para evitar que un dispositivo logre establecer la conexión con la red antes de autenticarse. Esto se logra mediante el uso de mecanismos de control de acceso al medio MAC[40], definido en el estándar IEEE 802.1D.

El proceso de encapsulación de una trama EAPoL involucra al medio de transmisión (802.3 o 802.11), el método de autenticación extensible EAP empleado y los datos.

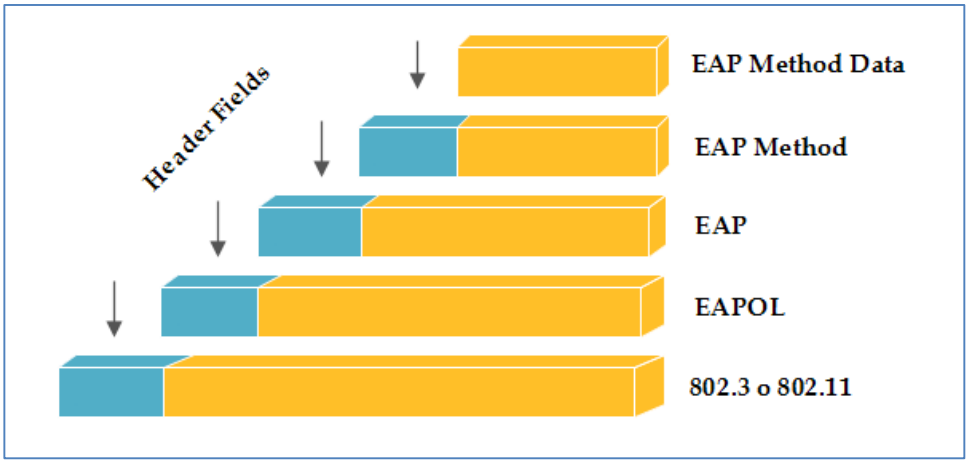


Figura 24. Encapsulación de EAPoL
Nota. Fuente: Adaptado de Geier, J. (2008). *Implementing 802.1X Security Solutions for Wired and Wireless Networks (p. 56).* Indianapolis: Wiley Publishing, Inc.

EL paquete EAPoL añade tres campos al paquete EAP, su estructura se muestra en la Figura 25.

[40] Medium Access Control – Control de Acceso al Medio.

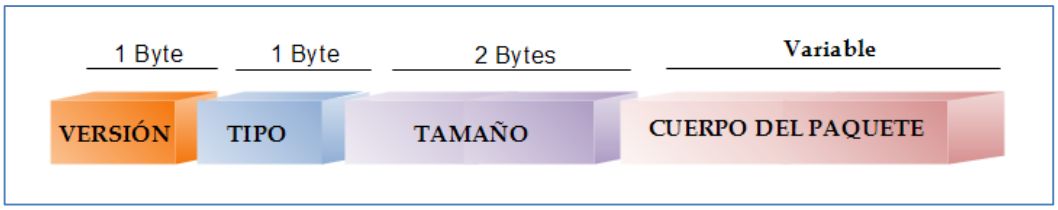


Figura 25. Estructura del mensaje EAPoL
Nota. Fuente: Adaptado de Geier, J. (2008). *Implementing 802.1X Security Solutions for Wired and Wireless Networks (p. 57).* Indianapolis: Wiley Publishing, Inc.

Versión. La longitud de este campo es de un byte, permite identificar la versión del paquete EAPoL en una comunicación. El valor asignado para las implementaciones de 802.1x es "0000 0002".

Tipo. La longitud de este campo es de un byte, la figura que se muestra a continuación muestra los diversos tipos de paquetes EAPoL con sus respectivos códigos de identificación.

Tabla 4. Tipos y códigos de los paquetes EAPoL

PACKET TYPE	TYPE FIELD VALUE
EAP-Packet	0000 0000 (Hex "00")
EAPOL-Start	0000 0001 (Hex "01")
EAPOL-Logoff	0000 0010 (Hex "02")
EAPOL-Key	0000 0011 (Hex "03")
EAPOL-Encapsulated-ASF-Alert	0000 0100 (Hex "04")

Nota. Fuente: Adaptado de Geier, J. (2008). *Implementing 802.1X Security Solutions for Wired and Wireless Networks (p. 58).* Indianapolis: Wiley Publishing, Inc.

Tamaño. La longitud de este campo es de dos bytes e indica el número de octetos del campo "cuerpo del paquete". Por ejemplo, un valor de "0000 0000 0001 1011" en el campo tamaño, indica que el cuerpo del paquete contiene 27 octetos de datos. Un valor de "0000 0000 0000 0000" significa que el paquete EAPOL no tiene el campo cuerpo del paquete, este es el caso de los paquetes EAPOL-Start y EAPOL-Logoff.

La longitud máxima del paquete EAPOL depende de las limitaciones del protocolo de enlace que se usen, tales como IEEE 802.3 o 802.11.

Cuerpo del paquete. Este campo representa la carga del paquete EAPOL y está presente en paquetes usados en el proceso de autenticación como EAP-Packet, EAPOL-Key, y EAP-Encapsulated-ASF-Alert.

1.5 LDAP

LDAP[41] es un protocolo basado en el modelo cliente-servidor para acceder a un servicio de directorio, permite almacenar información relacionada a una organización en particular, por ejemplo nombres de usuario, contraseñas, certificados digitales, cuentas de correo, etc. La versión actual es LDAP v.3 (versión 3), el estándar original para esta versión se desarrolló en 1997 publicados en los RFC 2251 – 2256, la actualización de los documentos se realizó en junio de 2006, mediante el uso de las RFC 4510 hasta la 4519 que describen en detalle las especificaciones técnicas del protocolo LDAP v.3.

1.5.1 SERVICIO DE DIRECTORIO

En términos informáticos un directorio es una base de datos especializada, generalmente contiene información descriptiva basada en atributos que almacenan valores de un conjunto de entidades como personas u organizaciones, y proporciona servicios de acceso a dicha información.

[41] LDAP Lightweight Directory Access Protocol

En una empresa el objetivo de LDAP, además de almacenar información relacionada con los procesos de autenticación y autorización, es funcionar como un servidor de directorio, donde se aloja información personal como números telefónicos, dirección domiciliaria, datos de contacto, correo electrónico, etc.

LDAP no es una base de datos relacional, es un protocolo que regula el acceso a los datos almacenados, optimizado especialmente para proporcionar una repuesta rápida a operaciones de búsqueda y lectura de la información.

1.5.2 ARQUITECTURA DE LDAP

LDAP define el contenido de los mensajes intercambiados entre un cliente y un servidor LDAP, así como el formato de los datos transportados. En una comunicación los mensajes intercambiados contienen información que especifica el tipo de operación solicitada por el cliente hacia el servidor, esta puede ser de búsqueda, lectura, modificación o eliminación de un dato.

La comunicación LDAP se realiza a través de TCP, un protocolo orientado a conexión, por lo que también se utilizan operaciones para establecer y terminar una sesión entre el cliente y servidor. Sin embargo, cuando se diseña un servidor de directorio LDAP, lo más relevante no es la estructura de los mensajes, sino la forma en que se organice la información en el directorio, el tipo de datos y el método que se use para protegerlos de accesos no autorizados.

La secuencia general de comunicación entre un cliente y un servidor LDAP se detalla en la Figura 26.

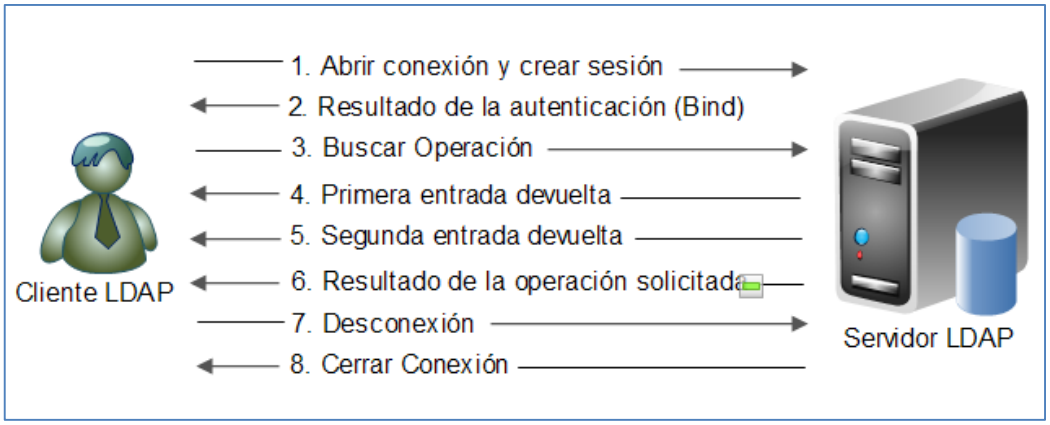


Figura 26. Conexión entre un cliente y un servidor LDAP
Nota. Fuente: Adaptado de Howes, T., Smith, M., & Good, G. (2003). *Understanding and Deploying LDAP Directory Services*. Boston: Pearson Education, Inc.

- El cliente establece una sesión con el servidor LDAP. En este primer paso se especifican datos como el nombre de host o la dirección IP y el número de puerto TCP[42] que el servidor utiliza para escuchar las peticiones de clientes que necesitan comunicarse con él.

- Luego el cliente procede a identificarse, en este punto se puede autenticar mediante el uso de un nombre de usuario y una contraseña o se puede establecer una sesión anónima con privilegios restringidos respecto a los derechos de acceso. Si se necesita aumentar el nivel de seguridad en la comunicación entre el cliente y servidor se debe usar algún método seguro, como la encriptación de datos.

- El siguiente paso es la ejecución de operaciones en los datos del directorio. LDAP permite realizar consultas, lecturas y actualizaciones de la información almacenada.

[42] TCP Protocolo de control de transmisión

La búsqueda y lectura son las operación que con más frecuencia se llevan a cabo, se utilizan filtros mediante condiciones booleanas que permiten encontrar los datos a través de coincidencias.

- Finalmente, una vez el cliente termine de hacer las consultas, se cierra la sesión con el servidor.

1.5.3 MODELO DE LDAP

El modelo de información LDAP define los tipos de datos y las unidades básicas de información que se puede almacenar en el directorio, para lo cual se utiliza los términos denominados entradas, atributos y valores. El conjunto de objetos con sus atributos se organizan de una manera lógica y jerárquica.

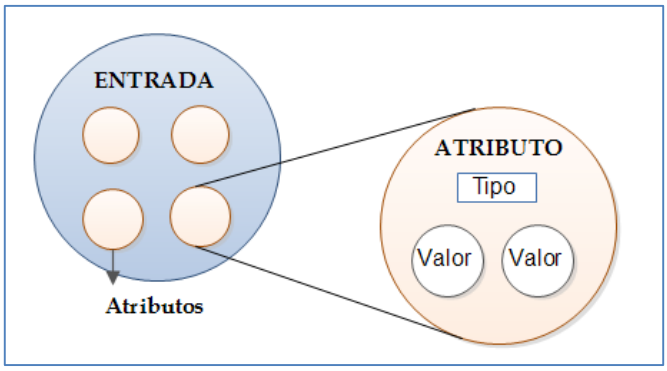


Figura 27. Entradas, atributos y valores
Nota. Fuente: Adaptado de Tuttle, S., Ehlenberger, A., Gorthi, R., Leiserson, J., Macbeth, R., Owen, N., . . . Yang, C. (2004). *Understanding LDAP Design and Implementation (p. 32)*. IBM Redbook Publication.

La unidad básica de información en un directorio es la entrada, que describe a un objeto del mundo real que puede ser: personas, departamentos, servidores, impresoras, etc. Un ejemplo de modelo típico de un directorio se puede apreciar en la figura 29, que muestra algunos objetos reales en una organización.

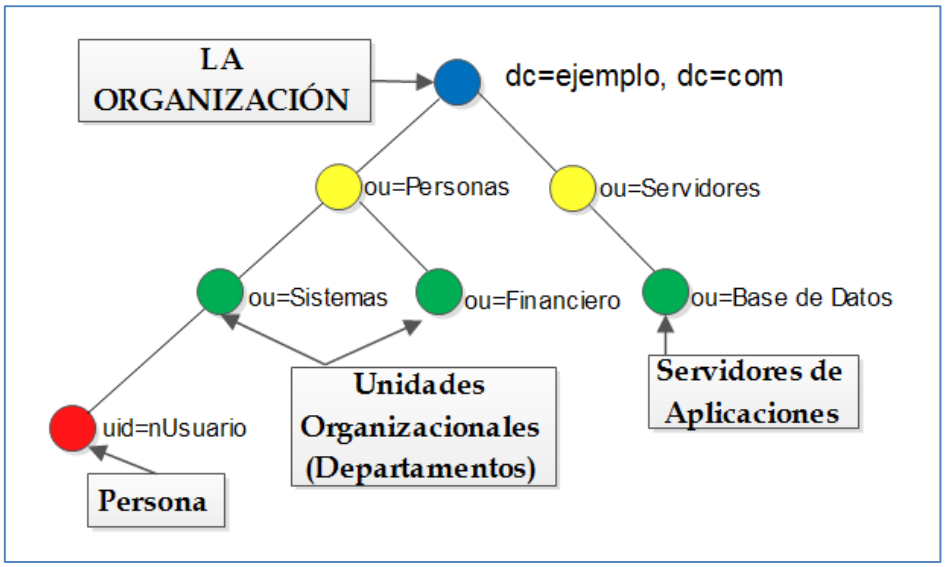


Figura 28. Estructura general de un directorio LDAP
Nota. Fuente: Adaptado de Howes, T., Smith, M., & Good, G. (2003). *Understanding and Deploying LDAP Directory Services*. Boston: Pearson Education, Inc.

Cada entrada en el directorio tiene un nombre distinguido (DN[43]). El DN es el nombre que identifica de forma exclusiva una entrada en el directorio, se compone de pares atributo=valor, separados por comas, por ejemplo, en la figura 29 la organización tiene el DN dc=ejemplo, dc=com.

Una entrada se compone de un conjunto de atributos que describen una característica particular del objeto, cada atributo posee un tipo y uno o más valores. La Tabla 5 muestra ejemplos de atributos y los valores que se les puede asignar.

[43] DN Distinguished Name

Tabla 5. Atributos y valores para una entrada

ATTRIBUTE TYPE	ATTRIBUTE VALUES
cn:	Barbara Jensen
sn:	Jensen
telephoneNumber:	+1 408 555 1212
mail:	babs@example.com

Nota. Fuente: Adaptado de Howes, T., Smith, M., & Good, G. (2003). *Understanding and Deploying LDAP Directory Services* (2nd ed.). Boston: Pearson Education, Inc.

1.5.3.1 LDIF

LDAP Data Interchange Format (LDIF) es un estándar que usa un formato basado en texto para describir las entradas de un directorio, se define en el RFC 2849. LDIF permite exportar e importar los datos almacenados a otro servidor de directorio, incluso si los servidores utilizan una base de datos interna con formatos diferentes.

Una entrada expresada en formato LDIF se compone de dos partes: un DN y una lista de atributos con sus valores. El DN, debe escribirse en la primera línea, está formado por las letras "dn" seguido de dos puntos (:) y el nombre completo de la entrada. Luego, se listan los atributos, que tienen un formato similar al DN, primero se indica el tipo, seguido de dos puntos (:), y el valor asignado al atributo.

El orden en el que se listen los atributos no es relevante, pueden aparecer en cualquier orden, sin embargo, es recomendable mantener una estructura que facilite la lectura y comprensión de los archivos LDIF. Un modelo general de entrada en formato LDIF para un usuario se muestra en la Figura 29.

```
dn: uid=bjensen, dc=example, dc=com
cn: Barbara Jensen
mail: bjenesen@example.com
uid: bjensen
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

Figura 29. Entrada en formato LDIF
Nota. Fuente: Adaptado de Butcher, M. (2007). *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services (p. 63).* Reino Unido: Birmingham: Packt Publishing Ltd.

1.5.3.2 ESQUEMA LDAP

Los esquemas LDAP se utilizan para definir adecuadamente los atributos, clases de objeto y diversas reglas para estructurar la información, se puede definir como un tipo especial de directiva que proporciona el formato necesario para construir el directorio.

Los principales elementos que se utilizan en la definición de un esquema LDAP son:

- **Definición de clase de objeto**: define una clase de objeto, incluido el identificador único, su nombre y los atributos que puede o debe tener. La definición de un esquema se almacena en el archivo core.schema, véase la Figura 30.

```
objectClass
  (
   2.5.6.6
   NAME 'person'
   DESC 'RFC4519: a person'
   SUP top STRUCTURAL
   MUST (sn $ cn)
   MAY (userPassword $ telephoneNumber $seeAlso $ description)
  )
```

Figura 30. Definición de clase de objeto.
Nota. Fuente: Adaptado de Butcher, M. (2007). *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services (p. 270).* Reino Unido: Birmingham: Packt Publishing Ltd.

- **Definición de atributos**: define un atributo, incluido su identificador único, el nombre, las reglas que definen los tipos de valores que se permiten almacenar y el procedimiento para llevar a cabo las operaciones. La definición de un atributo empieza con una directiva AttributeType, el resto se incluye entre paréntesis (Figura 31).

```
attributetype
  (
   2.5.4.20
   NAME telephoneNumber‘
   DESC ’RFC2256: Telephone Number‘
   EQUALITY telephoneNumberMatch
   SUBSTR telephoneNumberSubstringsMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32}
  )
```

Figura 31. Definición de atributos.
Nota. Fuente: Adaptado de Butcher, M. (2007). *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services (p. 274).* Reino Unido: Birmingham: Packt Publishing Ltd.

- **Identificadores de objetos**: asigna un nombre al identificador único. Se utiliza principalmente para acelerar la creación de esquemas.

- **Reglas de contenido DIT**: Especifican las clases de objetos que pueden ser utilizadas en una entrada, los tipos de atributos que se requieren y las acciones permitidas o prohibidas en función de la clase de objeto. La Figura 32 muestra un ejemplo para un objeto de la clase persona.

```
dn: cn=Thomas Reid, dc=example, dc=com
objectClass: person
cn: Thomas Reid
sn: Reid
userPassword:: DSFSUYJKHGH=
telephoneNumber: 555-555-5555
seeAlso: uid=david, ou=users, dc=example, dc=com
description: A basic user.
```

Figura 32. Objeto de clase persona.
Nota. Fuente: Adaptado de Butcher, M. (2007). *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services (p. 270).* Reino Unido: Birmingham: Packt Publishing Ltd.

Este registro contiene la información completa para todos los atributos del objeto, si se intenta agregar un tipo de atributo diferente que no se mencione en el esquema o si se trata de eliminar el valor de algún atributo requerido como CN o SN daría lugar a un error. Para conocer que atributos son requeridos y cuales son opcionales, se debe revisar la información almacenada en la definición de clase de objeto persona.

CAPITULO II

IDENTIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD Y PERFILES DE ACCESO DE LOS USUARIOS.

2.1 SITUACIÓN ACTUAL DE LA RED

> El GAD Municipal San Miguel de Urcuquí es un organismo autónomo, desconcentrado y descentralizado que impulsa el desarrollo social, étnico, cultural, económico y ético del cantón, que coordina y facilita los esfuerzos y talentos humanos, mediante la planificación, organización, dirección y control de los procesos político administrativos orientados a satisfacer las aspiraciones y necesidades ciudadanas. (GADMU, Misión Cantonal, 2011)

El GAD[44] Municipal de San Miguel de Urcuquí posee una infraestructura de red IP operativa que permite a los usuarios compartir recursos, servicios e información, a más de la interconexión de la red local con el internet, sin embargo no existen políticas de seguridad que controlen el tráfico de paquetes que circulan entre las redes.

El diseño de red actual posee conectividad pero no garantiza un nivel de seguridad apropiado debido a la falta de un mecanismo que controle el acceso a los usuarios que hacen uso de los recursos de red, razón por la cual los datos que transitan a través de la intranet están expuestos a sustracciones o modificaciones generando graves inconvenientes a los administradores de la red y consecuentemente a la Institución.

[44] GAD Gobierno Autónomo Descentralizado

2.1.1 TOPOLOGÍA DE RED

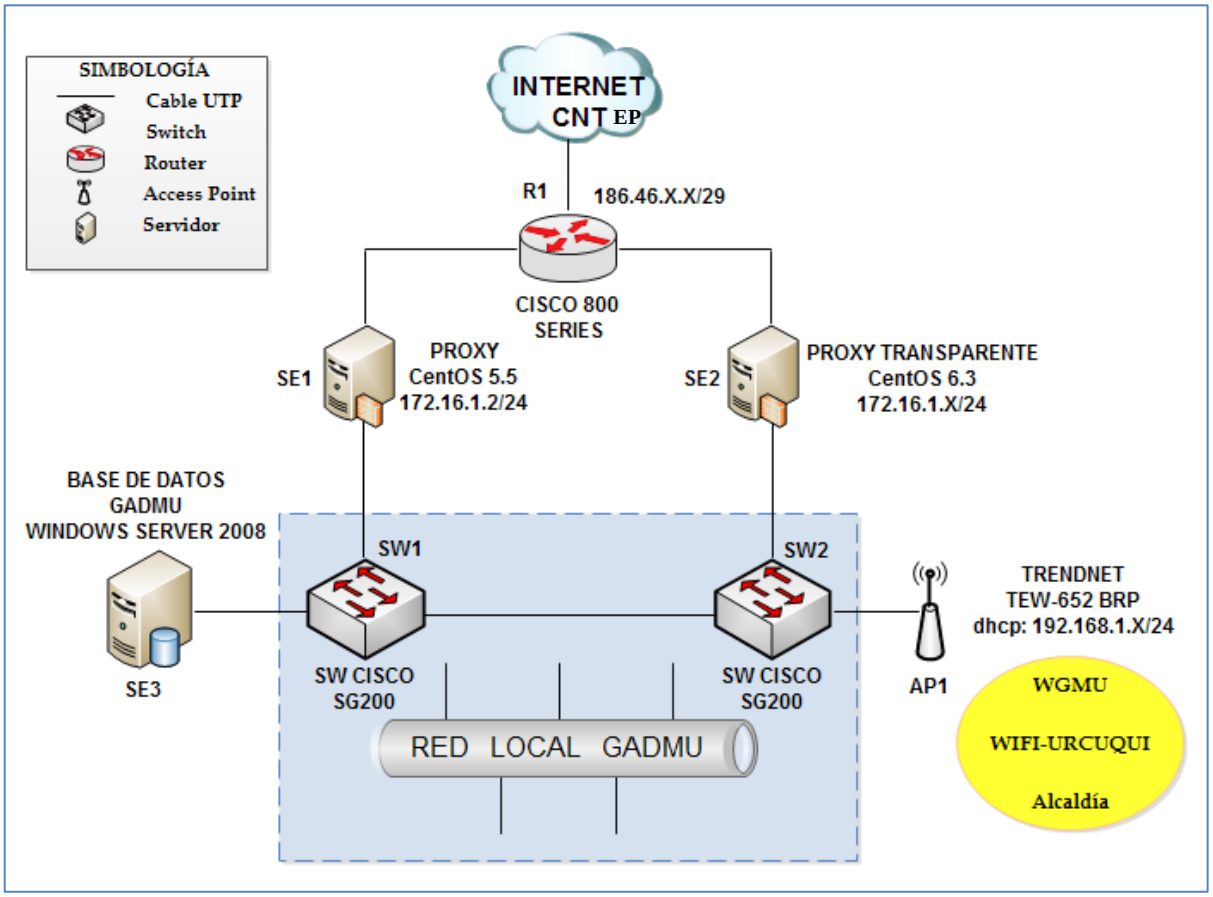


Figura 33. Topología Lógica de la red de datos del GADMU
Nota. Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui (2013).

2.1.1.1 Descripción

La infraestructura actual del GAD Municipal de San Miguel de Urcuqui no posee un diseño jerárquico de red, como se puede observar en la Figura 33, es una LAN plana de libre acceso que no cuenta con un sistemas de seguridad para su control, resulta vital para la institución administrar la red y proteger la información, recurso de mucho valor que de ser manipulada de manera inadecuada generaría pérdidas irreparables a la organización.

La interconexión con redes externas se lo realiza a través de CNT EP[45], único proveedor del servicio de internet de la Institución. Para la comunicación se ha asignado la VLAN 883, con un pool de direcciones IP públicas en el rango 186.46.X.X/29.

Para la conexión de los dispositivos de usuario final con la red local se utilizan los switch CISCO SMALL BUSINESS de la serie 200, los conmutadores son completamente administrables y gestionables mediante web pero actualmente no poseen ninguna configuración.

No existe un firewall que proteja y controle el tráfico de paquetes que circulan entre las redes LAN e Internet, la navegación de páginas web es restringida mediante un Proxy que corre sobre la plataforma Linux (CentOS 5.5) implementado en el servidor (SE1) HP ProLiant ML150 G6.

En el servidor HP ProLiant DL380 G7 (SE2) se ha instalado un servidor proxy transparente cuya función es restringir la navegación web exclusivamente de aquellos usuarios que acceden a la red usando los puntos de acceso inalámbricos del GAD Municipal San Miguel de Urcuqui. Los equipos que ofrecen el servicio Wi-Fi son los TRENDNET[46] TEW-652 BRP (ver Figura 33).

EL GADMU posee una base de datos con la información requerida para la gestión interna de la institución, como también el registro de avalúos, catastros, impuestos, etc. usados en la administración de los servicios ofrecidos a los ciudadanos del cantón Urcuqui.

[45] CNT EP. Corporación Nacional de Telecomunicaciones.
[46] TRENDNET, es un proveedor global de reconocidas soluciones para redes.

La página web Institucional se encuentra alojada en la Asociación de Municipalidades del Ecuador (AME), por tal razón no se cuenta con los privilegios necesarios para establecer reglas y políticas que controlen los accesos no autorizados.

Los requerimientos técnicos para la implementación del estándar 802.1x tanto en redes cableadas como inalámbricas establecen tres elementos básicos para su operación, un servidor de autenticación, el equipo autenticador (punto de acceso inalámbrico o switch) con soporte 802.1x y el suplicante instalado en todos los dispositivos de usuario final (ver Figura 20).

Por tal razón, en base a la topología de red del GADMU (ver Figura 33) y los elementos requeridos por el estándar IEEE 802.1X, se determina como viable la implementación del sistema de seguridad en la red interna de la Institución para el control de acceso.

- **Equipamiento**

Tabla 6. Equipamiento del GADMU

CANTIDAD	EQUIPO	MARCA	MODELO
1	Router	CISCO	800 Series 881
3	Router Inalámbrico	TRENDNET	TEW-652 BRP
2	Servidor	HP ProLiant	DL380 G7
1	Servidor	HP ProLiant	ML150 G6
2	Switch	CISCO	SG200-50

Nota: Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui (2013).

2.1.2 HARDWARE

El GAD Municipal de San Miguel de Urcuqui está equipado con 2 servidores HP ProLiant DL380 G7 ideales para ambientes de todo tipo y tamaño, eficientes para aplicaciones de virtualización, servidor de aplicaciones web, correo electrónico, base de datos, etc.

2.1.2.1 Servidores

Las especificaciones técnicas del servidor HP ProLiant DL380 G7 se muestran en la Tabla 7.

Tabla 7. Especificaciones Técnicas HP ProLiant DL380 G7

RECURSO	DESCRIPCIÓN
Número de Procesadores	2
Núcleo de Procesador	6
Velocidad del Procesador	2.53GHz
Tipo de Memoria	DDR3 RDIMM o UDIMM
RAM	16 GB
Tipo de Procesador	Intel(R) Xeon(R) E5649 @ 2.53GHz
Procesadores Compatibles	Intel® Xeon® 5600 series
Almacenamiento	1TB
Interfaz de Red	Two BCM5709C with dual-port Gigabit
Virtualización	Si

Nota. Fuente: Adaptado de Hewlett-Packard. (Abril de 2010). *HP ProLiant DL380 G7 Server.*
Obtenido de http://www.rorke.com/wp-content/uploads/2013/04/DLseriesserver.pdf

El GADMU además posee un servidor HP ProLiant ML 150 G6, cuyas especificaciones técnicas se detallan en la Tabla 8.

Tabla 8. Especificaciones Técnicas HP ProLiant ML 150 G6

RECURSO	DESCRIPCIÓN
Número de Procesadores	1
Núcleo de Procesador	4
Velocidad del Procesador	2.00GHz
Tipo de Memoria	DDR3
RAM	4 GB
Tipo de Procesador	Intel(R) Xeon(R) E5504 @ 2.00GHz
Procesadores Compatibles	Intel® Xeon® E5500 series
Almacenamiento	128 GB
Interfaz de Red	Embedded HP NC107i PCI Express Gigabit Server Adapter
Virtualización	Si

Nota. Fuente: Hewlett-Packard. (Marzo de 2009). *HP ProLiant ML150 G6 Server.* Obtenido de http://h18004.www1.hp.com/products/quickspecs/ds_00148/ds_00148.pdf

2.1.2.2 Switch de Acceso

Los equipos usados son los Switch Cisco Small Business de la serie 200, ofrecen funciones básicas de administración, seguridad y calidad de servicio (QoS), la administración y configuración se la realiza mediante una interfaz de usuario web. En la Tabla 9 se detallan las especificaciones del switch Cisco de la serie 200.

Tabla 9. Especificaciones switch cisco SG200-50

FUNCIÓN	DESCRIPCIÓN
Capacidad y velocidad de envío	100 Gbps
Protocolo de árbol de expansión (STP)	Activada de manera predeterminada
VLAN	Compatibilidad con hasta 256 VLAN simultáneas

VLAN de voz	El tráfico de voz se asigna automáticamente a una VLAN específica de voz y se trata con los niveles apropiados de QoS.
IEEE 802.1X (función de Autenticador)	Autenticación y administración 802.1X: RADIUS, algoritmo hash MD5.
Seguridad de puertos	Bloquea las direcciones MAC de los puertos y limita la cantidad de direcciones MAC detectadas.
Prevención de ataque de DoS	Prevención de denegación de servicio (DoS, Denial of Service)
Supervisión remota (RMON)	Agente de software RMON integrado compatible con un grupo RMON (estadísticas) para mejor administración, supervisión y análisis del tráfico.
Flash	16 MB (8 MB en SG200-08 y SG200-08P)
Memoria CPU	128 MB (32 MB en SG200-08 y SG200-08P)

Nota. Fuente: Adaptado de CISCO. (2012). *Cisco Small Business 200 Series Smart Switches.* Obtenido de http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps11229/data_sheet_c78-634369_Spanish.pdf

2.1.2.3 Puntos de Acceso inalámbricos

En la actualidad, la implementación de redes inalámbricas se considera como una solución de movilidad, flexibilidad y productividad, lo que ha permitido que esta tecnología crezca y esté presente en casi todos los lugares donde exista una red cableada.

Sin embargo, todas las ventajas que ofrece una red inalámbrica traen consigo muchos riesgos de seguridad que se deben contrarrestar, principalmente los fallos asociados a la falta de mecanismos de seguridad robustos que protejan los recursos de red frente a los accesos no autorizados.

Para brindar el servicio Wi-Fi, la institución utiliza puntos de acceso inalámbricos marca TRENDNET, las especificaciones técnicas de los equipos se pueden ver en la Tabla 10.

Tabla 10. Especificaciones Técnicas AP TRENDNET

FUNCIÓN	DESCRIPCIÓN
Estándares	Cableado: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX) Inalámbrico: IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11e QoS
WAN	1 puerto 10/100Mbps Auto-MDIX (internet)
LAN	4 puertos 10/100Mbps Auto-MDIX
Frecuencia	Banda 2.412~2.484GHz
Seguridad	WEP(HEX/ASCII): 64/128-bit WPA(AES/TKIP): WPA/WPA2, WPA-PSK/WPA2-PSK

Nota. Fuente: Adaptado de TRENDnet. (2013). *Especificaciones técnicas TEW-652BRP*. Obtenido de http://www.trendnet.com/langsp/products/proddetail.asp?prod=185_TEW-652BRP&cat=166

2.1.3 SOFTWARE

La identificación de los sistemas operativos instalados en cada uno de los equipos que se conectan a la red de datos del GAD Municipal de San Miguel de Urcuquí, es de suma importancia a la hora de elegir el método de autenticación del sistema AAA.

2.1.3.1 Sistema Operativo de Servidores

La infraestructura actual de red consta de un servidor proxy y un servidor de aplicaciones para base de datos. En la Tabla 11 se detallan los sistemas operativos instalados en cada uno de los equipos de la institución.

Tabla 11. Servidores GADMU

SERVIDOR	SISTEMA OPERATIVO	APLICACIÓN
HP ProLiant ML150 G6	CentOS 6.3	Proxy red cableada
HP ProLiant DL380 G7	CentOS 5.5	Proxy Transparente
HP ProLiant DL380 G7	Windows Server 2008	SQL Server 2005

Nota. Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui (2013).

2.1.3.2 Sistema Operativo de las estaciones de trabajo

El estándar 802.1X controla el acceso de los usuarios a la red mediante el proceso de autenticación, fue estandarizado para implementaciones tanto en redes cableadas como inalámbricas. Uno de los tres elementos del estándar 802.1x son los suplicantes, por tal razón, es de suma importancia identificar las plataformas instaladas en los equipos de los usuarios, que permita determinar si el sistema operativo soporta el método de autenticación que se utilizará o si por el contrario se requiera de algún software adicional.

Los usuarios del GADMU no utilizan una plataforma estandarizada, en la Tabla 12 se muestran los sistemas operativos instalados actualmente en los equipos de la institución, junto con el tipo de soporte disponible para la autenticación EAP.

Tabla 12. Sistemas Operativos usuarios GADMU

SISTEMA OPERATIVO	EAP-TLS	EAP-TTLS	EAP-PEAP
Windows XP	Cliente Nativo	Cliente de Tercero	Cliente Nativo
Windows 7	Cliente Nativo	Cliente de Tercero	Cliente Nativo
Windows 8	Cliente Nativo	Cliente Nativo	Cliente Nativo
Ubuntu 12.04 LTS	Cliente Nativo	Cliente Nativo	Cliente Nativo
Android OS	Cliente de Tercero	Cliente Nativo	Cliente Nativo

Nota: Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui (2013).

2.2 POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO

La información que se maneja en la red de datos interna del GAD Municipal San Miguel de Urcuqui es un activo de mucho valor para la institución, por tal motivo necesita ser protegida de forma adecuada frente a posibles amenazas y delitos informáticos a los que está expuesta la red de datos debido a la falta de mecanismos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

El término confidencialidad se refiere al control de acceso, evita que personas no autorizadas accedan a un recurso que no está permitido, la integridad asegura que no se ha modificado o sustraído la información desde la fuente al destino y finalmente la disponibilidad permite que los usuarios autorizados tengan acceso tanto a la información como a los sistemas en todo momento con una capacidad de respuesta rápida frente a posibles fallos.

No existe un método que proteja la información en un cien por ciento, pero se puede lograr un nivel aceptable mediante la aplicación de controles, como políticas, procedimientos o soluciones de software que aseguren el cumplimiento de los objetivos y requerimientos que la organización posea.

De forma general, la esencia de una política de seguridad es establecer normas y directrices para proteger tanto la información como los sistemas internos de la organización. Normalmente las instituciones en un inicio trabajan con políticas y procedimientos indocumentados, pero a medida que crecen se vuelve necesario e incluso indispensable tener un documento escrito con reglas y requerimientos de seguridad, que sirva como guía para

todos los usuarios que de una u otra forma utilizan los servicios de red para acceder a la información.

De acuerdo al estudio realizado, la unidad de Sistemas del GAD Municipal San Miguel de Urcuqui no posee una política para el control de acceso que sirva como base para el diseño del servicio AAA (Autenticación, Autorización, Contabilidad), por tal razón, se elabora un documento con los requerimientos mínimos de seguridad que la red de datos del GADMU necesita en base a la infraestructura actual de la red (ver Figura 33) y algunas recomendaciones proporcionadas por el estándar ISO/IEC 27002[47].

La ISO/IEC 27002:2005 establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización. La norma no es certificable, solo es una guía de buenas prácticas, incluye 39 objetivos de control y 133 controles, agrupados en once dominios, cada institución debe considerar previamente cuántos son realmente aplicables según sus propias necesidades.

Para el desarrollo del sistema AAA en la red datos del GADMU se usarán algunas recomendaciones del estándar ISO/IEC 27002:2005 relacionadas con el dominio Control de Accesos.

[47] ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información.

2.2.1 REQUERIMIENTOS DE LA ORGANIZACIÓN PARA EL CONTROL DE ACCESOS

Objetivo: Controlar los accesos a la información.

Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que:

> Se deberían controlar el acceso a la información, los recursos y aplicaciones en base a las necesidades de seguridad de la Organización. Las reglas deben considerar las políticas de autorización y distribución de la información.

2.2.1.1 Política de control de accesos

La información proporcionada a los usuarios se lo hará de acuerdo a sus funciones, bajo ninguna circunstancia los empleados de un departamento podrán conocer información utilizada en otra dependencia que no sea la suya.

La creación de un nuevo usuario en el sistema AAA estará a cargo del administrador de la red, salvo alguna excepción en la que se de privilegios a otro usuario de la unidad de sistemas para la creación y modificación de cuentas de usuario.

Para los casos donde se requiera eliminar un usuario del sistema AAA, se lo hará una vez verificado que el empleado haya terminado sus relaciones laborales con el GADMU o esté en proceso de hacerlo.

La regla general para el control de acceso, específicamente las usadas en el firewall se crearán en base a la política: está prohibido todo lo que no esté permitido explícitamente. La creación de las reglas será responsabilidad directa del administrador de la unidad de Sistemas o de cualquier usuario al que se le hubiera otorgado dichos privilegios.

2.2.2 GESTIÓN DE ACCESO DE USUARIO

Objetivo: Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que:

> Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Los procedimientos deberían cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

2.2.2.1 Registro de Usuarios

Se denomina usuario del sistema AAA a cualquier persona que trabaje o esté presente de forma activa en el GAD Municipal San Miguel de Urcuqui y que utilice la infraestructura de red para acceder a la información o aplicaciones que se encuentren disponibles con el fin de facilitar el desarrollo de sus actividades laborales dentro de la institución.

Se denomina usuarios invitados a las personas que sin tener relación laboral con el GADMU estén autorizados a usar parte de la infraestructura de red para acceder a los servicios, este es el caso particular de los usuarios WI-FI. Las personas deben solicitar al encargado de la unidad de sistemas una cuenta de acceso temporal a los servicios de red habilitados para ese tipo de usuario.

La vigencia de los privilegios de usuario está limitada al tiempo que labore una persona en la institución, por seguridad las contraseñas se deberán actualizar de forma continua. Las claves se caracterizan por ser únicas, personales e intransferibles y será responsabilidad del usuario el buen uso de ellas.

2.2.2.2 Gestión de Privilegios

Los privilegios de los usuarios se asignarán basados en la función del trabajador dentro de la empresa, como pueden ser número de VLAN, ancho de banda, restricción en la navegación de páginas web, etc...

La concesión de privilegios a un usuario para acceder a la red se lo hará una vez que el proceso de inclusión del trabajador a la institución haya terminado por completo, esta fase se realizara a la brevedad posible usando la documentación adecuada.

2.2.2.3 Gestión de contraseñas de usuario

El proceso para crear una cuenta de usuario nueva del servicio AAA, se lo realizará mediante una solicitud que permita identificar el tipo de usuario, los privilegios y el periodo

de vigencia, en los casos donde se requiera dar de baja una cuenta activa se verificará que la persona esté siendo retirada de sus funciones para proceder con la eliminación de la base de datos de usuarios.

La seguridad de la información depende en gran medida de la responsabilidad que los usuarios asuman a la hora de desarrollar sus actividades, por tal razón, se recomienda establecer sanciones para aquellas personas que accedan al sistema sin autorización.

2.2.2.4 Revisión de los derechos de acceso de los usuarios

La revisión de los derechos de acceso de los usuarios se recomienda hacer cada seis meses, en caso de existir alguna modificación o cambio de personal dentro de la misma organización se reasignarán nuevos privilegios a los usuarios. Todo este proceso es necesario con el fin de evitar que un usuario obtenga algún privilegio no autorizado, si se encuentran anomalías que supongan algún tipo de riesgo de seguridad se creará un registro para su control y revisión permanente.

2.2.3 RESPONSABILIDADES DEL USUARIO

Objetivo: Impedir el acceso de usuarios no autorizados, el robo de información y recursos para el tratamiento de la información.

Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que:

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

2.2.3.1 Uso de contraseña

"Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y uso de las contraseñas" (ISO-27002, 2005).

Todos los trabajadores del GADMU deben ser informados de las políticas de la institución acerca del uso de la contraseña, siendo ellos los responsables de mantener en completa confidencialidad su clave personal para el acceso a la red.

Las contraseñas no se deben guardar en ningún tipo de registro como papel, archivos digitales o dispositivos electrónicos a excepción de las personas autorizadas para hacerlo, por ejemplo los administradores de la unidad de sistemas que manejan diversas claves y demasiado extensas para ser memorizadas.

El cambio de contraseñas se lo podrá hacer cuando exista algún indicio de vulnerabilidad que represente un peligro para el sistema.

La clave que el usuario elija debe cumplir ciertas reglas que garanticen un nivel de seguridad aceptable:

- La longitud mínima debe ser de 10 caracteres
- Complejidad: Combinación de letras mayúsculas y minúsculas, números y al menos un carácter especial (signos de puntuación).
- No basarse en algo que alguien pueda adivinar como nombres, fechas, números de teléfono, etc.
- No usar palabras incluidas en diccionarios para evitar ataques de este tipo.
- Descartar por completo caracteres repetidos consecutivos.

La actualización de las contraseñas de usuario se lo hará por lo menos una vez al año, se prohíbe el uso de la misma clave para propósitos personales o cualquier actividad que no sea el acceso a la red del GADMU mediante el servicio AAA.

2.2.3.2 Equipo informático de usuario desatendido

"Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada" (ISO-27002, 2005).

Si el usuario necesita abandonar su puesto de trabajo deberá cerrar todas las cesiones activas antes de irse, el sistema deberá solicitar las credenciales de autenticación nuevamente para acceder a la red. Lo recomendable es que los usuarios no dejen sus puestos de trabajo desatendidos por un periodo de tiempo prolongado, en caso de hacerlo deben asegurarse que el equipo terminal esté apagado.

2.2.4 CONTROL DE ACCESO A LA RED

Objetivo: Impedir el acceso no autorizado a los servicios en red.

Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que:

El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:

- Que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones;
- Que se aplican los mecanismos de autenticación adecuados a los usuarios y equipos;
- El cumplimiento del control de los accesos de los usuarios a los servicios de información.

2.2.4.1 Política de uso de los servicios de red

"Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar" (ISO-27002, 2005).

Los usuarios de la red del GAD Municipal San Miguel de Urcuqui tendrán acceso directo a los servicios y aplicaciones dependiendo del rol que desempeñe dentro de la institución.

2.2.4.2 Autenticación de usuario para conexiones externas

"Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios" (ISO-27002, 2005).

La autenticación de usuarios remotos se debe realizar mediante aplicaciones que utilicen métodos criptográficos para garantizar que los datos viajen seguros por la red, las redes privadas virtuales (VPN[48]) son una excelente solución para este tipo de comunicación.

2.2.4.3 Autenticación de nodos de la red

Todos los nodos de la red, especialmente los equipos inalámbricos deberán soportar el estándar 802.1X, la política de seguridad será usar la base de datos MySQL para almacenar todos los equipos inalámbricos que funcionarán como autenticador de los usuarios del servicio AAA con la finalidad de garantizar la legitimidad de los dispositivos que sirven como medio de acceso para los clientes de la red de datos del GADMU.

2.2.4.4 Segregación en las redes

"Se deberían segregar los grupos de usuarios, servicios y sistemas de información en las redes" (ISO-27002, 2005).

La red de datos institucional se dividirá en dominios lógicos para un mayor control y facilidad de administración mediante la implementación de VLANs (redes de área local

[48] VPN Virtual Private Network

virtuales). Los criterios a seguir para la segregación de las redes serán los requisitos de control de acceso que la unidad de sistemas haya planificado de acuerdo a los requerimientos de la organización.

En el caso de las redes inalámbricas se recomienda usar un firewall y una VLAN diferente que separe el tráfico de los usuarios temporales, junto con un servidor RADIUS para controlar los puntos de acceso. Se recomienda utilizar el protocolo WPA2[49]-Enterprise, sistema de autenticación que usa el estándar 802.1X/EAP para proteger la red.

2.2.4.5 Control de conexión a las redes

Todos los usuarios de la red de datos del GAD Municipal San Miguel de Urcuqui deberán usar el método de autenticación EAP-TTLS para acceder, las credenciales de autenticación se obtendrán siguiendo el procedimiento y las recomendaciones indicadas en los apartados anteriores, específicamente en el punto 2.2 referente a la política de seguridad de control de acceso.

Para proteger la red de datos del GADMU de conexiones externas provenientes del internet se crearan filtros de tráfico por medio de listas de control de acceso aplicadas en un firewall ubicado en el perímetro de la red.

[49] WPA2 Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2

2.2.4.6 Control de encaminamiento en la red

"Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de accesos a las aplicaciones de negocio" (ISO-27002, 2005).

Una posible solución para este control es la implementación de un Proxy usando SQUID[50], aplicación que permite restringir la navegación de páginas web, así como la optimización del uso de ancho de banda en las conexiones. Un servidor proxy en la red más un firewall bien configurado representa la mejor defensa frente a cualquier amenaza externa que pudiera afectar la intranet del GAD Municipal San Miguel de Urcuqui.

2.2.5 ORDENADORES PORTÁTILES

Objetivo: Garantizar la seguridad de la información en el uso de recursos de informática móvil.

Los principios del estándar ISO 27002 (2005) para este objetivo de control indican que:

> La protección exigible debería estar en relación a los riesgos específicos que ocasionan estas formas específicas de trabajo. En el uso de la informática móvil deberían considerarse los riesgos de trabajar en entornos desprotegidos y aplicar la protección conveniente.

[50] Programa de software libre que implementa un servidor proxy.

2.2.5.1 Informática móvil

Cuando se requiera acceder a la red mediante dispositivos móviles como portátiles, teléfonos inteligentes, agendas electrónicas entre otros se debe tener especial cuidado para asegurar que la información privada de la institución no se exponga a posibles delitos informáticos, una solución para este control es separar el tráfico mediante una VLAN de usuarios invitados donde los privilegios se limiten a la navegación de páginas web, con el fin de bloquear totalmente el acceso a la red de datos de la institución.

2.3 REQUERIMIENTOS DE SEGURIDAD

Cada proceso del sistema AAA requiere de parámetros específicos que se deben cumplir a la hora de implementar la solución, el diseño de red debe incluir un firewall con tres interfaces de red (WAN, LAN, DMZ) y la segmentación de la red interna (VLAN) del GAD Municipal San Miguel de Urcuquí.

2.3.1 VLAN

Una VLAN (red de área local virtual) es una subred IP separada de manera lógica, permite que múltiples redes IP existan en el mismo equipo conmutado (switch). En la Figura 34 se muestra un ejemplo de la segmentación de redes usando VLAN.

Las VLAN trabajan en la capa 2 del modelo OSI, todo el tráfico que se genera dentro de una red virtual permanece dentro de esa VLAN, esto hace que los equipos conectados a distintas VLAN no tengan conectividad directa a través de la capa MAC Ethernet.

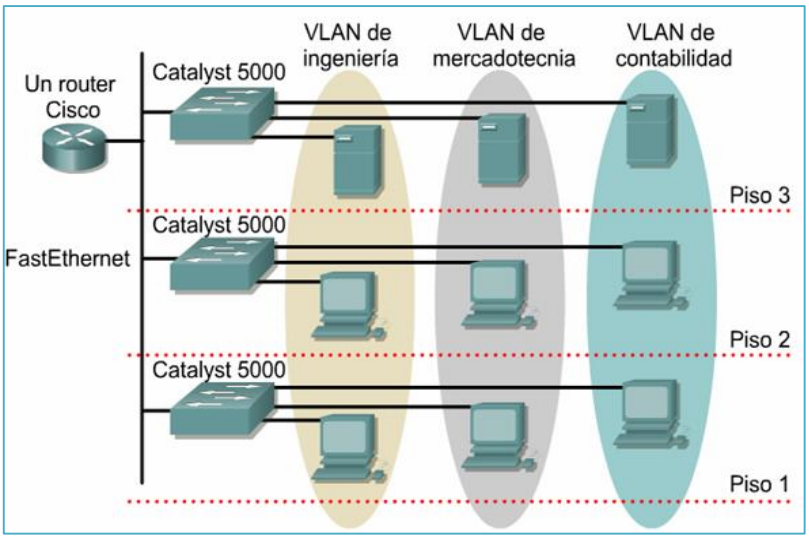


Figura 34. Red de área local virtual (VLAN)
Nota. Fuente: adaptado de http://electrotelematica.wordpress.com/2011/03/08/vlan/

Para lograr la comunicación entre dispositivos de redes virtuales diferentes se debe usar un equipo de capa 3 (router) con el fin de encaminar el tráfico correctamente, si se usa un router tradicional cada una de sus interfaces se debe conectar a una sola VLAN generando un desperdicio de puertos, la solución a este problema de eficiencia es emplear equipos que soporten el estándar 802.1Q mediante enlaces troncales, mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico.

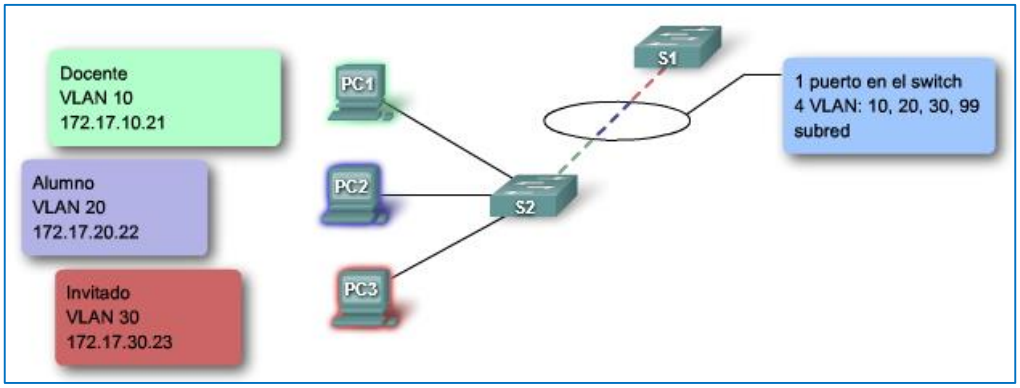


Figura 35. Enlace Troncal transporta Múltiples VLAN
Nota. Fuente: adaptado de CISCO. (2008). *CCNA 3 Exploration 4.0: Conmutación y conexión inalámbrica de LAN*. Recuperado de http://es.scribd.com/doc/17481738/Cisco-CCNA-3-Exploration-Conmutacion-y-Conexion-Inalambrica-de-Lan-Version-40-Espanol-

2.3.1.1 Direccionamiento IP

En la infraestructura actual de red de datos del GAD Municipal San Miguel de Urcuqui no se ha implementado la tecnología de VLAN para la segregación de redes, de acuerdo a la política de seguridad es recomendable hacerlo, por tal razón en la Tabla 13 se muestra un posible diseño lógico con la distribución de redes virtuales y el direccionamiento IP requerido para cada uno de los departamentos de la institución, elaborado de acuerdo a la información proporcionada por el administrador de la unidad de Sistemas.

Tabla 13. Distribución de VLAN red GADMU

VLAN ID	DEPARTAMENTO	Nro. U	SUBRED	MÁSCARA
100	DATACENTER	10	172.25.1.0	/24
2	ALCALDÍA	2	172.25.2.0	/24
3	PROCURADURÍA SINDICA	2	172.25.3.0	/24
4	COMISARIA	5	172.25.4.0	/24
5	DIRECCIÓN DE PLANIFICACIÓN CIUDADANA	8	172.25.5.0	/24
6	SECRETARÍA GENERAL	6	172.25.6.0	/24
7	DIRECCIÓN ADMINISTRATIVA	12	172.25.7.0	/24
8	DIRECCIÓN FINANCIERA	12	172.25.8.0	/24
9	DIRECCIÓN DE OBRAS PÚBLICAS	12	172.25.9.0	/24
10	DIRECCIÓN DESARROLLO SOSTENIBLE	9	172.25.10.0	/24
11	DESARROLLO SOCIAL Y COMUNICACIÓN	4	172.25.11.0	/24
12	PATRONATO MUNICIPAL	7	172.25.12.0	/24
13	AUDITORIA	1	172.25.13.0	/24
14	BIBLIOTECA	6	172.25.14.0	/24
15	INFOCENTROS	6	172.25.15.0	/24
16	Wi-Fi	x	172.25.16.0	/24

Nota. Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui. (2013).

2.3.2 FIREWALL – PROXY

El firewall-proxy del GAD Municipal San Miguel de Urcuquí se diseña como una solución basada en software, la función principal será controlar el tráfico de datos y las solicitudes de acceso a páginas web de acuerdo a las políticas de seguridad definidas en función de los requerimientos de la institución.

2.3.2.1 Firewall

El firewall es un punto de control para el tráfico que entra y sale de la red, logrando que el acceso a los servicios de red se permita exclusivamente a los usuarios autorizados, además define distintos niveles de acceso basados en privilegios grupales con lo que se garantiza el uso eficiente de la red.

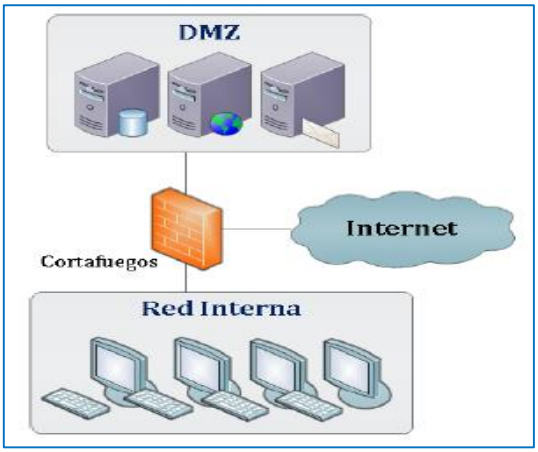


Figura 36. Ubicación del Firewall en una red
Nota. Fuente: adaptado de
http://www.securenet.cz/en-firewalls-and-routers.php

2.3.2.1.1 Políticas del Firewall

Existen dos principios básicos a la hora de diseñar las reglas de un firewall, usar una política restrictiva en la que se rechaza todo tráfico excepto el que está explícitamente

permitido, o usar una política permisiva donde se permite todo tráfico excepto el que esté explícitamente prohibido.

Para el diseño del firewall del GAD Municipal San Miguel de Urcuquí se usará la política restrictiva en base a las recomendaciones establecidas en el punto 2.2.1.1 referente a la policía de control de accesos. A continuación se listan algunos criterios para crear las reglas, tomando en cuenta el tipo de tráfico manejado por la red de datos de la institución.

- Permitir el tráfico de redes internas (DMZ, local) al firewall.
- Permitir o restringir el tráfico entre redes internas.
- Permitir el tráfico de la red local a Internet.
- Restringir el tráfico del firewall a redes externas.
- Bloquear el tráfico de redes externas al firewall.
- Bloquear el tráfico de redes externas a redes internas (DMZ, local).

2.3.2.2 Proxy

Un servidor Proxy es un equipo intermediario ubicado entre el navegador Web del usuario e Internet, como política de seguridad se recomienda instalarlo en la zona desmilitarizada (DMZ).

El proxy comúnmente usado es el http, con el cual se bloquea el acceso a diversas páginas web por motivos de seguridad y rendimiento, como regla general únicamente se debe aceptar conexiones provenientes de los equipos de la red interna.

2.3.2.2.1 Reglas de acceso Proxy

La configuración del servidor proxy deberá cumplir con ciertas reglas básicas de seguridad de acuerdo a los requerimientos de la institución:

- Los puertos permitidos serán: 3128, 8080
- Definir subredes para cada VLAN existente, ver Tabla 20.
- Restringir la navegación Web (bloquear sitios peligroso)
- Restringir el acceso a contenido por extensiones
- Servidor DHCP [51]múltiple para redes virtuales

2.3.3 CONTROL DE ACCESO A LA RED (SERVIDOR AAA)

Los parámetros de autenticación, autorización y contabilidad que se detallan a continuación se utilizarán de base para elaborar el pliego de condiciones técnicas requeridas en la implementación del servidor AAA en el GAD Municipal San Miguel de Urcuquí.

2.3.3.1 Autenticación

Los elementos necesarios para implementar el servicio de autenticación en el GADMU son:

- Un switch con soporte 802.1X para los usuarios de la red cableada.
- Un router inalámbrico con soporte 802.1X para los usuarios Wi-Fi.
- Un servidor FreeRADIUS habilitado el método de autenticación EAP-TTLS.

[51] DHCP Dynamic Host Configuration Protocol

- Un software suplicante instalado en los sistemas operativos clientes que no soporten el método de autenticación EAP-TTLS.

2.3.3.2 Autorización

Los requerimientos para implementar el servicio de autorización en la red del GADMU son:

- Diseño e implementación de las redes de área local (VLAN) en los equipos de distribución del GADMU.
- Un servidor OpenLDAP para el registro de credenciales de usuario de todos los trabajadores de la institución que tienen acceso a la red.
- Instalar el esquema FreeRADIUS en el servidor OpenLDAP.

2.3.3.3 Contabilidad

Para completar el diseño del servidor AAA se deberá instalar una base de datos usando MySQL en la que se registrará información referente al acceso de usuarios a la red, FreeRADIUS contiene plantillas que facilitan la creación de tablas en MySQL donde se ingresará los datos automáticamente.

Finalmente se usarán las funcionalidades de OpenSSL, una herramienta para la creación de certificados digitales requeridos en el servidor FreeRADIUS y OpenLDAP con el fin de establecer conexiones seguras para la comunicación.

CAPÍTULO III

DISEÑO DE LA INFRAESTRUCTURA DE RED TCP/IP CON SERVICIO AAA

3.1 ARQUITECTURA DEL SERVICIO AAA

El servicio AAA de la red de datos del GAD Municipal San Miguel de Urcuqui se diseña en base al estándar IEEE 802.1x para el control de acceso a la red, el modelo usado en la implementación se muestra en el esquema de la Figura 37. Todas las consideraciones de diseño que se describen a continuación, se basan en los requerimientos del estándar 802.1x usando como método de autenticación EAP-TTLS.

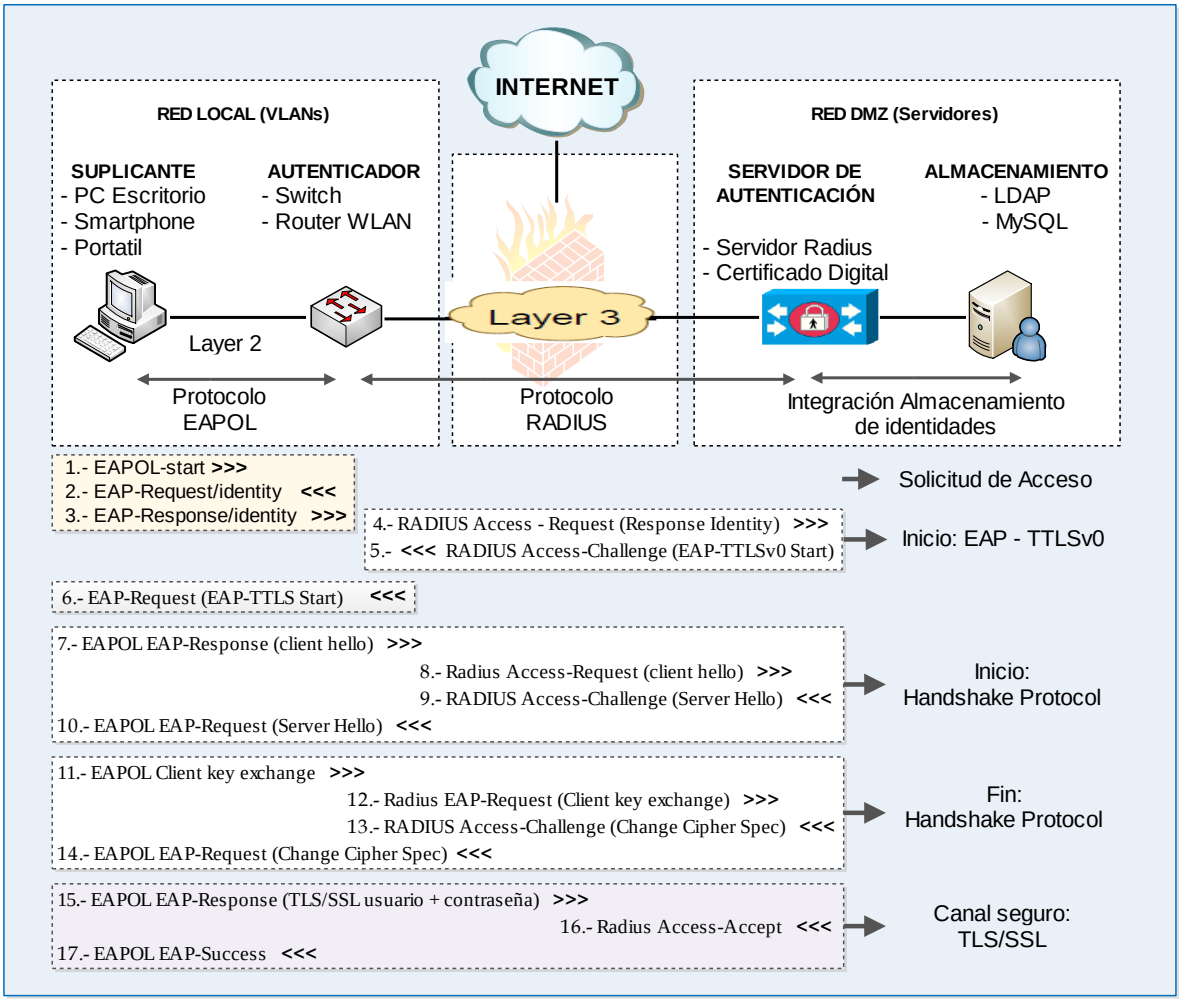


Figura 37. Infraestructura de acceso 802.1X / EAP-TTLS GADMU
Nota. Fuente: Adaptado de http://d2zmdbbm9feqrf.cloudfront.net/2011/anz/pdf/BRKSEC-2005.pdf

3.1.1 CONSIDERACIONES TÉCNICAS 802.1X / EAP-TTLS

Los componentes básicos de un sistema 802.1x son: suplicante, autenticador y el servidor de autenticación, sin embargo, la solución planteada en la red de datos del GADMU requiere cuatro componentes adicionales, una autoridad certificadora, un firewall, un directorio LDAP y una base de datos SQL. En la Figura 1, se presenta un escenario donde se integra los elementos adicionales requeridos.

- La CA (Autoridad Certificadora) se emplea para generar el certificado digital que el servidor RADIUS utiliza en el proceso de autenticación EAP-TTLS.
- El firewall en la arquitectura 802.1x realiza la función de router, es decir, permite la comunicación entre las diferentes zonas de red.
- El directorio LDAP permite almacenar las credenciales de usuario de todos los usuarios del GADMU y las políticas de acceso configuradas mediante la asignación de VLANs.
- La base de datos SQL registra los equipos autenticadores de la red y la información generada en el proceso de contabilidad.

3.1.1.1 Usuario (Suplicante)

EAP-TTLS no requiere la instalación de certificados digitales en el equipo del usuario (pc de escritorio, portátil, Smartphone, etc.), simplemente el suplicante debe ser compatible con el método de autenticación.

EAP-TTLS es soportado de forma nativa por plataformas como OSX de Apple, Android, iPhone OS, Linux y Windows 8, para utilizar EAP-TTLS en sistemas operativos como Windows 7 o en versiones inferiores, se requiere de un suplicante externo, por ejemplo SecureW2.

Si el sistema operativo requiere de un software adicional para soportar EAP-TTLS se debe instalar y luego configurar los parámetros asociados a 802.1X y EAP-TTLS usando el asistente de conexión de red.

Para que el usuario verifique la validez del certificado digital del servidor RADIUS, se debe añadir la clave pública de la autoridad certificadora en la raíz del equipo local, utilizando el formato .DER para que sea reconocido por los sistemas operativos creados bajo la plataforma Windows.

3.1.1.2 Equipo autenticador

Un cliente radius es cualquier dispositivo que ofrece el servicio de acceso a la red, en el caso de las redes cableadas el más común es el switch y en las inalámbricas el Access Point.

En los conmutadores de red cableados se debe activar el servicio 802.1X de forma global y además en cada uno de los puertos donde se requiera autenticar a un usuario. Para las redes inalámbricas se debe activar el modo de seguridad WPA2-Enterprise, que utiliza como método de autenticación 802.1X/EAP.

Los equipos de autenticación y suplicantes son los únicos elementos rígidos del sistema AAA, debido a que su configuración se limita a las prestaciones de fábrica del equipo, a diferencia del resto, que son una solución basada en software (Linux) y por lo tanto se adaptan a funciones personalizadas.

3.1.1.3 Servidor RADIUS

En el servidor RADIUS se debe habilitar el método de autenticación EAP-TTLS y los parámetros asociados a este mecanismo de acceso.

Se definen los servidores que se integran al servicio AAA, como el directorio LDAP y la base de datos SQL. Es importante tomar en cuenta que al usar LDAP como base de datos externa en los procesos de autenticación y autorización se debe emplear PAP (Password Authentication Protocol) como método autenticación interno, debido a la compatibilidad con los algoritmos de cifrado que utiliza LDAP (SHA1[52], SHA2, md5) para almacenar las contraseñas.

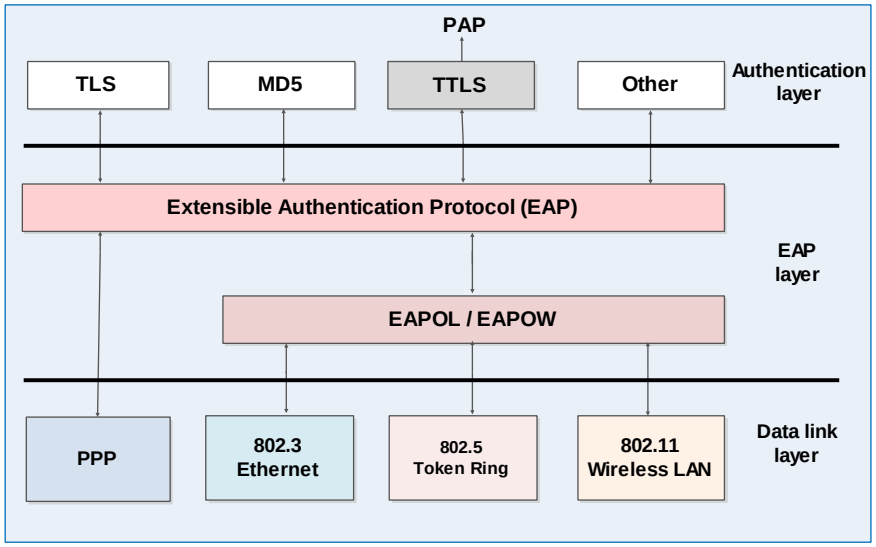


Figura 38. Arquitectura EAP-TTLS-PAP
Nota. Fuente: http://wire.cs.nctu.edu.tw/wire1x/COMMAG-05-00270-post.pdf

[52] SHA1. Secure Hash Algorithm 1

PAP es un protocolo simple de autenticación que transmite las credenciales de autenticación en texto plano, sin cifrar, esto no representa ninguna vulnerabilidad de seguridad para el sistema AAA, debido a que al usarlo junto a EAP-TTLS, los datos se transmiten de forma segura a través de un canal encriptado TLS empleando certificados digitales.

3.1.1.4 Protocolos 802.1X

El equipo autenticador establece y maneja la conexión entre los usuarios y el servidor RADIUS usando dos protocolos específicos, el switch y suplicante se comunican usando el protocolo de capa 2 EAPOL (EAP sobre LAN) y esta información se transmite al servidor de autenticación empleando el protocolo RADIUS, ver Figura 39.

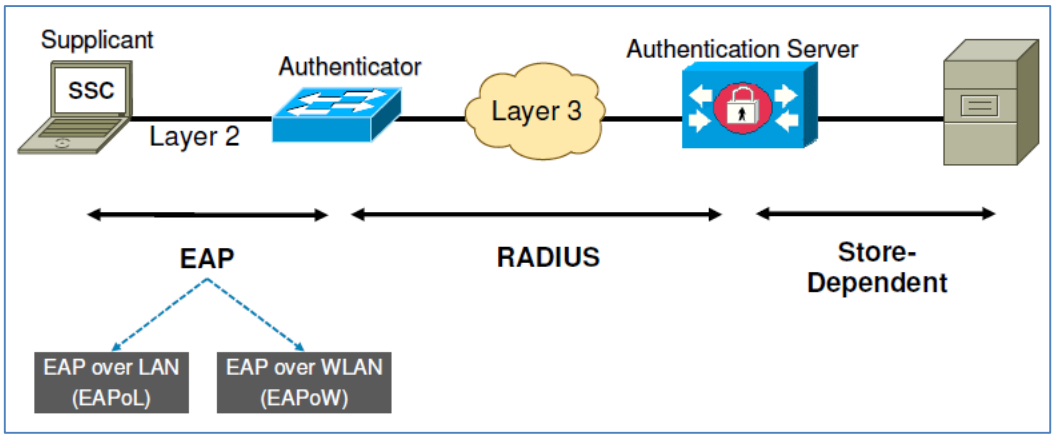


Figura 39. Protocolos usados en una comunicación 802.1X
Nota. Fuente: Recuperado de http://d2zmdbbm9feqrf.cloudfront.net/2011/anz/pdf/BRKSEC-2005.pdf

- **Encapsulación EAPOL**

Durante todo el proceso de intercambio de paquetes entre el suplicante y el cliente radius se manejan tramas EAPOL, es decir se encapsulan los mensajes EAP en la trama

Ethernet, para identificar un mensaje EAPOL se inserta en el campo “Tipo” de la trama Ethernet el número 888E en formato hexadecimal, ver Figura 4.

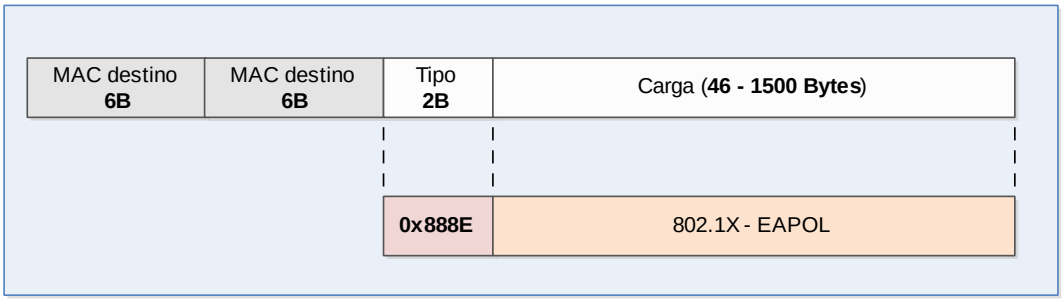


Figura 40. Mensaje EAP encapsulado en trama Ethernet
Nota. Fuente: Adaptado de http://es.scribd.com/doc/6081671/31/Formato-de-trama-para-802-1x

- **Encapsulación RADIUS**

RADIUS es un protocolo de capa aplicación que utiliza el mecanismo de transporte UDP para el intercambio de paquetes entre el autenticador y servidor radius. Por defecto, los puertos de escucha son: 1812 para mensajes de autenticación y 1813 para contabilidad. Como se muestra en la Figura 5, los mensajes RADIUS se encapsulan en la carga útil del paquete UDP.

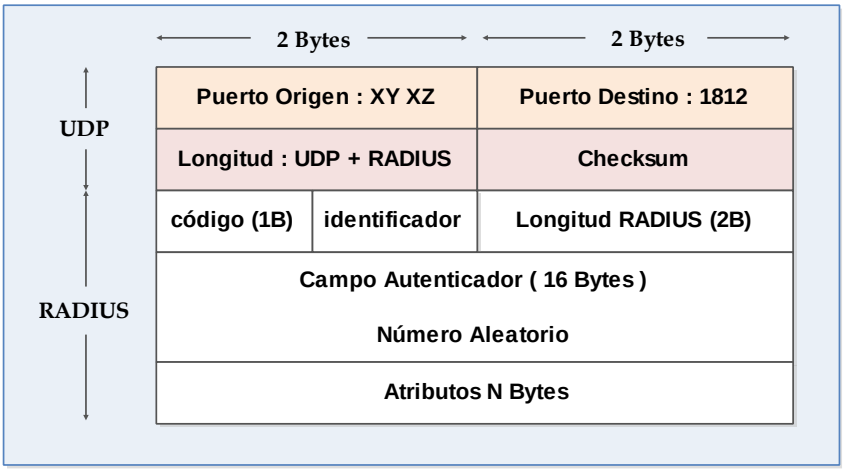


Figura 41. Encapsulación del paquete radius en UDP
Nota. Fuente: Captura de la interfaz gráfica Wireshark

3.1.1.5 ENTRAMADO 802.1X / EAP-TTLS

A continuación se describe, paso a paso, el proceso de entramado y la secuencia de operación del sistema AAA empleando 802.1X /EAP-TTLS, el análisis se desarrolla usando el esquema general de red mostrado en la Figura 37.

1. El inicio de la comunicación se produce cuando el suplicante envía el paquete EAPOL – Start, solicitando acceso al cliente radius; esto significa que el campo "Tipo" tiene asignado el valor 01 hexadecimal, ver Figura 42.

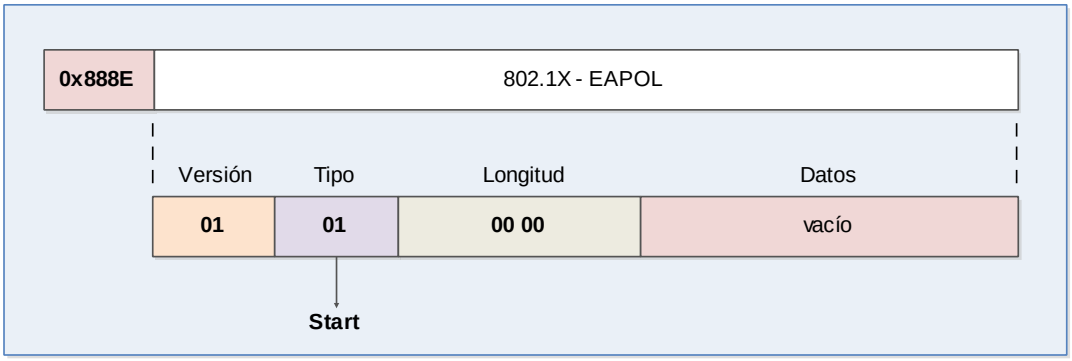


Figura 42. EAPOL-Start
Nota. Fuente: Captura de la interfaz gráfica Wireshark

2. En esta etapa del proceso el autenticador tiene bloqueado el puerto de acceso, solo recibe tramas 802.1X, el resto son descartadas. Cuando el switch recibe una trama EAPOL-Start solicita al suplicante un identificador válido para el acceso, el formato de trama para esta clase de solicitud se muestra en la Figura 43.

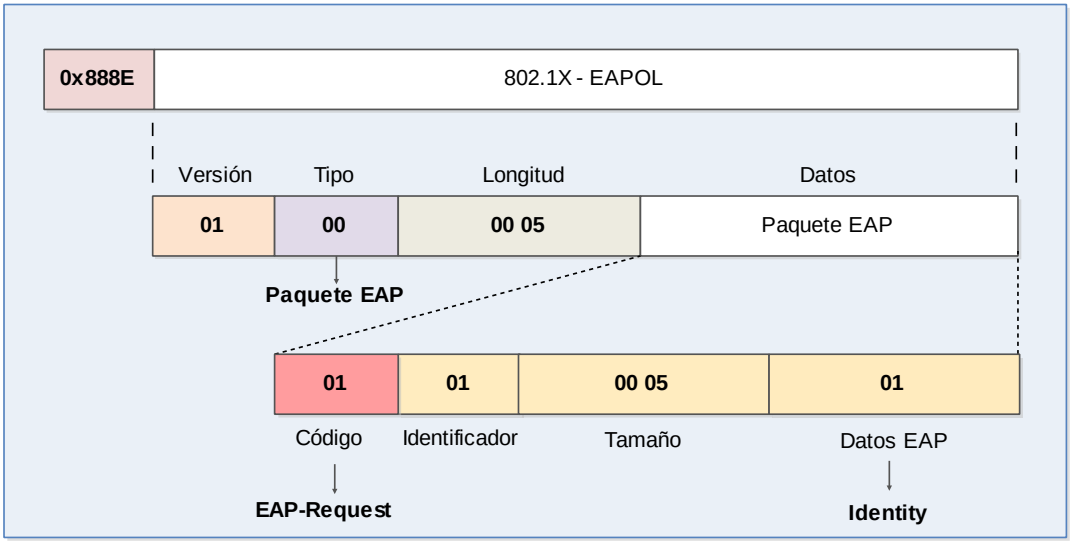


Figura 43. EAP-Request Identity
Nota. Fuente: Captura de la interfaz gráfica Wireshark

3. Con el método de autenticación EAP-TTLS es posible usar una identidad anónima para establecer el túnel seguro, de esta manera el nombre de usuario enviado por el suplicante se protege. Los datos se envían con un formato similar al mostrado en la Figura 44.

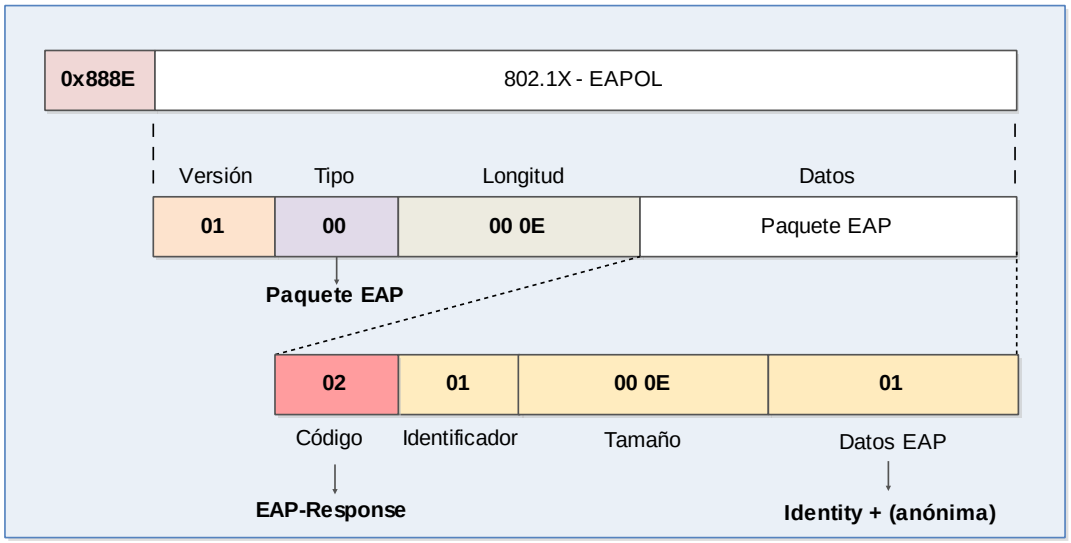


Figura 44. EAP-Response Identity
Nota. Fuente: Captura de la interfaz gráfica Wireshark

4. El autenticador extrae el mensaje recibido y lo encapsula en un paquete RADIUS. Los datos se envían al servidor a través de atributos (AVP) que contienen información del suplicante y del equipo autenticador a través del cual el usuario intenta acceder a la red, ver Figura 45.

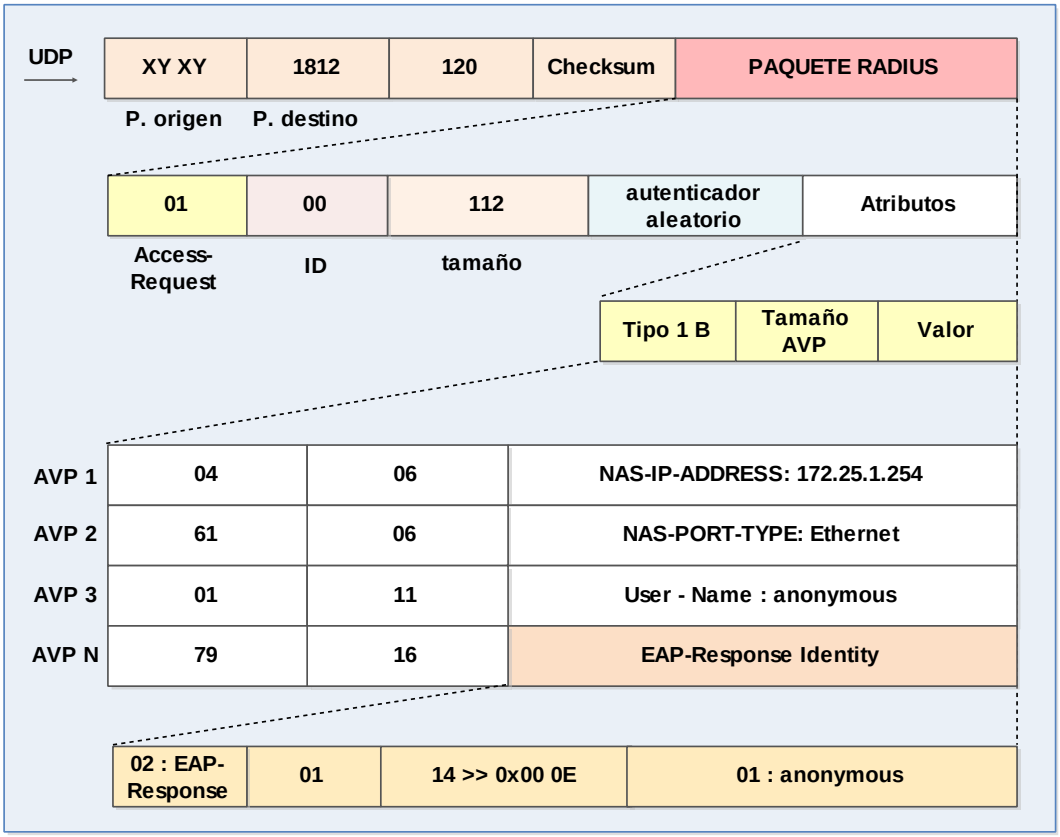


Figura 45. RADIUS Access - Request (Response Identity)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

5. En esta fase, el servidor inicia el proceso de autenticación. Para que el suplicante identifique el método de autenticación, el servidor envía el paquete usando el código 21 (EAP-TTLS) y las banderas seteadas en (0010 0000) que indican el inicio del mensaje y la versión TTLSv0, ver Figura 46.

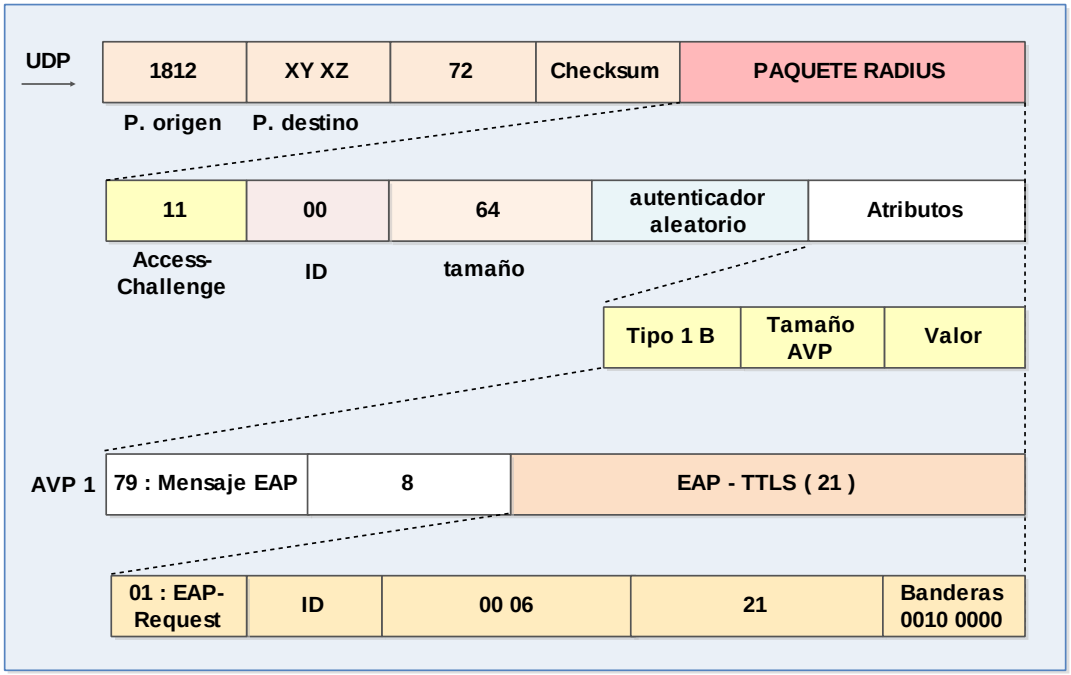


Figura 46. RADIUS Access-Challenge (EAP-TTLSv0 Start)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

6. Una vez iniciado el proceso EAP, el autenticador deja de tomar decisiones, simplemente se encarga de comunicar al suplicante con el servidor mediante los protocolos EAPOL Y RADIUS. La Figura 47 muestra como los datos se insertan en la trama Ethernet.

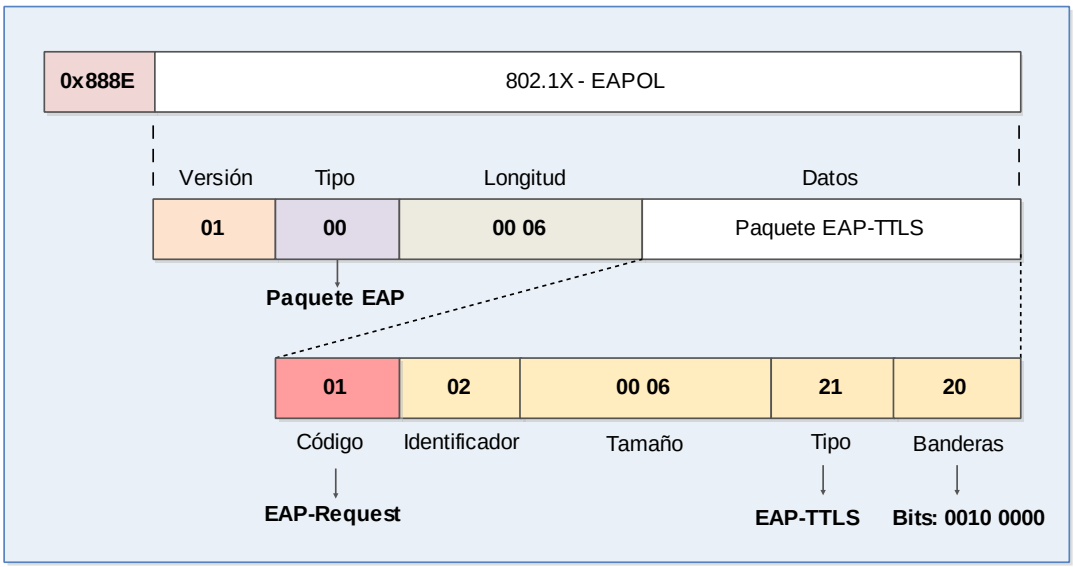


Figura 47. EAP-Request (EAP-TTLSv0 Start)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

7. Cuando el suplicante recibe el mensaje de inicio EAP-TTLSv0, arranca el proceso de intercambio de paquetes empleando el protocolo Handshake, que consiste en la transmisión de una secuencia de mensajes para negociar los parámetros de seguridad de la sesión TLS, utilizada para la transferencia de datos entre el suplicante y servidor.

   "Client Hello" suele ser el primer mensaje de la secuencia para la configuración de la sesión TLS/SSL. Algunos de los parámetros que se incluyen son:

   - **Versión**: El número de versión más alto soportado por el suplicante.
   - **Random:** Una serie de 4 octetos que incluye la fecha y hora del usuario, además de un número aleatorio generado criptográficamente
   - **Cipher Suite:** Lista con algoritmos de cifrado disponibles en el suplicante.
   - **Compression Algorithm:** Algoritmos de compresión soportados por el cliente.

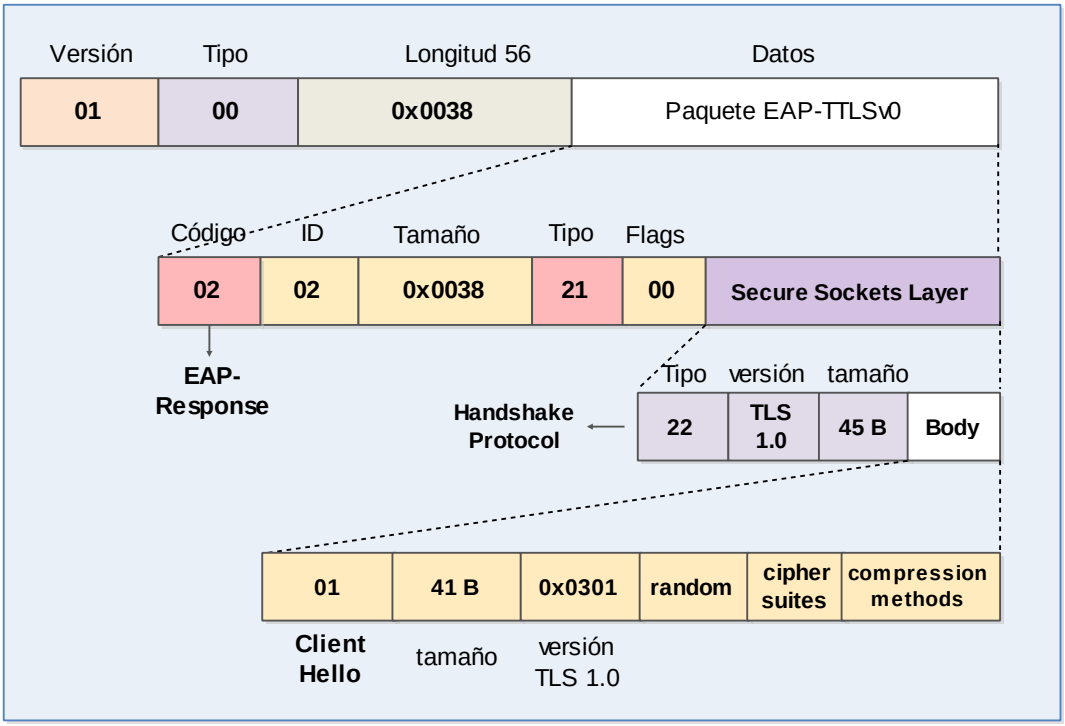


Figura 48. EAPOL EAP-Response (client hello)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

8. Proceso de encapsulación EAPOL – RADIUS, el mensaje Client Hello se envía al servidor usando el protocolo radius, la estructura se muestra en la Figura 49.

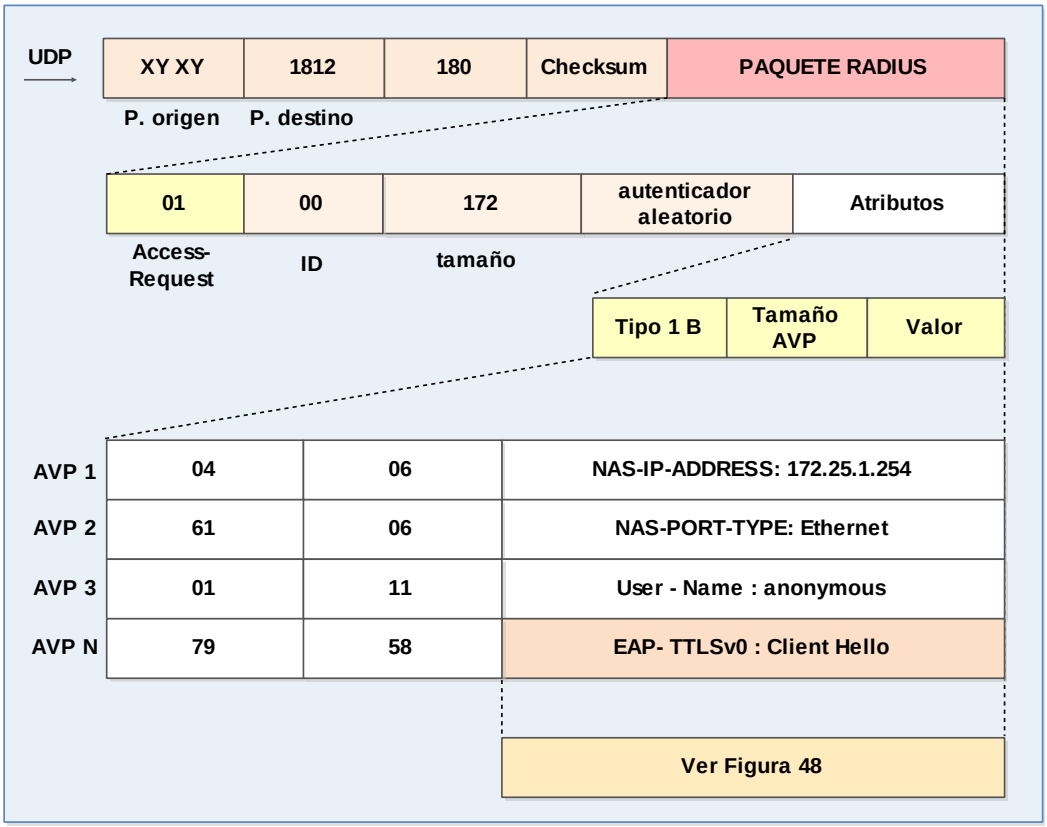


Figura 49. Radius Access-Request (client hello)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

9. El servidor debe responder el mensaje de saludo del cliente con una serie de paquetes que incluyen: el mensaje Server Hello, el certificado digital del servidor RADIUS y el mensaje Server Hello Done. La estructura del mensaje se muestra en la Figura 50.

- **Server Hello:** Contiene los parámetros (random, Cipher Suite y Compression Algorithm)

- **Certificate:** El servidor RADIUS envía el certificado digital con la clave pública del servidor. El cliente lo usará para autenticar el servidor y para cifrar la clave secreta.
- **Server Hello Done:** Este mensaje no contiene datos e indica que el servidor ha finalizado el envío de paquetes y espera una respuesta del suplicante.

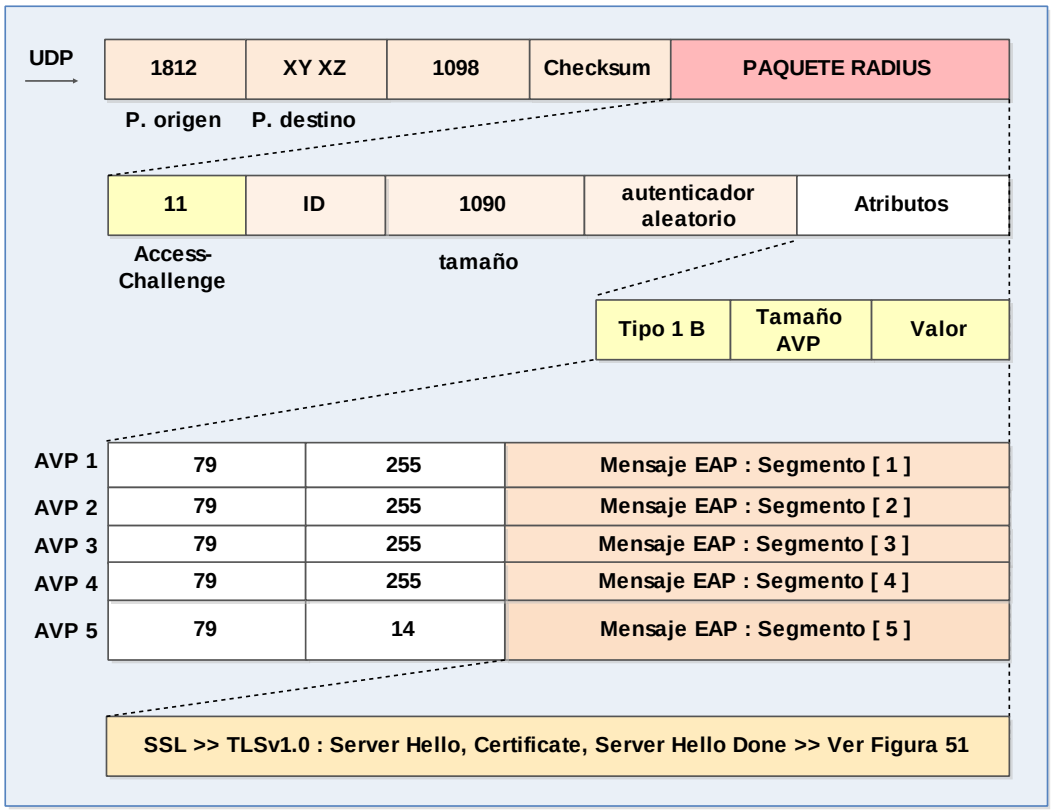


Figura 50. RADIUS Access-Challenge (Server Hello)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

10. Proceso de encapsulación RADIUS – EAPOL, el mensaje completo incluye el paquete Server Hello, el certificado digital del servidor con la clave pública y el mensaje Server Hello Done, la estructura se muestra en la Figura 51.

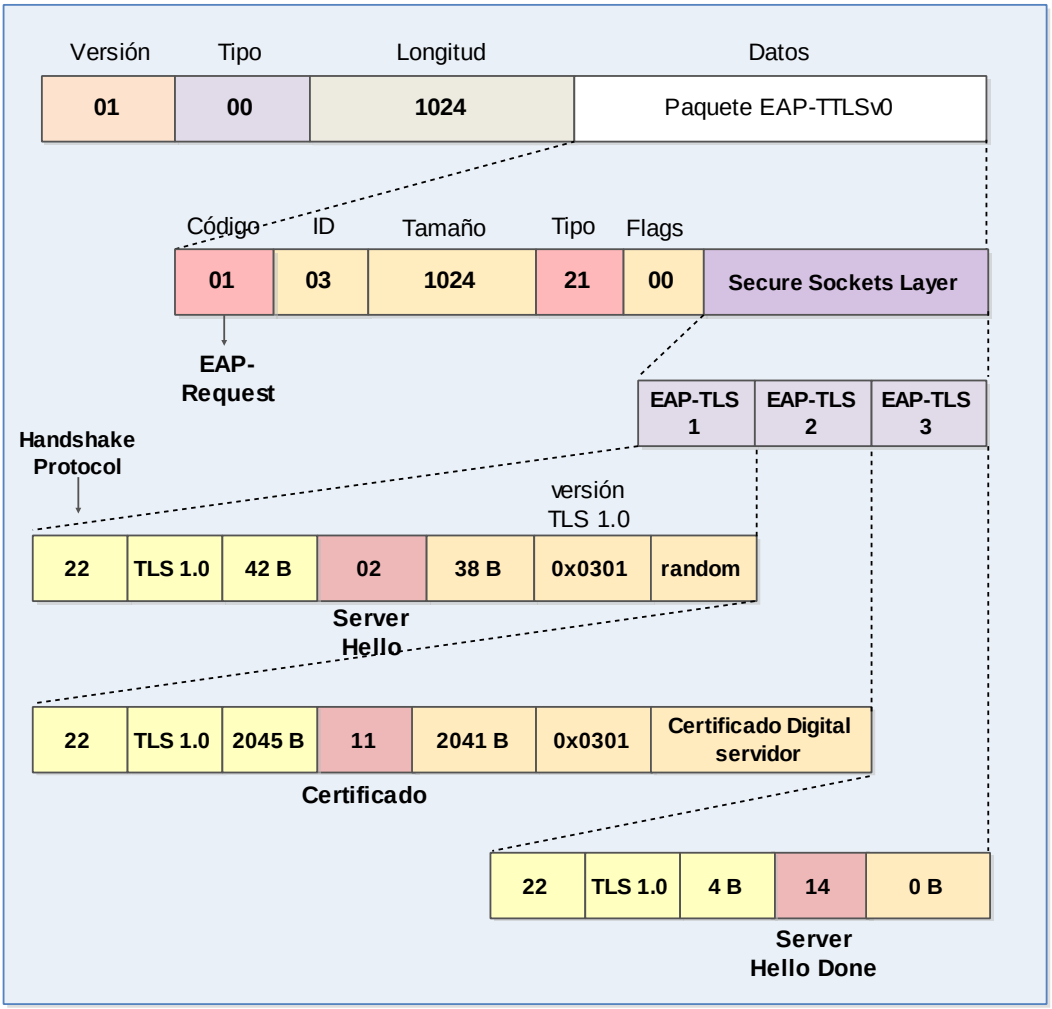


Figura 51. EAPOL EAP-Request (Server Hello)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

11. El suplicante envía un mensaje de intercambio de claves secretas generadas a partir de los datos recibidos. Las claves se calculan empleando los valores aleatorios generados en los mensajes Client y Server Hello.

    Antes de transmitir la clave secreta al servidor, se cifra mediante la clave pública del certificado del servidor. Tanto el suplicante como el servidor realizan el mismo proceso de forma local y obtienen la clave privada para la sesión segura.

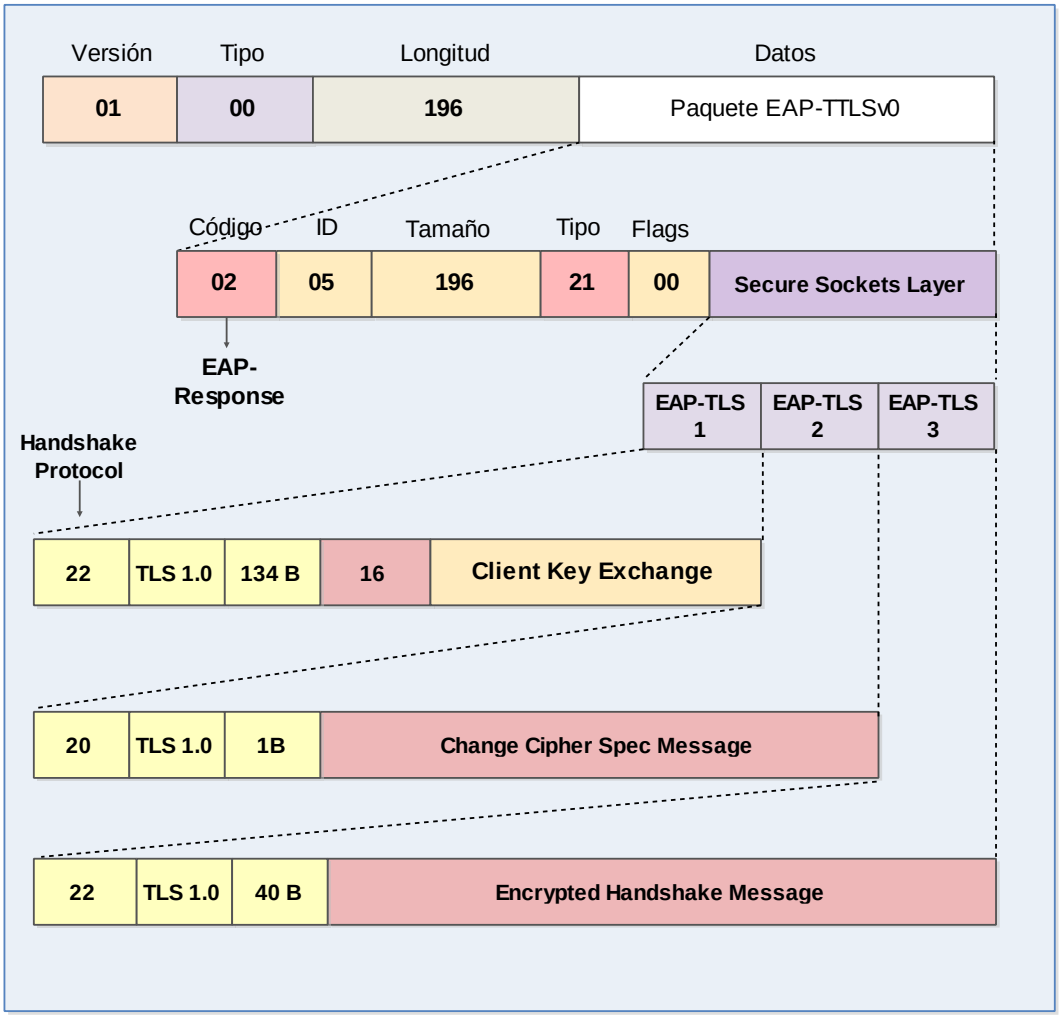


Figura 52. EAPOL Client key exchange
Nota. Fuente: Captura de la interfaz gráfica Wireshark

12. Proceso de encapsulación EAPOL – RADIUS, el autenticador reenvía la clave del cliente cifrada con la clave pública del servidor a través de los atributos RADIUS, la estructura completa del mensaje se muestra en la Figura 53.

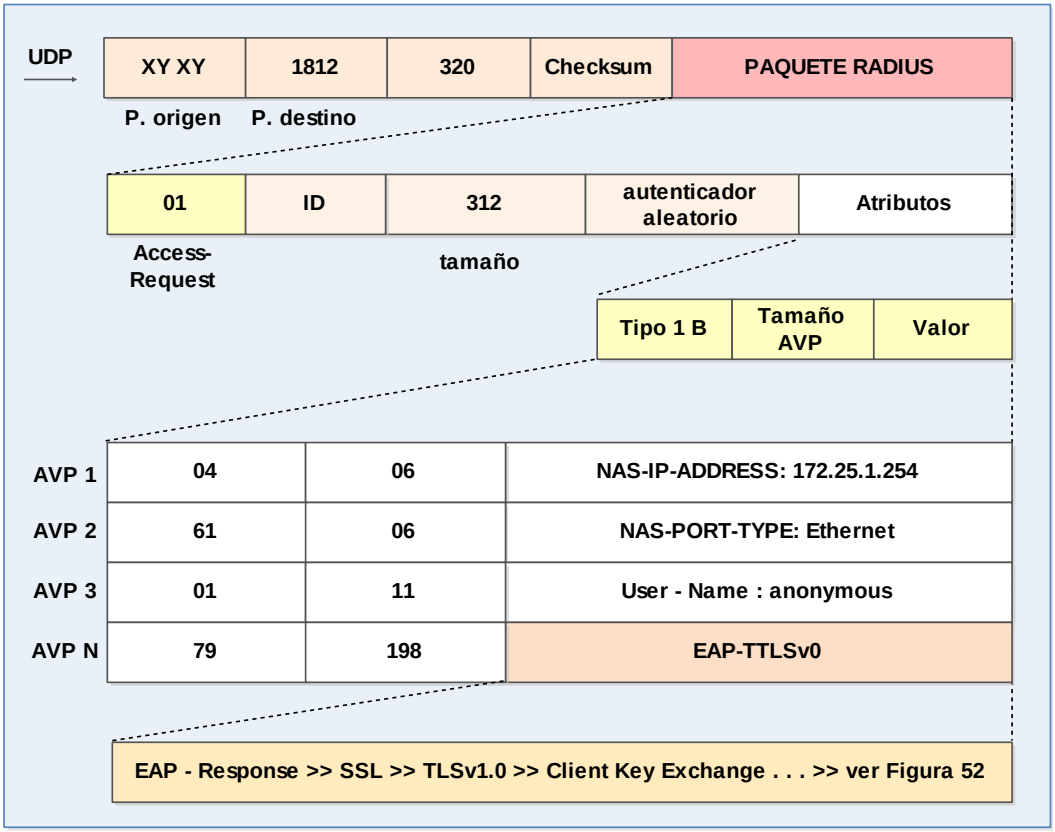


Figura 53. Radius EAP-Request (Client key exchange)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

13. Si el servidor es capaz de descifrar estos datos y completar el protocolo, el cliente tiene la seguridad de que el servidor tiene la clave privada correcta. Este paso es crucial para demostrar la autenticidad del servidor. Sólo el servidor con la clave privada que coincide con la clave pública del certificado puede descifrar los datos y continuar la negociación del protocolo TLS/SSL.

"Change Cipher Spec Message". Este mensaje notifica al cliente que el servidor RADIUS iniciará el cifrado de mensajes usando los parámetros establecidos durante el proceso de negociación TLS.

“Encrypted Handshake Message”. Este mensaje es un valor (hash), resultado de la clave de sesión y el secreto. Si el cliente puede descifrar correctamente el mensaje y validar datos contenidos, comprueba que el Protocolo Handshake TLS/SSL se ha realizado correctamente.

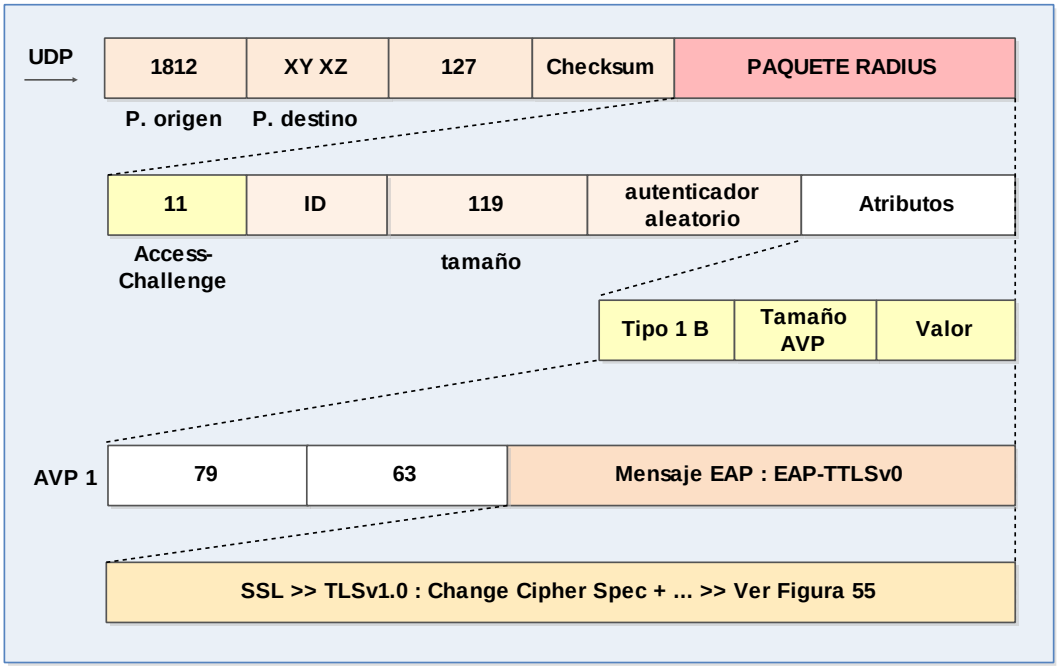


Figura 54. RADIUS Access-Challenge (Change Cipher Spec)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

14. Proceso de encapsulación RADIUS – EAPOL, el autenticador reenvía el mensaje del servidor, indicando al suplicante la finalización del Protocolo Handshake TLS/SSL, la estructura de la trama se muestra en la Figura 55.

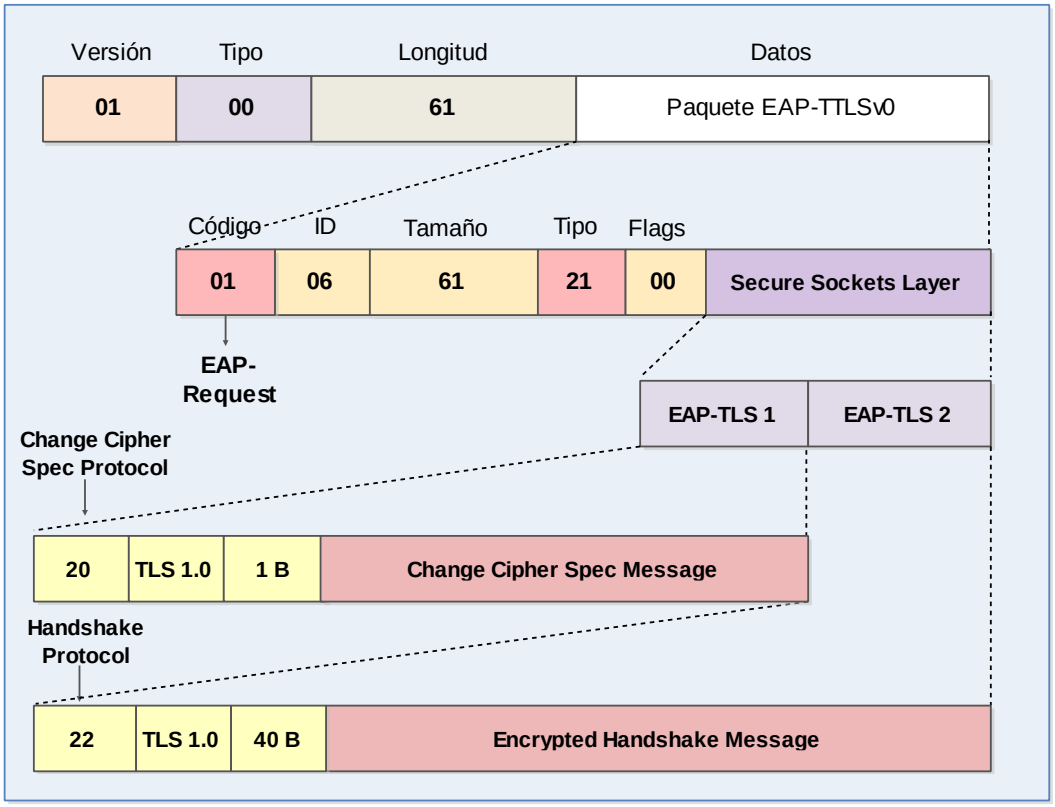


Figura 55. EAPOL EAP-Request (Change Cipher Spec)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

15. Una vez establecido el túnel, el suplicante usa el canal TLS/SSL para enviar las credenciales de acceso (usuario + contraseña) de forma segura, ver Figura 56.

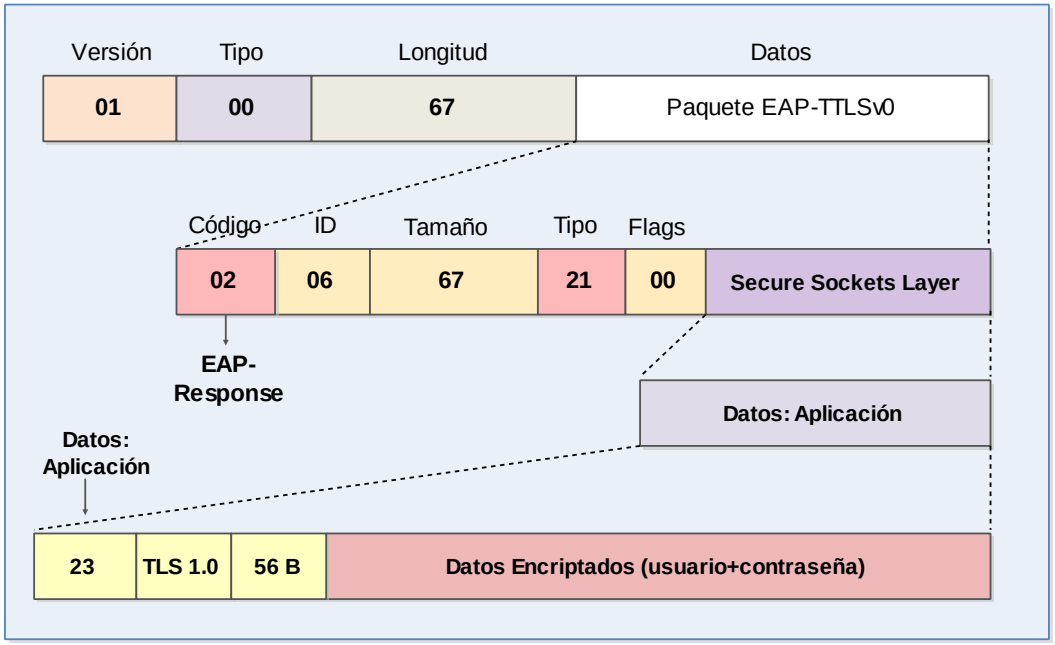


Figura 56. EAPOL EAP-Response (TLS/SSL usuario + contraseña)
Nota. Fuente: Captura de la interfaz gráfica Wireshark

16. El servidor RADIUS verifica internamente en el directorio LDAP si las credenciales de usuario enviadas por el suplicante son válidas, y si procede, responde con un mensaje EAP Access-Accept, ver Figura 57.

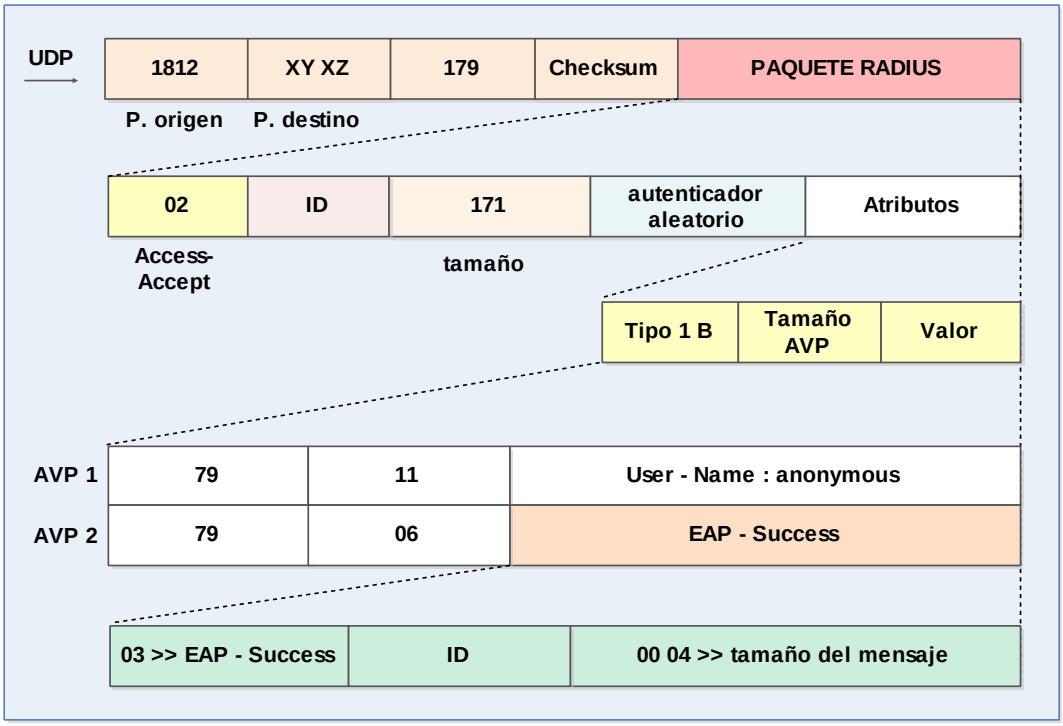


Figura 57. Radius Access-Accept
Nota. Fuente: Captura de la interfaz gráfica Wireshark

17. Finalmente, el autenticador configura el estado del puerto como Autorizado y envía un paquete EAPOL EAP-Success al suplicante, informando que la autenticación ha sido exitosa. La estructura del mensaje se muestra en la Figura 58.

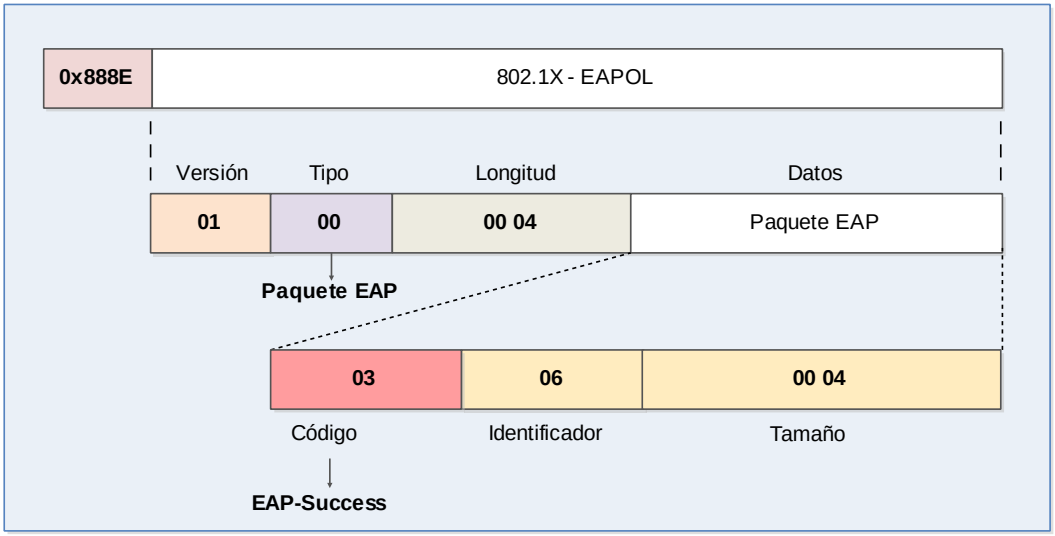


Figura 58. EAPOL EAP-Success
Nota. Fuente: Captura de la interfaz gráfica Wireshark

3.2 INTEGRACIÓN DEL SERVICIO AAA EN LA RED DEL GADMU

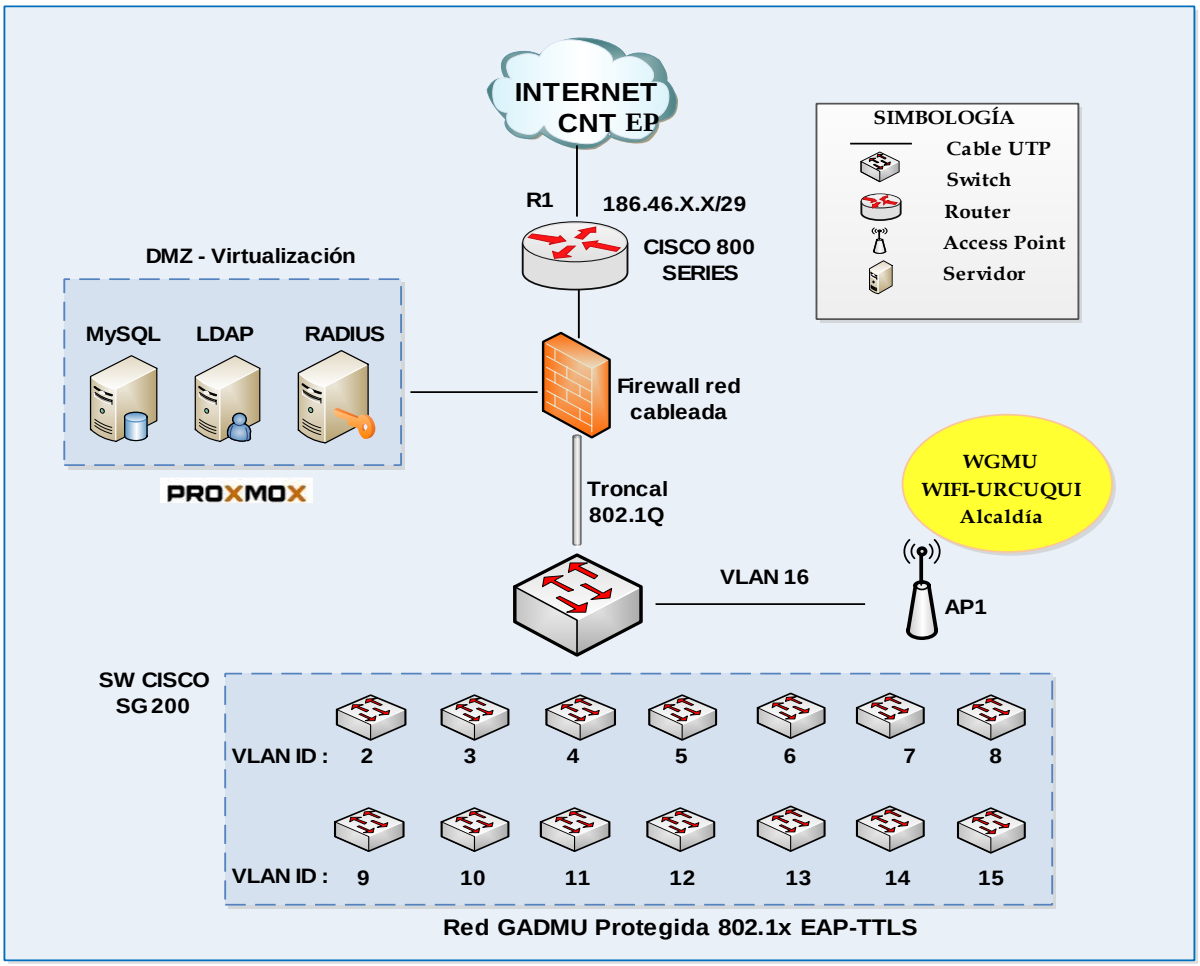


Figura 59. Integración del servicio AAA en la red del GADMU
Nota. Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui. (2013)

3.3 HERRAMIENTAS DE SOFTWARE LIBRE

El diseño del sistema AAA mostrado en la Figura 23, se base en el estándar 802.1X / EAP-TTLS, los servicios y las aplicaciones de gestión utilizadas se implementan usando herramientas de software libre. En la Tabla 1, se detalla el software requerido.

Tabla 14. Herramientas Open Source – servicio AAA

SOFTWARE	APLICACIÓN	VERSIÓN
PROXMOX VE	Virtualización de Servidores	3.0
UBUNTU SERVER	Sistema operativo base de Servidores	12.04 LTS
FREERADIUS	Servidor de Autenticación	2.1.10
OPENLDAP	Servidor de Directorio	2.4.35
JXPLORER	Gestor de OpenLDAP	3.3
MYSQL	Base de Datos (Accounting)	5.6
PHPMYADMIN	Gestor WEB de MYSQL	4.0.4.1
SHOREWALL	Firewall	4.4.0
WEBMIN	Administrador WEB de Shorewall	1.630
TINYCA2	Administrador de Autoridad Certificadora	0.7.5
SECUREW2	Suplicante Windows 7	4.1.0

Nota. Fuente: Recuperado de las páginas oficiales del software.

3.3.1 VIRTUALIZACIÓN DE PLATAFORMA

La virtualización es una tecnología que permite la ejecución de múltiples servidores en el mismo hardware, funcionan como sistemas físicos separados pero en realidad comparten recursos como: memoria, procesamiento, red, almacenamiento, etc.

Un software denominado hipervisor se encarga de gestionar las máquinas virtuales aislándolas entre sí, esto permite que cada máquina virtual pueda llevar un sistema operativo diferente de manera eficaz y sin conflictos.

En la Figura 60, se muestran los dos tipos de hipervisores que se usan en la virtualización de servidores.

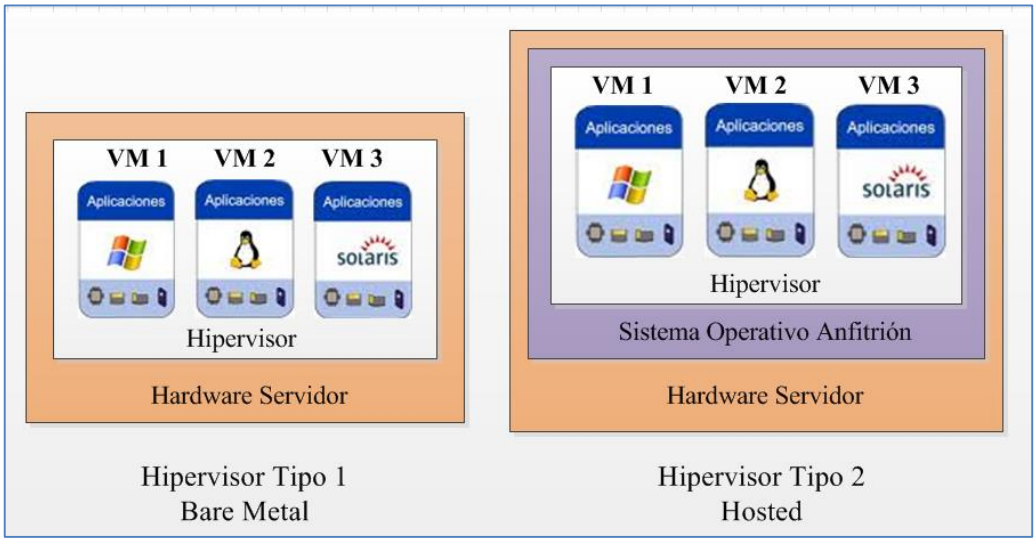


Figura 60. Tipos de Hipervisores

Nota. Fuente: Adaptado de http://ciam.ucol.mx/portal/portafolios/gutierrez_manuel/libros/server%20virtualization%20for%20dummies.pdf

Los Hipervisores tipo 1 conocidos como nativos o bare-metal se instalan directamente en el hardware del servidor físico, actualmente existen algunas soluciones que brindan este servicio: VMware ESXi, VMware ESX, Xen, KVM, Hyper-V Server.

Los Hipervisores tipo 2 (hosted) se instalan dentro de un sistema operativo anfitrión, las máquinas virtuales se ejecutan en un tercer nivel, ejemplos de este tipo son: VirtualBox, VMware, Parallels Desktop, Virtual PC, QEMU.

3.3.1.1 Ventajas de Virtualización

La virtualización es una tecnología clave que deben usar las organizaciones para optimizar los recursos de sus centros de datos, los beneficios que se pueden obtener con esta solución son:

- **Consumo de Recursos.** El modelo cliente servidor usado por la mayoría de aplicaciones con el fin de aislar los sistemas para evitar conflictos de interoperabilidad conlleva tener recursos subutilizados, la virtualización optimiza el uso del hardware del servidor.

- **Ahorro de Energía**. La migración de servidores físicos a máquinas virtuales permite implementar todos los sistemas informáticos de la empresa en un solo hardware, lo que significa reducir el consumo mensual de energía y los costos de refrigeración para el centro de datos.

- **Rápida Expansión.** La virtualización de servidores proporciona flexibilidad a la hora de actualizar o implementar un nuevo sistema. El administrador de red puede clonar una máquina virtual existente para conseguir un servidor funcional en pocos minutos de forma eficiente, evitando todo el proceso que se necesitaría en caso de usar servidores físicos para cada uno de los servicios de red.

- **Entornos de Prueba y desarrollo**. El aislamiento de aplicaciones usando servidores virtuales permite crear entornos controlados de prueba para el desarrollo de nuevos sistemas sin que estos comprometan la seguridad de la red.

- **Flexibilidad.** La virtualización reemplaza el hardware físico con uno virtual, lo que garantiza un mayor nivel de flexibilidad para los administradores de red al momento de elegir el hardware apropiado que las aplicaciones requieren.

3.3.1.2 Limitaciones de Virtualización

Un sistema operativo virtualizado no alcanza el mismo rendimiento que uno instalado directamente en el hardware físico, el hipervisor que se encarga de administrar y gestionar los recursos del servidor hace que las máquinas virtuales se vean afectadas en un pequeño porcentaje. No todos los métodos de virtualización ofrecen las mismas especificaciones técnicas, el rendimiento de cada uno dependerá del tipo de virtualización que se utilice en base a las necesidades de la organización.

En el esquema tradicional sin virtualización, si un servidor tiene un fallo a nivel de hardware únicamente la aplicación instalada deja de operar, sin embargo en un entorno virtual se tiene un único punto de fallo para todas las máquinas virtuales, cualquier daño en el hardware del servidor físico afecta a todos los sistemas operativos instalados en él. La solución a este inconveniente es usar soluciones de alta disponibilidad (clustering) que permiten tener redundancia a nivel de hardware, si un servidor físico cae, las máquinas virtuales automáticamente se ejecutan desde otro servidor.

3.3.1.3 Virtualización de servidores AAA – GADMU

Existen distintos enfoques cuando se utiliza la virtualización de plataforma, en términos generales consiste en gestionar todo el hardware del servidor físico mediante un hipervisor de

manera que múltiples sistema operativos puedan ejecutarse de manera independiente, este proceso es muy importante, ya que cada máquina virtual ve a las demás como máquinas independientes sin saber que comparte con ella ciertos recursos.

Para virtualizar los servidores AAA, se utiliza el entorno Virtual PROXMOX. Ofrece dos tecnologías de virtualización: OpenVZ y KVM.

- **OpenVZ:** Esta tecnología usa contenedores para crear los servidores virtuales, donde los sistemas operativos invitados comparten el kernel con el sistema sobre el cual está instalado.

  En este método no existe el hipervisor, lo que genera ciertas ventajas y limitaciones en relación a otros sistemas de virtualización que si lo utilizan. Por un lado mejora el rendimiento de los servidores virtuales alcanzando niveles muy cercanos al nativo logrando soluciones mucho más ligeras.

  La limitación se encuentra en la compatibilidad, el hecho de compartir el kernel no permite ejecutar sistemas operativos de plataformas distintas, por ejemplo, no es posible usar OpenVZ para virtualizar servidores Windows.

En la Figura 61 se puede apreciar la arquitectura de virtualización a través de contenedores virtuales.

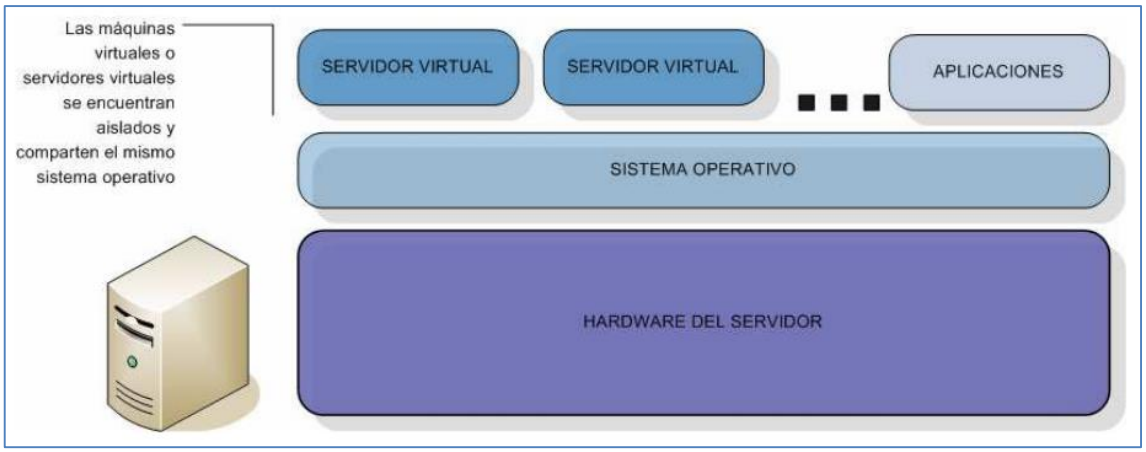


Figura 61. Virtualización de servidores Linux basada en Contenedores Virtuales
Nota. Fuente: Recuperado de http://www.adminso.es/images/6/6d/Eugenio_cap1.pdf

- **Virtualización a nivel del kernel.** Este modelo de virtualización usa el kernel de Linux para ejecutar las máquinas virtuales, es decir el núcleo actúa como hipervisor. Los servidores virtuales se ejecutan en el espacio de usuario del sistema base como procesos totalmente independientes.

  La solución más conocida es KVM[53], la cual permite ejecutar múltiples máquinas virtuales Linux o Windows sin la necesidad de modificar el sistema operativo invitado.

  La arquitectura de virtualización a nivel de kernel se puede ver en la Figura 62.

[53] Kernel-based Virtual Machine

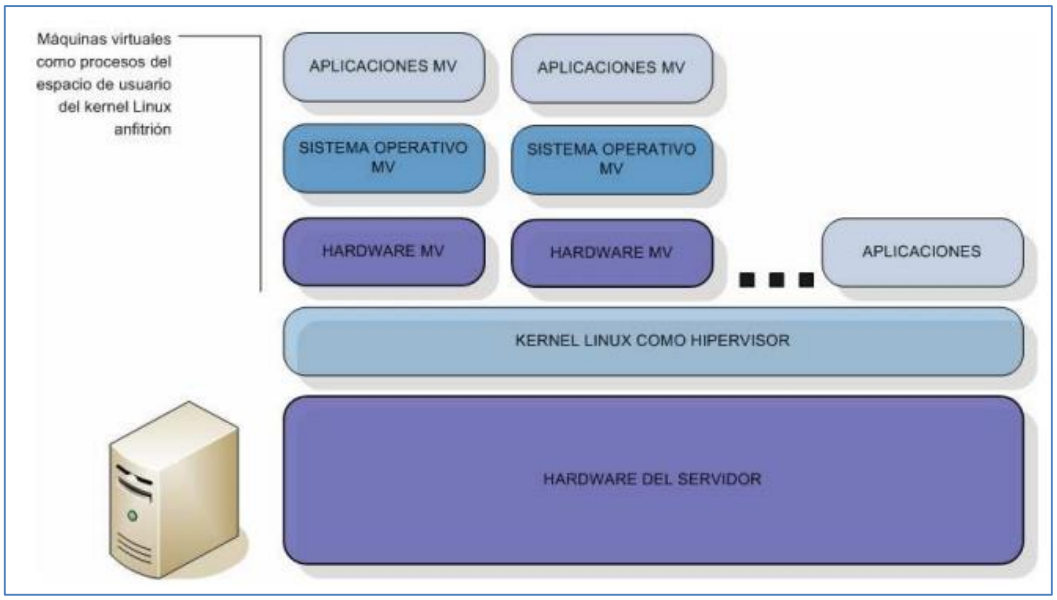


Figura 62. Virtualización de servidores - KVM
Nota. Fuente: Recuperado de http://www.adminso.es/images/6/6d/Eugenio_cap1.pdf

KVM ha sido la primera tecnología de virtualización escogida para formar parte del kernel Linux, por tal razón, en la actualizad se convierte en una de las soluciones más completas que se debe tomar en cuenta a la hora seleccionar un método de virtualización para servidores.

3.3.1.4 Tecnologías de Virtualización

En la Tabla 15 se presenta una comparación de las características y el rendimiento de diversas tecnologías de virtualización para Linux, desarrolladas bajo licencias públicas y propietarias.

Tabla 15. Tecnologías de Virtualización

	Full Virt	Para Virt	Contenedores	Licencia	CPU/ memoria hot plug	Rendimiento	Notas
Xen	x	x	-	GPL	x	Paravirt muy rápido, full Virt medio	full Virt needs VT / AMD-V
KVM	x	x	-	GPL	x	Paravirt muy rápido, full Virt medio	full and Paravirt needs VT / AMD-V,
OpenVZ	-	-	x	GPL	-	Nativo	Migración en vivo
Linux VServer	-	-	x	GPL	-	Nativo	-
Virtual Box	x	-	-	GPL/ Propietaria	-	rápido/muy rápido	kernel GPL
VMware Server	x	-	-	Propietaria	-	medio/rápido	kernel propietario
VMware ESX	x	-	-	Propietaria	-	medio/rápido	-

Nota. Fuente: Recuperado de http://virt.kernelnewbies.org/TechComparison

3.3.1.5 Proxmox VE

Para la implementación del servidor AAA se utilizará la virtualización de servidores mediante la herramienta Proxmox VE 3.0 (Proxmox Virtual Environment).

El entorno virtual Proxmox es una solución completa para la gestión de máquinas virtuales, proyecto de código abierto liberado bajo la licencia pública AGPL[54] versión 3. Está basado en KVM y OpenVZ para la creación de máquinas virtuales, almacenamiento, virtualización de redes y tecnologías de alta disponibilidad (HA clusters).

[54] Affero General Public License

Proxmox provee funciones a nivel corporativo cuya gestión se la realiza mediante una interfaz web, esto permite optimizar el uso de los recursos de hardware logrando virtualizar fácilmente cualquier sistema operativo bajo plataformas Linux o Windows.

3.3.2 SISTEMA OPERATIVO BASE

GNU/Linux es un sistema operativo libre que ha logrado convertirse en una solución muy potente a la hora de montar un servidor por todas las características y ventajas que tiene. Principalmente cuando se trata de instalaciones sobre infraestructuras de gran tamaño, donde la gran cantidad de usuarios, hace que la implementación de una solución con software privado resulte poco viable debido a su elevado costo de licenciamiento.

Existen varias distribuciones GNU/Linux que se pueden obtener libremente a través de Internet, las cuales contienen todo lo necesario para instalar un sistema Linux bastante completo.

Tabla 16. Requerimientos mínimos GNU/Linux

	DEBIAN 7.0	Ubuntu Server 12.04 TLS	CentOS 6.4	openSUSE 12.3
Arquitecturas Soportadas	Intel i386 amd64 Intel 64	Intel i386 amd64 Intel 64	Intel i386 amd64 Intel 64	Intel i386 amd64 Intel 64
RAM	64 – 256 MB	128 – 256 MB	392 MB	512 MB
Disco duro	1 GB	1 GB	2 GB	3 GB
Versión Kernel Linux	3.2	3.5	2.6.32	3.1.0

Nota. Fuente: Recuperado de las páginas oficiales del software

3.3.3 FreeRADIUS

FreeRADIUS es la base de múltiples productos comerciales, siendo este el más utilizado por las organizaciones en la implementación de servidores AAA.

La principal razón para elegir FreeRADIUS como servidor de autenticación en la red del GAD municipal San Miguel de Urcuqui es su calidad relacionada con su coste, FreeRADIUS es un proyecto de código abierto soportado por múltiples plataformas que por su rendimiento se convierte en uno de los más versátiles del mercado, inclusive comparándolo con los de pago. Además numerosas empresas fabricantes de equipos de comunicaciones incluyen el soporte en sus dispositivos.

FreeRADIUS es un paquete estándar soportado por múltiples sistemas operativos, permite realizar instalaciones a gran escala empleando múltiples servidores AAA. Soporta conexiones con varios tipos de bases de datos, tanto para la autorización como para la contabilidad, es compatible con una gran cantidad de métodos de autenticación que en conjunto forman un sistema AAA muy robusto y confiable.

3.3.3.1 Eap-ttls

El servidor FreeRADIUS soporta el método de autenticación EAP-TTLS requerido en el diseño del servicio AAA, el cual ofrece varias ventajas técnicas que garantizan un nivel adecuado de seguridad para el control de acceso a la red de datos del GAD Municipal de San Miguel de Urcuqui.

- EAP-TTLS es un método de autenticación basado en TLS/SSL.
- Todos los datos confidenciales circulan totalmente cifrados.
- No se expone la identidad del usuario.
- La autenticación se realiza solo con certificados de servidor.
- EAP-TTLS tiene la capacidad de soportar una amplia variedad de métodos de autenticación internos.
- EAP-TTLS no es vulnerable a ataques MITM, ni de diccionarios.
- Los usuarios con sistemas operativos Windows (7 o inferiores) requieren la instalación de un suplicante externo.

3.3.4 OPENLDAP

El GAD Municipal San Miguel de Urcuqui no cuenta con un directorio de usuarios para almacenar las credenciales de acceso requeridas en el proceso de autenticación a la red de datos, por lo que se creará un directorio utilizando OpenLDAP.

El esquema del directorio se diseña usando como referencia las unidades departamentales de la institución, se creara un grupo de usuarios por cada VLAN, las contraseñas se establecerán y almacenarán siguiendo las recomendaciones de la política de seguridad para el control de accesos indicadas en el capítulo II.

La estructura del directorio LDAP para el GADMU se debe construir de acuerdo a los niveles jerárquicos mostrados en la Figura 63.

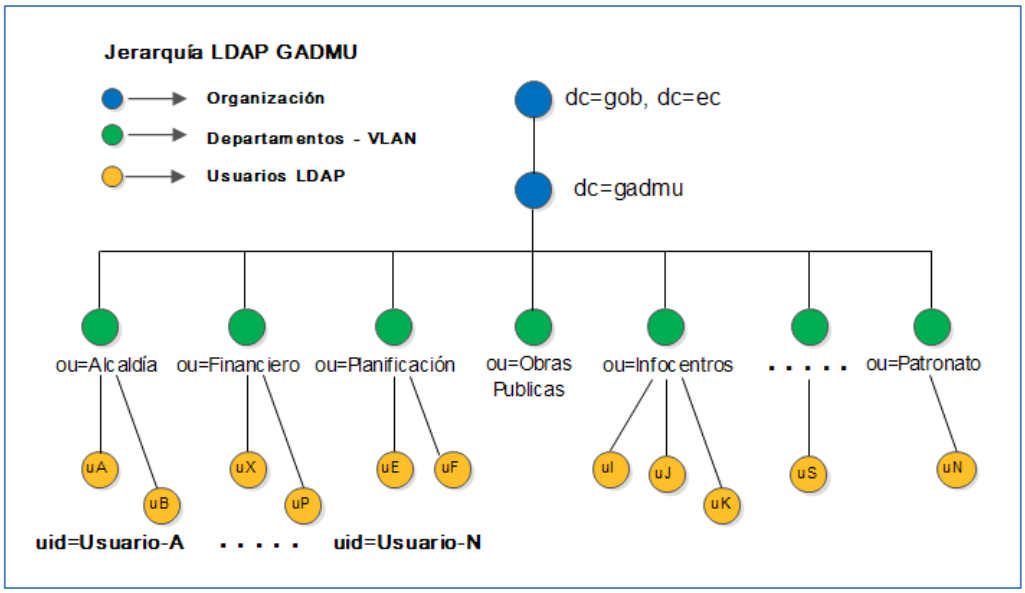


Figura 63. Jerarquía LDAP GADMU

Nota. Fuente: Diseño basado en la Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui. (2013)

Cada usuario de la red del GADMU representa una entrada en el directorio LDAP, compuesta de un conjunto de atributos, los cuales a su vez se definen por el tipo y sus respectivos valores.

Tabla 17. Especificaciones de entrada LDAP

TIPO DE ATRIBUTO	DESCRIPCIÓN	VALOR
cn	Nombre de usuario LDAP	Nombre
objectClass	Define atributos requeridos	Person, uidObject, radiusProfile
sn	Apellido de usuario LDAP	Apellido
uid	**Identificador de usuario AAA**	primera letra del nombre + apellido
radiusTunnelMediumType	Estándar para redes LAN y WLAN	IEEE-802
radiusTunnelType	Tipo de túnel que se inicia	VLAN
radiusTunnelPrivateGroupId	Número de VLAN para el usuario	Identificador de VLAN
userPassword	**Contraseña de acceso al sistema AAA**	Debe cumplir la política de uso de contraseñas (CAPÍTULO II)

Nota. Fuente: Diseño basado en la Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui. (2013)

En la Tabla 17, se definen las especificaciones de los atributos para las entradas con las que se debe construir el directorio LDAP, el campo tipo define la clase de información que se va a almacenar y el campo valor contiene los datos en sí.

El atributo: clase de objeto, define los parámetros requeridos para construir la entrada en el directorio LDAP. La clase persona permite asignar un nombre (cn) y un apellido (sn) al objeto, la clase (uidObject) representa el ID de usuario que se utiliza para autenticarse al sistema AAA, el atributo (userPassword) almacena la contraseña que se deberá guardar usando el formato SHA (Algoritmo de Hash Seguro).

3.3.4.1 Integración con FreeRADIUS

Por defecto OpenLDAP no permite la asignación dinámica de VLANs, se requiere la adición de un esquema con atributos especiales para conseguirlo, mismo que se incluye en los directorios de FreeRADIUS.

El equipo autenticador (switch 802.1x) debe tener el soporte para DVA (Asignación de VLAN Dinámica) a través de un servidor RADIUS.

Para conseguir que un dispositivo se autentique y autorice a un puerto usando la asignación dinámica de VLAN se debe cumplir con el siguiente proceso.

- El servidor FreeRADIUS debe autenticar al usuario y asignarle una VLAN al dispositivo de forma dinámica.

- La VLAN asignada deberá estar creada previamente en el switch, misma que no puede ser la predeterminada.

- Finalmente, el servidor OpenLDAP debe enviar los tres tipos de atributos RADIUS requeridos.

  RadiusTunnelMediumType: IEEE-802

  RadiusTunnelType: VLAN

  RadiusTunnelPrivateGroupId: 2 (Identificador de VLAN)

3.3.4.2 JXplorer

JXplorer es una herramienta de gestión para servidores LDAP basado en código abierto, se puede utilizar para leer, buscar y editar cualquier directorio LDAP.

JXplorer es un cliente LDAP completamente funcional, se puede instalar en cualquier sistema operativo que soporte Java como Windows, Solaris, Linux, OSX, etc. Las funciones de este buscador permiten realizar las siguientes acciones.

- Conectarse a cualquier directorio que soporte LDAP para ejecutar acciones de navegación, búsqueda y modificación
- Leer esquemas del directorio directamente, sin la necesidad de acceder a los archivos de configuración
- Mediante su interfaz gráfica se puede cortar, pegar y editar cualquier ramificación del directorio.
- Importar y exportar archivos LDIF.

- Personalizar la apariencia del explorador.
- Ejecutar sobre una extensa variedad de plataformas con soporte JAVA.
- Establecer comunicaciones seguras mediante SSL/TLS.

3.3.5 MYSQL

MySQL es un sistema de gestión de código abierto para bases de datos relacionales. Los datos se almacenan en tablas separadas con el fin de acceder a la información de manera rápida y flexible.

SQL[55] es uno de los lenguajes de consulta de alto nivel más utilizado, definido en el estándar ASI/ISO SQL.

3.3.5.1 Integración con FreeRADIUS

FreeRADIUS tiene la capacidad de usar MySQL como base de datos para el proceso de autenticación y contabilidad en el servicio AAA, la instalación de FreeRADIUS incluye scripts de configuración que permiten crear automáticamente las tablas para el ingreso de la información.

Para el diseño del servidor AAA del GAD Municipal San Miguel de Urcuqui se usarán las plantillas MySQL para registrar los equipos autenticadores (switch y router inalámbrico) autorizados a brindar acceso a la red de datos de la institución, así como el registro de los datos de contabilidad de las conexiones de usuario efectuadas.

[55] Structured Query Language

3.3.6 OPENSSL

OpenSSL es un proyecto de software libre que permite la implantación de infraestructuras PKI sobre Linux. Es una potente solución criptográfica que provee las herramientas necesarias para el uso de protocolos SSL y TLS con certificados digitales principalmente. En la actualidad existen muchas aplicaciones que se basan en OpenSSL, como Apache, FreeRADIUS, correo electrónico cifrado, etc.

Secure Sockets Layer (SSL) y Transport Layer Security (TLS) son protocolos criptográficos que proporcionan comunicaciones protegidas entre los extremos de una red (internet), esta tecnología ofrece a los usuarios un canal seguro para la transmisión de la información con el fin de evitar la intercepción, robo o falsificación de datos.

Cuando se establece un canal seguro mediante SSL el proceso es transparente para el usuario, por ejemplo, una persona que utiliza un navegador para acceder a una página web protegida mediante SSL, envía sus datos cifrados sin conocer que lo está haciendo debido a que no tiene la necesidad de ejecutar operaciones adicionales.

3.3.6.1 TinyCA

El método de autenticación EAP-TTLS que se utilizará en la red de datos del GAD Municipal San Miguel de Urcuqui necesita de un certificado digital en el servidor FreeRADIUS, para lo cual se requiere una Autoridad Certificadora (CA[56]) que emita y gestione el sistema de certificados que se instalarán en los servidores de la institución.

[56] Autoridad Certificadora es una entidad que emite certificados digitales.

TinyCA ofrece una interfaz gráfica de usuario simple para administrar una pequeña Autoridad Certificadora, funciona como front-end para OpenSSL, con una CA propia se puede crear certificados de servidores y de clientes para cualquier servicio que demande la institución, por ejemplo servidores WEB, correo electrónico, servidores de autenticación, VPN, etc.

La versión actual de TinyCA2 ofrece las siguientes características:

- Posibilidad de crear CAs ilimitadas
- Creación y Revocación de certificados
- Generar certificados digitales de servidor para aplicaciones como: Apache, Postfix, OpenLDAP, Cyrus, OpenVPN, OpenSWAN, FreeRADIUS. Los certificados se pueden exportar como: PEM, DER, TXT y PKCS#12
- Generar certificados digitales de clientes: Netscape, Opera, Internet Explorer, Outlook (Express) y FreeS/WAN. Los certificados se pueden exportar como: PEM, DER, TXT y PKCS#12
- Revocación de certificados en formatos: PEM, DER y TXT
- Soporta varios idiomas: inglés, español, alemán, sueco, francés.

3.3.7 FIREWALL – SHOREWALL

El firewall se diseña usando una topología perimetral con tres zonas de seguridad, ver Figura 59. Los servidores: FreeRADIUS, OpenLDAP y MySQL se instalan en la DMZ, la zona LAN utiliza una interfaz en modo troncal para permitir la comunicación entre las VLANs de la red local y la zona WAN permite el acceso a internet.

- **Arquitectura de zonas**

Una zona identifica el origen o destino de un paquete y se utilizan para definir las reglas de acceso. El sistema AAA requiere de tres zonas bien definidas que se asocian a una interfaz física del firewall, el resto de zonas corresponden a las VLAN, zonas virtuales que se usan en la definición de las reglas de acceso.

```
#ZONA      TIPO DE ZONA     DESCRIPCIÓN

wan        ipv4             # Acceso a internet
dmz        ipv4             # Servidores AAA
fw         firewall         # Servidor Firewall
loc        ipv4             # Autenticadores (switch cisco)
v2         ipv4             # VLAN Alcaldía
v3         ipv4             # VLAN Procuraduría Síndica
v4         ipv4             # VLAN Comisaría
v5         ipv4             # VLAN Dirección de Planificación
v6         ipv4             # VLAN Secretaría General
v7         ipv4             # VLAN Dirección Administrativa
v8         ipv4             # VLAN Dirección Financiera
v9         ipv4             # VLAN Dirección Obras Públicas
v10        ipv4             # VLAN Desarrollo Sostenible
v11        ipv4             # VLAN Des. Social y Comunicación
v12        ipv4             # VLAN Patronato Municipal
v13        ipv4             # VLAN Auditoría
v14        ipv4             # VLAN Biblioteca
v15        ipv4             # VLAN Sistemas
```

- **Interfaces del Firewall**

Se definen las interfaces de red que deben asociarse a las zonas creadas, en el caso de las VLAN no se vinculan con ninguna interfaz física directamente, se debe habilitar interfaces virtuales usando el estándar 802.1q para el manejo de enlaces troncales que permiten la comunicación de redes distintas usando el mismo medio de comunicación físico.

```
#ZONA      INTERFAZ      DESCRIPCIÓN

dmz        eth2          # Interfaz física del firewall
wan        eth1          # Interfaz física del firewall
loc        eth0          # Interfaz física del firewall
v2         eth0.2        # Interfaz virtual 2 en eth0
v3         eth0.3        # Interfaz virtual 3 en eth0
v4         eth0.4        # Interfaz virtual 4 en eth0
v5         eth0.5        # Interfaz virtual 5 en eth0
v6         eth0.6        # Interfaz virtual 6 en eth0
v7         eth0.7        # Interfaz virtual 7 en eth0
v8         eth0.8        # Interfaz virtual 8 en eth0
v9         eth0.9        # Interfaz virtual 9 en eth0
v10        eth0.10       # Interfaz virtual 10 en eth0
```

- **Política por defecto (denegar todo)**

El firewall se debe configurar siguiendo las recomendaciones de la política de seguridad elaborada en el capítulo dos, el cual establece como norma de seguridad que todo tráfico de paquetes entre zonas, por defecto se deniega.

```
#FUENTE    DESTINO    POLÍTICA

dmz        loc        ACCEPT
fw         all        REJECT
dmz        all        REJECT
loc        all        REJECT
wan        all        DROP
all        all        REJECT
```

- **Reglas específicas del firewall**

El objetivo principal de un sistema de seguridad es controlar el tráfico que entra y sale de la red mediante el análisis de paquetes, esto se logra a través de un conjunto de reglas que permiten o deniegan el acceso a servicios, redes y puertos entre las distintas zonas del firewall. Las acciones comúnmente usadas para crear las reglas son: ACCEPT, DROP, REJECT, DNAT, REDIRECT, CONTINUE, LOG, etc.

```
#ACCIÓN    ORIGEN    DESTINO    PROTOCOLO    PUERTO-DESTINO

#Reglas de redirección de puertos: Proxy

REDIRECT        loc        8081       tcp        80
REDIRECT        v2         8081       tcp        80
REDIRECT        v3         8081       tcp        80
REDIRECT        v4         8081       tcp        80
REDIRECT        v5         8081       tcp        80
REDIRECT        v6         8081       tcp        80
REDIRECT        v7         8081       tcp        80
REDIRECT        v8         8081       tcp        80
REDIRECT        v9         8081       tcp        80
REDIRECT        v10        8081       tcp        80
REDIRECT        v11        8081       tcp        80
REDIRECT        v12        8081       tcp        80
REDIRECT        v13        8081       tcp        80
REDIRECT        v14        8081       tcp        80

#Reglas para permitir acceso al servicio VoIP

REJECT     loc        dmz:10.10.10.200     tcp        5060
REJECT     loc        dmz:10.10.10.200     udp        5060
ACCEPT     v2         dmz:10.10.10.200     tcp        5060
ACCEPT     v2         dmz:10.10.10.200     udp        5060
ACCEPT     v3         dmz:10.10.10.200     tcp        5060
ACCEPT     v4         dmz:10.10.10.200     udp        5060
ACCEPT     v5         dmz:10.10.10.200     tcp        5060
ACCEPT     v5         dmz:10.10.10.200     udp        5060
ACCEPT     v6         dmz:10.10.10.200     tcp        5060
ACCEPT     v6         dmz:10.10.10.200     udp        5060
REJECT     v12        dmz:10.10.10.200     tcp        5060
REJECT     v12        dmz:10.10.10.200     udp        5060
REJECT     v13        dmz:10.10.10.200     tcp        5060
REJECT     v13        dmz:10.10.10.200     udp        5060
REJECT     v14        dmz:10.10.10.200     tcp        5060
REJECT     v14        dmz:10.10.10.200     udp        5060
REJECT     v15        dmz:10.10.10.200     tcp        5060
REJECT     v15        dmz:10.10.10.200     udp        5060
ACCEPT     v100       dmz:10.10.10.200     tcp        5060
ACCEPT     v100       dmz:10.10.10.200     udp        5060

#Reglas para acceso a la administración de servidores AAA

ACCEPT     v100    dmz:10.10.10.10         tcp   8006  #Proxmox
ACCEPT     v100    dmz:10.10.10.3          tcp   389   #LDAP
ACCEPT     v100    loc:172.25.1.254        tcp   80    #SW cisco
ACCEPT     v100    loc:172.25.1.253        tcp   8080  #AP
```

#Reglas para denegar acceso a Facebook por puerto seguro

```
ACCEPT     v100            wan:$IP_FACEBOOK     tcp        443
REJECT     loc             wan:$IP_FACEBOOK     tcp        443
ACCEPT     v2:172.25.2.4   wan:$IP_FACEBOOK     tcp        443
REJECT     v2              wan:$IP_FACEBOOK     tcp        443
REJECT     v3              wan:$IP_FACEBOOK     tcp        443
REJECT     v4              wan:$IP_FACEBOOK     tcp        443
ACCEPT     v5:172.25.5.4   wan:$IP_FACEBOOK     tcp        443
REJECT     v5              wan:$IP_FACEBOOK     tcp        443
REJECT     v6              wan:$IP_FACEBOOK     tcp        443
ACCEPT     v7:172.25.7.4   wan:$IP_FACEBOOK     tcp        443
REJECT     v7              wan:$IP_FACEBOOK     tcp        443
ACCEPT     v8:172.25.8.4   wan:$IP_FACEBOOK     tcp        443
REJECT     v8              wan:$IP_FACEBOOK     tcp        443
ACCEPT     v9:172.25.9.4   wan:$IP_FACEBOOK     tcp        443
REJECT     v9              wan:$IP_FACEBOOK     tcp        443
REJECT     v10             wan:$IP_FACEBOOK     tcp        443
REJECT     v10             wan:$IP_FACEBOOK     tcp        443
REJECT     v11             wan:$IP_FACEBOOK     tcp        443
REJECT     v12             wan:$IP_FACEBOOK     tcp        443
REJECT     v13             wan:$IP_FACEBOOK     tcp        443
REJECT     v14             wan:$IP_FACEBOOK     tcp        443
REJECT     v15             wan:$IP_FACEBOOK     tcp        443
```

 # Acceso a Internet

```
ACCEPT          fw          wan         tcp         80,53,443
ACCEPT          fw          wan         udp         53
ACCEPT          loc         wan         tcp         80,53,443
ACCEPT          loc         wan         udp         53
ACCEPT          v2          wan         tcp         80,53,443
ACCEPT          v2          wan         udp         53
ACCEPT          v3          wan         tcp         80,53,443
ACCEPT          v3          wan         udp         53
ACCEPT          v4          wan         tcp         80,53,443
ACCEPT          v4          wan         udp         53
ACCEPT          v5          wan         tcp         80,53,443
ACCEPT          v5          wan         udp         53
ACCEPT          v6          wan         tcp         80,53,443
ACCEPT          v6          wan         udp         53
ACCEPT          v7          wan         tcp         80,53,443
ACCEPT          v7          wan         udp         53
ACCEPT          v8          wan         tcp         80,53,443
ACCEPT          v8          wan         udp         53
ACCEPT          v9          wan         tcp         80,53,443
ACCEPT          v9          wan         udp         53
ACCEPT          v10         wan         tcp         80,53,443
ACCEPT          v10         wan         udp         53
ACCEPT          v12         wan         tcp         80,53,443
ACCEPT          v12         wan         udp         53
ACCEPT          v13         wan         tcp         80,53,443
ACCEPT          v13         wan         udp         53
```

```
ACCEPT          v14         wan         tcp         80,53,443
ACCEPT          v14         wan         udp         53
REJECT          v15         wan         tcp         80,53,443
ACCEPT          v15         wan         udp         53
ACCEPT          v100        wan         tcp         80,53,443
ACCEPT          v100        wan         udp         53
```

#Reglas de conectividad

```
ACCEPT          fw          wan                     icmp
ACCEPT          loc         wan                     icmp
ACCEPT          v15         dmz:10.10.10.2          icmp
ACCEPT          v15         dmz:10.10.10.3          icmp
ACCEPT          v15         dmz:10.10.10.4          icmp
ACCEPT          v15         dmz:10.10.10.5          icmp
```

#Reglas para permitir el servicio AAA

```
ACCEPT          loc         dmz         udp         1812,1813
```

La regla que no debe faltar en el firewall para que el servicio AAA funcione correctamente, es aceptar los paquetes que llegan de la red local (usuarios que intentan autenticarse) hacia la zona dmz (servidor de autenticación) por el protocolo UDP a los puertos de autenticación y contabilidad 1812 y 1813 respectivamente.

3.3.8 PROXY

Los usuarios que han logrado autenticarse correctamente al sistema, son redireccionados a una sub red virtual (VLAN) de acuerdo a las políticas establecidas y las funciones que desempeña el trabajador en la institución, esto implica que el sistema debe ser capaz de asignarle una dirección IP al dispositivo de manera automática mediante DHCP.

El servidor proxy debe funcionar en modo transparente debido a que los usuarios una vez autenticados establecerán conexiones con distintas subredes, esto hará que la tarjeta de red de los dispositivos se configure dinámicamente con una puerta de enlace diferente.

- **Servidor Proxy**

 # Definición de VLAN

```
acl     sinproxy      src        "/etc/squid3/ipsinproxy"
acl     loc           src        172.25.1.0/24
acl     vlan2         src        172.25.2.0/24
acl     vlan3         src        172.25.3.0/24
acl     vlan4         src        172.25.4.0/24
acl     vlan5         src        172.25.5.0/24
acl     vlan6         src        172.25.6.0/24
acl     vlan7         src        172.25.7.0/24
acl     vlan8         src        172.25.8.0/24
acl     vlan9         src        172.25.9.0/24
acl     vlan10        src        172.25.10.0/24
acl     vlan11        src        172.25.11.0/24
acl     vlan12        src        172.25.12.0/24
…
```

 # Definición de reglas: horario, palabras y dominios

```
acl   horario-am      time       MTWHF   08:00-12:00
acl   horario-pm      time       MTWHF   13:00-20:05
acl   palabras-nopermitidas url_regex       "/etc$
acl   dominios-nopermitidos dstdomain       "/etc$
```

 # Permitir o denegar el acceso

```
http_access           allow      localhost
http_access           allow      sinproxy
http_access           deny       palabras-nopermitidas
http_access           deny       dominios-nopermitidos
http_access           allow      loc
http_access           allow      vlan2
http_access           allow      vlan3
http_access           allow      vlan4
http_access           allow      vlan5
http_access           allow      vlan6
http_access           allow      vlan7
http_access           allow      vlan8
http_access           allow      vlan9
http_access           allow      vlan10
http_access           allow      vlan11
…
http_access           deny       all
```

 # Proxy transparente

```
http_port http_port 8081 transparent
```

- **Servidor DHCP de múltiples VLAN**

```
subnet 172.25.14.0  netmask 255.255.255.0
{
range 172.25.14.10 172.25.14.20 ;
option routers 172.25.14.1;
option domain-name-servers 8.8.8.8;
option subnet-mask 255.255.255.0;
option broadcast-address 172.25.14.255;
default-lease-time 600;
max-lease-time 7200;
}

subnet 172.25.15.0  netmask 255.255.255.0
{
range 172.25.15.10 172.25.15.20 ;
option routers 172.25.15.1;
option domain-name-servers 8.8.8.8;
option subnet-mask 255.255.255.0;
option broadcast-address 172.25.15.255;
default-lease-time 600;
max-lease-time 7200;
}

subnet 172.25.100.0  netmask 255.255.255.0
{
range 172.25.100.10 172.25.100.20 ;
option routers 172.25.100.1;
option domain-name-servers 8.8.8.8;
option subnet-mask 255.255.255.0;
option broadcast-address 172.25.100.255;
default-lease-time 600;
max-lease-time 7200;
}

deny unknown-clients;
host usuario-admin {hardware ethernet
00:16:76:D7:47:3F;fixed-address 172.25.100.10;}
```

CAPÍTULO IV

IMPLEMENTACIÓN DEL SERVIDOR AAA Y PRUEBAS DE FUNCIONAMIENTO

4.1 TOPOLOGÍA DE RED UTILIZADA

En base al esquema actual de la red del GAD Municipal San Miguel de Urcuqui, se implementa el servicio AAA en un escenario (ver Figura 64) con equipos de similares características e iguales funcionalidades con la finalidad de garantizar que la solución es factible implementarla en la red de datos de la institución.

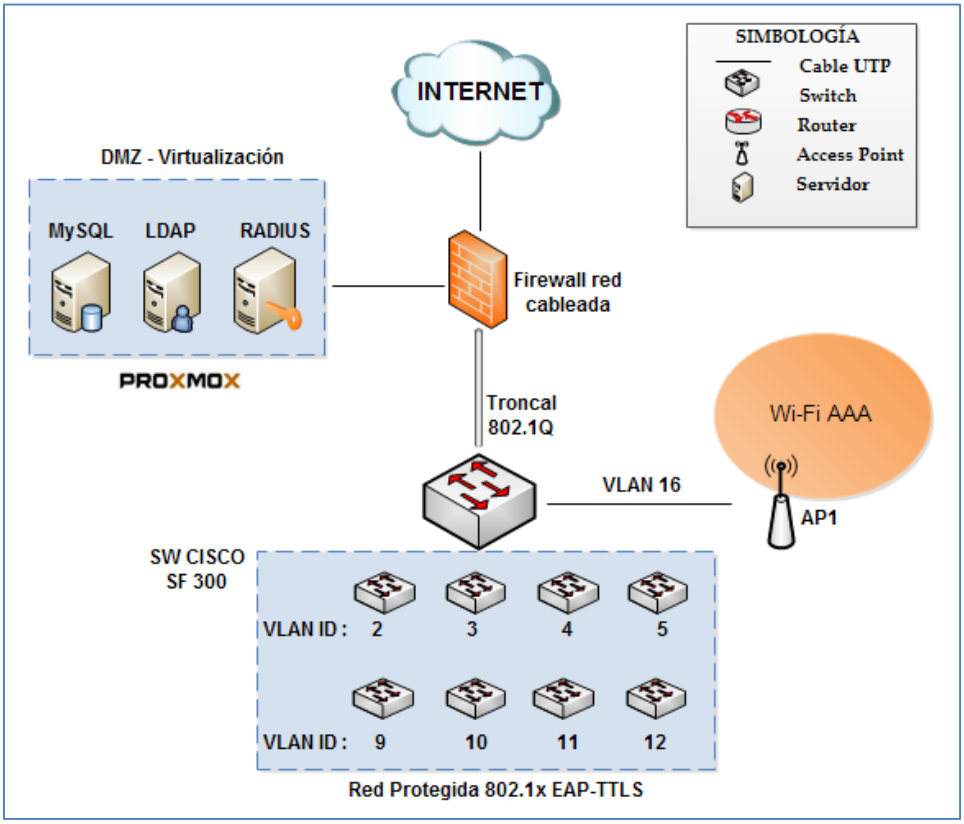


Figura 64. Esquema de red con servicio AAA
Nota. Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui. (2013).

4.2 DIRECCIONAMIENTO IP DE LA RED

El esquema de direccionamiento IP utilizado para la configuración de equipos y redes del sistema AAA se muestra en las Tablas 17, 18 y 19.

Tabla 18. Direccionamiento IP general del Firewall Principal

ZONA	DESCRIPCIÓN	SUBRED	MÁSCARA	INTERFAZ
Red Externa	Acceso a Internet	192.168.8.X	/24	eth1
DMZ	Servidores	10.10.10.1	/24	eth2
Red Interna	Departamentos (VLANs)	172.25.X.X	/24	eth0

Nota. Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui. (2013).

Tabla 19. Direccionamiento IP DMZ (Servidor AAA)

Servidor	DESCRIPCIÓN	DIR. IP	MÁSCARA	GATEWAY	INTERFAZ
FreeRADIUS	Servidor de Autenticación	10.10.10.2	/24	10.10.10.1	eth2
OpenLDAP	Servidor de Autorización	10.10.10.3	/24	10.10.10.1	eth2
MySQL	Servidor de Contabilidad	10.10.10.4	/24	10.10.10.1	eth2

Nota. Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui. (2013).

Tabla 20. Direccionamiento IP de la red Interna (VLANs)

VLAN ID	NOMBRE DE VLAN	INTERFAZ	DIRECCIÓN IP	MÁSCARA
2	ALCALDÍA	eth0.2	172.25.2.1	/24
3	PROCURADURÍA	eth0.3	172.25.3.1	/24
4	COMISARIA	eth0.4	172.25.4.1	/24
5	PLANIFICACIÓN	eth0.5	172.25.5.1	/24

6	SECRETARÍA GENERAL	eth0.6	172.25.6.1	/24
7	ADMINISTRATIVO	eth0.7	172.25.7.1	/24
8	FINANCIERO	eth0.8	172.25.8.1	/24
9	OBRASPÚBLICAS	eth0.9	172.25.9.1	/24
10	DESARROLLO SOSTENIBLE	eth0.10	172.25.10.1	/24
11	DESARROLLO SOCIAL	eth0.11	172.25.11.1	/24
12	PATRONATO	eth0.12	172.25.12.1	/24
13	AUDITORIA	eth0.13	172.25.13.1	/24
14	BIBLIOTECA	eth0.14	172.25.14.1	/24
15	INFOCENTROS	eth0.15	172.25.15.1	/24
16	Wi-Fi	eth0.16	172.25.16.1	/24

Nota. Fuente: Infraestructura actual de red del GAD Municipal de San Miguel de Urcuqui. (2013).

4.3 SERVIDOR AAA

El servicio AAA requiere la instalación de tres servidores: FreeRADIUS para el servicio de autenticación EAP-TTLS, OpenLDAP como directorio de almacenamiento de credenciales de usuario y la base de datos MySQL para el registro de clientes NAS de RADIUS, así como el servicio de Acconunting.

Para optimizar el uso de hardware se utiliza la tecnología de virtualización Proxmox VE 3.0, específicamente a través de contenedores virtuales, una de las soluciones de mejor rendimiento para servidores Linux.

4.3.1 PROXMOX VE

La tecnología de contenedores virtuales usa imágenes precargadas para instalar sistemas operativos Linux de forma eficiente, el procedimiento para crear una máquina virtual en Proxmox VE 3.0 empleando OpenVZ (contenedor virtual) se detalla en el Anexo A.

La asignación de recursos de hardware para los contenedores OpenVZ de los servidores AAA se muestra en la Tabla 20.

Tabla 21. Recursos virtuales servidor AAA

PARÁMETROS	FREERADIUS	OPENLDAP	MYSQL
procesadores	1	1	1
disco duro	6 GB	6 GB	6 GB
hostname	freeradius	openldap	mysqlserver
memoria	512 MB	512 MB	512 MB
Nodo	proxmox-aaa	proxmox-aaa	proxmox-aaa
plantilla	Ubuntu 12.04	Ubuntu 12.04	Ubuntu 12.04
swap	512 MB	512 MB	512 MB
vmid	200	210	220

Nota. Fuente: Obtenido de la interfaz gráfica del servidor virtual PROXMOX VE 3.0

4.3.2 CERTIFICADOS DIGITALES CON TINYCA2

Usando TinyCA2 se crea la autoridad certificadora raíz para el GAD Municipal San Miguel de Urcuqui, con la finalidad de emitir y gestionar todo el sistema de certificados que se requieran en los servidores de la institución.

4.3.2.1 Autoridad certificadora raíz gadmu-CA

El certificado raíz gadmu-CA se instala en el repositorio de certificados de confianza de todos los clientes EAP-TTLS, esto permite al suplicante verificar que el servidor al que se está autenticando es el verdadero, evitando de esta manera que las claves de acceso se expongan fácilmente ante cualquier persona.

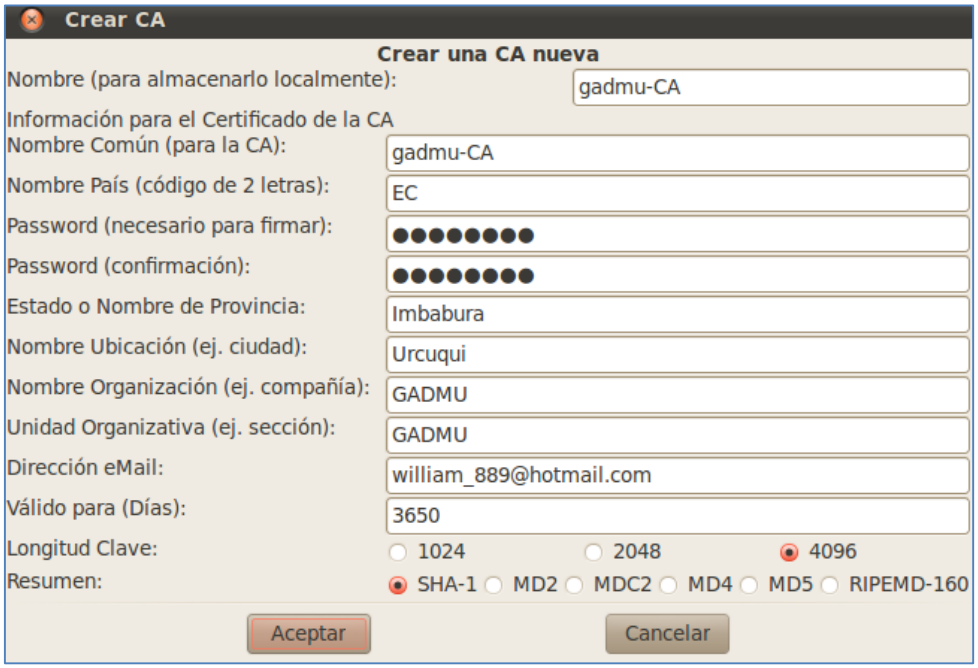


Figura 65. Creación de la Autoridad Certificadora Raíz
Nota. Fuente: Captura de la interfaz gráfica TinyCA2.

El procedimiento requerido para copiar la clave pública del certificado gadmu-CA en el almacén de entidades raíz de confianza de un equipo con Windows 7 se detalla en el Anexo B. Una vez creada la autoridad certificadora raíz se puede emitir certificados de todo tipo, específicamente los de servidor, requeridos en el proceso de autenticación EAP-TTLS de FreeRADIUS.

4.3.2.2 Certificado servidor FreeRADIUS

Solicitar a la autoridad certificadora un nuevo certificado para el servidor FreeRADIUS, para lo cual se requiere generar una solicitud de certificado (CSR) y proceder a firmarlo definitivamente.

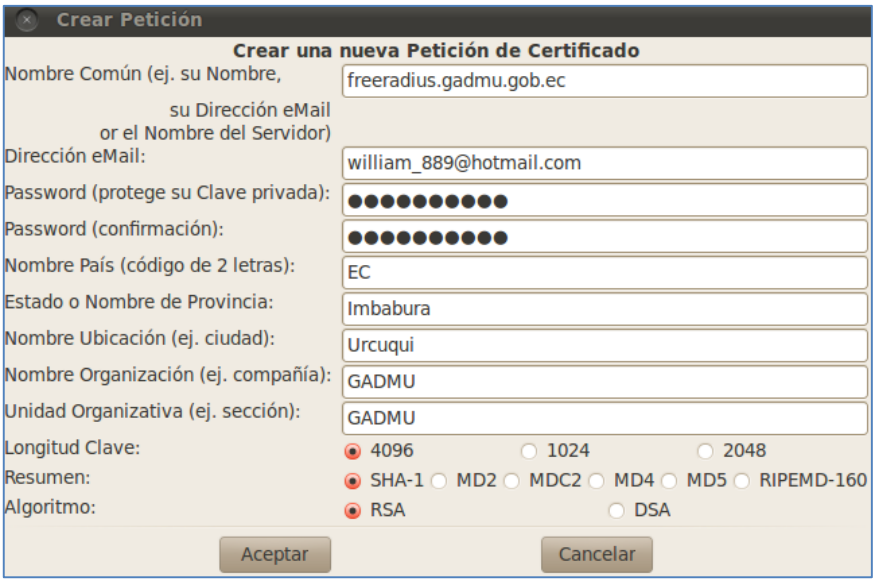


Figura 66. Solicitud de certificado para el servidor freeradius.
Nota. Fuente: Captura de la interfaz gráfica TinyCA2.

Para que el certificado del servidor FreeRADIUS sea firmado por la Autoridad Certificadora del GADMU se debe ingresar la contraseña de la CA y el tiempo de validez en días.

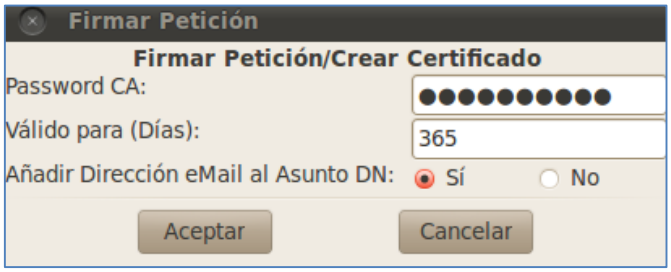


Figura 67. Firma de nuevo certificado digital.
Nota. Fuente: Captura de la interfaz gráfica TinyCA2.

Una vez creada la CA y el certificado del servidor FreeRADIUS, se los debe exportar en un formato adecuado para que sean reconocidos por los sistemas operativos del cliente y servidor, el formato .DER se utiliza para los clientes Windows y el formato .PEM para los servidores Linux.

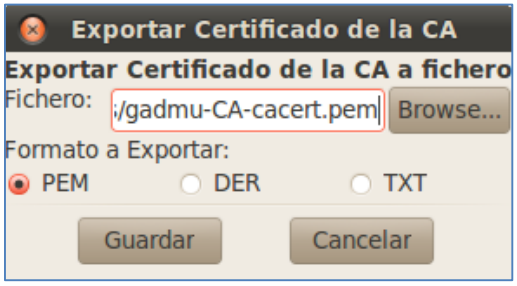


Figura 68. Exportar certificado digital en formato PEM.
Nota. Fuente: Captura de la interfaz gráfica TinyCA2.

Al final, se deben obtener los siguientes archivos:

- freeradius-keycert.der: Certificado y clave privada de freeradius (Windows).
- freeradius-keycert.pem: Certificado y clave privada de freeradius (Linux).
- gadmu-CA-cacert.der: Certificado raíz de la CA en codificación DER.
- gadmu-CA-cacert.pem: Certificado raíz de la CA en codificación PEM.

4.3.3 SERVIDOR FREERADIUS

El servidor FreeRADIUS y sus dependencias se pueden descargar directamente desde los repositorios mediante el comando mostrado en la Figura 69. Una de las grandes ventajas que representa utilizar Ubuntu Server 12.04 como sistema operativo base es el manejo de un repositorio actualizado, esto agiliza el proceso de instalación de cualquier software y sus dependencias.

4.3.3.1 Instalación

En el caso de Freeradius, la instalación por defecto desde los repositorios, incluye el soporte para métodos de autenticación EAP (TLS, PEAP, TTLS) y el manejo de certificados digitales a través OpenSSL.

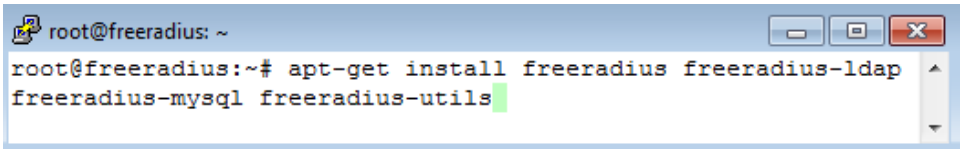


Figura 69. Instalación del servidor freeradius en Ubuntu Server 12.04 LTS
Nota. Fuente: Captura de consola puTTY.

Posterior a la instalación se obtienen varios archivos de configuración (ver Figura 70) usados para personalizar el servidor FreeRADIUS de acuerdo a los requerimientos establecidos para el servidor AAA de la red de datos de GAD Municipal San Miguel de Urcuqui.

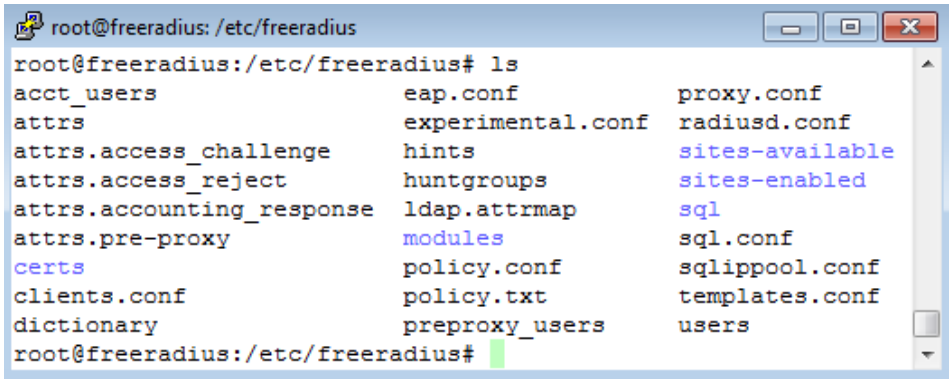


Figura 70. Archivos de configuración de freeradius 2.1.10
Nota. Fuente: Captura de consola puTTY.

Una vez instalado el servidor, se debe ejecutar el script de freeradius (start, stop, restart) con el fin de verificar que no existen errores al arrancar el servicio, el script se encuentra en el directorio /etc/init.d/ que incluye por defecto los archivos de arranque de todos los servicios del sistema.

En la etapa de pruebas se recomienda iniciar freeradius en modo debug (depuración) con el fin de observar el proceso de arranque de cada uno de los módulos de autenticación, autorización y contabilidad, esto se lo hace mediante el comando freeradius –X.

4.3.3.2 Eap-ttls

En el archivo /etc/freeradius/eap.conf se debe habilitar EAP-TTLS como método de autenticación por defecto para el sistema AAA, dentro del túnel TTLS se puede usar cualquier tipo de autenticación, los desarrolladores de FreeRADIUS recomiendan usar MD5.

```
eap {
        default_eap_type = ttls
        timer_expire     = 60
        ignore_unknown_eap_types = yes
        cisco_accounting_username_bug = no
        max_sessions = 4096

        ttls {
                default_eap_type = md5
                copy_request_to_tunnel = no
                use_tunneled_reply = no
        }
}
```

Figura 71. EAP-TTLS método de autenticación por defecto.
Nota. Fuente: Captura de consola puTTY, fragmento de archivo eap.conf

Cuando el servidor arranca por primera vez genera certificados de prueba que simplifican la instalación de freeradius, especialmente cuando se trabaja con métodos de autenticación EAP-TLS, TTLS o PEAP. No se recomienda usarlos en entornos de producción, esto representaría una vulnerabilidad para el sistema AAA.

Para que FreeRADIUS trabaje con certificados propios generados mediante la herramienta TinyCA2, se los debe almacenar en cualquier directorio del servidor e indicar a freeradius la ruta para que los pueda encontrar.

- Copiar archivos y directorios de forma remota en Linux a través de SSH.

```
root@freeradius:~# scp -r certificados@10.10.10.69:/home/
certificados/certificados/ /etc/freeradius/certs/
certificados@10.10.10.69's password:
gadmu-CA-cacert.pem     100% 2520     2.5KB/s   00:00
gadmu-CA-cacert.der     100% 1821     1.8KB/s   00:00
freeradius-keycert.der 100% 1831     1.8KB/s   00:00
freeradius-keycert.pem 100% 5997     5.9KB/s   00:00
root@freeradius:~#
```

Figura 72. Copia de certificados digitales (CA y servidor freeradius).
Nota. Fuente: Captura de consola puTTY.

- Generar los ficheros random y dh (deffie-helman) utilizados para el establecimiento de las sesiones TLS y la encriptación.

  Comando para generar fichero "random" *#dd if=/dev/urandom of=random count=2*

  Comando para generar fichero "dh" *#openssl dhparam –out dh 1024*

- Finalmente, en el archivo eap.conf se establece la ruta de acceso a los certificados digitales de la Autoridad certificadora y el servidor FreeRADIUS.

```
tls {
        certdir = /etc/freeradius/certs
        cadir = /etc/freeradius/certs
        private_key_password = freeradius
        private_key_file = ${certdir}/freeradius-keycert.pem
        certificate_file = ${certdir}/freeradius-keycert.pem
        CA_file = ${cadir}/gadmu-CA-cacert.pem
        dh_file = ${certdir}/dh
        random_file = ${certdir}/random
        cipher_list = "DEFAULT"
```

Figura 73. Configuración de las rutas de acceso a los certificados.
Nota. Fuente: Captura de consola puTTY, fragmento de archivo eap.conf

4.3.3.3 Integración con LDAP

En el archivo /etc/freeradius/modules/ldap se configura la dirección IP del servidor LDAP y los parámetros de autenticación de un usuario habilitado, a través del cual se accederá al directorio para realizar las consultas y verificación de las credenciales de usuarios.

```
ldap {
      server = "10.10.10.3"
      identity = "cn=admin,dc=gadmu,dc=gob,dc=ec"
      password = adminldap
      basedn = "dc=gadmu,dc=gob,dc=ec"
      filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
      base_filter = "(objectclass=radiusprofile)"
      ldap_connections_number = 5
      timeout = 4
      timelimit = 3
      net_timeout = 1
      }
```

Figura 74. Integración del servidor LDAP con freeradius.
Nota. Fuente: Captura de consola puTTY, fragmento de archivo ldap

Para que el servidor freeradius realice la autenticación y autorización de usuarios mediante el directorio LDAP externo se debe habilitar algunas opciones en los archivos de configuración (default e inner-tunnel) ubicados en /etc/freeradius/sites-available/, como se muestra en la Figura 75.

```
authorize {

        #  The ldap module will set Auth-Type to LDAP if it has not
        #  already been set
        ldap
}

authenticate {

        # Uncomment it if you want to use ldap for authentication
        #
        # Note that this means "check plain-text password against
        # the ldap database", which means that EAP won't work,
        # as it does not supply a plain-text password.
        Auth-Type LDAP {
                ldap
        }
```

Figura 75. Habilitar LDAP en los procesos de Autenticación y Autorización.
Nota. Fuente: Captura de consola puTTY, fragmento de archivo default

4.3.3.4 Integración con MySQL

Para usar la base de datos MySQL con FreeRADIUS se debe modificar algunos parámetros.

- Incluir el módulo SQL en el archivo de configuración principal de freeradius ubicado en /etc/freeradius/radiusd.conf

  $INCLUDE sql.conf

- En el archivo /etc/freeradius/sql.conf indicar el tipo de base de datos empleada, la dirección IP del servidor, las credenciales de acceso y el nombre de la base de datos RADIUS.

```
sql {
      database = "mysql"
      driver = "rlm_sql_${database}"
      # Connection info:
      server = "10.10.10.4"
      login = "radius"
      password = "mysqlsecret2"
      radius_db = "radius"
```

Figura 76. Integrar base de datos MySQL a freeradius.
Nota. Fuente: Captura de consola puTTY, fragmento de archivo sql.conf

- La opción “readclients” del archivo de configuración sql.conf permite a freeradius identificar los clientes registrados en la base de datos MySQL (tabla “nas”) al iniciar el servicio radius, por razones de seguridad no es posible agregar nuevos autenticadores mientras el servidor RADIUS se encuentra operando.

```
# Set to 'yes' to read radius clients from the database ('nas' table)
# Clients will ONLY be read on server startup.  For performance
# and security reasons, finding clients via SQL queries CANNOT
# be done "live" while the server is running.
#
readclients = yes
# Table to keep radius client info
nas_table = "nas"
```

Figura 77. Identificación de clientes radius desde base de datos MySQL.
Nota. Fuente: Captura de consola puTTY, fragmento de archivo sql.conf

- Por último, se debe indicar a FreeRADIUS en qué etapas del proceso AAA se debe conectar a MySQL para realizar consultas o registrar los datos de autenticación de los usuarios. Las modificaciones se realizan en el archivo de configuración /etc/freeradius/sites-enabled/default.

```
authorize {
        sql
}
accounting {
        #  See "Accounting queries" in sql.conf
        sql
}
session {
        radutmp
        sql
}
post-auth {
        Post-Auth-Type REJECT {
                sql
                attr_filter.access_reject
        }
}
```

Figura 78. Integración de SQL en el proceso de Accounting
Nota. Fuente: Captura de consola puTTY, fragmento de archivo default

4.3.4 SERVIDOR OPENLDAP

Acceder al contenedor virtual mediante una conexión SSH e instalar el servidor LDAP, además del paquete ldap-utils que incluye herramientas básicas para la administración del servidor.

4.3.4.1 Instalación

Para instalar OpenLDAP en distribuciones basadas en debían, como Ubuntu Server 12.04 LTS se usa el siguiente comando: # sudo apt-get install slapd ldap-utils, durante el proceso de configuración del servidor se establece la contraseña para el usuario administrador del directorio LDAP (por defecto: admin), ver Figura 79.

Figura 79. Solicitud de contraseña para el usuario admin de LDAP.
Nota. Fuente: Captura de consola puTTY, instalación del servidor LDAP

Posterior a la instalación se obtiene una configuración base lista para trabajar sobre ella, no es recomendable modificar la base de datos directamente sobre los archivos de configuración, cualquier cambio se lo debe realizar a través de las utilidades de LDAP (comandos) o empleando algún gestor gráfico, por ejemplo JXplorer.

4.3.4.2 Añadir esquema radius

Debido al uso de VLANs en el diseño de red es necesario añadir un esquema al servidor LDAP para permitir la configuración de atributos adicionales que se requieren en el proceso de autorización.

El esquema se lo puede obtener a través de internet o directamente del servidor FreeRADIUS que lo incluye por defecto en la instalación, para lo cual se accede al archivo

ubicado en /usr/share/doc/freeradius/examples/openldap.schema y se copia en el directorio /etc/ldap/schema/ del servidor OpenLDAP.

Para añadir el nuevo esquema al directorio se debe transformar el archivo openldap.schema a uno con formato LDIF, para conseguirlo se recomienda usar el siguiente proceso.

- Crear un archivo temporal (/tmp/schema.conf) donde se indique la ubicación del esquema radius que se va a incluir (include /etc/ldap/schema/radius.schema).

- Crear un directorio temporal mediante el comando #mkdir /tmp/out, que almacene toda la estructura de ficheros LDIF generados a partir del esquema radius, el comando usado para la conversión es: #slaptest -f /tmp/schema.conf -F /tmp/out/

- Como resultado se obtiene el esquema radius en formato ldif, el cual requiere un par de modificaciones en sus líneas para evitar posibles errores al momento de agregarlo al directorio. En las Figuras 80 y 81 se muestra específicamente los cambios que se deben realizar.

```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 25778d76
dn: cn={0}radius
objectClass: olcSchemaConfig
cn: {0}radius
```

Figura 80. Configuración original del archivo radius.ldif
Nota. Fuente: Captura de consola puTTY, fragmento de archivo cn\=\{0\}radius.ldif

```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 25778d76
dn: cn=radius,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: radius
```

Figura 81. Nueva configuración del archivo radius.ldif
Nota. Fuente: Captura de consola puTTY, fragmento de archivo cn\=\{0\}radius.ldif

Finalmente, una vez realizados los cambios indicados se añade el esquema al directorio principal LDAP usando el comando: ldapadd -Q -Y EXTERNAL -H ldapi:/// -f /tmp/out/cn\=config/cn\=schema/cn\=\{0\}radius.ldif

Para verificar que el esquema radius se agregó correctamente al directorio se puede usar el comando: ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config dn; o directamente con el gestor JXplorer mediante su interfaz gráfica, como se muestra en la Figura 82.

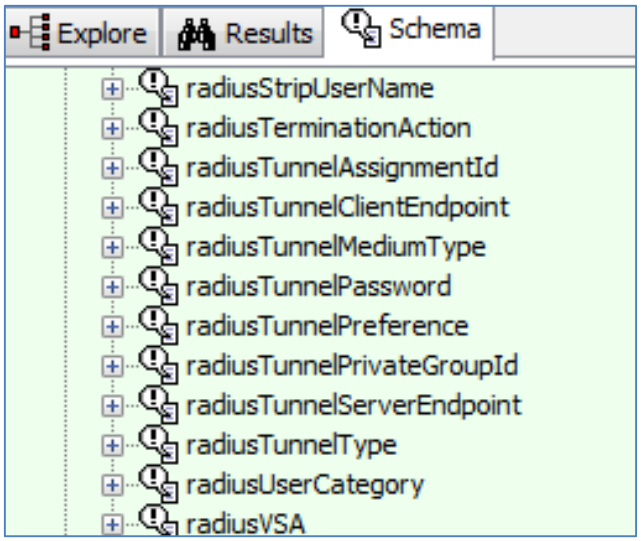


Figura 82. JXplorer esquema con atributos radius
Nota. Fuente: Captura de interfaz gráfica JXplorer

4.3.4.3 JXplorer

Para la gestión y administración de las cuentas de usuario del servicio AAA se usará JXplorer, un buscador y editor de código abierto para plataformas LDAP. El directorio completo se construye tomando como referencia la estructura diseñada en el capítulo 3, ver Figura 63.

Para establecer una conexión con el directorio OpenLDAP usando JXplorer, se debe usar el nombre de usuario (admin) y la contraseña del administrador LDAP configurada durante el proceso de instalación del servidor como se muestra en la Figura 83.

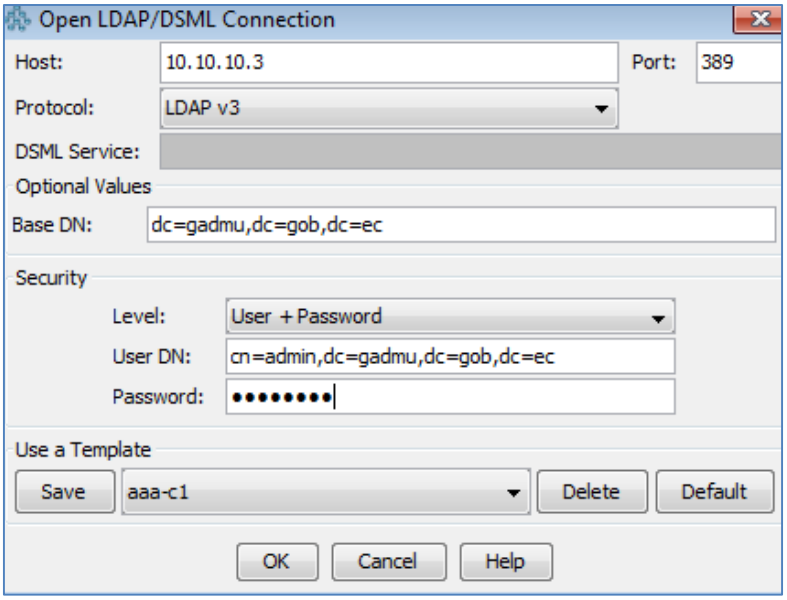


Figura 83. Conexión con Openldap usando JXplorer
Nota. Fuente: Captura de interfaz gráfica JXplorer

Por cada departamento del GAD Municipal San Miguel de Urcuqui se crea una unidad organizativa y los usuarios se agregan de acuerdo al rol que desempeñen dentro de la institución. En la Figura 84 se muestra la estructura completa del directorio LDAP una vez creada.

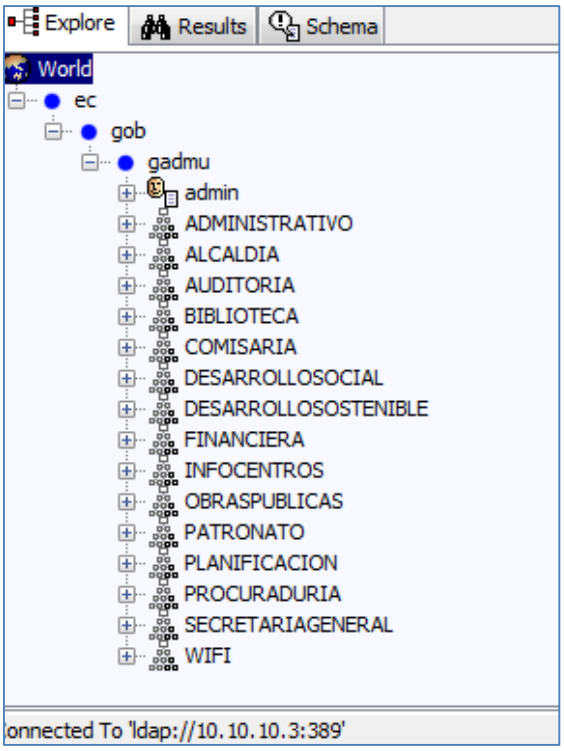


Figura 84. Directorio LDAP del GADMU
Nota. Fuente: Captura de interfaz gráfica JXplorer

4.3.5 SERVIDOR MYSQL

Para la instalación de la base de datos MySQL se descarga el paquete lamp-server, una combinación de software basada en código abierto que incluye: el servidor HTTP apache, la base de datos MySQL y algunos componentes extras que se requieren para construir la base de datos que se usará en el proceso de contabilidad del servicio AAA.

- En primer lugar, se accede a la consola del servidor creado mediante Proxmox VE usando la dirección IP 10.10.10.4/24 y se instalan los paquetes mediante el comando: tasksel install lamp-server

- El proceso de instalación es automático, no requiere de configuraciones complejas. El servidor simplemente solicita una contraseña para el usuario root de MySQL que se usa posteriormente para la creación de las bases de datos.

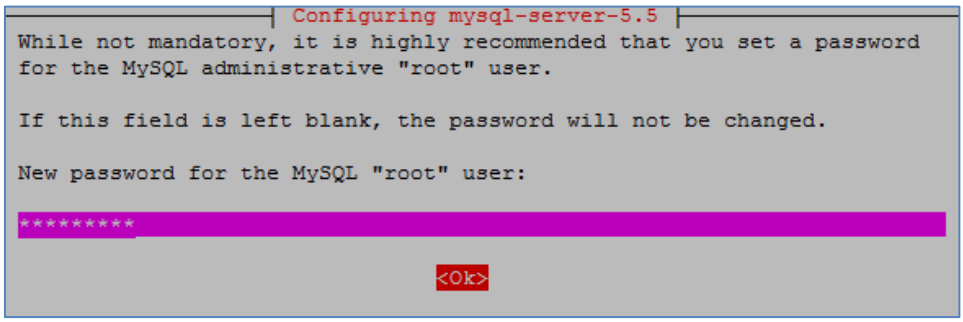


Figura 85. Solicitud de contraseña para el usuario root de MySQL
Nota. Fuente: Captura de consola puTTY, instalación de MySQL

Para evitar que la administración de la base de datos se vuelva compleja se usa phpMyAdmin, un gestor web para MySQL que facilita la memorización de una gran cantidad comandos por consola.

- La instalación de la herramienta web se realiza mediante el comando: apt-get install phpmyadmin, una vez terminado el proceso se reinicia el servidor http apache con el comando > service apache2 restart.

  Finalmente se accede a la base de datos usando: 10.10.10.4/phpmyadmin en un navegador web. El archivo principal para la configuración de phpmyadmin se encuentra en: /etc/phpmyadmin/config.inc.php

Una vez preparado el servidor MySQL se debe crear una base de datos RADIUS con algunas tablas y campos relacionados. Para evitar el trabajo de crear campo por campo toda la estructura de la base de datos de forma manual, FreeRADIUS incorpora scripts SQL para automatizar este proceso.

- Crear la base de datos radius y elegir el formato de codificación para los datos, por defecto se usa utf8_general_ci.

Figura 86. Creación de la base de datos radius
Nota. Fuente: Captura de la interfaz gráfica de PhpMyAdmin

- Crear un usuario privilegiado para manejar la base de datos radius.

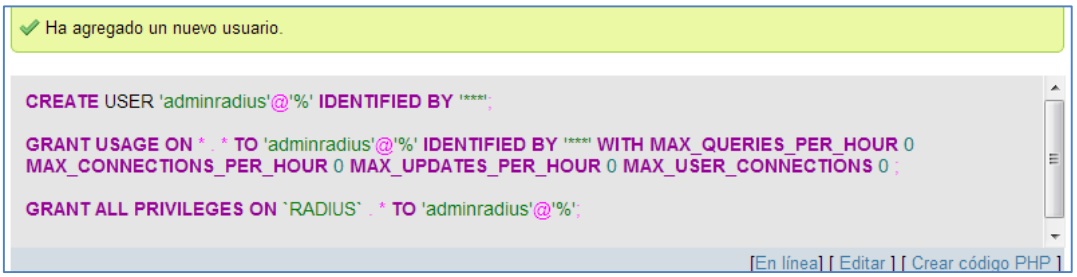


Figura 87. Creación de un usuario privilegiado para la base de datos radius
Nota. Fuente: Captura de la interfaz gráfica de PhpMyAdmin

- Crear toda la estructura de la base de datos RADIUS mediante los scripts SQL incluidos en la instalación de FreeRADIUS.

```
root@mysqlserver:/etc/freeradius# cat schema.sql | mysql -uroot -pmysqlroot radius
```

```
root@mysqlserver:/etc/freeradius# cat nas.sql | mysql -uroot -pmysqlroot radius
```

- Por último, usando phpmyadmin se agregan los equipos autenticadores en la tabla "nas" de la base de datos "radius", se debe ingresar la dirección IP y el secreto compartido de cada cliente RADIUS, el resto de campos son opcionales y se puede omitir su configuración.

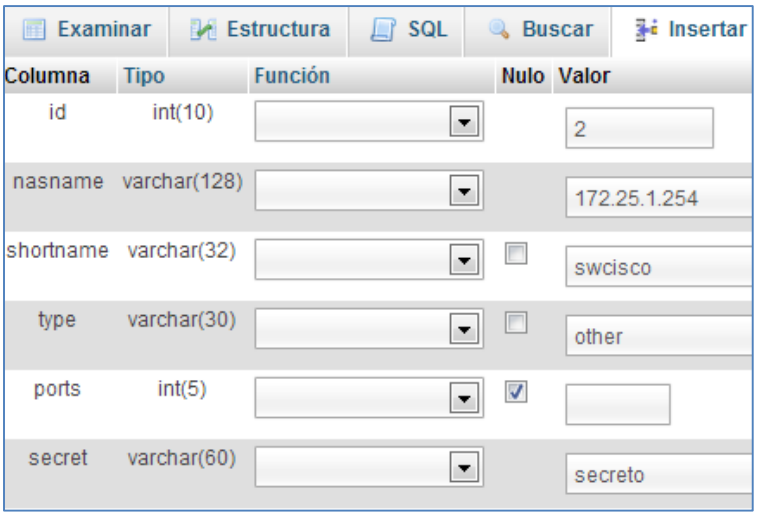


Figura 88. Insertando nuevo cliente radius en phpmyadmin
Nota. Fuente: Captura de la interfaz gráfica de PhpMyAdmin

4.4 AUTENTICADOR CABLEADO

La implementación del servicio 802.1x para el control de acceso a redes cableadas se lo hace en el switch Cisco Small Business SF300, conmutador de red que opera como dispositivo de capa 2 o 3 según se lo configure. Soporta la mayoría de funciones ofrecidas por los switch Cisco Small Business SG200, que es la tecnología actual implementada en la red de datos del GAD Municipal San Miguel de Urcuqui.

4.4.1 VLAN

La configuración de las redes de área local virtual (VLAN) se lo hace a través de la interfaz web del switch, la dirección IP por defecto requerida para el acceso es 192.168.1.254, y se debe autenticar usando la clave cisco tanto para el nombre de usuario como la contraseña.

Cambiar la dirección IP estática y la puerta de enlace predeterminada del switch cisco, la misma que servirá como identificador para el servidor RADIUS.

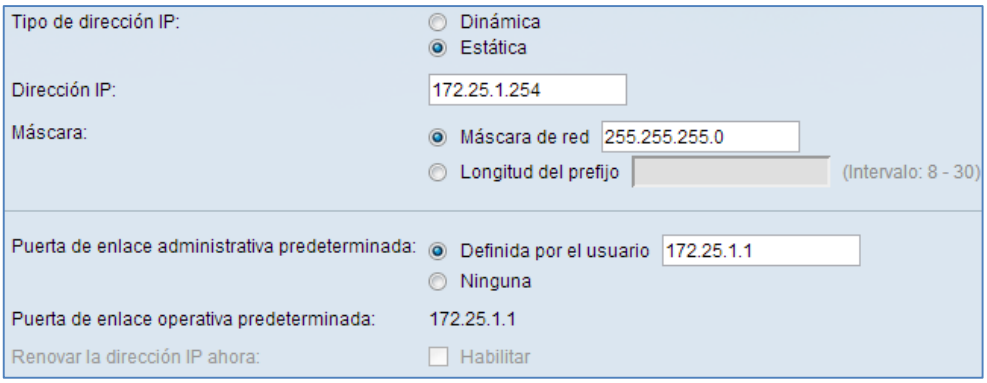


Figura 89. Asignación de dirección IP al switch SF-300
Nota. Fuente: Captura de la interfaz web del switch cisco SF-300

El primer paso es crear las VLAN para cada unidad departamental del GAD Municipal San Miguel de Urcuquí de acuerdo a las especificaciones mostradas en la Tabla 19, para lo cual se accede al menú: Administración de VLAN > crear VLAN > Añadir.

Se despliega una ventana donde se debe establecer el identificador y nombre de la VLAN, como se muestra en la Figura 90.

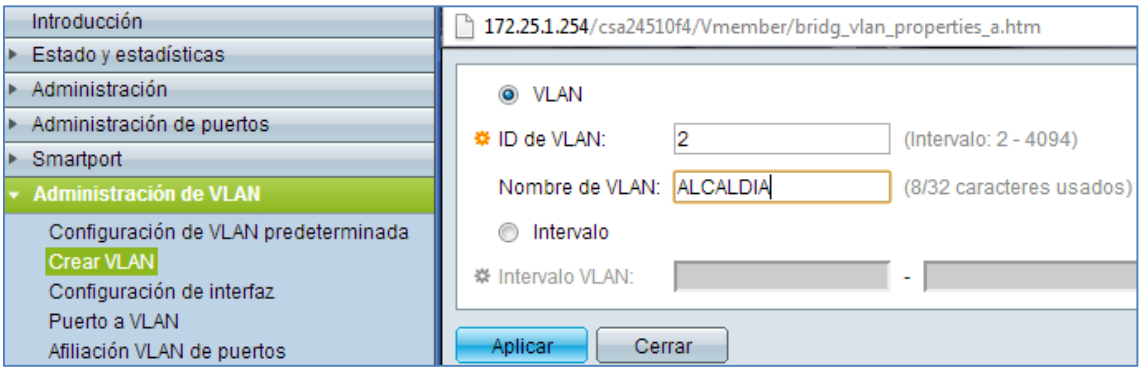


Figura 90. Creación de VLAN switch cisco SF-300
Nota. Fuente: Captura de la interfaz web del switch cisco SF-300

El mismo proceso se lo debe realizar para cada una de las VLAN, hasta completar todas las requeridas.

Figura 91. Resumen de VLANs creadas switch cisco FS-300
Nota. Fuente: Captura de la interfaz web del switch cisco SF-300

Luego, se configuran los puertos del switch en modo general, de esta manera se asignan los puertos a las VLAN en forma dinámica.

Para lo cual, se accede al menú: Administración de VLAN > Configuración de Interfaz, en la tabla desplegada se selecciona la interfaz del switch que se desea editar y se establece el puerto en modo general como se muestra en la Figura 92.

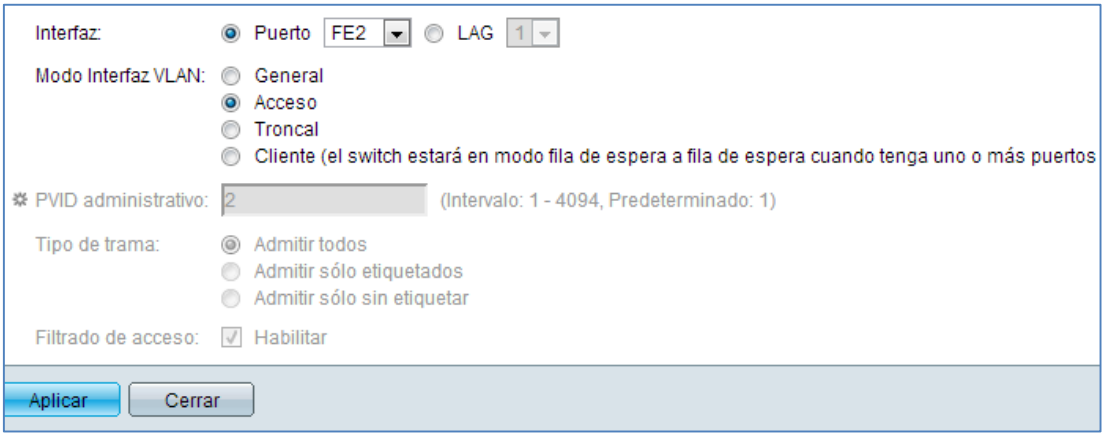


Figura 92. Configuración de puerto FE2 en modo general switch cisco SF-300
Nota. Fuente: Captura de la interfaz web del switch cisco SF-300

Una vez finalizado el proceso de creación de VLANs se debe configurar un puerto en modo troncal y añadir los identificadores de VLAN con la finalidad de transportar el tráfico de todas las redes virtuales etiquetadas y permitir la comunicación entre ellas.

Para ello se accede al menú: Administración de VLAN > Afiliación VLAN de puertos > Unir VLAN, en el cuadro desplegado se selecciona el puerto FE1 configurado en modo troncal y se agregan todas la VLAN creadas, ver Figura 93.

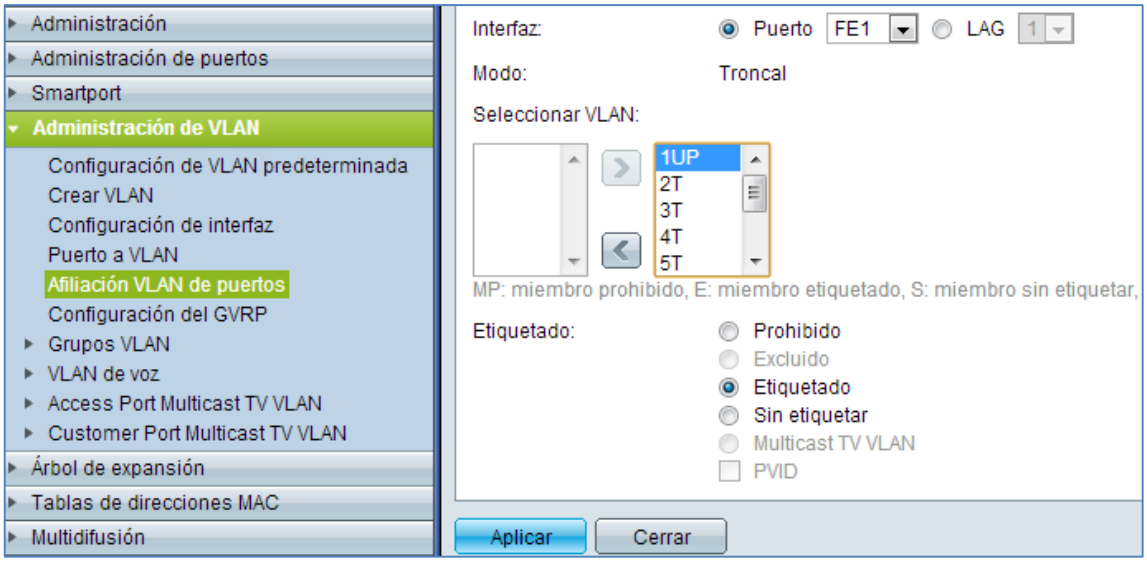


Figura 93. Permitir el tráfico de las VLAN de acceso a través del puerto troncal.
Nota. Fuente: Captura de la interfaz web del switch cisco SF-300

4.4.2 802.1X

El dispositivo cisco SF-300 es un cliente RADIUS que se basa en un servidor AAA para proporcionar seguridad centralizada en la red, controla el acceso de usuarios a través de los procesos de autenticación y autorización.

Para activar el servicio RADIUS se accede al menú: Seguridad > RADIUS > Añadir. En la página desplegada se debe configurar los parámetros del servidor FreeRADIUS que se usará como servidor de autenticación para la red de datos del GADMU.

Los valores que se deben ingresar son:

- **Versión IP:** Es el tipo de versión IP usada por el servidor RADIUS (IPv4).

- **Dirección IP del servidor:** Ingresar la dirección IP del servidor (10.10.10.2).

- **Prioridad:** En el caso de tener más de un servidor RADIUS la prioridad determina el orden en que el switch intenta comunicarse con los servidores para autenticar a un usuario. El dispositivo comienza con el de mayor prioridad, que corresponde al valor cero.

- **Cadena clave:** Se usa para autenticar y cifrar los atributos RADIUS que se envían entre el switch y el servidor, la clave debe ser la misma que se estableció en el servidor FreeRADIUS.

- **Tiempo de espera para respuesta:** Es el tiempo en segundos que el equipo espera una respuesta del servidor FreeRADIUS antes de volver a realizar la consulta o cambiar a otro servidor si lo hubiera.

- **Puerto de autenticación:** Es el número de puerto UDP del servidor RADIUS usado para las solicitudes de autenticación.

- **Puerto de contabilidad:** Es el número de puerto UDP del servidor RADIUS usado para las solicitudes de contabilidad.

- **Número de reintentos:** Es el número de solicitudes que se envían al servidor RADIUS antes de considerar que se ha producido un error.

- **Tiempo muerto:** Número de minutos de espera antes de desviar las solicitudes de servicio de un servidor RADIUS que no responde a otro.

- **Tipo de uso:** Se debe seleccionar la opción 802.1X para habilitar el control de acceso a través del servidor RADIUS.

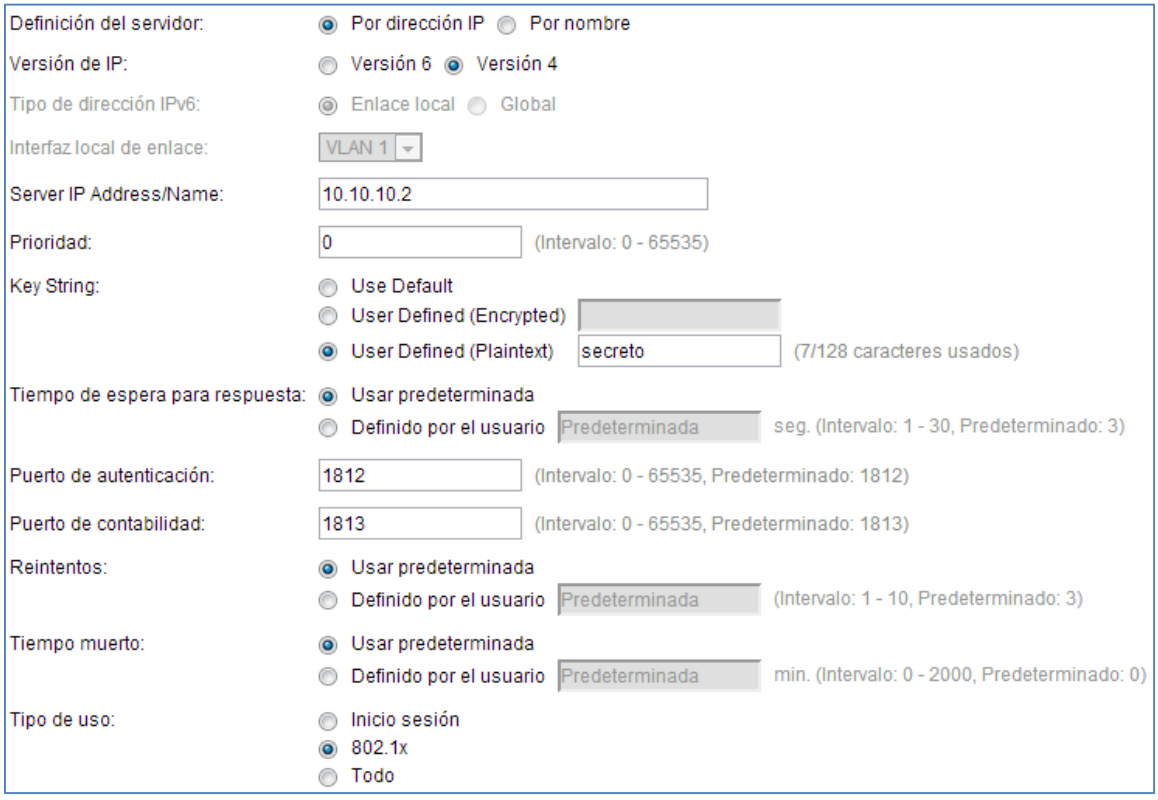


Figura 94. Configuración del servidor RADIUS en el switch cisco SF-300
Nota. Fuente: Captura de la interfaz web del switch cisco SF-300

Luego de haber añadido el servidor RADIUS se debe configurar los parámetros del estándar IEEE 802.1X en el switch SF-300, para que 802.1X funcione se debe activar tanto en forma global como individual en cada puerto.

Para definir la autenticación basada en puerto de manera global se accede al menú: Seguridad > 802.1X > Propiedades, en la página desplegada se habilita la opción de autenticación y se selecciona el método RADIUS.

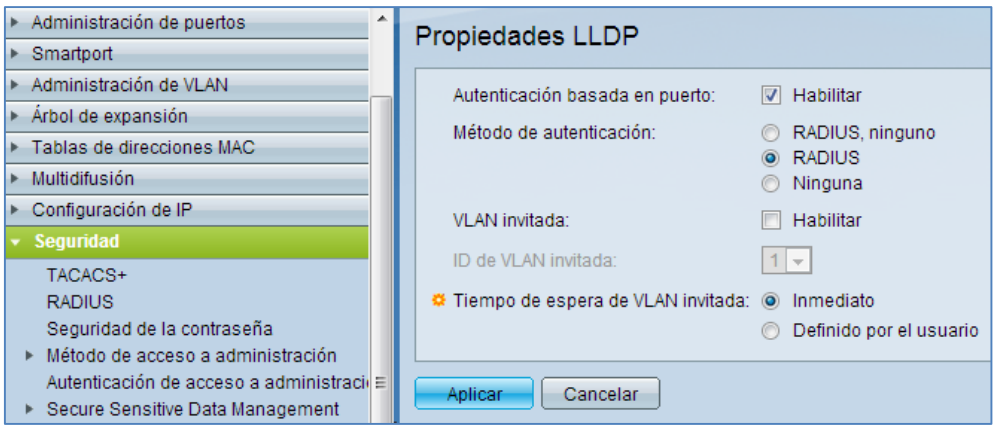


Figura 95. Autenticación basada en puerto global switch cisco SF-300
Nota. Fuente: Captura de la interfaz web del switch cisco SF-300

En la página Seguridad > 802.1X > Autenticación del Puerto, se deben definir varios parámetros del estándar 802.1X para cada puerto.

- **Puerto:** Seleccionar la interfaz del switch para habilitar la autenticación.

- **Control del puerto administrativo:** El modo automático hace que la interfaz cambie entre el estado autorizado y no autorizado según el intercambio de paquetes de autenticación entre el switch y el suplicante.

- **Asignación RADIUS VLAN:** La asignación dinámica de VLAN funciona exclusivamente cuando el modo 802.1X está configurado en sesión múltiple. Esta opción hace que un puerto autenticado correctamente se una a la VLAN asignada por el servidor RADIUS de forma automática.

  Los atributos que el servidor debe enviar al switch son: Tunnel-Type = VLAN, Tunnel-Medium-Type = 802 y Tunnel-Private-Group-Id = ID de VLAN.

El resto de parámetros tienen valores por defecto y no se recomienda cambiarlos, a menos que se requiera dar una configuración más personalizada. La Figura 96 muestra la página que permite habilitar la autenticación basada en puertos para la interfaz FE2 del switch SF-300.

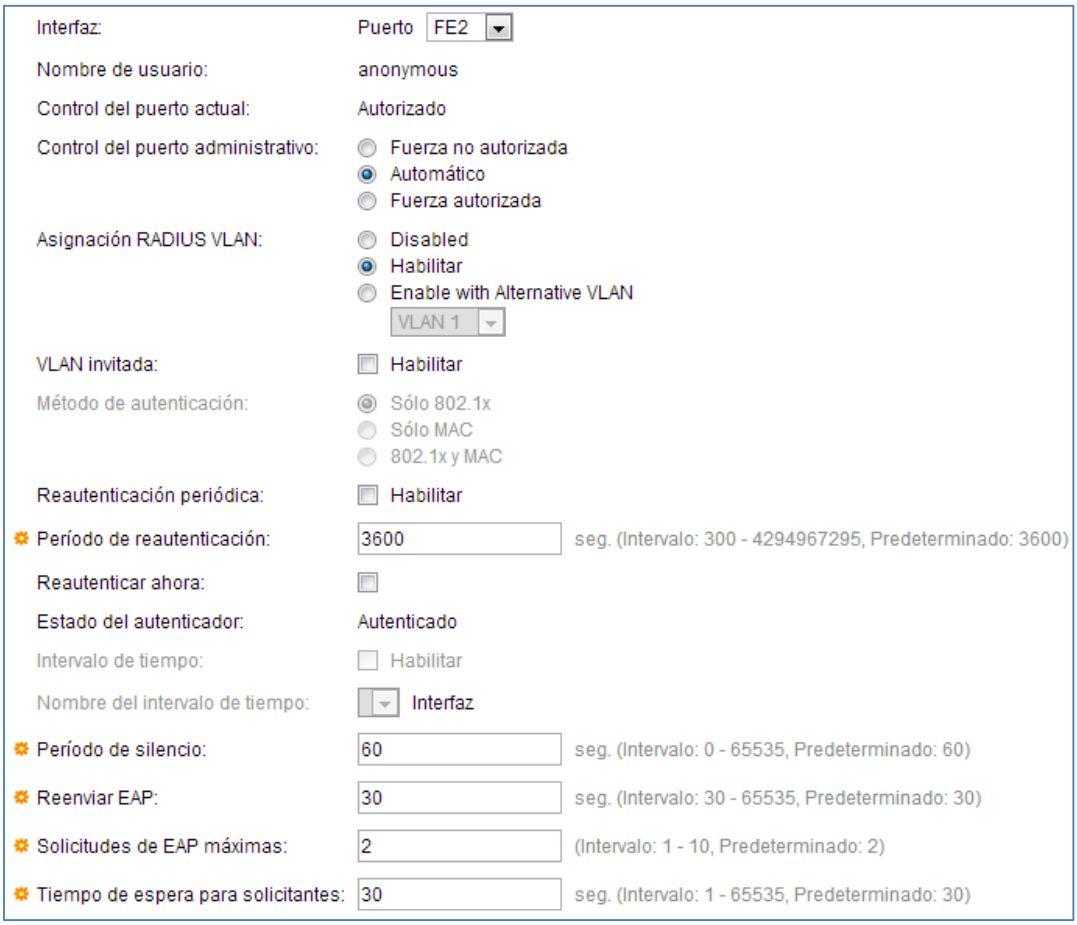


Figura 96. Definición de parámetros 802.1X en el puerto FE2
Nota. Fuente: Captura de la interfaz web del switch cisco SF-300

4.5 AUTENTICADOR INALÁMBRICO

Como autenticador inalámbrico se emplea el router AP Linksys WRT-54GL el cual utiliza un hardware compatible con Linux, por lo que permite cargar un firmware distinto al original. El sistema operativo usado en el router inalámbrico para realizar las pruebas de funcionalidad es DD-WRT, un firmware basado en Linux y liberado bajo la licencia GPL, para instalarlo es necesario descargar los archivos DD-WRT de su página oficial y cargarlo en el AP accediendo al menú: Administración > Firmware Upgrade > Seleccionar Archivo > Upgrade.

Una vez terminado el proceso de actualización del firmware se procede con la configuración del Access Point WRT-54GL para habilitar la seguridad inalámbrica mediante el servidor RADIUS.

El primer paso es asignar la dirección IP 172.25.1.253/24 a la conexión WAN, misma que servirá como identificador del dispositivo cuando se configuren los clientes en el servidor MySQL.

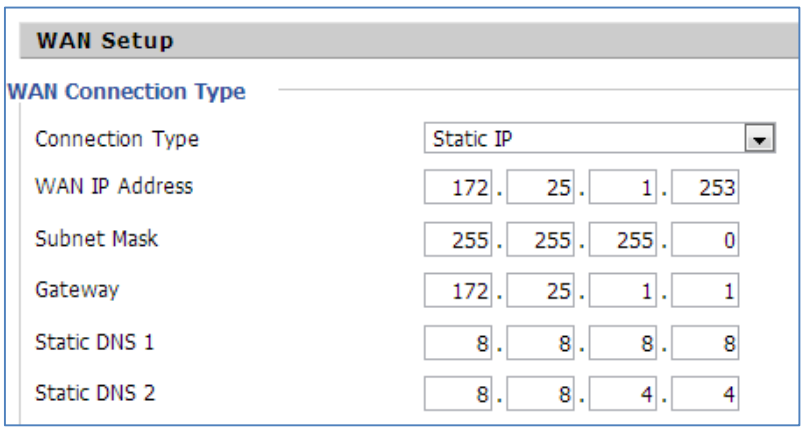


Figura 97. Configuración de la interfaz WAN AP WRT-54GL
Nota. Fuente: Captura de la interfaz web del AP WRT-54GL

Luego, especificar los parámetros básicos para la red inalámbrica: modo de trabajo, SSID, canal inalámbrico, etc. La configuración completa se puede ver en la Figura 98.

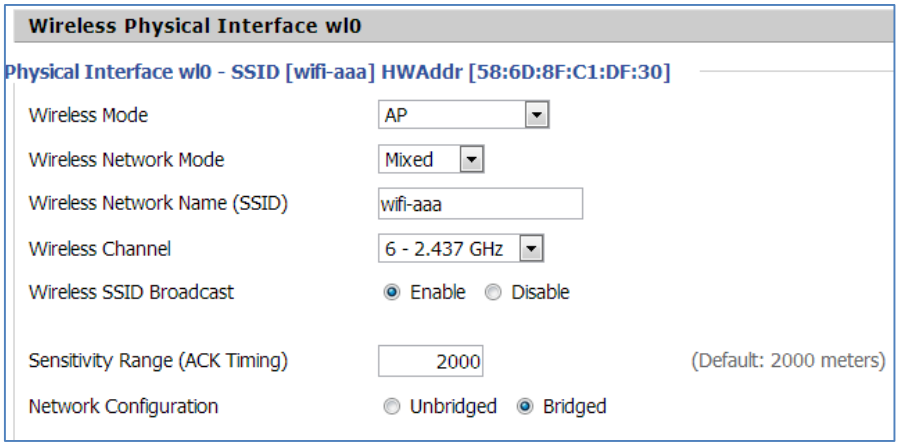


Figura 98. Configuración de red inalámbrica AP WRT-54GL
Nota. Fuente: Captura de la interfaz web del AP WRT-54GL

Finalmente, en el menú: Wireless > Wireless Security, se establece WPA2-Enterprise como el modo de seguridad por defecto para los usuarios de la red inalámbrica, empleando los algoritmos TKIP y AES en conjunto para lograr mayor compatibilidad con los suplicantes. En la Figura 99, se pueden ver todos los parámetros configurados en el AP WRT-54GL.

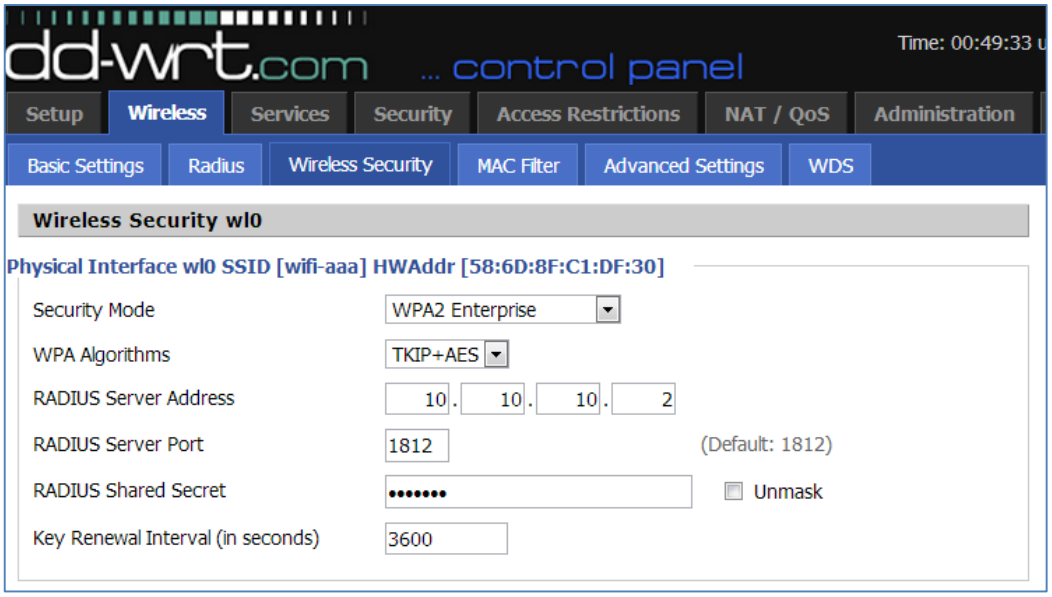


Figura 99. Configuración del servidor RADIUS AP WRT-54GL
Nota. Fuente: Captura de la interfaz web del AP WRT-54GL

4.6 SUPLICANTE

Para acceder a la red de datos protegida por el sistema AAA, los usuarios requieren de un software adicional (suplicante) que soporte el método de autenticación EAP-TTLS implementado, cualquier dispositivo que incumpla con este requerimiento no podrá conectarse a la infraestructura de red de ninguna forma.

SecureW2 es un cliente TTLS para las plataformas Windows, en el caso de sistemas operativos como GNU/Linux o Android no es necesaria su instalación debido a que tienen soporte nativo para este tipo de autenticación, incluso Windows en su última versión (Windows 8) lo trae por defecto.

4.6.1 CONFIGURACIÓN DE SECUREW2

Para activar el método de autenticación EAP-TTLS a un equipo de la red cableada usando SecureW2 como suplicante se debe realizar el siguiente proceso.

- Descargar e instalar el software SewureW2, ver Figura 100.

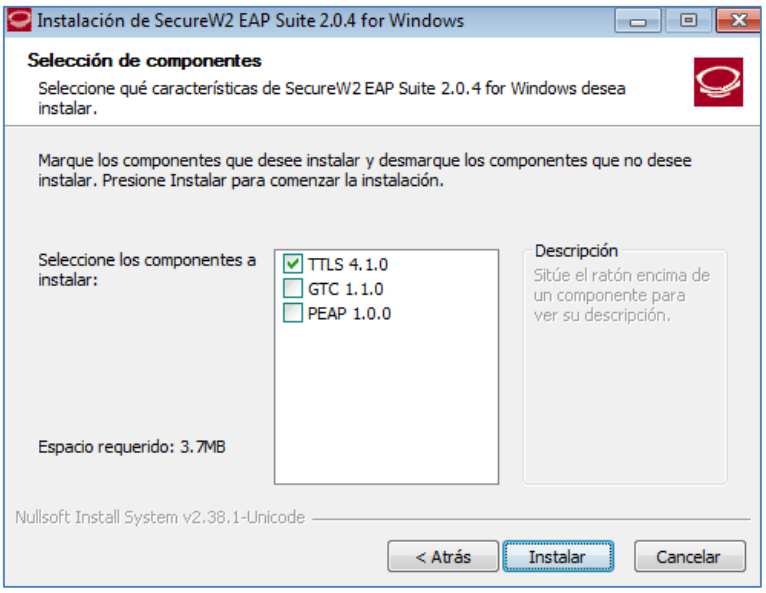


Figura 100. Instalación de suplicante SecureW2 en Windows 7
Nota. Fuente: Captura de la interfaz gráfica de SecureW2

- En el menú Autenticación, seleccionar la opción SecureW2 EAP-TTLS, ubicada en las propiedades de conexión de área local del equipo, ver Figura 101.

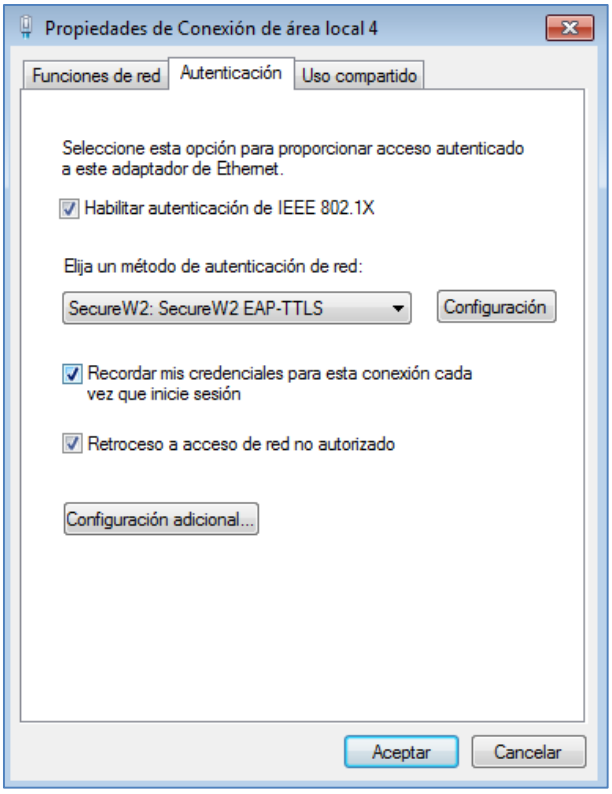


Figura 101. Habilitar autenticación EAP-TTLS
Nota. Fuente: Captura de la conexión de área local W7

- Luego, se accede al menú configuración para establecer los parámetros básicos requeridos para la conexión con el servidor FreeRADIUS.

- En el menú conexión se recomienda usar una identidad anónima para autenticarse, esto evita que las credenciales de usuario se expongan a posibles sustracciones.

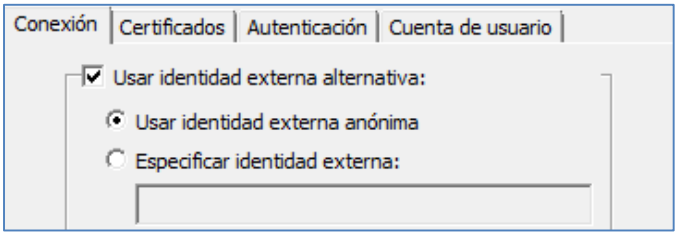


Figura 102. Activación del uso de identidad anónima SecureW2
Nota. Fuente: Captura de la interfaz gráfica de SecureW2

- En la opción certificados, se habilita la opción: comprobar certificado de servidor, esto hace que el cliente SecureW2 verifique que el servidor RADIUS con el que va intercambiar las credenciales de autenticación sea el verdadero. El proceso para añadir el certificado del servidor FreeRADIUS en los clientes Windows se detalla en el anexo B.

Figura 103. Comprobar certificado de servidor
Nota. Fuente: Captura de la interfaz gráfica de SecureW2

- Finalmente, en el menú cuenta de usuario se agrega el nombre y contraseña de un usuario validado para acceder a la red usando el servicio AAA.

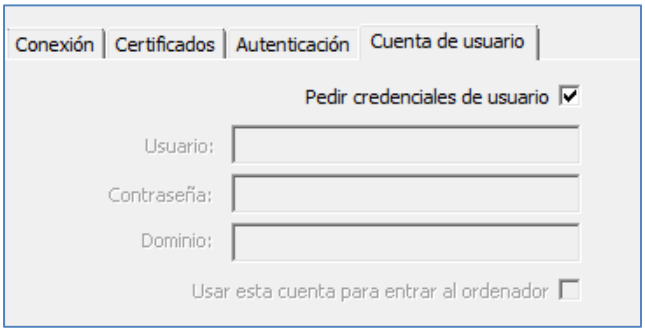


Figura 104. Configuración de las credenciales de usuario en SecureW2
Nota. Fuente: Captura de la interfaz gráfica de SecureW2

Para activar el método de autenticación EAP-TTLS a un equipo de la red inalámbrica usando SecureW2 como suplicante se debe realizar el siguiente proceso.

- Acceder al menú: administración de redes inalámbricas y agregar un nuevo perfil.

Figura 105. Creación de un perfil inalámbrico Windows 7
Nota. Fuente: Captura de la interfaz de administración de redes inalámbricas Windows 7

- Asignar un nombre a la red, seleccionar el mecanismo de seguridad y el tipo de cifrado usado para establecer la nueva conexión.

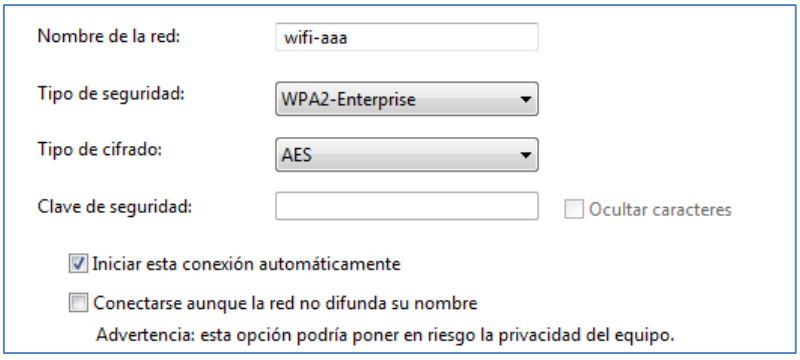


Figura 106. Información de la nueva red inalámbrica
Nota. Fuente: Captura de la interfaz de administración de redes inalámbricas Windows 7

- Una vez creado el nuevo perfil de red inalámbrico, se configuran los parámetros del suplicante SecureW2 siguiendo el mismo procedimiento utilizado en el adaptador de red cableado.

4.7 FIREWALL

La implementación del firewall se lo realiza a nivel de software, usando la distribución Ubuntu Server 12.04 LTS como plataforma base. Las especificaciones técnicas del servidor empleado se detallan en la Tabla 22.

Tabla 22. Especificaciones técnicas servidor Firewall - AAA

RECURSO	DESCRIPCIÓN
Número de Procesadores	1
Núcleo de Procesador	2
Velocidad del Procesador	2.60GHz
Almacenamiento	500 GB
RAM	2 GB
Tipo de Procesador	Pentium(R) Dual-Core @ 2.60GHz
Tarjetas de Red	3

Nota. Fuente: Obtenido de las especificaciones propias del equipo.

De acuerdo al esquema de red mostrado en la Figura 1, se deben configurar tres zonas en el firewall, una interfaz de red que permita la conexión a internet, la segunda para la zona desmilitarizada (DMZ de servidores) y la tercera para la red local de la institución. La asignación de IP para cada interfaz de red se realiza en base a la Tabla 17.

Figura 107. Configuración de las interfaces de Red Firewall - AAA
Nota. Fuente: Captura de la interfaz gráfica Webmin, módulo Shorewall.

4.7.1 VLANS CON 802.1Q

Para lograr la comunicación entre equipos de diferentes VLANs es necesario usar un dispositivo de capa 3 que realice el proceso de enrutamiento de paquetes de distintas redes. El puerto del router debe soportar el protocolo IEEE 802.1Q, mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.

La implementación del estándar IEEE 802.1Q se realiza en el puerto eth0 del Firewall GNU/Linux, para activar el servicio se debe configurar los requerimientos básicos que habilitan las interfaces virtuales en la tarjeta de red Ethernet.

- Instalar el paquete vlan > apt-get install vlan

- Añadir el módulo 802.1q al kernel del servidor firewall > modprobe 802.1q

- Añadir el módulo 802.1q al archivo /etc/modules, esto permite cargarlo automáticamente después de cada reinicio del sistema.

  El comando usado es: `#su -c 'echo "8021q" >> /etc/modules'`

- Configurar el puerto eth0 como interfaz VLAN 802.1q usando las herramientas de configuración de red del sistema operativo Ubuntu Server 12.04 LTS.

- Editar el archivo /etc/network/interfaces, para definir las VLANs y las direcciones IP asociadas a cada interfaz virtual.

```
ssh start/running, process 3572
root@firewall-aaa:~# cat /proc/net/vlan/config
VLAN Dev name    | VLAN ID
Name-Type: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
eth0.2          | 2  | eth0
eth0.3          | 3  | eth0
eth0.4          | 4  | eth0
eth0.5          | 5  | eth0
eth0.6          | 6  | eth0
eth0.7          | 7  | eth0
eth0.8          | 8  | eth0
eth0.9          | 9  | eth0
root@firewall-aaa:~#
```

Figura 108. Redes virtuales creadas en la interfaz eth0 del Firewall - AAA
Nota. Fuente: Captura de consola puTTY, servidor firewall-aaa

4.7.2 HERRAMIENTA DE ADMINISTRACIÓN: WEBMIN

La mayoría de servidores basados en distribuciones GNU/Linux no poseen una interfaz gráfica de usuario principalmente por razones de seguridad y rendimiento, la forma común de administrarlos es desde terminales remotos de texto, sin embargo actualmente se lo puede hacer mediante interfaces Web que permiten controlar todas las funciones vitales del servidor, así como los servicios que ejecuta.

Webmin es un proyecto de software libre que ofrece una interfaz Web para la administración de sistemas GNU/Linux, utiliza SSL para establecer sesiones seguras y cifrar los datos de usuarios, el puerto de escucha por defecto para acceder al servicio es el 10000.

- Para instalar Webmin en el servidor se debe descargar ciertas librerías para evitar errores de dependencia de paquetes.

```
apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-
runtime libio-pty-perl apt-show-versions python
```

Figura 109. Instalación de las dependencias para el software Webmin
Nota. Fuente: Recuperado de http://webmin.com/deb.html

- De la página oficial de Webmin descargar e instalar la última versión del software usando los comandos de la Figura 110.

```
wget http://prdownloads.sourceforge.net/webadmin/webmin_1.630_all.deb
```

then run the command :

```
dpkg --install webmin_1.630_all.deb
```

Figura 110. Descarga e instalación de Webmin en Ubuntu Server 12.04 LTS
Nota. Fuente: Recuperado de http://webmin.com/deb.html

- Una vez instalado, se accede a la interfaz de Webmin usando la dirección IP del servidor y el puerto de escucha por defecto.

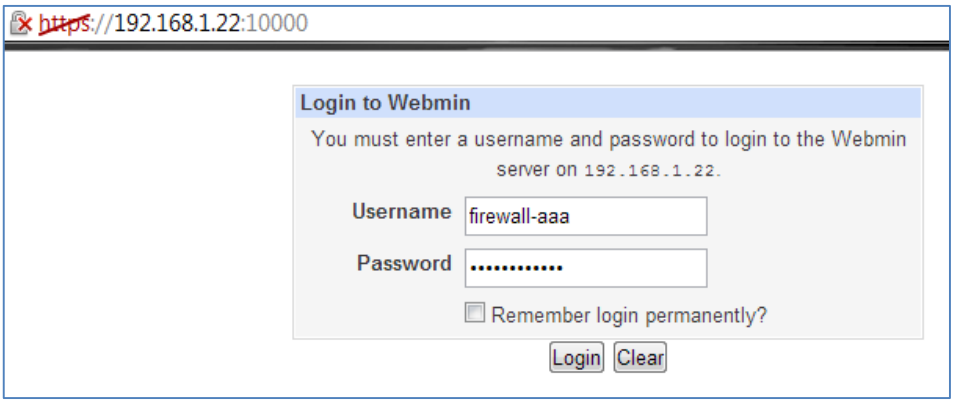


Figura 111. Acceso a la herramienta Webmin usando un navegador web
Nota. Fuente: Captura de la interfaz gráfica Webmin

4.7.3 SHOREWALL

Shorewall es una herramienta de código abierto que permite crear firewalls robustos sobre plataformas GNU/Linux, se basa en el sistema Netfilter/iptables integrados por defecto en el kernel de Linux, mediante el cual se definen las reglas y políticas para el manejo de los paquetes que transitan a través de él.

La configuración y administración de Shorewall se lo hace con la herramienta de administración Webmin instalada, el procedimiento general seguido para la puesta en marcha del firewall se detalla a continuación:

- Editar los parámetros básicos para activar el servicio Shorewall en Ubuntu Server.
- Definir las zonas de red: WAN, LAN, DMZ, FW, VLANs.
- Agregar las interfaces de red del sistema que usará Shorewall para la gestión de las reglas y políticas del firewall.
- Configurar las acciones por defecto para el tráfico entre zonas del firewall.
- Definir las reglas para permitir o denegar el acceso a servicios o puertos desde y hacia las zonas del firewall.

4.7.3.1 Archivo de configuración

En el archivo de configuración principal del firewall ubicado en /etc/shorewall/ shorewall.conf, verificar que los parámetros STARTUP_ENABLED e IP_FORWARDING estén configurados correctamente.

STARTUP_ENABLED = yes; permite que el servicio de Shorewall arranque cuando inicia el servidor.

IP_FORWARDING = on; permite que los paquetes sean capaces de pasar de una interfaz a otra, por ejemplo, que los usuarios de la red local (eth0) accedan a internet a través de la interfaz de red WAN (eth1).

4.7.3.2 Zonas de red

De acuerdo a los requerimientos del servidor AAA se definen tres zonas de red, las cuales se asocian a cada una de las interfaces físicas del firewall, el archivo para la configuración manual de zonas se almacena en /etc/shorewall/zones.

El proceso para agregar una nueva zona de red o editar una ya creada se muestra en la Figura 112.

Figura 112. Zonas de red Shorewall
Nota. Fuente: Captura de la interfaz gráfica Webmin, módulo Shorewall.

4.7.3.3 Interfaces de red

Tomando en cuenta las consideraciones técnicas realizadas en el diseño del servidor AAA se definen las interfaces físicas para las zonas de servidores (DMZ) y acceso a la WAN, el resto de interfaces se deben virtualizar por cada VLAN del sistema.

El procedimiento para asociar una zona de red a una interfaz del firewall se muestra en la Figura 113, el archivo para la configuración manual de las interfaces de red se almacena en /etc/shorewall/interfaces.

Figura 113. Interfaces de red asocias a una zona Shorewall
Nota. Fuente: Captura de la interfaz gráfica Webmin, módulo Shorewall.

4.7.3.4 Políticas por defecto

Se establece las políticas por defecto para los paquetes que viajan entre una zona y otra, el archivo para la configuración manual de las políticas se almacena en /etc/shorewall/policy. Las acciones que se pueden efectuar con las solicitudes de acceso son:

- ACCEPT: Aceptar la conexión.
- DROP: Ignorar la conexión.
- REJECT: Rechazar la conexión.
- CONTINUE: Dejar que la solicitud de conexión continúe para que sea procesada por otra regla.

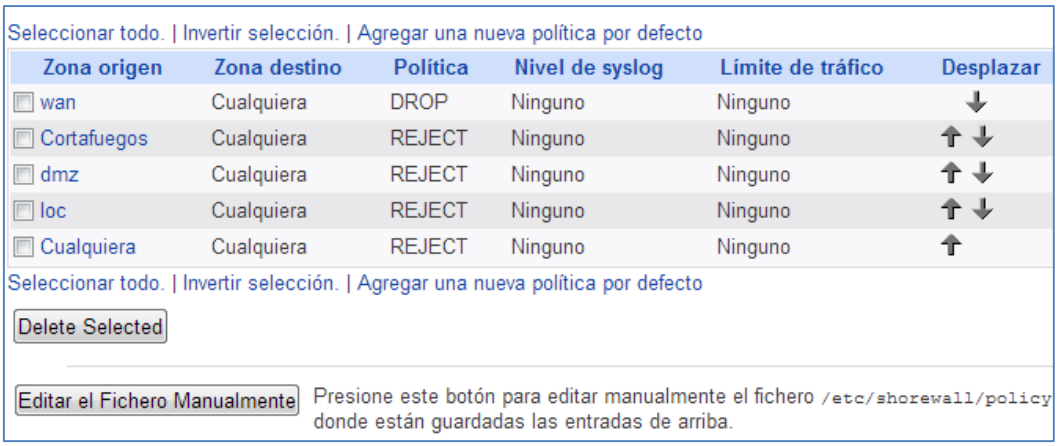


Figura 114. Políticas por defecto Shorewall
Nota. Fuente: Captura de la interfaz gráfica Webmin, módulo Shorewall.

4.7.3.5 Reglas del firewall

Las reglas del firewall permiten personalizarlo de tal forma que se adapte a todos los requerimientos establecidos en la política de control de acceso a la red. El archivo para la configuración manual de las reglas se almacena en /etc/shorewall/rules.

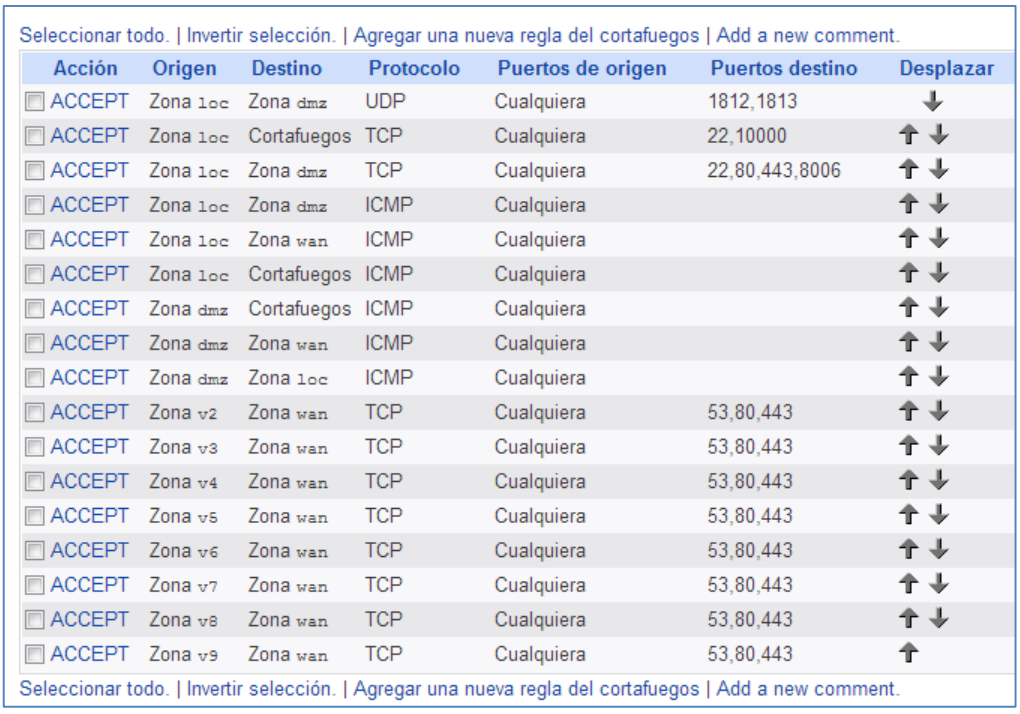


Figura 115. Reglas del Firewall - AAA
Nota. Fuente: Captura de la interfaz gráfica Webmin, módulo Shorewall.

4.8 ANÁLISIS DE RESULTADOS

Para analizar y verificar que el proceso de autenticación EAP-TTLSv0 diseñado para ofrecer el servicio AAA en la red de datos del GAD Municipal de Urcuqui cumple con los requerimientos establecidos en el RFC 5281 se utiliza Wireshark, un analizador de protocolos que permite ver todo el tráfico que pasa a través de una interfaz de red.

El proceso empleado para establecer una sesión segura usando el método de autenticación EAP-TTLS requiere del intercambio de varios paquetes entre el suplicante, equipo autenticador y servidor RADIUS.

En la comunicación suplicante – autenticador se maneja el protocolo EAPOL para encapsular los paquetes EAP sobre Ethernet y esta información a su vez se encapsula en paquetes RADIUS para transmitirla desde el equipo autenticador hacia el servidor. El intercambio de paquetes en una autenticación EAP-TTLS exitosa es algo extenso, por tal razón se lo analiza en fases para facilitar su comprensión.

EAP-TTLS Fase 1. Solicitud de acceso, intercambio de paquetes entre el suplicante y el equipo autenticador (switch SF 300).

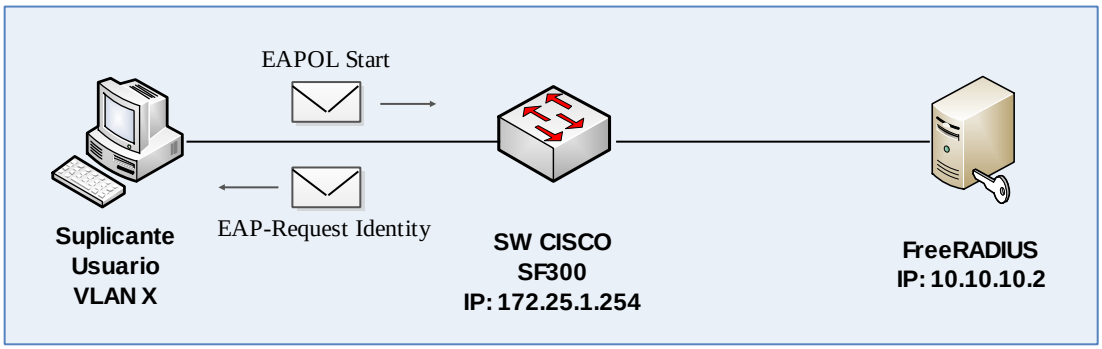


Figura 116. Esquema EAP-TTLS Fase 1
Nota. Fuente: Adaptado de http://tools.ietf.org/pdf/rfc5281.pdf

- El suplicante inicia el proceso enviando el paquete EAPOL start al switch, solicitando acceso a la red.

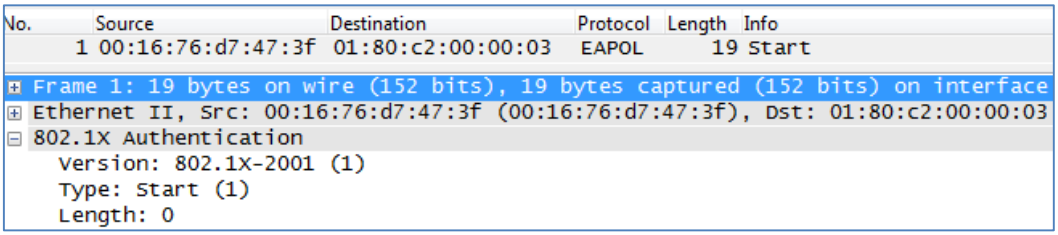


Figura 117. Paquete EAPOL Start
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El switch responde con un paquete EAP-Request Identity, confirmando que existe el servicio requerido y solicitando la identificación de usuario.

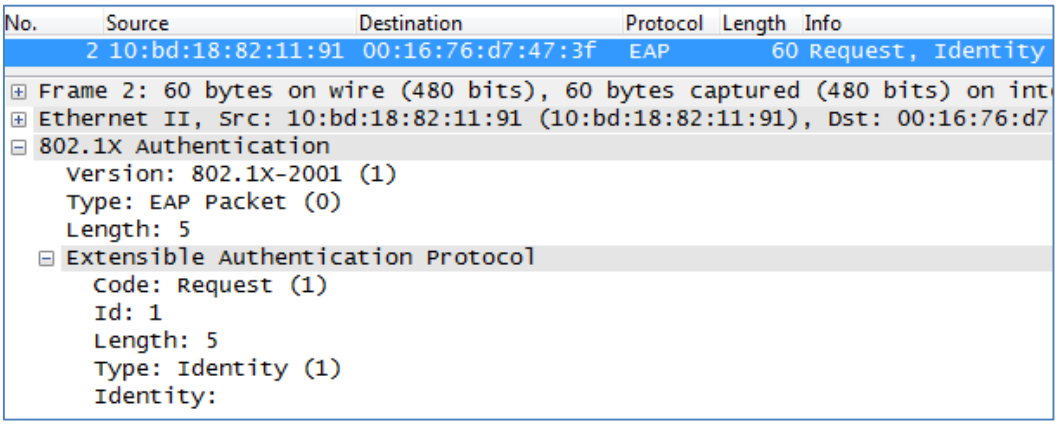


Figura 118. Paquete EAP-Request/Identity
Nota. Fuente: Captura de la interfaz gráfica Wireshark

EAP-TTLS Fase 2. Reenvío de paquetes entre el switch y el servidor FreeRADIUS, definición del método de autenticación a emplear (EAP-TTLS).

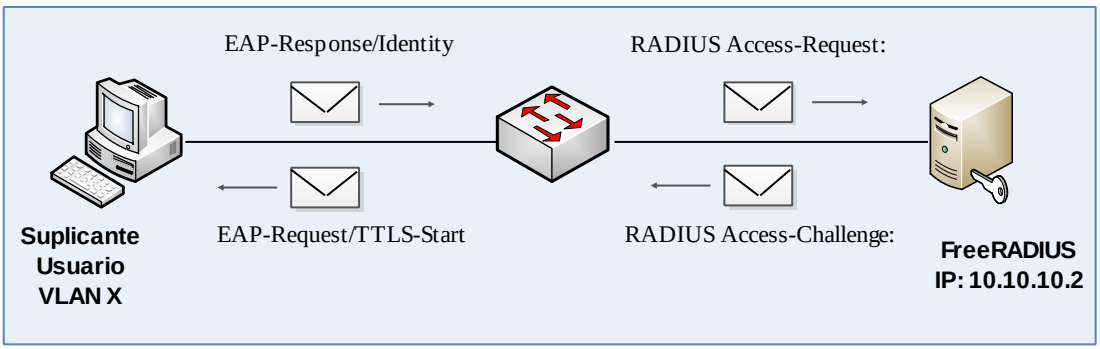


Figura 119. Esquema EAP-TTLS Fase 2
Nota. Fuente: Adaptado de http://tools.ietf.org/pdf/rfc5281.pdf

- El suplicante SecureW2 envía una identidad anónima con el fin de proteger las verdaderas credenciales del usuario en un paquete EAP-Response Identity, esta configuración garantiza un mayor nivel de seguridad frente a cualquier intento de robo de las identificaciones de usuario.

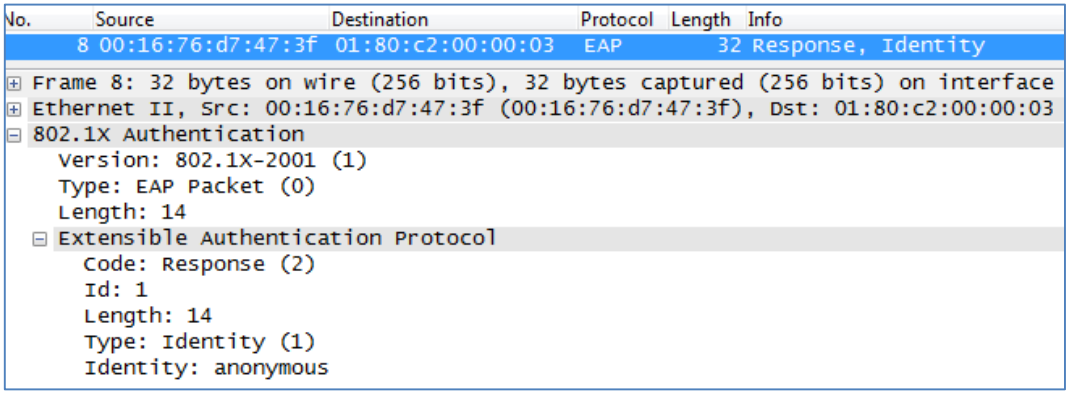


Figura 120. Paquete EAP-Response/Identity
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El switch encapsula el paquete EAPOL Response con la identificación de usuario recibida (anónima) y lo reenvía hacia el servidor AAA usando el protocolo RADIUS. En el mensaje se incluyen atributos importantes como la dirección IP del NAS, el tipo, el número de puerto, etc.

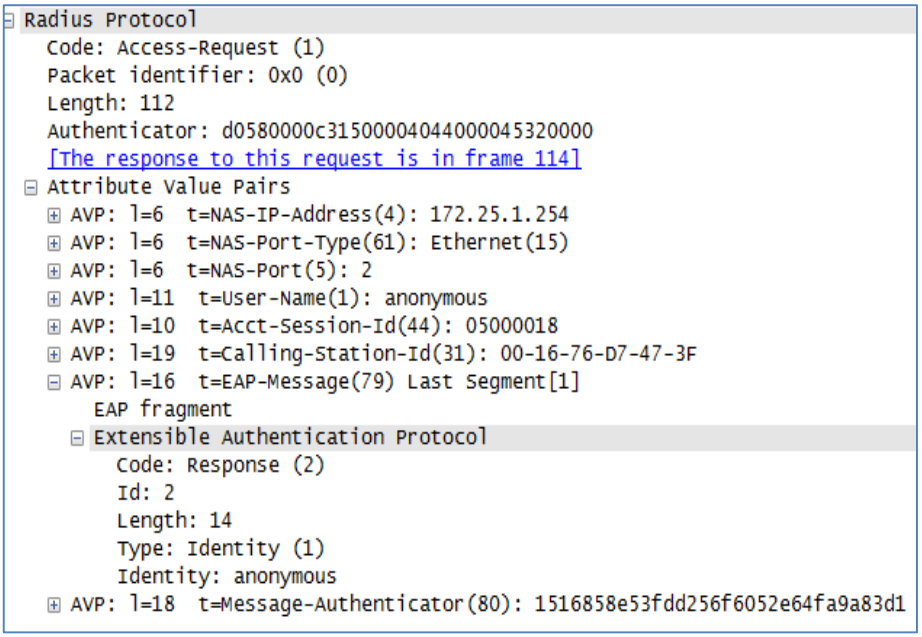


Figura 121. Paquete RADIUS Access-Request
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El servidor FreeRADIUS recupera la información, verifica que la identificación de usuario sea válida, y envía un paquete RADIUS Access-Challenge indicando al usuario el inicio del proceso de autenticación EAP-TTLS.

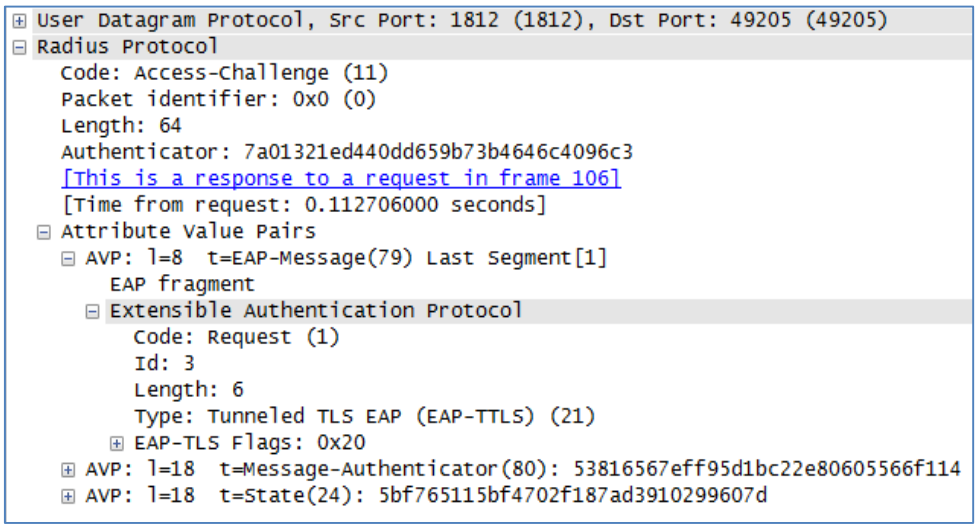


Figura 122. Paquete RADIUS Access-Challenge: EAP-Request/TTLS-Start
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El switch transmite la solicitud de inicio EAP-TTLS del servidor RADIUS, indicando al suplicante el método de autenticación EAP a utilizar.

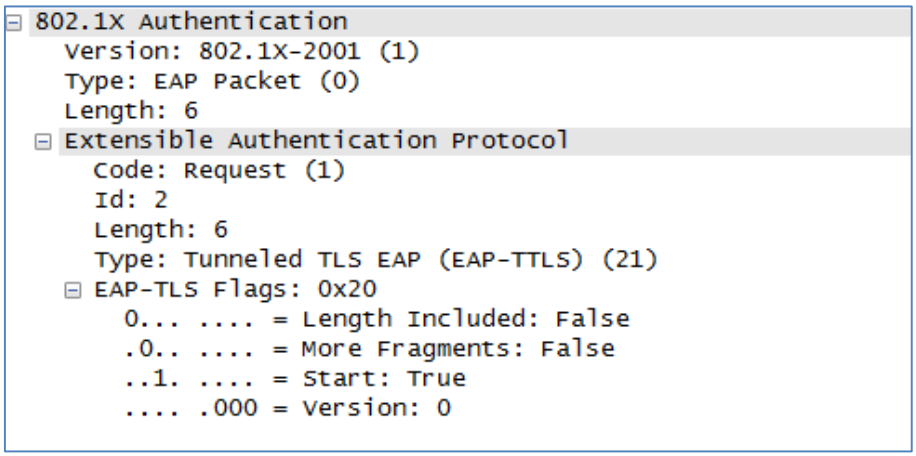


Figura 123. Paquete EAP-Request/TTLS-Start
Nota. Fuente: Captura de la interfaz gráfica Wireshark

EAP-TTLS Fase 3. Establecimiento del canal seguro TLS.

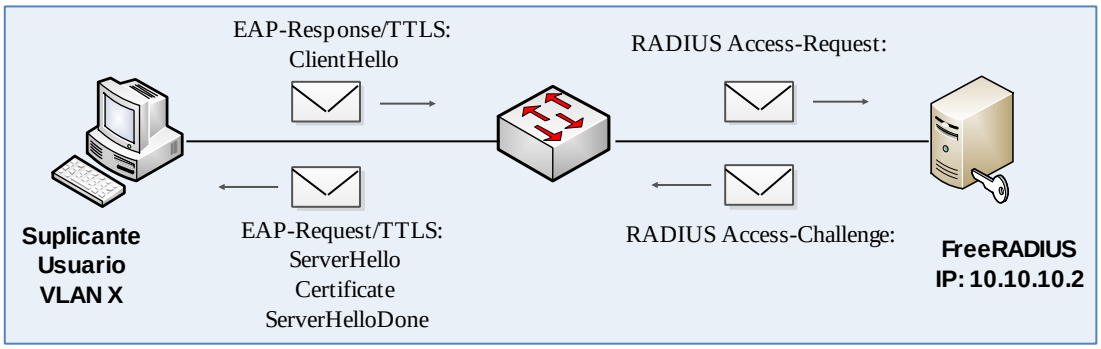


Figura 124. Esquemas EAP-TTLS Fase 3
Nota. Fuente: Adaptado de http://tools.ietf.org/pdf/rfc5281.pdf

- El usuario inicia el intercambio de mensajes con un paquete EAP-Response/TTLS Client Hello.

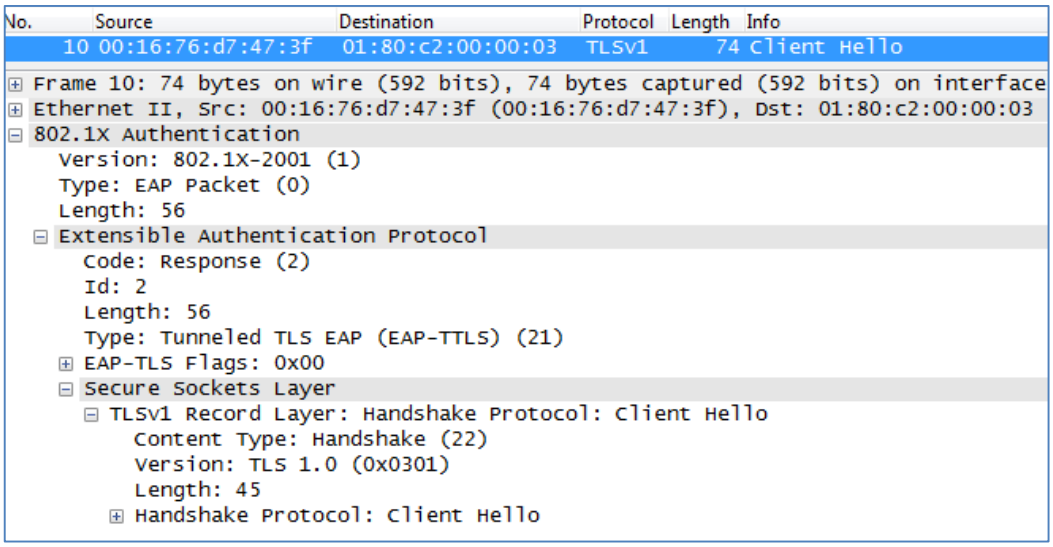


Figura 125. Paquete EAP-Response/TTLS: ClientHello
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El switch encapsula el mensaje Client Hello en un paquete RADIUS Access-Request y lo transmite al servidor.

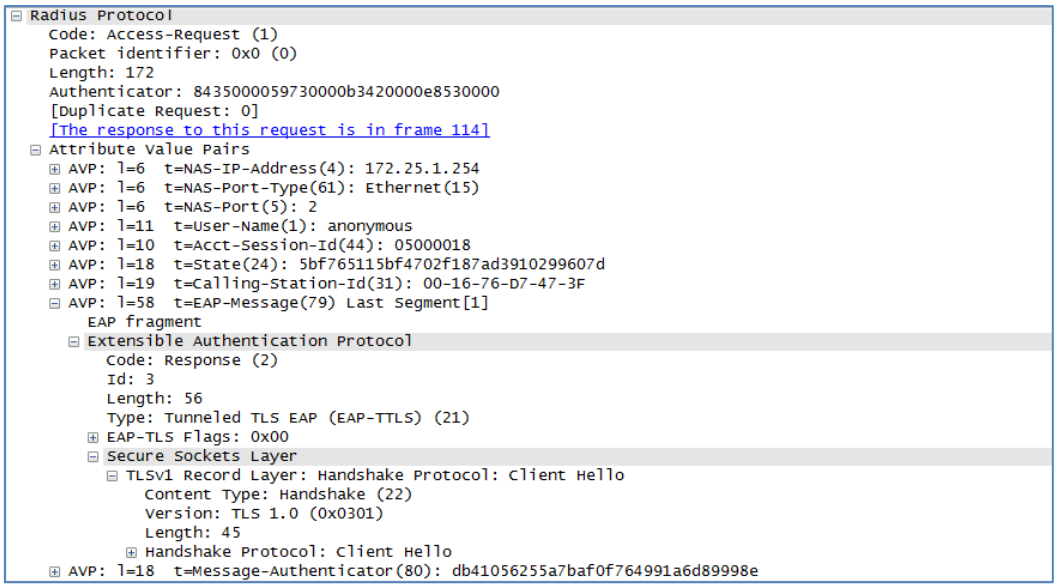


Figura 126. Paquete RADIUS Access-Request: EAP-Response/TTLS: ClientHello
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El servidor RADIUS responde el saludo mediante el paquete RADIUS Access-Challenge: EAP-Request/TTLS: ServerHello, además incluye la clave pública del certificado del servidor FreeRADIUS requerido para establecer el túnel encriptado.

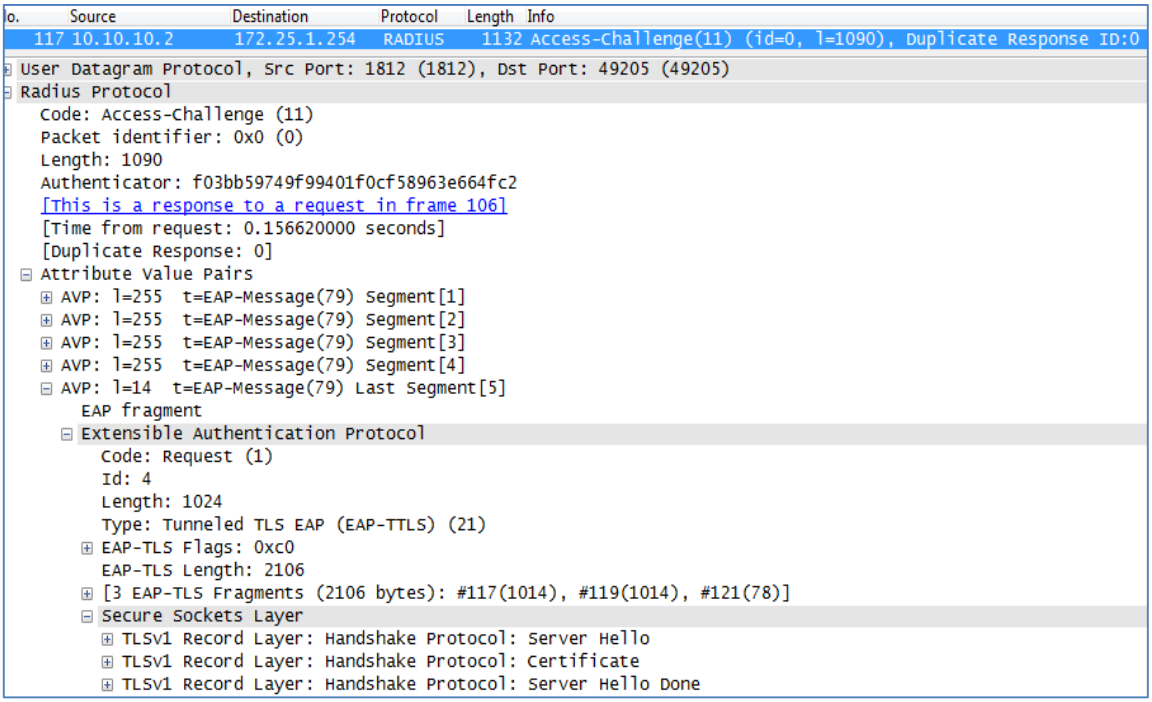


Figura 127. Paquete RADIUS Access-Challenge: EAP-Request/TTLS: ServerHello, Certificate, ServerHelloDone
Nota. Fuente: Captura de la interfaz gráfica Wireshark

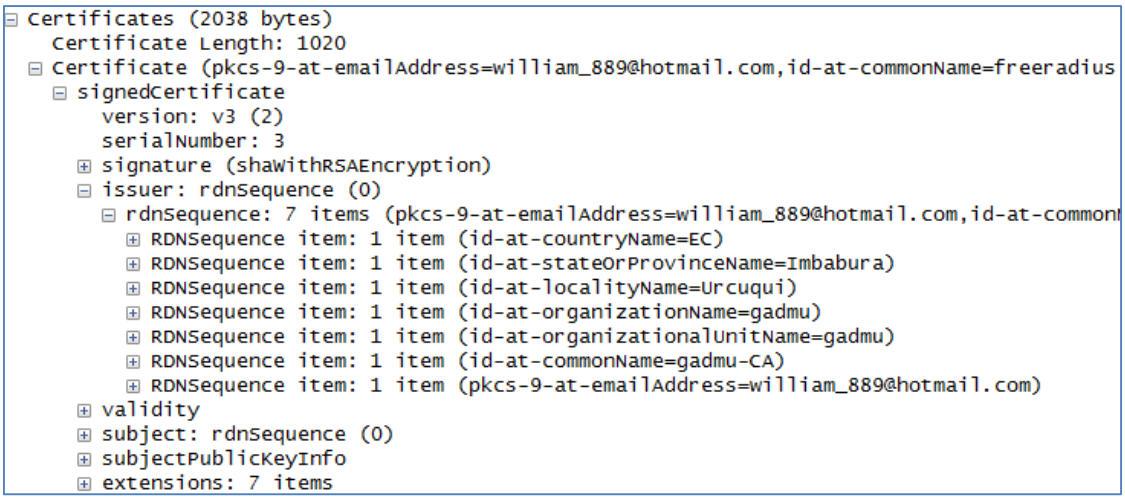


Figura 128. Clave pública del certificado digital del servidor freeradius
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El switch recupera el mensaje del servidor RADIUS que incluye el paquete Server Hello, además del certificado digital y lo transmite al suplicante.

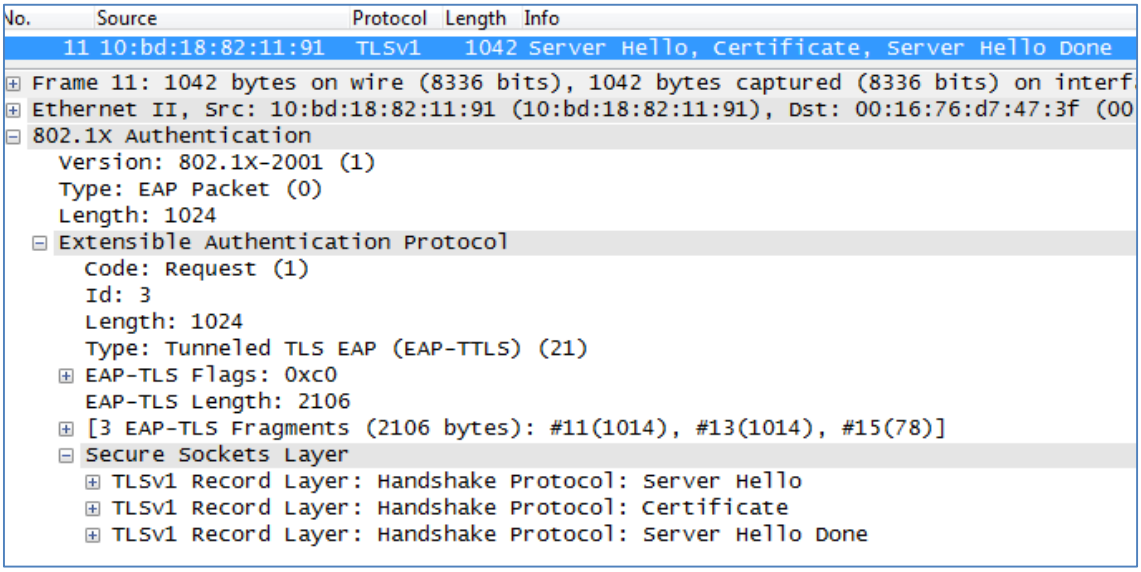


Figura 129. Paquete EAP-Request passthrough
Nota. Fuente: Captura de la interfaz gráfica Wireshark

EAP-TTLS Fase 4. Creación del túnel encriptado para el envío de credenciales de autenticación de forma segura.

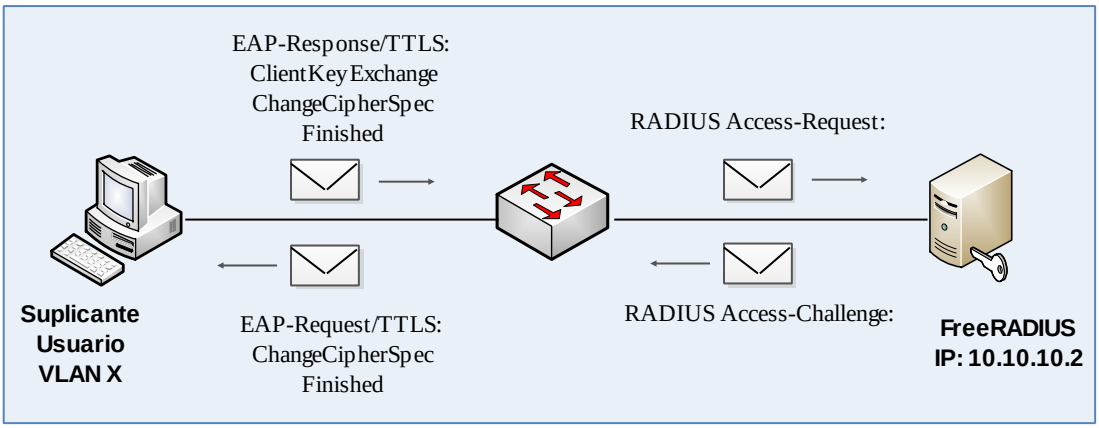


Figura 130. Esquema EAP-TTLS Fase 4
Nota. Fuente: Adaptado de http://tools.ietf.org/pdf/rfc5281.pdf

Al recibir el mensaje "Hello done" del servidor FreeRADIUS, el suplicante SecureW2 verifica la validez del certificado digital mediante la lista de autoridades certificadoras de confianza instaladas en el equipo local.

- El suplicante genera el mensaje " ClientKeyExchange", y lo transmite cifrado con la clave pública del servidor.

```
802.1X Authentication
   Version: 802.1X-2001 (1)
   Type: EAP Packet (0)
   Length: 196
Extensible Authentication Protocol
     Code: Response (2)
     Id: 5
     Length: 196
     Type: Tunneled TLS EAP (EAP-TTLS) (21)
   EAP-TLS Flags: 0x00
   Secure Sockets Layer
     TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
     TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
         Content Type: Change Cipher Spec (20)
         Version: TLS 1.0 (0x0301)
         Length: 1
         Change Cipher Spec Message
     TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
         Content Type: Handshake (22)
         Version: TLS 1.0 (0x0301)
         Length: 40
         Handshake Protocol: Encrypted Handshake Message
```

Figura 131. Paquete EAP-Response/TTLS: ClientKeyExchange
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El switch envía el mensaje EAP-Response/TTLS: ClientKeyExchange encapsulado en un paquete RADIUS hacia el servidor.

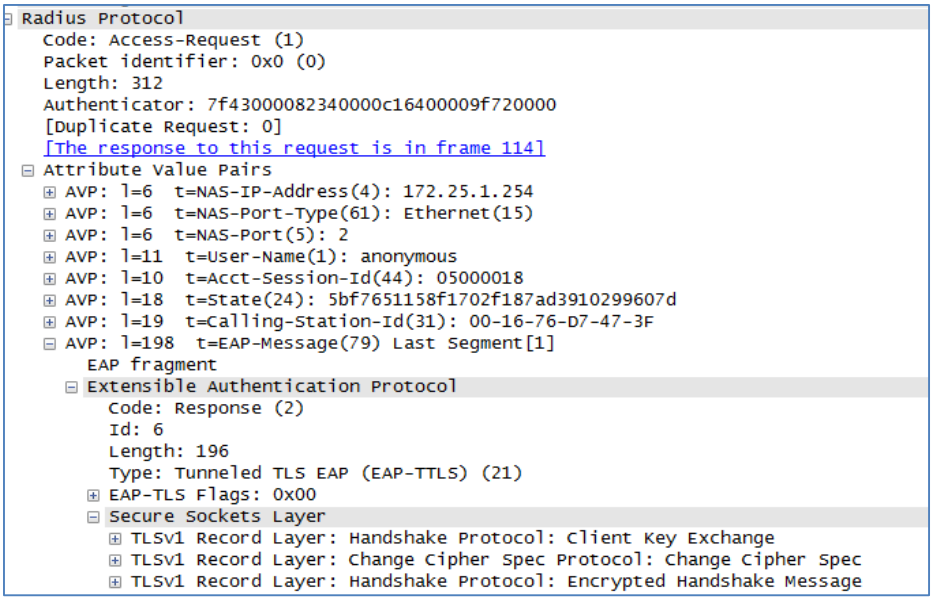


Figura 132. Paquete RADIUS Access-Request: EAP-Response passthrough
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El servidor FreeRADIUS responde al suplicante con mensajes "change cipher spec" indicando la finalización del proceso de cifrado.

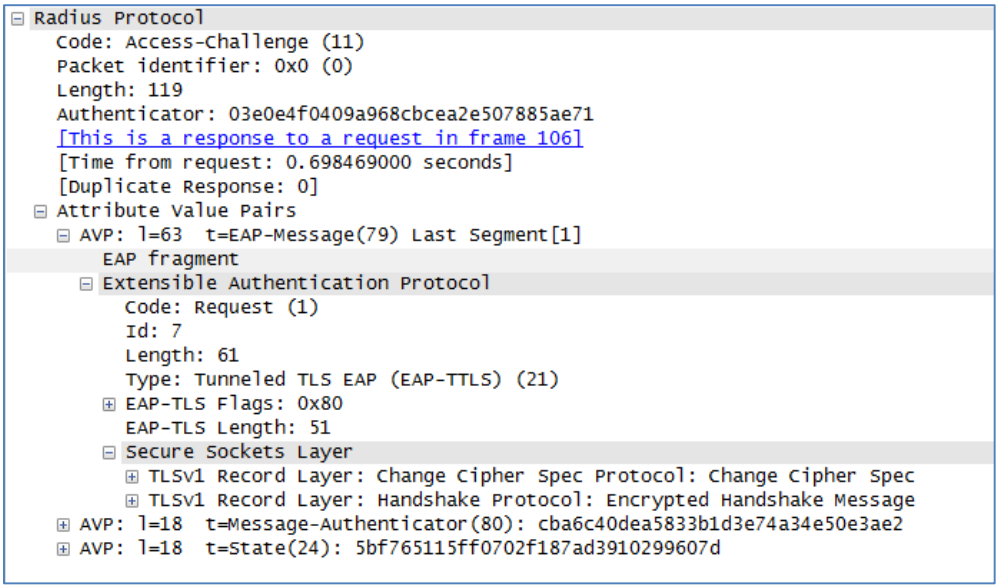


Figura 133. Paquete RADIUS Access-Challenge: EAP-Request/TTLS: ChangeCipherSpec Finished
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El switch continúa con su función de intermediario, reenviando los paquetes del servidor RADIUS al suplicante.

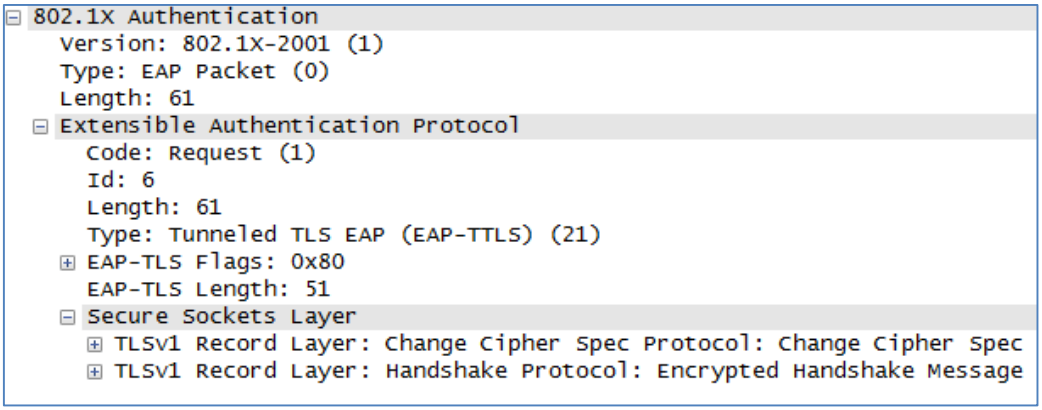


Figura 134. Paquete EAP-Request passthrough
Nota. Fuente: Captura de la interfaz gráfica Wireshark

EAP-TTLS Fase 5. Transmisión de las credenciales de usuario encriptados a través del túnel seguro.

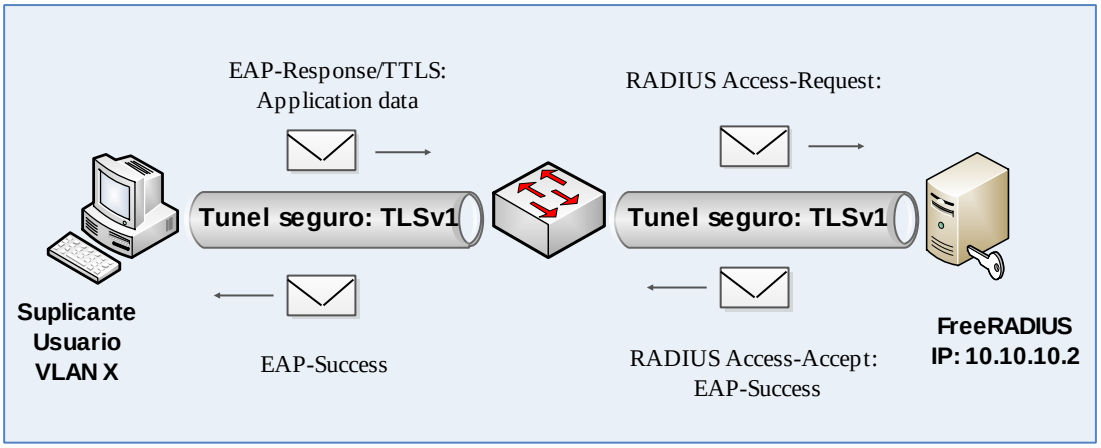


Figura 135. Esquema EAP-TTLS Fase 5
Nota. Fuente: Adaptado de http://tools.ietf.org/pdf/rfc5281.pdf

- El suplicante envía los datos de acceso (usuario y contraseña) encriptados.

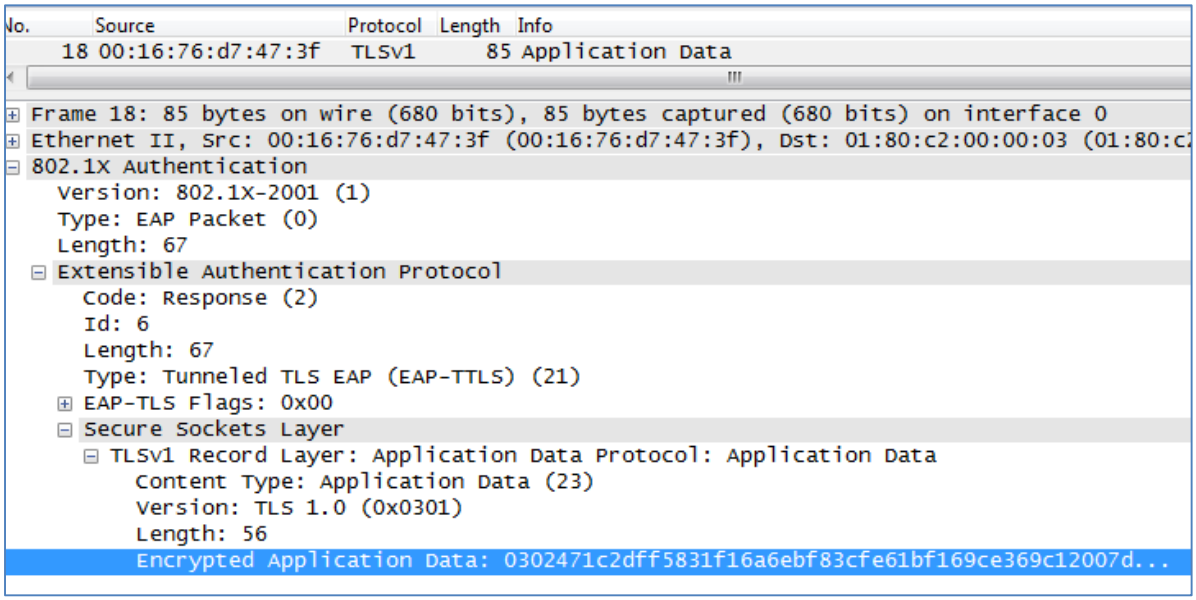


Figura 136. Credenciales de usuario encriptados
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- El equipo autenticador, como en las fases anteriores reenvía los datos de acceso (usuario y contraseña) encriptados al servidor usando el protocolo RADIUS

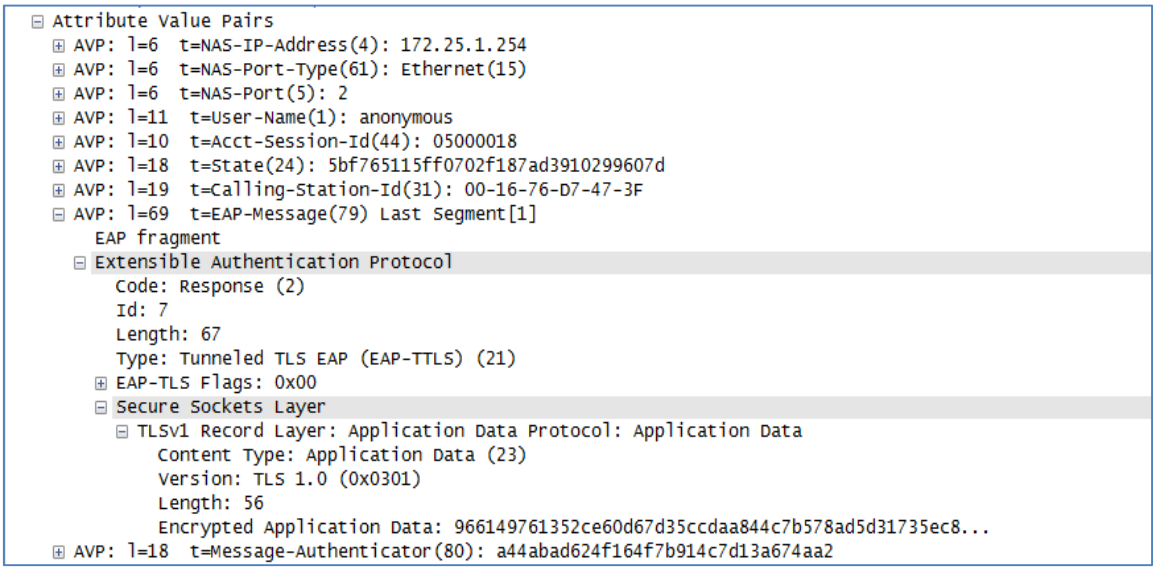


Figura 137. Paquete RADIUS con credenciales de usuario encriptados
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- Una vez que el servidor FreeRADIUS consulta en el directorio LDAP y verifica que las credenciales de usuario son válidas, envía un paquete RADIUS Access-Accept al switch para permitir el acceso del equipo a la red.

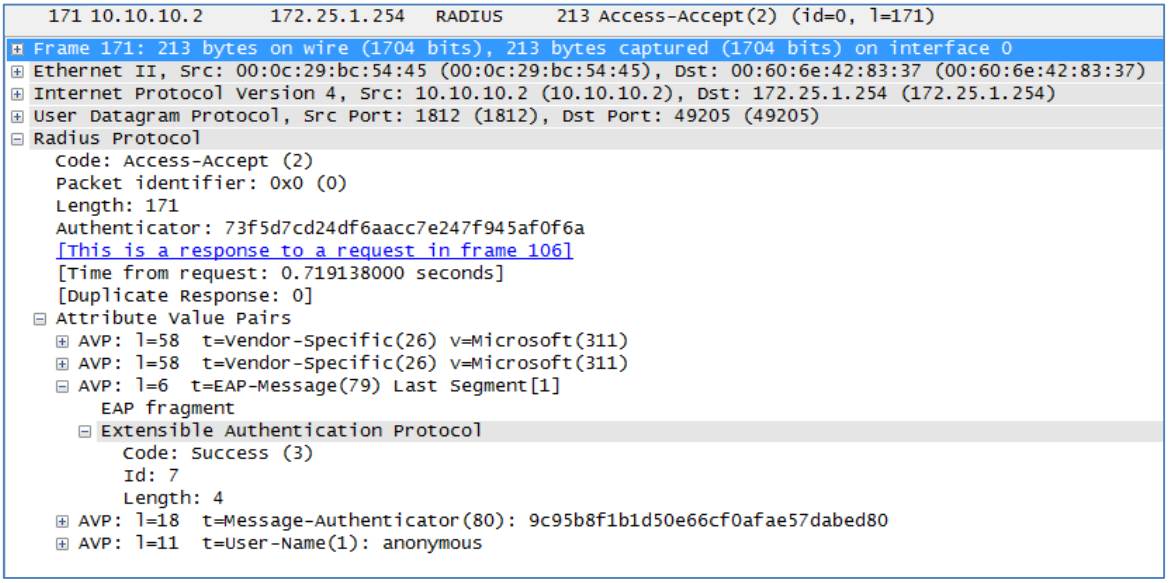


Figura 138. Paquete RADIUS Access-Accept: EAP-Success
Nota. Fuente: Captura de la interfaz gráfica Wireshark

- Finalmente, el equipo autenticador habilita el puerto de acceso y envía un paquete EAP-Success al suplicante informándole que el proceso de autenticación ha sido exitoso.

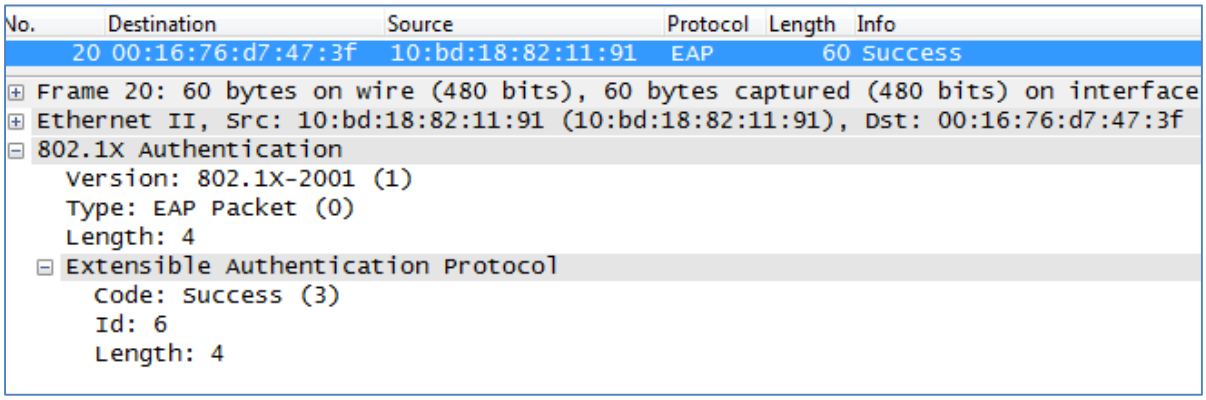


Figura 139. Paquete EAP-Success
Nota. Fuente: Captura de la interfaz gráfica Wireshark

4.8.1 PRUEBAS DE APLICACIÓN

Una vez realizado el análisis paso a paso del entramado 802.1x en una comunicación AAA, se verificó que el envío de las credenciales de acceso se realiza de forma confiable a través de una sesión segura establecida entre el dispositivo de usuario y el servidor RADIUS, usando para esto, el método de autenticación EAP-TTLS que basa su seguridad en certificados digitales.

Todos los elementos requeridos por el sistema AAA para proveer los servicios de autenticación, autorización y contabilidad a la red fueron implementados en un servidor virtualizado (PROXMOX VE) que facilitan las tareas de migración y respaldo de servidores. A continuación se muestran los resultados obtenidos de las pruebas realizadas a nivel de aplicación, ejecutadas en posibles escenarios que pudieran presentarse al momento de acceder al sistema AAA.

4.8.1.1 Autenticación de usuarios

Se denegó el acceso a todo dispositivo que intento conectarse a la red a través de un puerto configurado con 802.1x sin tener instalado el software suplicante.

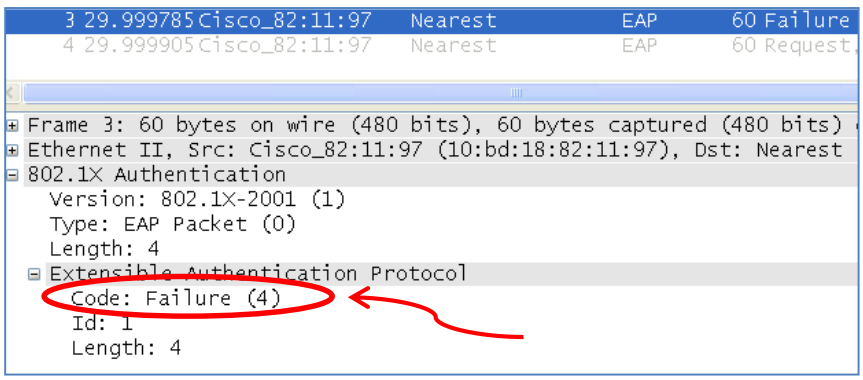


Figura 140. Acceso denegado utilizando dispositivo sin suplicante
Nota. Fuente: Captura de la interfaz gráfica Wireshark

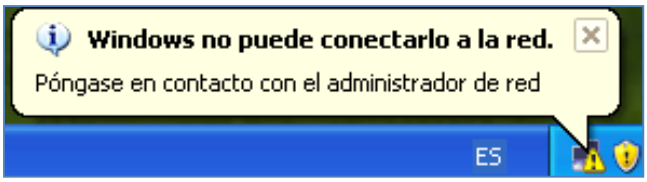


Figura 141. Acceso denegado: mensaje Windows XP
Nota. Fuente: Captura de la interfaz gráfica Windows XP

Se configuro EAP-TTLS como único método de autenticación habilitado para permitir el acceso a la red, por tal razón, las solicitudes de acceso donde se emplearon métodos de autenticación diferentes fueron bloqueadas por el servidor.

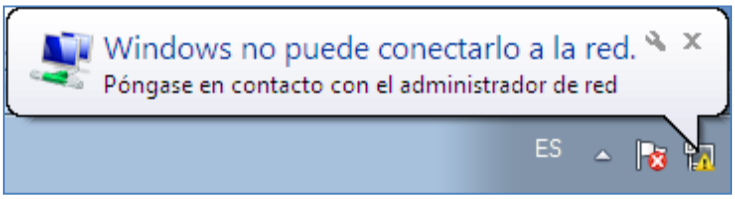


Figura 142. Acceso denegado: mensaje en Windows 7
Nota. Fuente: Captura de la interfaz gráfica Windows 7

Se intentó autenticar un dispositivo empleando el método de autenticación EAP-PEAP que es similar a EAP-TTLS, el sistema rechazo exitosamente la solicitud debido a las políticas de acceso definidas en el servidor RADIUS (ver Figura 143).

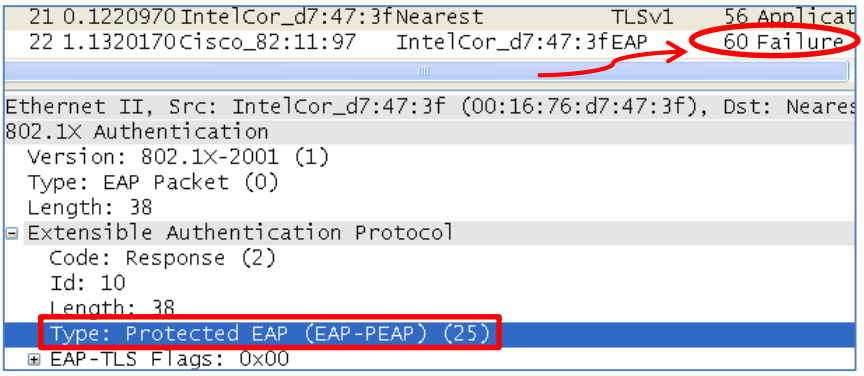


Figura 143. Autenticación fallida usando PEAP
Nota. Fuente: Captura de la interfaz gráfica Wireshark

Todos los intento de acceso utilizando credenciales de autenticación erróneas (nombre de usuario o contraseña) fueron rechazados por el servidor radius.

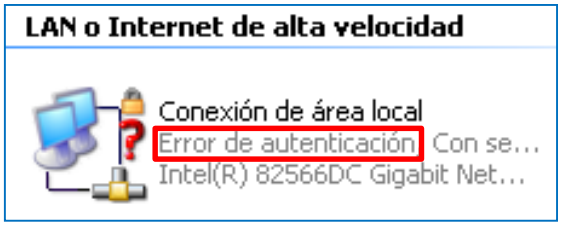


Figura 144. Fallo de autenticación: nombre de usuario o contraseña erróneos.
Nota. Fuente: Interfaz gráfica Windows XP

Cuando se habilita la verificación de certificado digital del servidor en el suplicante, se añade seguridad al proceso de autenticación, debido a que el dispositivo comprueba si el certificado digital del servidor RADIUS coincide con el instalado en su almacén de certificados raíz de confianza. Se comprobó que cuando se realiza una solicitud de acceso utilizando un certificado digital diferente al del servidor, el proceso de autenticación falla, denegando el acceso del dispositivo a la red.

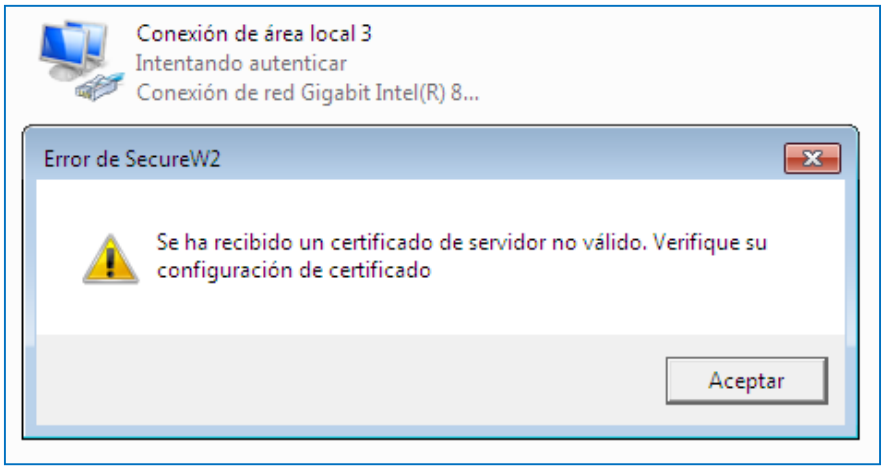


Figura 145. Error de autenticación: certificado digital de servidor RADIUS inválido.
Nota. Fuente: Captura de la interfaz gráfica Windows 7

Accedieron exitosamente todos los usuarios que cumplieron con los requerimientos de autenticación del sistema AAA. En la Figura 146 se muestra el mensaje desplegado al momento de realizar una solicitud de acceso válida, utilizando EAP-TTLS como método de autenticación.

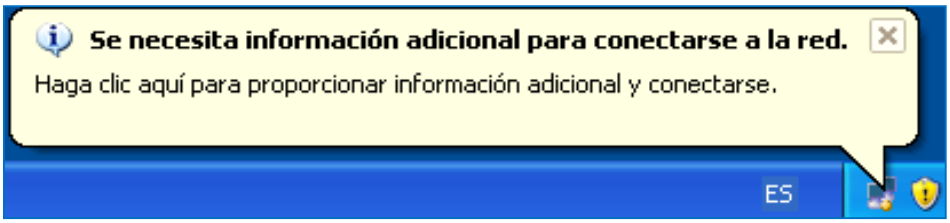


Figura 146. Mensaje de una solicitud de acceso válida utilizando EAP-TTLS
Nota. Fuente: Captura de la interfaz gráfica Windows XP

Los parámetros que se configuraron en el dispositivo para acceder a la red de forma correcta se muestran en la siguiente lista.

- Software suplicante instalado en el dispositivo de usuario con soporte 802.1x.
- Configuración de EAP-TTLS como método de autenticación a la red.
- Certificado digital del servidor RADIUS instalado en el almacén de certificados raíz de confianza del dispositivo.
- Credenciales de autenticación válidas (nombre de usuario y contraseña).

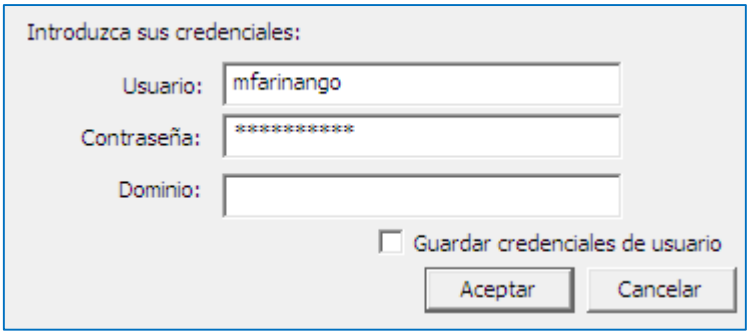


Figura 147. Ingreso de credenciales de autenticación al sistema AAA.
Nota. Fuente: Captura de la interfaz gráfica Secure W2.

4.8.1.2 Autorización de servicios a usuarios autenticados

La asignación de recursos de red se realizado de manera automática mediante la asignación dinámica de VLAN, usando el mismo dispositivo de red se autenticó a dos usuarios diferentes. Como resultado, cada usuario obtuvo una dirección IP dentro de una distinta subred, logrando que los recursos se trasladen de forma dinámica de acuerdo al ID de usuario utilizado en el proceso de autenticación.

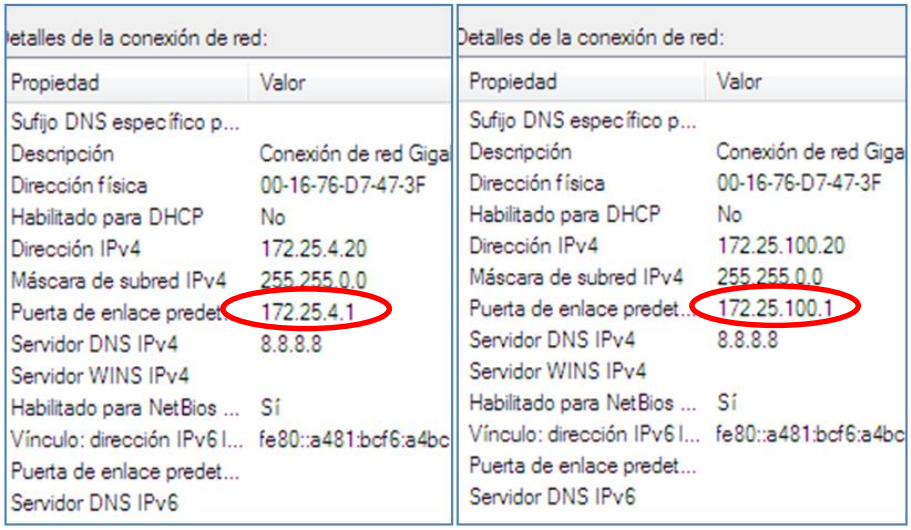


Figura 148. Autenticación de distintos usuarios en el mismo dispositivo.
Nota. Fuente: Captura de la interfaz gráfica: conexiones de red en Windows 7

Administración de recursos centralizada: Fue posible modificar las políticas de acceso definidas para un usuario sin la necesidad de realizar cambios en el firewall o en la infraestructura de red, esto es importante cuando un trabajador se traslada o cambian el área de trabajo. Simplemente, se modifica el ID de VLAN en el directorio LDAP y la próxima vez que el usuario se autentique accederá con nuevos privilegios a la red.

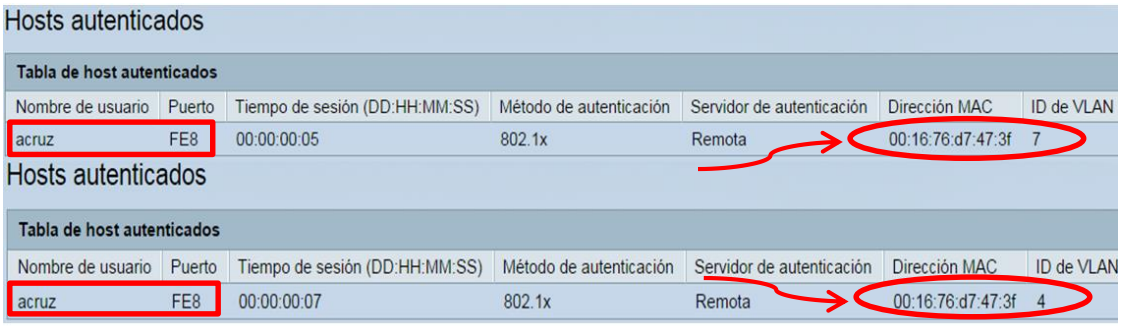


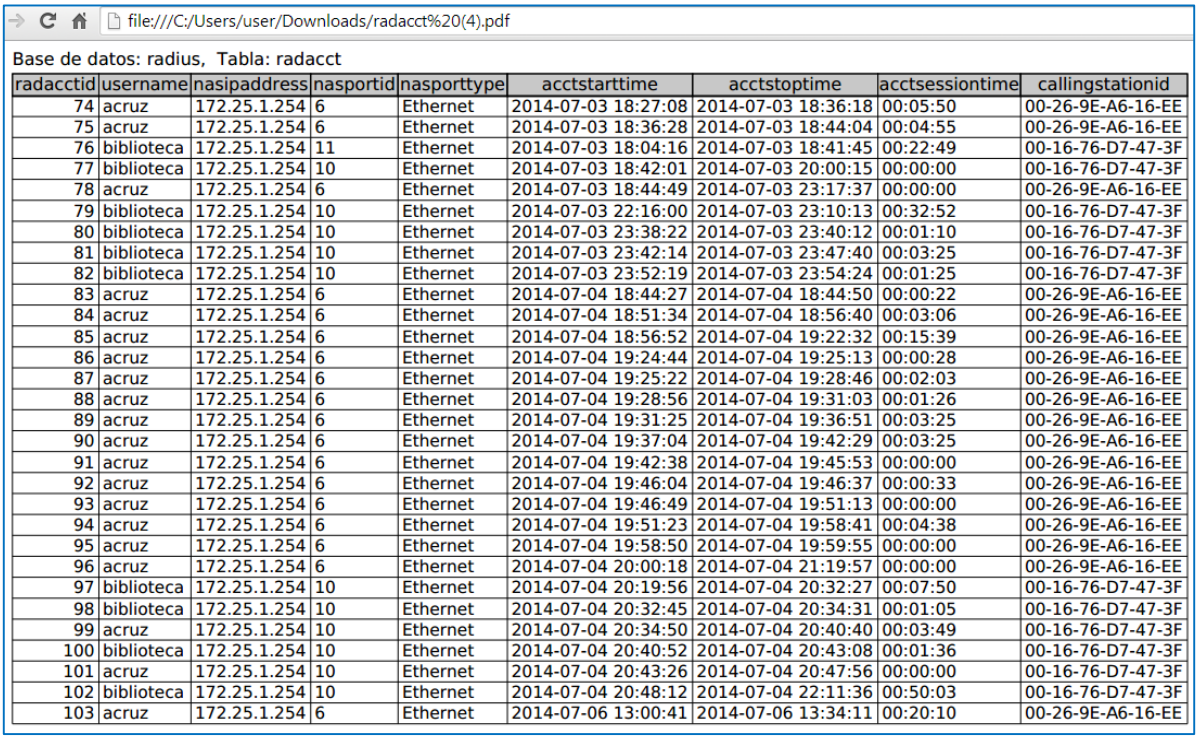
Figura 149. Modificación dinámica de políticas de acceso
Nota. Fuente: Captura de la interfaz gráfica: Hosts autenticados en switch CISCO SF-300

De acuerdo a las políticas de red definidas para cada grupo de usuarios (VLAN), se restringió la navegación a ciertas páginas web mediante el uso del proxy (modo transparente). Adicionalmente, las reglas de acceso al servicio de voz IP, la administración web del entorno de virtualización y los servidores AAA fueron controladas de manera exitosa por el firewall.

Figura 150. Bloqueo de páginas web mediante proxy transparente.
Nota. Fuente: Captura de la interfaz gráfica del navegador google chrome.

4.8.1.3 Contabilidad: Registro de información

El servicio de contabilidad funcionó correctamente, registrando en la base de datos MySQL toda la información de acceso generada por el usuario al momento de autenticarse. Se obtuvo datos como: ID de usuario autenticado, dirección MAC del dispositivo, equipo autenticador de acceso a la red (NAS) utilizado, hora de inicio y fin de sesión.



file:///C:/Users/user/Downloads/radacct%20(4).pdf

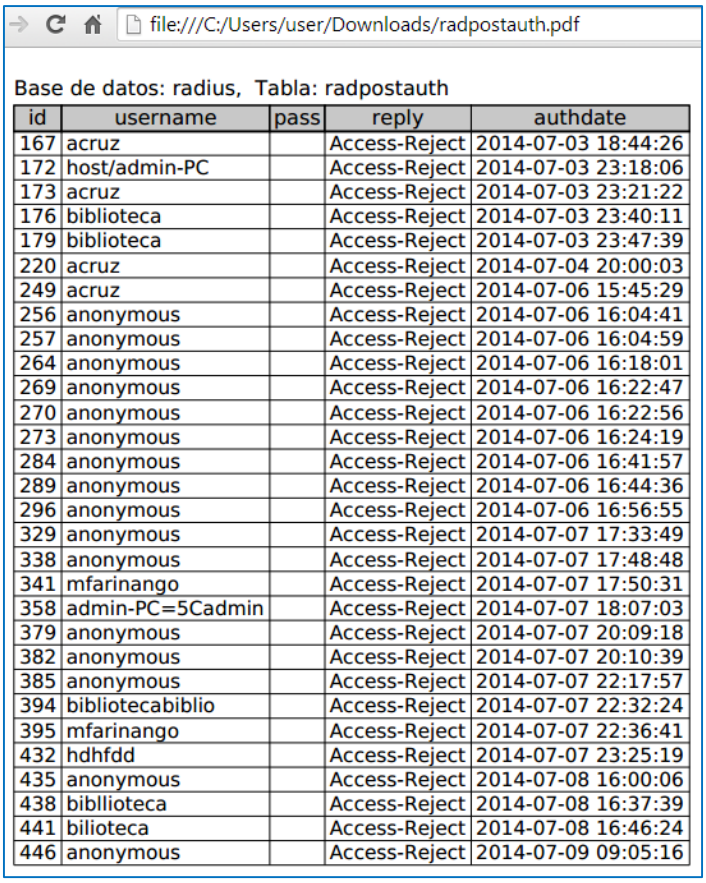
Base de datos: radius, Tabla: radacct

radacctid	username	nasipaddress	nasportid	nasporttype	acctstarttime	acctstoptime	acctsessiontime	callingstationid
74	acruz	172.25.1.254	6	Ethernet	2014-07-03 18:27:08	2014-07-03 18:36:18	00:05:50	00-26-9E-A6-16-EE
75	acruz	172.25.1.254	6	Ethernet	2014-07-03 18:36:28	2014-07-03 18:44:04	00:04:55	00-26-9E-A6-16-EE
76	biblioteca	172.25.1.254	11	Ethernet	2014-07-03 18:04:16	2014-07-03 18:41:45	00:22:49	00-16-76-D7-47-3F
77	biblioteca	172.25.1.254	10	Ethernet	2014-07-03 18:42:01	2014-07-03 20:00:15	00:00:00	00-16-76-D7-47-3F
78	acruz	172.25.1.254	6	Ethernet	2014-07-03 18:44:49	2014-07-03 23:17:37	00:00:00	00-26-9E-A6-16-EE
79	biblioteca	172.25.1.254	10	Ethernet	2014-07-03 22:16:00	2014-07-03 23:10:13	00:32:52	00-16-76-D7-47-3F
80	biblioteca	172.25.1.254	10	Ethernet	2014-07-03 23:38:22	2014-07-03 23:40:12	00:01:10	00-16-76-D7-47-3F
81	biblioteca	172.25.1.254	10	Ethernet	2014-07-03 23:42:14	2014-07-03 23:47:40	00:03:25	00-16-76-D7-47-3F
82	biblioteca	172.25.1.254	10	Ethernet	2014-07-03 23:52:19	2014-07-03 23:54:24	00:01:25	00-16-76-D7-47-3F
83	acruz	172.25.1.254	6	Ethernet	2014-07-04 18:44:27	2014-07-04 18:44:50	00:00:22	00-26-9E-A6-16-EE
84	acruz	172.25.1.254	6	Ethernet	2014-07-04 18:51:34	2014-07-04 18:56:40	00:03:06	00-26-9E-A6-16-EE
85	acruz	172.25.1.254	6	Ethernet	2014-07-04 18:56:52	2014-07-04 19:22:32	00:15:39	00-26-9E-A6-16-EE
86	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:24:44	2014-07-04 19:25:13	00:00:28	00-26-9E-A6-16-EE
87	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:25:22	2014-07-04 19:28:46	00:02:03	00-26-9E-A6-16-EE
88	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:28:56	2014-07-04 19:31:03	00:01:26	00-26-9E-A6-16-EE
89	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:31:25	2014-07-04 19:36:51	00:03:25	00-26-9E-A6-16-EE
90	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:37:04	2014-07-04 19:42:29	00:03:25	00-26-9E-A6-16-EE
91	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:42:38	2014-07-04 19:45:53	00:00:00	00-26-9E-A6-16-EE
92	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:46:04	2014-07-04 19:46:37	00:00:33	00-26-9E-A6-16-EE
93	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:46:49	2014-07-04 19:51:13	00:00:00	00-26-9E-A6-16-EE
94	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:51:23	2014-07-04 19:58:41	00:04:38	00-26-9E-A6-16-EE
95	acruz	172.25.1.254	6	Ethernet	2014-07-04 19:58:50	2014-07-04 19:59:55	00:00:00	00-26-9E-A6-16-EE
96	acruz	172.25.1.254	6	Ethernet	2014-07-04 20:00:18	2014-07-04 21:19:57	00:00:00	00-26-9E-A6-16-EE
97	biblioteca	172.25.1.254	10	Ethernet	2014-07-04 20:19:56	2014-07-04 20:32:27	00:07:50	00-16-76-D7-47-3F
98	biblioteca	172.25.1.254	10	Ethernet	2014-07-04 20:32:45	2014-07-04 20:34:31	00:01:05	00-16-76-D7-47-3F
99	acruz	172.25.1.254	10	Ethernet	2014-07-04 20:34:50	2014-07-04 20:40:40	00:03:49	00-16-76-D7-47-3F
100	biblioteca	172.25.1.254	10	Ethernet	2014-07-04 20:40:52	2014-07-04 20:43:08	00:01:36	00-16-76-D7-47-3F
101	acruz	172.25.1.254	10	Ethernet	2014-07-04 20:43:26	2014-07-04 20:47:56	00:00:00	00-16-76-D7-47-3F
102	biblioteca	172.25.1.254	10	Ethernet	2014-07-04 20:48:12	2014-07-04 22:11:36	00:50:03	00-16-76-D7-47-3F
103	acruz	172.25.1.254	6	Ethernet	2014-07-06 13:00:41	2014-07-06 13:34:11	00:20:10	00-26-9E-A6-16-EE

Figura 151. Registro de datos de autenticación de usuarios del sistema AAA.
Nota. Fuente: Captura de la interfaz gráfica del servidor MySQL

Finalmente, se realizaron varias consultas en la base de datos MySQL para obtener un registro resumido de todos los intentos de acceso fallidos al sistema AAA. En la Figura 152 se muestra el resultado de la consulta SQL.

```
SELECT *
FROM radpostauth
WHERE (`radpostauth`.`reply` LIKE '%Reject%');
```



Base de datos: radius, Tabla: radpostauth

id	username	pass	reply	authdate
167	acruz		Access-Reject	2014-07-03 18:44:26
172	host/admin-PC		Access-Reject	2014-07-03 23:18:06
173	acruz		Access-Reject	2014-07-03 23:21:22
176	biblioteca		Access-Reject	2014-07-03 23:40:11
179	biblioteca		Access-Reject	2014-07-03 23:47:39
220	acruz		Access-Reject	2014-07-04 20:00:03
249	acruz		Access-Reject	2014-07-06 15:45:29
256	anonymous		Access-Reject	2014-07-06 16:04:41
257	anonymous		Access-Reject	2014-07-06 16:04:59
264	anonymous		Access-Reject	2014-07-06 16:18:01
269	anonymous		Access-Reject	2014-07-06 16:22:47
270	anonymous		Access-Reject	2014-07-06 16:22:56
273	anonymous		Access-Reject	2014-07-06 16:24:19
284	anonymous		Access-Reject	2014-07-06 16:41:57
289	anonymous		Access-Reject	2014-07-06 16:44:36
296	anonymous		Access-Reject	2014-07-06 16:56:55
329	anonymous		Access-Reject	2014-07-07 17:33:49
338	anonymous		Access-Reject	2014-07-07 17:48:48
341	mfarinango		Access-Reject	2014-07-07 17:50:31
358	admin-PC=5Cadmin		Access-Reject	2014-07-07 18:07:03
379	anonymous		Access-Reject	2014-07-07 20:09:18
382	anonymous		Access-Reject	2014-07-07 20:10:39
385	anonymous		Access-Reject	2014-07-07 22:17:57
394	bibliotecabiblio		Access-Reject	2014-07-07 22:32:24
395	mfarinango		Access-Reject	2014-07-07 22:36:41
432	hdhfdd		Access-Reject	2014-07-07 23:25:19
435	anonymous		Access-Reject	2014-07-08 16:00:06
438	biblioteca		Access-Reject	2014-07-08 16:37:39
441	bilioteca		Access-Reject	2014-07-08 16:46:24
446	anonymous		Access-Reject	2014-07-09 09:05:16

Figura 152. Registro de intentos de accesos rechazados
Nota. Fuente: Captura de la interfaz gráfica del servidor MySQL

Todas las pruebas de acceso a la red con servicio AAA mostradas, se realizaron empleando los sistemas operativos que actualmente tienen los equipos del GAD Municipal San Miguel de Urcuquí, entre ellos: Windows XP, Windows 7 y Android.

CAPÍTULO V

ANÁLISIS COSTO - BENEFICIO

5.1 ANÁLISIS COSTO-BENEFICIO

Cuando se plantea soluciones de seguridad para la información y las redes de datos, medir con precisión el costo beneficio resulta una tarea un tanto compleja, debido a que esta clase de proyectos representan una inversión que no proporciona beneficios económicos, pero si, la prevención de pérdidas.

El análisis costo-beneficio del sistema AAA para la red de datos del GAD Municipal San Miguel de Urcuqui se realiza mediante el método ROSI[57] (Return on Security Investment).

5.2 REQUERIMIENTOS PARA EL CÁLCULO ROSI

El retorno de la inversión en seguridad se emplea para determinar la viabilidad de un proyecto, los términos manejados en el cálculo de ROSI son: disminución de riesgo y costo.

La disminución del riesgo se asume como el beneficio de la solución en seguridad y el costo representa el valor total requerido para implantar el sistema.

[57] ROSI. Retorno sobre la inversión de seguridad.

5.2.1 ROI (Return on investment)

El retorno de la inversión es el beneficio obtenido de una inversión en relación con los costos que ésta representa, expresado como un porcentaje. El ROI no implica necesariamente dinero, sin embargo, con frecuencia lo más práctico es expresar las unidades en términos monetarios, para facilitar así la comparación.

El cálculo del ROI se realiza empleando la ecuación mostrada en la Figura 153.

$$ROI = \frac{Gain\ from\ investment - Cost\ of\ investment}{Cost\ of\ investment}$$

Figura 153. Ecuación del Retorno de inversión (ROI)
Nota. Fuente: ENISA European Network and Information Security (2012). *Introduction to Return on Security Investment (p. 2).* Recuperado de http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

5.2.2 ROSI

El concepto para el cálculo del ROI se aplica a todas las inversiones, cuando se trata de seguridad se emplea ROSI (retorno de la inversión de seguridad). El método para el cálculo del retorno de la inversión (ROI) no es apropiado usarlo en la medición de soluciones relacionadas con la seguridad.

La seguridad, generalmente, no es una inversión que genere un beneficio económico, se trata de prevenir pérdidas. En otras palabras, cuando se invierte en seguridad, las instituciones no esperan ganancias, el objetivo es reducir los riesgos que amenazan los activos. Con este enfoque, la evaluación del rendimiento de la inversión de seguridad se realiza mediante el cálculo de la cantidad de pérdida que evitó gracias a la inversión.

5.3 METODOLOGÍA PARA EL CÁLCULO DEL ROSI

El análisis de la inversión en seguridad implica la evaluación de la cantidad de pérdida potencial que se podría evitar, por lo tanto, el valor monetario de la inversión tiene que ser comparado con el valor monetario de la reducción de riesgos. Este valor monetario se puede estimar mediante una evaluación cuantitativa del riesgo.

Los conceptos que se deben tomar en cuenta a la hora de cuantificar los riesgos son: SLE (Expectativa de pérdida por evento), ARO (Tasa anual de ocurrencia) y ALE (Expectativa de pérdida anual).

5.3.1 SLE (Expectativa de pérdida por evento)

SLE es la cantidad esperada de dinero, que se pierde cuando se produce una situación de riesgo. Debido a la naturaleza de un incidente cibernético, la mayor complejidad es identificar todos los activos sobre los cuales el incidente produce un impacto.

Por ejemplo, cuando un portátil es robado en una empresa, no sólo se pierde el valor monetario de la propia computadora, sino también la institución pierde: productividad, reputación y seguramente el costo de la pérdida de la propiedad intelectual.

El costo total de un incidente debe incluir el costo de las pérdidas directas (por ejemplo: el tiempo de inactividad del servicio, el reemplazo de hardware, reemplazo de la pérdida de datos, etc.) y el costo de los efectos indirectos (tiempo de investigación, pérdida de la reputación, etc.)

No hay valores universales para la expectativa de pérdida por evento (SLE). Lo que se incluye en el cálculo de SLE depende exclusivamente de la institución. Una entidad puede estimar el valor SLE de un ordenador portátil robado, como el valor propio de la computadora (por ejemplo, 2.000 dólares), mientras que otra organización que trata con información altamente sensible podría valorar esta pérdida en 50.000 dólares, debido a que afectaría su imagen, sus posibles contratos y su ventaja competitiva.

5.3.2 ARO (Tasa anual de ocurrencia)

ARO (Annual Rate of Occurrence) es la probabilidad de que un riesgo ocurra en un año, estos datos son una aproximación y dependen de muchos factores.

Por ejemplo: la probabilidad de un fallo en el disco está influenciada por la temperatura de funcionamiento, un robo dependerá de la ubicación de la de activos, un ataque de código malicioso disminuye significativamente con la implementación de un antivirus eficaz, etc.

5.3.3 ALE (Expectativa de pérdida anual)

ALE (Annual Loss Expectancy) es la pérdida económica anual que se produce a causa de un riesgo específico afectando a un activo específico. Se calcula usando la ecuación mostrada en la Figura 154.

$$ALE = ARO * SLE$$

Figura 154. Fórmula del ALE

5.4 CÁLCULO DE ROSI

El cálculo de ROSI combina el análisis cuantitativo de los riesgos y el costo de implementación del sistema de seguridad. La ecuación general requerida para el cálculo de ROSI se muestra en la Figura 155.

$$ROSI = \frac{Monetary\ loss\ reduction - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

Figura 155. Fórmula para el cálculo de ROSI
Nota. Fuente: ENISA European Network and Information Security (2012). *Introduction to Return on Security Investment (p. 5).* Recuperado de http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

La implementación de un sistema de seguridad eficaz reduce el ALE, cuanto más efectiva es la solución, más se reduce la pérdida económica anual.

Para calcular el valor del retorno sobre la inversión en seguridad (ROSI) se utiliza la herramienta de software proporcionada por el estándar ISO 27001, la cual es gratuita y se puede acceder a través del enlace http://www.iso27001standard.com/es/rosi/return-on-security-investment

5.4.1 Cálculo del costo de un incidente

El primer paso para el cálculo del retorno de la inversión en seguridad es determinar el costo de un incidente, los parámetros requeridos por la calculadora ROSI de la ISO 27001 y sus respectivos valores se detallan en la Tabla 23 y 24.

Tabla 23. Parámetros para el cálculo del costo de un incidente

PARÁMETROS DE UN INCIDENTE	VALOR
Sector del incidente	Telecomunicaciones
Tipo de incidente	Actividad Maliciosa
Descripción del incidente potencial	Acceso no autorizada
Medidas de seguridad existentes	Ninguna
¿Cuánto tiempo durarían las consecuencias negativas de este incidente?	1 día
¿Cuánto tiempo durarían las consecuencias negativas de este incidente?	Infraestructura de red
Procesos comerciales que serían afectados por este incidente	Ninguna
Datos que serían afectados por este incidente	Conectividad de red
Activos físicos que serían afectados por este incidente	Dispositivos de red

Nota. Fuente: Adaptado de http://www.iso27001standard.com/es/herramientas/rosi/

Tabla 24. Cálculo del costo de un incidente

PARÁMETROS DE UN INCIDENTE	VALOR (USD)
Costo de servicios externos:	1000
Costo de adquisición de equipamiento, bienes o materiales	0
Costos de empleados para la resolución del incidente	500
Multas legales y/o contractuales	0
Descripción de otros gastos no mencionados anteriormente	0
Descripción de otros gastos no mencionados anteriormente	0
Margen promedio de sus ingresos (% de sus ingresos)	0
Ingresos perdidos de clientes actuales	0
Ingresos perdidos de clientes potenciales	0
Reclamaciones de seguro	0
Costo total de un incidente = Expectativa de pérdida por evento (SLE)	**1500**

Nota. Fuente: Adaptado de http://www.iso27001standard.com/es/herramientas/rosi/

El software calcula el costo de la expectativa de pérdida por evento (SLE) automáticamente en la moneda seleccionada.

SLE = Costo de servicios externos + Costos de adquisición + Costos de empleados + Multas + Otros gastos - Reclamaciones de seguro + (Ingresos perdidos de clientes actuales + Ingresos perdidos de clientes potenciales) * Margen promedio.

Finalmente, se calcula la expectativa de pérdida anual (ALE) para el incidente. La probabilidad de que ocurra el incidente se estableció cada 3 meses.

Por lo tanto, ALE = SLE*Probabilidad = 1500*4 = **6000 USD.**

5.4.2 Cálculo de los costos de la protección

Si el costo anual de las medidas de seguridad que se implementan para mitigar los costos de un incidente es menor que la Expectativa de pérdida anual (ALE), entonces las medidas de seguridad serán rentables.

En la Tabla 25, se detallan los valores usados en el software para el cálculo de los costos de la protección.

Tabla 25. Cálculo de la Expectativa de pérdida anual (ALE)

PARÁMETROS DE LA PROTECCIÓN	VALOR
Descripción de medidas de seguridad	Servidor AAA
Frecuencia del incidente después de aplicar las medidas de seguridad	Una vez por año
Porcentaje de reducción del Costo total de un incidente	75 %
Valor de adquisición de medidas de seguridad	3000 USD
¿Por cuántos años se utilizarán estas medidas de seguridad?	10
Valor de las medidas de seguridad luego de su utilización	0 USD

Costos anuales de entidades externas necesarias para las medidas de seguridad	1000 USD
Cantidad anual de días-hombre necesarias para las medidas de seguridad	1
Costo promedio anual de un empleado	9000 USD
Cantidad de días laborales anuales por un empleado	250
Monto total de otros gastos de protección	0 USD
Costo anual de las medidas de seguridad	**1336.00 USD**

Nota. Fuente: Adaptado de http://www.iso27001standard.com/es/herramientas/rosi/

5.4.3 Análisis costo beneficio de la solución

Para el análisis costo beneficio de la solución es necesario volver a calcular el costo total del incidente (SLE) y la expectativa de pérdida anual (ALE) luego de aplicadas las medidas de seguridad. Si el valor del retorno de la inversión en seguridad (ROSI) es positivo es rentable la solución.

- **Costo total de un incidente (SLE), luego de aplicadas las medidas de seguridad.**

SLE (con las medidas de seguridad aplicadas) = SLE (inicial, sin medidas de seguridad) * (100 - % de reducción de SLE)

SLE (con las medidas de seguridad aplicadas) = (1500) * ((100 – 75)/100)

SLE (con las medidas de seguridad aplicadas) = (1500) * ((100 – 75)/100)

SLE (con las medidas de seguridad aplicadas) = **375**

- **Exposición al riesgo en un año para este incidente (ALE), luego de aplicadas las medidas de seguridad.**

ALE = SLE (con las medidas de seguridad aplicadas) * Frecuencia del incidente (con las medidas de seguridad aplicadas)

ALE = (375) * (1) = **375**

- **Reducción del riesgo.**

La reducción del riesgo es la reducción de la exposición al riesgo en un año (ALE) como consecuencia de la aplicación de las medidas de seguridad.

Reducción del riesgo = ALE (inicial, sin medidas de seguridad) - ALE (con las medidas de seguridad aplicadas)

Reducción del riesgo = 6000 – 375 = **5625.00**

- **Retorno sobre la Inversión en Seguridad (ROSI) – en valores absolutos.**

El valor del beneficio anual generado por la inversión en medidas de seguridad que se obtiene se muestra a continuación.

ROSI = reducción de riesgo monetario - costo anual de protección

ROSI = 5625.00 - 1336.00 = **4289.00**

- **Retorno sobre la Inversión en Seguridad (ROSI) – en porcentaje de costos de protección.**

El beneficio presentado como porcentaje sobre el costo de las medidas de seguridad es el siguiente.

ROSI (porcentaje) = ROSI (valores absolutos) / costo anual de protección * 100%

ROSI (porcentaje) = (4289.00/1336.00)*100%

ROSI (porcentaje) = **321.03%**

Considerando que los valores obtenidos del cálculo del retorno de la inversión en seguridad son positivos y en base al análisis realizado, se puede determinar que la implementación del sistema de control de acceso y administración de recursos de red en el GAD Municipal San Miguel de Urcuqui es viable, debido a que, con una baja inversión se obtiene un nivel de seguridad elevado para toda la infraestructura de red de la institución.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

Con la implementación del servidor AAA utilizando software libre se logró controlar el acceso a todos los usuarios de forma centralizada y la asignación dinámica de recursos de red se realizó exitosamente de acuerdo al rol que desempeña cada trabajador dentro de la institución, obteniendo una relación costo beneficio positiva que garantiza la viabilidad del proyecto.

- Se determinó el método de autenticación EAP-TTLS como el más adecuado y seguro para implementar el sistema AAA en el GAD Municipal de San Miguel de Urcuquí, que a través de un canal seguro establecido mediante certificados digitales garantizan la confidencialidad de los datos en el proceso de autenticación.

- Integrando el servidor RADIUS con el directorio LDAP se logró una administración centralizada del sistema AAA, sincronizando las cuentas de usuario de autenticación con los privilegios de acceso para el proceso autorización.

- Se denegó el acceso a todos los usuarios que no cumplieron con los requerimientos de autenticación y se asignó de manera dinámica los recursos de red utilizando redes virtuales (VLAN) dinámicas.

- Los tres servidores usados para proveer el servicio de autenticación, autorización y auditoria en la red del GADMU se instalaron sobre el entorno de virtualización PROXMOX, lo cual garantiza una reducción de costos significativa al momento de su implementación.

- Cuando se utiliza un directorio LDAP para almacenar las credenciales de usuario, el sistema automáticamente almacena las contraseñas de usuario usando algoritmos hash, debido a que estos hash son irreversibles es necesario elegir PAP como método de autenticación interno dentro del túnel TLS.

- La información de contabilidad es posible registrar en una base de datos relacional SQL únicamente cuando el equipo autenticador (router inalámbrico o switch) es capaz de enviar los datos relacionados con la contabilidad 802.1x, caso contrario el administrador de red tiene la posibilidad de administrar el servicio usando los registros log por defecto generados por el servidor FreeRADIUS.

- Los equipos autenticadores usados en la implementación del sistema, soportan el servicio de contabilidad 802.1x, lo que permitió registrar en la base de datos MYSQL toda la información referente a los usuarios que accedieron al sistema correctamente y los intentos fallidos de conexión, detallando el día y la hora de dicho acceso o rechazo.

- En las pruebas de acceso se utilizó el sistema operativo Windows 7 debido a que no tiene soporte nativo para el método de autenticación EAP-TTLS y se debe instalar un suplicante para añadir la funcionalidad, el software empleado fue SecureW2.

- La asignación dinámica de VLAN se lo hizo a través del directorio LDAP, para que un puerto del switch pueda moverse dinámicamente entre una y otra red virtual se debe configurar en modo general, si el puerto está en modo acceso es miembro sin etiquetar de una sola VLAN por lo que no se puede unir a redes diferentes.

- Se pudo comprobar que los recursos de hardware utilizados mientras el servidor AAA está funcionando son bajos, lo que facilita la implementación del servicio en un hardware de bajo costo, sin limitar las características y funcionalidades del servidor AAA.

6.2 RECOMENDACIONES

- El costo de implementación del servicio AAA se limita en gran medida a los equipos autenticadores de la red, es decir los equipos que ofrecen el servicio de acceso, como son: switch y router inalámbrico, es indispensable verificar que los dispositivos soporten el servicio 802.1x antes de planear su implementación.

- Promover el uso del software libre en los proyectos universitarios por las ventajas que proporciona, como: bajo costo, soporte continuo por parte de la comunidad, libertad de controlar los sistemas de acuerdo a sus propias configuraciones y requerimientos, etc.

- La revisión de los privilegios de acceso de los usuarios se recomienda hacer cada seis meses, en caso de existir alguna modificación o cambio de personal dentro de la misma organización se debe reasignar los privilegios, para los usuarios que dejan de

utilizar el directorio LDAP se debe eliminar sus registros con el fin de facilitar la administración del sistema.

- Se debe aislar totalmente a los usuarios de la red cableada e inalámbrica, debido a las vulnerabilidades que por naturaleza tiene una red wireless a través de reglas y políticas que se deben definir en el firewall de red.

- Para que el sistema AAA brinde una seguridad robusta se debe capacitar a los usuarios que usarán el servicio mediante la socialización de las políticas de seguridad de acceso a la red sugeridas en el capítulo dos.

- En un sistema de producción con muchos usuarios se debe monitorear periódicamente el consumo de recursos de los servidores RADIUS, LDAP y MYSQL para evitar que el sistema de virtualización falle debido a sobrecargas.

- En entornos de producción se recomienda manejar redundancia a nivel de servidores, puesto que se trata de un sistema integral que trabaja en conjunto y la falla de cualquier elemento AAA generaría la denegación de acceso de todos los usuarios a la red.

- Se recomienda la implementación del sistema AAA en las empresas con redes cableadas o inalámbricas que requieran controlar el acceso de los usuarios y evitar accesos no autorizados a los recursos de red para garantizar un nivel elevado de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control. (2 de Febrero de 2010). Obtenido de IEEE Std 802.1X-2010: http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H. (Junio de 2004). *Extensible Authentication Protocol (EAP).* Obtenido de http://tools.ietf.org/pdf/rfc3748.pdf

Butcher, M. (2007). *Mastering OpenLDAP: Configuring, Securing, and Integrating Directory Services.* Reino Unido: Birmingham: Packt Publishing Ltd.

CISCO. (2008). *CCNA 3 Exploration 4.0: Conmutación y conexión inalámbrica de LAN*. Obtenido de http://es.scribd.com/doc/17481738/Cisco-CCNA-3-Exploration-Conmutacion-y-Conexion-Inalambrica-de-Lan-Version-40-Espanol-

CISCO. (2012). *Cisco Small Business 200 Series Smart Switches*. Obtenido de http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps11229/data_sheet_c78-634369_Spanish.pdf

Cisco Systems, I. (10 de Diciembre de 2008). *Cisco IOS Security Configuration Guide: Release 12.4*. Obtenido de http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.pdf

Cole, E., Krutz, R., & Conley, J. (2009). *Network Security Bible* (2nd ed.). Indianapolis: Wiley Publishing, Inc.

Coleman, D., Westcott, D., Harkins, B., & Jackman, S. (2010). *Certified Wireless Security Professional Official Study Guide.* Indianapolis: Wiley Publishing, Inc.

Congdon, P., & Packard, H. (Marzo de 2000). *IEEE 802.1X Overview: Port Based Network Access*. Obtenido de http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF

Cudbard-Bell, A. (15 de Septiembre de 2012). *wiki.freeRADIUS*. Obtenido de protocol/EAP PEAP: http://wiki.freeradius.org/protocol/EAP-PEAP

Fernández, Y., Ramos, A., & García, J. (2008). *RADIUS / AAA / 802.1X : Sistemas basados en la autenticación en Windows y GNU/Linux*. Madrid: RA-MA Editorial.

Funk, P., & Blake, S. (Agosto de 2008). *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0).* Obtenido de http://tools.ietf.org/pdf/rfc5281.pdf

GADMU. (Marzo de 2011). *Misión Cantonal*. Obtenido de http://www.municipiourcuqui.gob.ec/munurcuqui/index.php/2012-10-01-19-49-35/vision-y-mision

Gast, M. (2005). *802.11 Wireless Networks: The Definitive Guide, 2nd Edition.* United States of America: O'Reilly Media, Inc.

Geier, J. (2008). *Implementing 802.1X Security Solutions for Wired and Wireless Networks.* Indianapolis: Wiley Publishing, Inc.

Hewlett-Packard. (Marzo de 2009). *HP ProLiant ML150 G6 Server.* Obtenido de http://h18004.www1.hp.com/products/quickspecs/ds_00148/ds_00148.pdf

Hewlett-Packard. (Abril de 2010). *HP ProLiant DL380 G7 Server.* Obtenido de http://www.rorke.com/wp-content/uploads/2013/04/DLseriesserver.pdf

Howes, T., Smith, M., & Good, G. (2003). *Understanding and Deploying LDAP Directory Services* (2nd ed.). Boston: Pearson Education, Inc.

ISO-27002. (2005). *PORTAL DE SOLUCIONES TÉCNICAS Y ORGANIZATIVAS A LOS CONTROLES DE ISO/IEC 27002*. Obtenido de https://iso27002.wiki.zoho.com/

Jackiewicz, T. (2005). *Deploying OpenLDAP*. United States of America: Apress L. P.

Juniper-Networks. (Septiembre de 2010). *802.1X: Port-Based Authentication standard for network access control (NAC).* Obtenido de http://www.juniper.net/us/en/local/pdf/whitepapers/2000216-en.pdf

Nakhjiri, M., & Nakhjiri , M. (2005). *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility.* USA: John Wiley & Sons Ltd. doi: 10.1002/0470017465.

Postel, J. (28 de Agosto de 1980). *User Datagram Protocol.* Obtenido de http://tools.ietf.org/pdf/rfc768.pdf

Rigney, C. (Junio de 2000). *RADIUS Accounting.* Obtenido de http://tools.ietf.org/pdf/rfc2866.pdf

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (Junio de 2000). *Remote Authentication Dial In User Service (RADIUS).* Obtenido de http://tools.ietf.org/pdf/rfc2865.pdf

Simon, D., Aboba, B., & Hurst, R. (Marzo de 2008). *The EAP-TLS Authentication Protocol.* Obtenido de http://tools.ietf.org/pdf/rfc5216.pdf

Thomas, T. (30 de Diciembre de 2004). *Network Security First-Step.* Indianapolis: Cisco Press.

TRENDnet. (2013). *Especificaciones técnicas TEW-652BRP*. Obtenido de http://www.trendnet.com/langsp/products/proddetail.asp?prod=185_TEW-652BRP&cat=166

Tuttle, S., Ehlenberger, A., Gorthi, R., Leiserson, J., Macbeth, R., Owen, N., . . . Yang, C. (2004). *Understanding LDAP Design and Implementation* (2nd ed.). IBM Redbook Publication.

GLOSARIO DE TÉRMINOS

AAA: Autenticación, Autorización y Contabilidad.

ALE: Expectativa de pérdida anual.

ARO: Tasa anual de ocurrencia.

AVP: Método de encapsulación de información usado en una comunicación RADIUS

ATM: Cajero automático.

CA: Autoridad Certificadora es una entidad que emite certificados digitales.

CHAP: Protocolo de autenticación basado en un sistema desafío-respuesta.

CISCO: Empresa multinacional dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

CNT EP: Corporación Nacional de Telecomunicaciones.

CONMUTADOR: Dispositivo digital lógico de interconexión de redes de computadoras.

DATOS: Aplicación informática para almacenamiento de información de forma organizada.

DMZ: Zona desmilitarizada.

DN: Nombre distinguido.

EAP: Protocolo de autenticación extensible.

EAPOL: EAP over LAN – definido en el estándar IEEE 802.1x.

GAD: Gobierno Autónomo Descentralizado.

GPL: Licencia pública general.

IANA: Autoridad de Asignación de Números en Internet.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.

ISO/IEC 27002: Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información.

KVM: Máquina virtual basada en kernel.

LDAP: Protocolo ligero de acceso a directorios.

MAC: Control de Acceso al Medio.

MD5: Algoritmo de reducción criptográfico de 128 bits.

MiTM: ataque en el que el enemigo adquiere la capacidad de interceptar y modificar los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

NAS: Servidor de acceso a la red.

OSI: Modelo de interconexión de sistemas abiertos.

PAP: protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto mediante contraseña.

PIN: Número de identificación Personal.

PKI: Infraestructura de clave pública.

POLÍTICA: Conjunto de reglas que indican los privilegios de cada uno de los usuarios de red.

PPP: Protocolo punto a punto que permite establecer una comunicación a nivel de la capa de enlace TCP/IP.

RADIUS: Autenticación Remota para usuarios de Servicio Telefónico.

ROSI: Retorno sobre la inversión de seguridad.

RFC: Request for Comments, documento que explica en detalle un protocolo de internet.

SHA1: Algoritmo de resumen seguro 1

SHARED SECRET: Contraseña secreta conocida solo por las partes involucradas en una comunicación segura.

SLE: Expectativa de pérdida por evento.

SQL: Lenguaje de consulta estructurado.

SQUID: Programa de software libre que implementa un servidor proxy.

SSL: Capa de conexión segura.

SUPLICANTE: Software requerido para iniciar el proceso de autenticación.

TCP: Protocolo de control de transmisión.

TLS: Seguridad en la Capa de Transporte.

TTLS: Seguridad en la Capa de Transporte tunelado.

UDP: Protocolo de transporte basado en el intercambio de datagramas.

VLAN: Red de área local virtual.

VPN: Red privada virtual.

XOR: Operador lógico.

WPA2: Acceso Protegido Wi-Fi 2.

802.1X: Norma del IEEE para el control de acceso a la red basada en puertos.

ANEXO A

CREACIÓN DE UN CONTENEDOR VIRTUAL UTILIZANDO EL ENTORNO DE VIRTUALIZACIÓN PROXMOX-VE

La implementación de los servidores se realiza sobre la plataforma de virtualización PROXMOX, empleando la tecnología de contenedores virtuales OpenVZ.

La administración del entorno virtual Proxmox se lo puede hacer desde el propio servidor mediante consola o a través de la interfaz gráfica.

- Para acceder al servidor Proxmox se debe usar un navegador web, ingresando la dirección IP asignada en la instalación y el puerto 8006 por defecto.

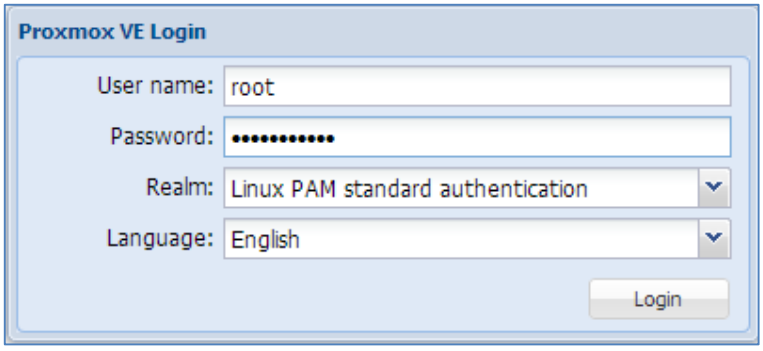


Figura 156. Autenticación gráfica Proxmox VE

Una vez que se haya superado el proceso de autenticación en el servidor, se procede a crear el contenedor virtual mediante OpenVZ.

- En la configuración general del nuevo servidor se establece un identificador numérico, el nombre del host y la contraseña de acceso.

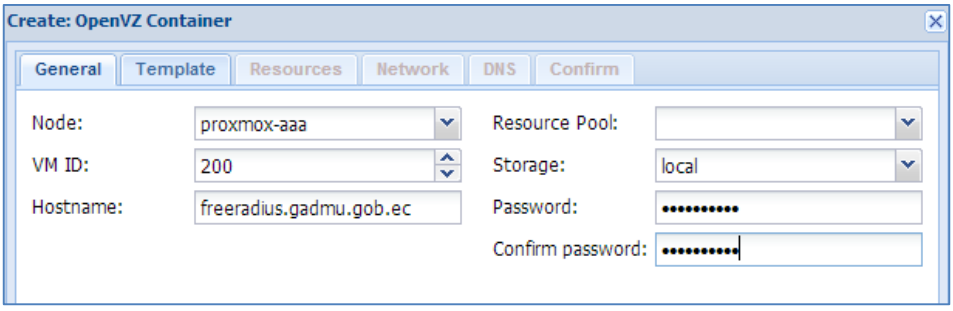


Figura 157. Configuración general del contenedor OpenVZ

- En el menú "Template" se selecciona el sistema operativo del nuevo servidor virtual, una plantilla es una imagen precargada que contiene todos los paquetes base requeridos para poner en funcionamiento el nuevo entorno virtual.

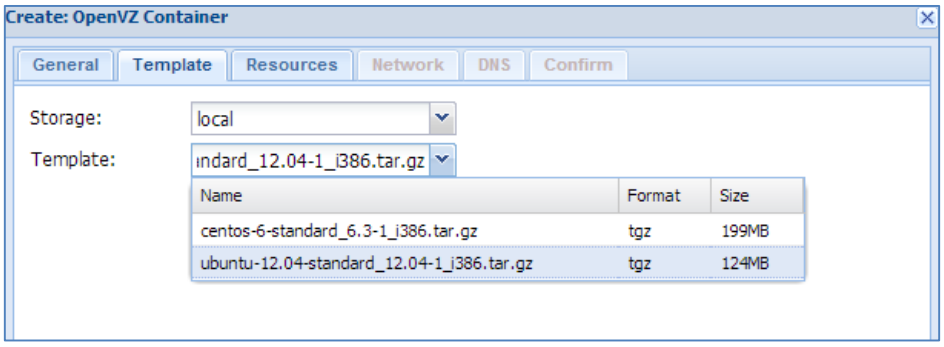


Figura 158. Selección de la plantilla Ubuntu 12.04

- En la siguiente ventana se asignan los recursos al nuevo servidor virtual, los cuales son: memoria, espacio en disco para almacenamiento y número de procesadores.

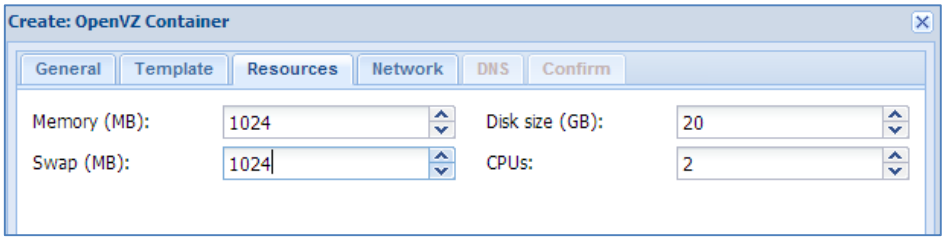


Figura 159. Asignación de recursos al servidor

- En la opción red se debe ingresar la dirección IP del nuevo servidor, como se muestra en la Figura b.

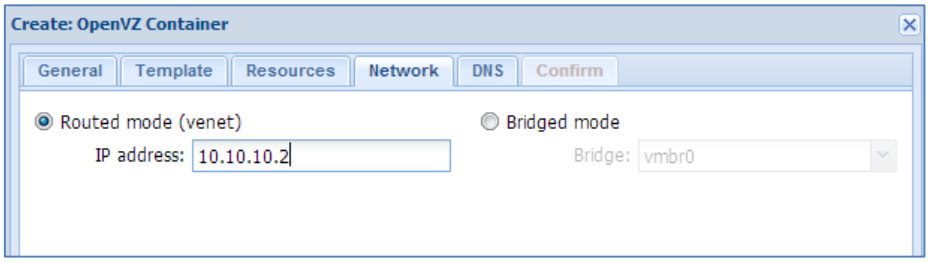


Figura 160. Asignación de dirección IP al servidor

- Antes de finalizar el proceso de creación del contendor virtual, se muestra una ventana con todos los parámetros configurados para el nuevo servidor.

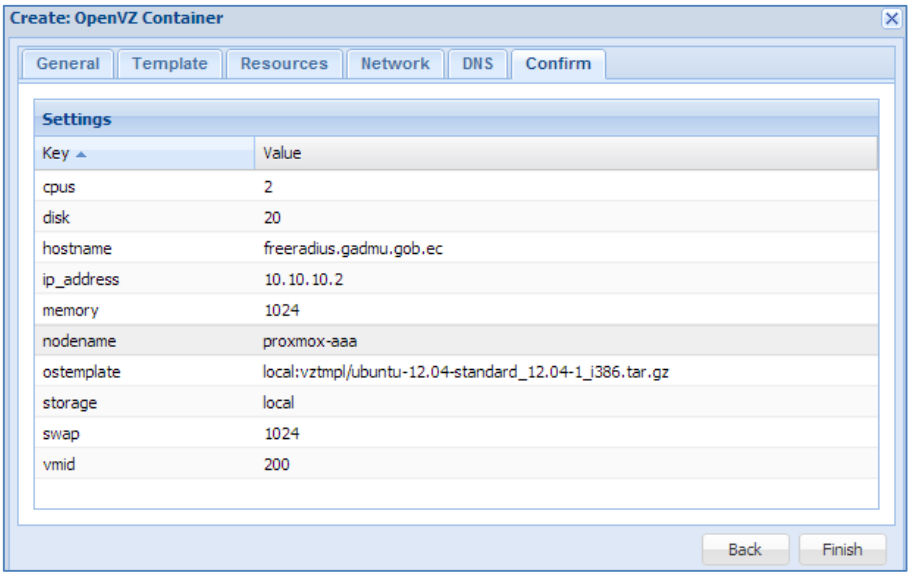


Figura 161. Resumen del nuevo servidor virtual

Luego de crear los servidores virtuales, se puede administrar y monitorear cada máquina virtual desde la interfaz gráfica de Proxmox.

ANEXO B

ADMINISTRAR CERTIFICADOS RAÍZ DE CONFIANZA EN WINDOWS 7

El Certificado raíz “gadmu-CA-cacert” correspondiente a la autoridad certificadora, es indispensable instalarlo en los dispositivos de los usuarios del sistema AAA para que accedan de forma segura a la infraestructura de red usando EAP-TTLS como método de autenticación. Para agregar certificados al almacén de entidades de certificación raíz de confianza en un equipo local, se debe realizar el siguiente proceso.

- Copiar los certificados digitales de la autoridad certificadora y el servidor freeradius (certificado + clave privada) en cualquier medio de almacenamiento.

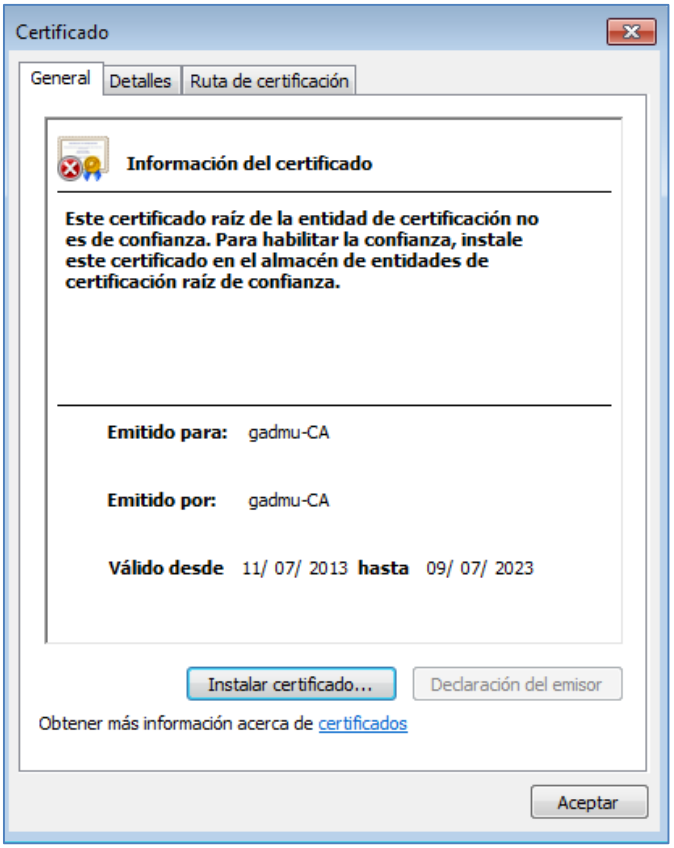


Figura 162. Certificado Raíz de la Autoridad Certificadora

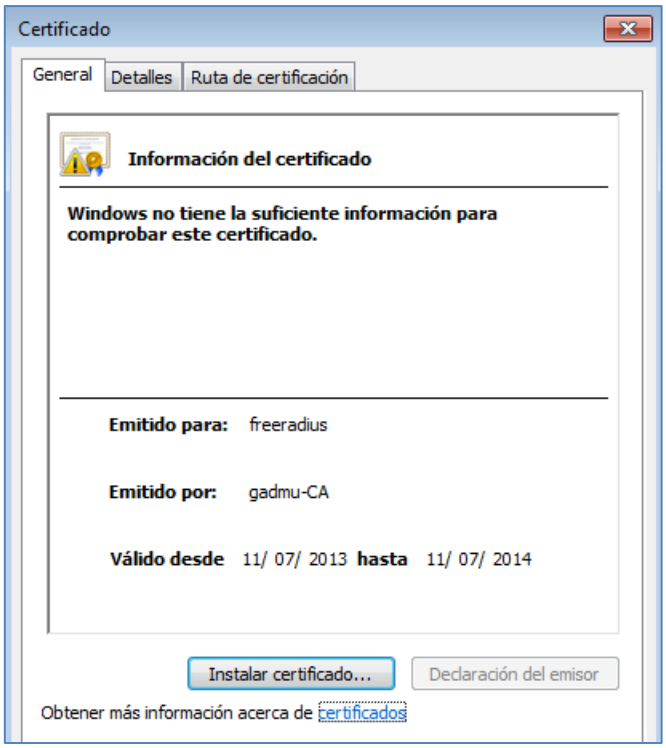


Figura 163. Certificado del Servidor FreeRADIUS

El certificado del servidor FreeRADIUS se debe instalar en el contenedor "Personal" del equipo cliente, mientras que el certificado de la Autoridad Certificadora se agrega al contenedor "Entidades de certificación raíz de confianza".

- Para instalar los certificados, se debe abrir la consola de administración de Microsoft (mmc).

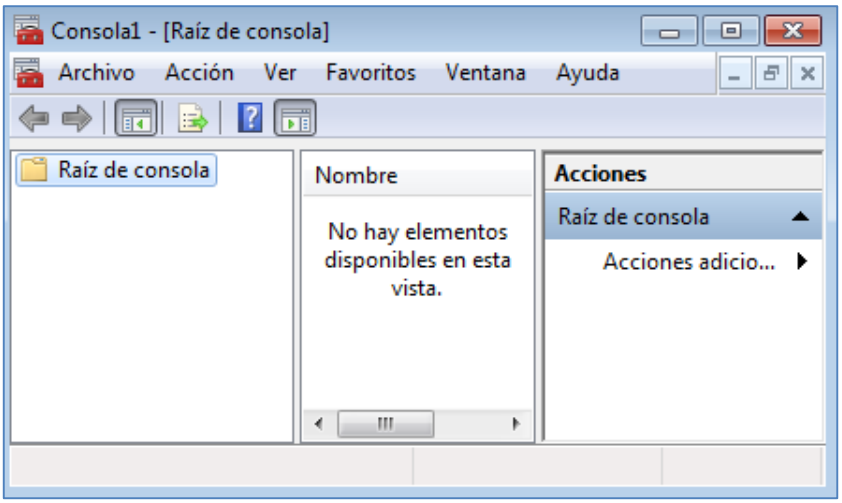


Figura 164. Consola de administración de Microsoft

- Antes de abrir la consola se aceptan los cambios que el programa va a realizar en el equipo y en el menú archivo se escoge la opción: Agregar o quitar complemento.

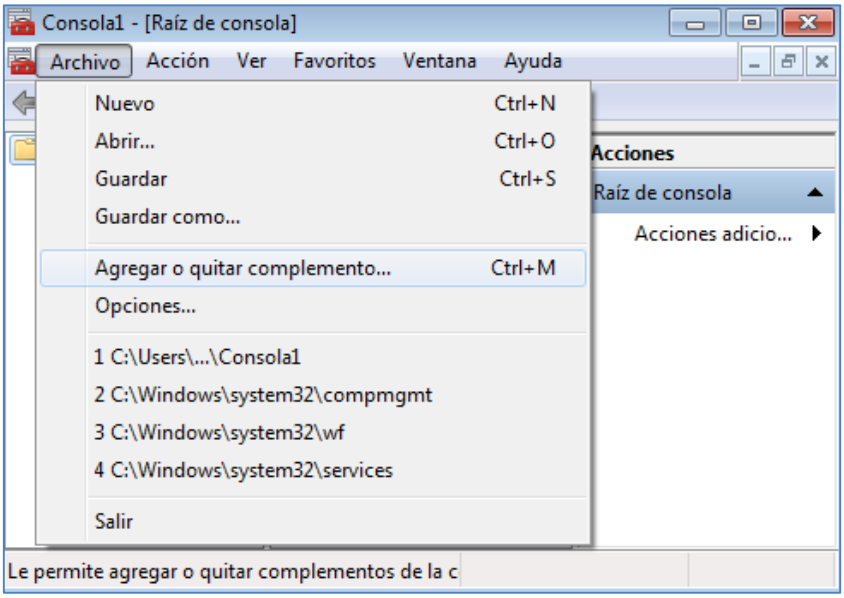


Figura 165. Agregar o quitar complemento (consola Windows 7)

- De la lista de componentes disponibles, se agrega la opción Certificados.

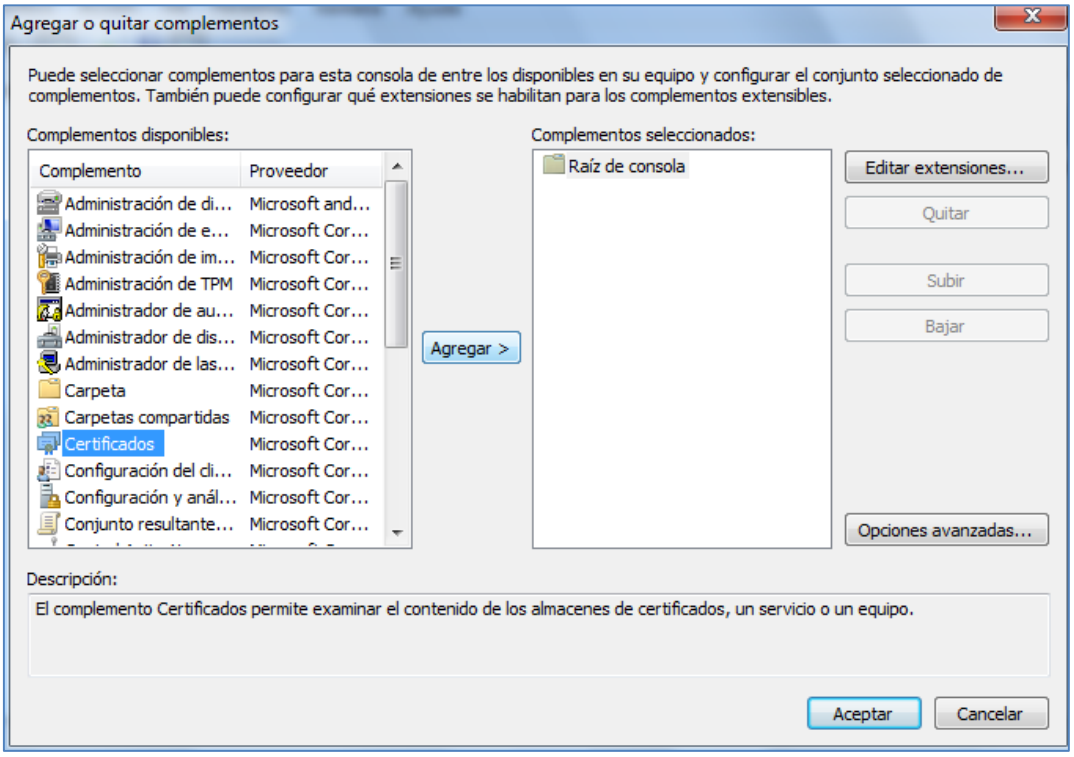


Figura 166. Complementos disponibles para la nueva consola

- En la ventana desplegada, se escoge la opción “Cuenta de Equipo” y finalmente se selecciona el equipo que se usará para administrar el complemento.

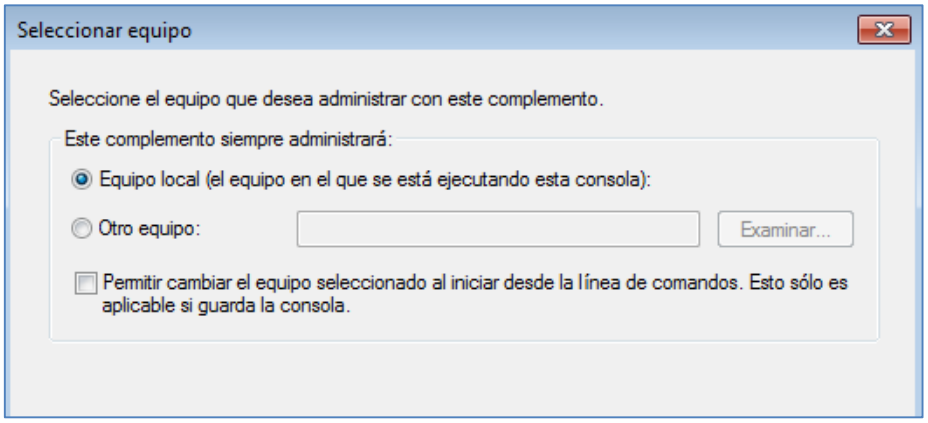


Figura 167. Administración de Certificados desde equipo local

- El certificado de la CA (gadmu-CA-cacert) se importa en el almacén “Entidades de certificación raíz de confianza”

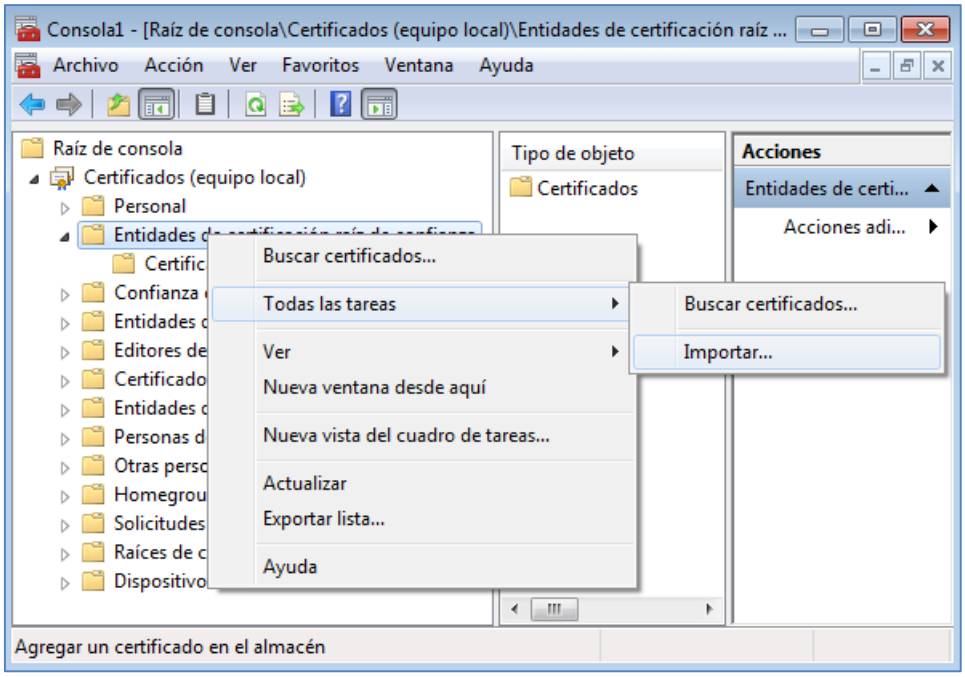


Figura 168. Importación del certificado digital de la CA

- Se despliega un asistente para la importación de certificados digitales.

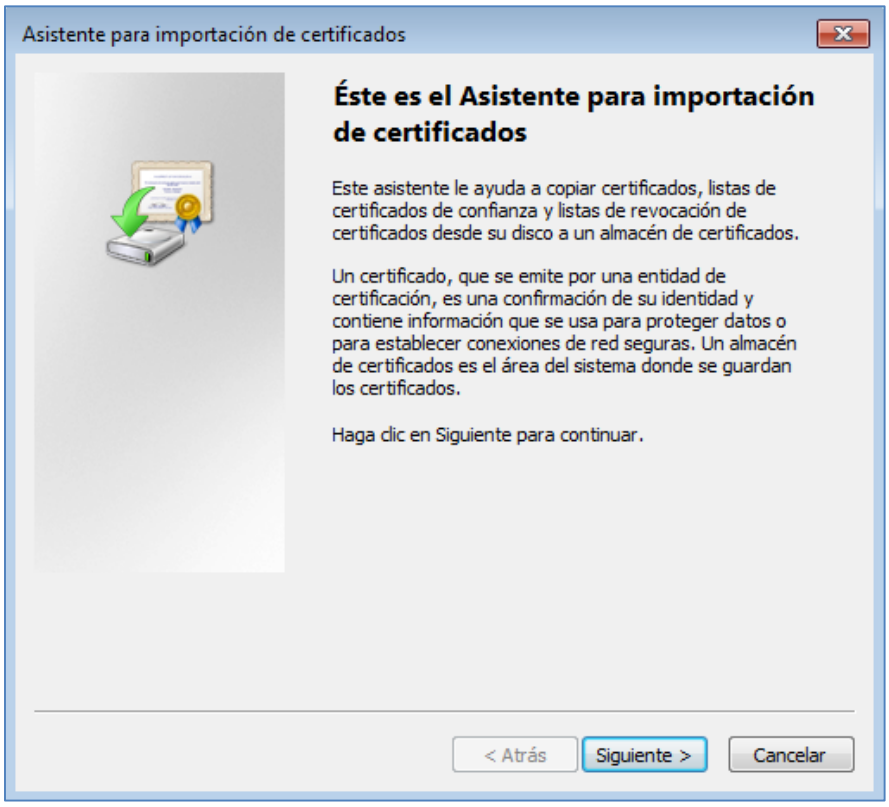


Figura 169. Asistente para importación de certificados

- En la siguiente ventana se debe indicar la ubicación del certificado digital que se requiere importar.

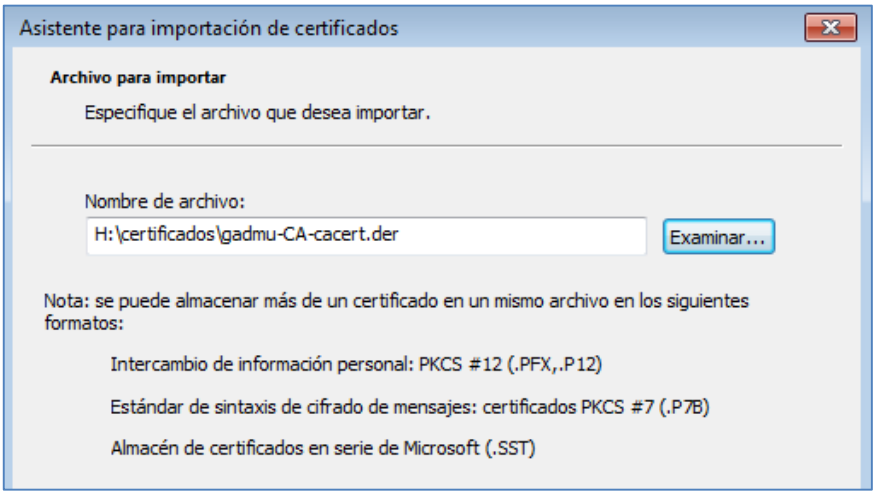


Figura 170. Importación de certificado gadmu-CA-cacert

- Por último, el certificado digital gadmu-CA-cacert se guarda en el almacén “Entidades de certificación raíz de confianza”

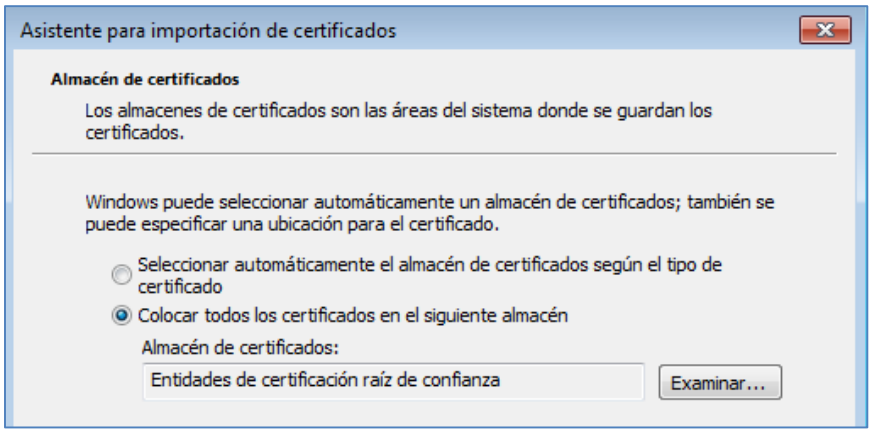


Figura 171. Almacén de certificados: Entidades de certificación raíz de confianza

- Una vez finalizado el proceso de importación de certificados, el asistente muestra un mensaje de información.

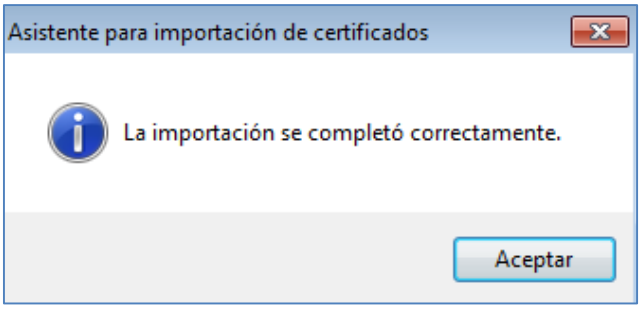


Figura 172. Mensaje de finalización de importación de certificados

ANEXO C

PLIEGO DE ESPECIFICACIONES TÉCNICAS Y ECONÓMICAS PARA LA IMPLEMENTACIÓN DEL SERVIDOR AAA

El documento presenta las principales consideraciones técnicas y económicas requeridas para la implementación del sistema AAA empleando el estándar IEEE 802.1x – EAP-TTLS en el GAD Municipal San Miguel de Urcuquí.

1. OBJETIVO

El objetivo del presente documento es definir los requerimientos técnicos mínimos, necesarios para el control de acceso y administración de los recursos de red mediante un servidor AAA en la red de datos del GADMU.

2. CONSIDERACIONES GENERALES

2.1. El pliego de prescripciones técnicas tiene por objetivo definir los requisitos de obligatorio cumplimiento para cumplir con el servicio AAA.

2.2. Los requerimientos establecidos en el presente documento son exigencias mínimas, por lo tanto, son de carácter abierto, los oferentes tienen la posibilidad de presentar una mejor solución, siempre y cuando cumplan con los requerimientos mínimos solicitados.

2.3. Se debe presentar una solución única que cumpla las condiciones mínimas del sistema AAA, si se oferta más de una solución "No se tomará en cuenta".

3. ESPECIFICACIONES TÉCNICAS (DE OBLIGATORIO CUMPLIMIENTO)

La arquitectura de red 802.1X/EAP-TTLS requiere de tres componentes para operar, cada uno de los cuales debe cumplir requerimientos específicos para que el sistema AAA trabaje de manera segura.

3.1. Suplicante

El software que se instala en los dispositivos de usuario final utilizado para acceder a la red (cableada o inalámbrica) debe soportar el método de autenticación EAP-TTLS.

Tabla 26. Requerimientos técnicos Suplicante

SISTEMA OPERATIVO	EAP-TTLS
Windows XP	SecureW2
Windows 7	SecureW2
Windows 8	Cliente Nativo
Ubuntu 12.04 LTS	Cliente Nativo
Android OS	Cliente Nativo

3.2. Dispositivos autenticadores

Los equipos que ofrecen el servicio de acceso a la red y se ubican entre los dispositivos de usuario que requieren ser autenticados y la plataforma de servidores AAA, deben cumplir con los requerimientos técnicos detallados en la Tabla 27.

Tabla 27. Requerimientos técnicos de los equipos autenticadores

REQUERIMIENTO	DESCRIPCIÓN
RENDIMIENTO	
Capacidad	▪ 48 puertos 10/100 ▪ 2 puertos 10/100/1000
FUNCIONES DE CAPA 2	
RADIUS	✓ Seguridad RADIUS
Autenticación	✓ IEEE 802.1X (función de Autenticador)
VLAN	▪ 256 VLAN simultáneas ▪ VLAN de administración ▪ VLAN de usuarios temporales sin autenticación ▪ Asignación dinámica de VLAN mediante servidor Radius con autenticación 802.1x
Contabilidad	✓ Soporte de IEEE 802.1X Acconunting

3.3. Servidores

La implementación de los servidores: RADIUS, LDAP y SQL deberá realizarse empleando la tecnología de virtualización de plataforma. Los requerimientos mínimos de hardware para el servidor se detallan en la Tabla 28.

Tabla 28. Requerimientos hardware del servidor

RECURSO	DESCRIPCIÓN
Procesador	I7 @ 3.46 GHz
RAM	16 GB DDR3 RDIMM o UDIMM
Almacenamiento	1TB
Interfaces de Red	4
Virtualización de Hardware	Intel VT-x/AMD-v

3.4. Servicios

Cada uno de los servicios del sistema AAA (autenticación, autorización y contabilidad) deben cumplir parámetros mínimos de funcionalidad que permitan el control de acceso y la administración de recursos de red en el GADMU. En la Tabla 29 se detallan los requerimientos.

Tabla 29. Requerimientos del Sistema AAA

SERVICIO	DESCRIPCIÓN
AUTENTICACIÓN	
Servidor	FreeRADIUS
Control de acceso	IEEE 802.1x
Método de autenticación	EAP-TTLS
Conexión	Equipo Autenticador (SW CISCO)
AUTORIZACIÓN	
Servidor	OpenLDAP
Almacenamiento de contraseña	Algoritmo MD5 o SHA
Asignación de recursos	Soporte de VLAN dinámica
Conexión	Servidor FreeRADIUS
CONTABILIDAD	
Servidor	MySQL
Conexión	Servidor FreeRADIUS
FIREWALL	
Zona wan	Salida a internet
Zona dmz	Servidores AAA
Zona local	Interfaces virtuales por cada VLAN
Comunicación inter-VLAN	Soporte 802.1Q (Troncal)
Proxy	Modo Transparente

4. ESPECIFICACIONES ECONÓMICAS

Las especificaciones económicas del proyecto se calculan tomando en cuenta el uso de herramientas basadas en software libre en cada servicio del sistema AAA y la compatibilidad que existe con los equipos de red disponibles en el GAD Municipal San Miguel de Urcuquí.

El costo de implementación incluye: manual de administración del sistema AAA y seis horas de capacitación al personal de la unidad de sistemas de la institución.

Tabla 30. Especificaciones económicas del sistema AAA

SERVICIO	DESCRIPCIÓN	CANTIDAD	COSTO ($) TOTAL
SOFTWARE			
Servidor RADIUS	FreeRADIUS	1	0
Servidor LDAP	OpenLDAP	1	0
Servidor SQL	MySQL	1	0
Plataforma de Virtualización	PROXMOX VE	1	0
Autoridad Certificadora	TinyCA	1	0
Software Suplicante	Secure W2	1	0
HARDWARE			
Equipos de acceso	Cisco SG-200 disponible	2	0
Servidor	HP DL380 G7 disponible	1	0
IMPLEMENTACIÓN			
Entorno de Virtualización	PROXMOX-VE	1	400
Instalación Sistema Operativo base	Ubuntu server 12.04 LTS	4	400
Configuración de servicios AAA	RADIUS/LDAP/MySQL	3	1200
Configuración políticas de acceso	Firewall-Proxy	1	400
VLAN dinámicas	Switch cisco SG-200	2	300
Capacitación	Sistema AAA	6 horas	300
TOTAL (dólares)			**3000**

ANEXO D
MANUAL DE ADMINISTRACIÓN

MANUAL DE ADMINISTRACIÓN

AAA / 802.1X / EAP-TTLS

Desarrollado por:
William Vaca Aguirre.

UNIVERSIDAD TÉCNICA DEL NORTE
FICA - CIERCOM

Ibarra, 2014

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Introducción

El presente manual de administración es una guía básica para la gestión del sistema AAA (Autenticación, Autorización, Auditoría), sistema encargado del control de acceso y gestión de recursos de red del GAD Municipal San Miguel de Urcuquí.

El documento está dirigido a los administradores de la unidad de sistemas del GADMU, a través de esta guía podrá gestionar el entorno de virtualización PROXMOX, crear usuarios y grupos en el directorio LDAP, definir nuevas reglas y políticas de acceso para los usuarios y en general, solucionar cualquier evento que se presente una vez que el sistema se encuentre en un entorno de producción.

1 ENTORNO DE VIRTUALIZACIÓN PROXMOX

Proxmox Virtual Environment es una completa plataforma de virtualización de servidores, basada en KVM y contenedores. Posee una interfaz gráfica muy sencilla que facilita la realización de tareas como: migración en vivo de máquinas virtuales, clustering de servidores, respaldos automáticos y la asignación de recursos (red, memoria, espacio en disco, etc.) en tiempo real, sin reinicio del sistema.

1.1 INGRESO AL SISTEMA DE VIRTUALIZACIÓN

Para ingresar al entorno de virtualización PROXMOX, se debe digitar la dirección https://10.10.10.10:8006 en la barra de navegación de un explorador de internet.

Se desplegará una pantalla de conexión con el servidor, ingrese el nombre de usuario **root** y la correspondiente **contraseña**, adicionalmente se escoge el idioma que se usara en la administración del sistema (véase Figura 1).

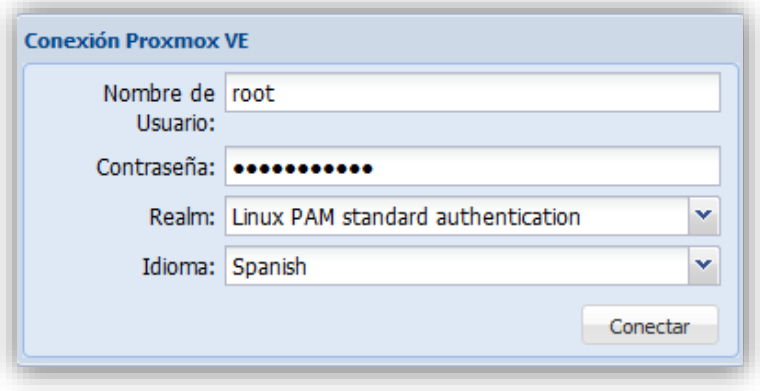


Figura 1. Conexión PROXMOX VE

1.2 CONTENEDORES VIRTUALES OPENVZ

En la parte superior izquierda se muestra una estructura de directorios que resumen el sistema completo de virtualización.

Para visualizar todos los contenedores virtuales instalados se debe seleccionar el menú "OpenVZ Container", el sistema AAA mostrará los tres servidores disponibles: Autenticación: freeradius, Autorización: OpenLDAP y Contabilidad: MySQL (véase Figura 2).

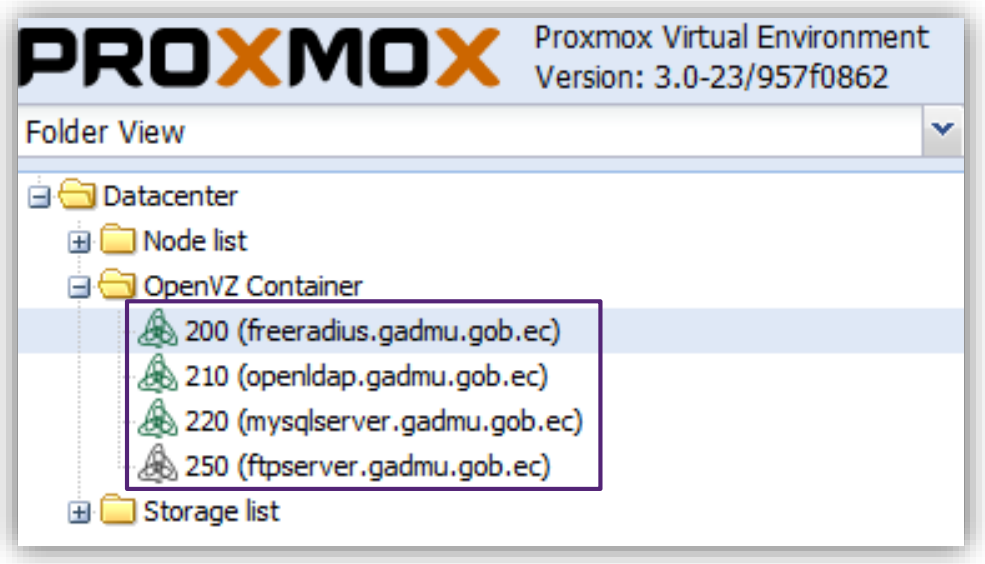


Figura 2. Contenedores virtuales OpenVZ

1.3 INICIO DE SERVICIOS AAA

El arranque del servidor AAA se realiza en el siguiente orden: primero el servidor MySQL, luego el directorio LDAP y finalmente el servidor RADIUS.

Las modificaciones que se realicen en el directorio de usuarios (LDAP) no requieren del reinicio del servicio para ser validados a diferencia del servidor de registro (MySQL), debido a que el servidor RADIUS cuando arranca el servicio establece la conexión una sola vez con la base de datos, esto hace que los cambios posteriores no tomen efecto.

Para encender un servidor se selecciona el contenedor virtual (doble clic), y en la parte superior derecha de la interfaz se escoge la opción “Iniciar” como se muestra en la Figura 3.

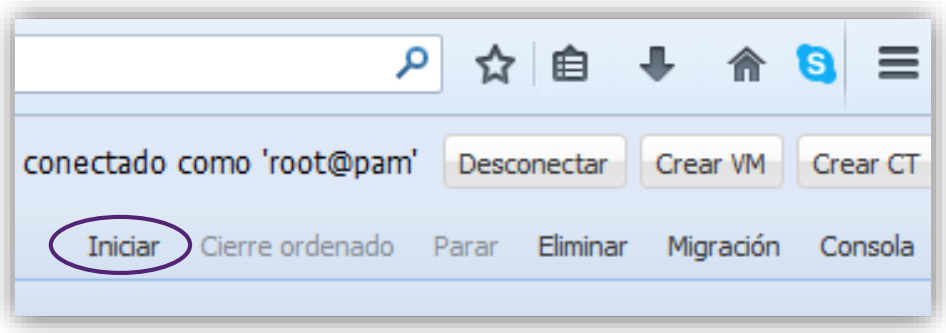


Figura 3. Inicio de un contenedor virtual

1.3.1 RECURSOS DE UN CONTENEDOR VIRTUAL

La adecuada gestión de los recursos virtuales asignados a cada servidor permite prevenir cualquier sobrecarga debido a elevadas demandas de usuarios que pudieran provocar la caída de un servicio.

En la Figura 4 se muestra el resumen completo de un servidor activo, la información incluye: cantidad de recursos asignados, capacidad de memoria utilizada y tiempo de uso.

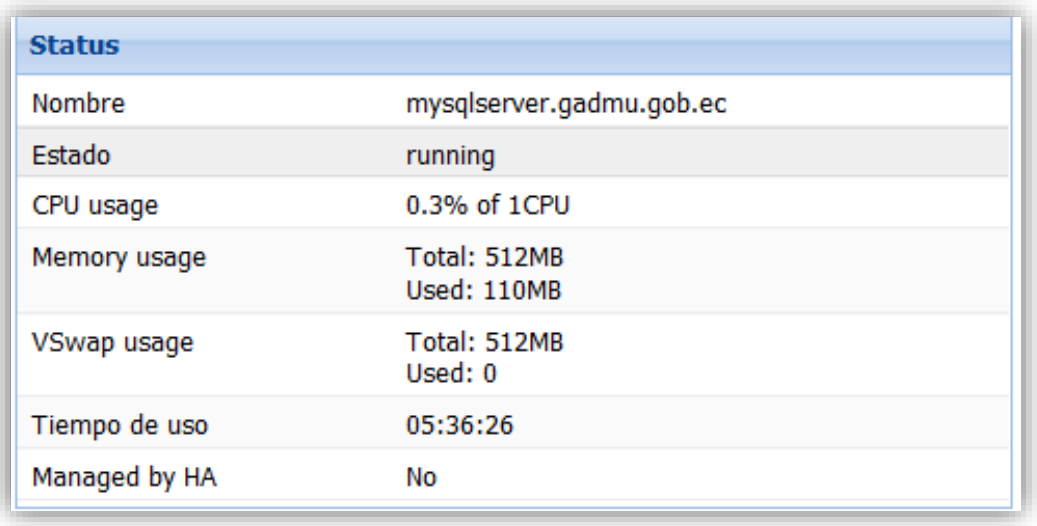


Figura 4. Estado de un contenedor virtual

1.3.1.1 Modificación dinámica de recursos virtuales

Para editar los recursos asignados a un contenedor virtual, ingrese al menú "Recursos", a continuación, en la ventana desplegada se aumenta o disminuye la capacidad de memoria, disco o procesador de acuerdo a los requerimientos (véase Figura 5).

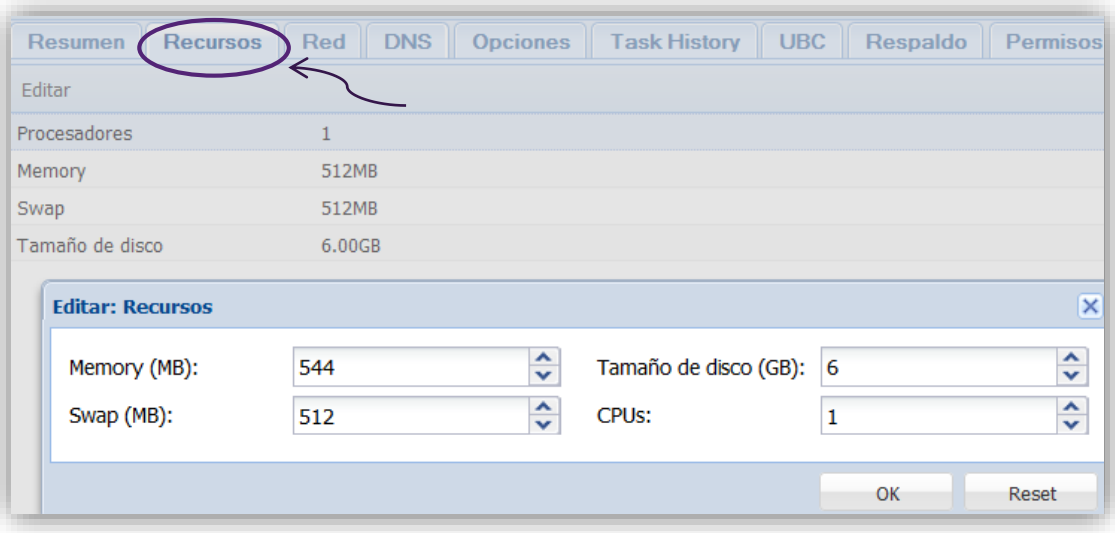


Figura 5. Edición dinámica de recursos

1.3.1.2 Red

Para modificar la dirección IP de un contenedor virtual acceda al menú **Red**, en esta sección es posible agregar varias interfaces de red al servidor, así como también, eliminar una creada anteriormente (Figura 6).

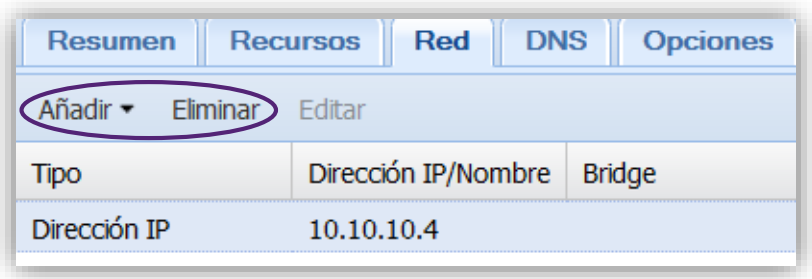


Figura 6. Parámetros de Red

1.3.1.3 DNS

En la opción servicio de nombres de dominio es posible modificar el nombre del servidor, el dominio y la dirección IP del servidor DNS.

Para cambiar la configuración, haga clic en el botón DNS y luego en **editar** (Figura 7).

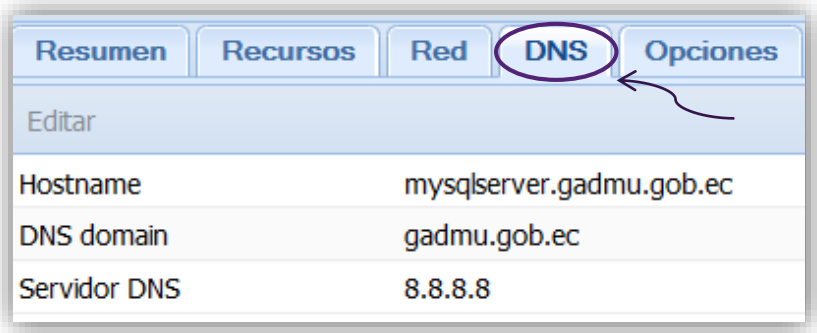


Figura 7. Edición del DNS de un contenedor virtual

1.4 GESTIÓN DE USUARIOS

La autenticación y autorización se realiza mediante la conexión del servidor RADIUS con el directorio LDAP que almacena las credenciales de autenticación de todos los usuarios del sistema AAA.

Durante el proceso de registro de un nuevo usuario se deben considerar las reglas definidas en la política de seguridad para el control de acceso a la red, las cuales establecen los siguientes requerimientos:

- La longitud mínima de contraseña: 10 caracteres
- Complejidad: Combinación de letras mayúsculas y minúsculas, números y al menos un carácter especial (signos de puntuación).
- No basarse en algo que alguien pueda adivinar como nombres, fechas, números de teléfono, etc.
- No usar palabras incluidas en diccionarios para evitar ataques de este tipo.
- Descartar por completo caracteres repetidos consecutivos.

1.4.1 ACCESO AL DIRECTORIO USANDO JXPLORER

Para acceder al directorio de usuarios se usará el navegador gráfico desarrollado en código abierto JXplorer, esta herramienta trabaja sobre múltiples plataformas. La descarga del software lo puede hacer a través del siguiente enlace: http://jxplorer.org/downloads/users.html

Una vez realizada la descarga y posterior instalación, se despliega una interfaz gráfica como se muestra en la Figura 8.

Figura 8. Interfaz gráfica JXplorer

La conexión con el servidor OpenLDAP se puede hacer como usuario anónimo o administrador. Usando la identificación anónima se accede al servidor con privilegios únicamente de lectura, quedando restringidas varias operaciones (crear, modificar y eliminar), las cuales son propiedad exclusiva del usuario administrador.

Para establecer una conexión con privilegios de administrador ingrese la siguiente información:

- Dirección IP del servidor OpenLDAP: 10.10.10.3
- Protocolo del servidor: LDAP versión 3
- Base DN: dc=gadmu, dc=gob, dc=ec
- Usuario administrador: cn=admin, dc=gadmu, dc=gob, dc=ec
- Contraseña

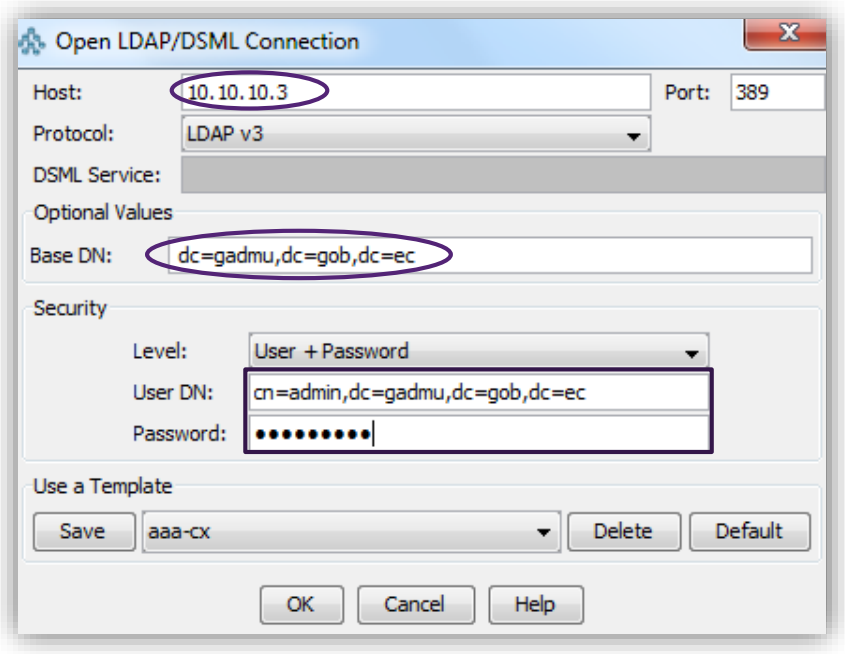


Figura 9. Conexión con servidor LDAP

1.4.1.1 Gestión de grupos

Una vez autenticado con privilegios de administrador se establece la conexión con el directorio LDAP, toda la información se encuentra organizada jerárquicamente y en grupos de usuarios mediante unidades organizativas (OU).

Cada departamento del GAD Municipal San Miguel de Urcuquí está representado por una unidad organizativa, que a su vez agrupa a los usuarios pertenecientes a dicho departamento.

Para crear una nueva unidad organizativa (nuevo departamento institucional), haga clic derecho sobre el nombre de la organización "**gadmu**" y en el menú desplegado elija "**new**" para crear la nueva entrada en el directorio LDAP (véase Figura 10).

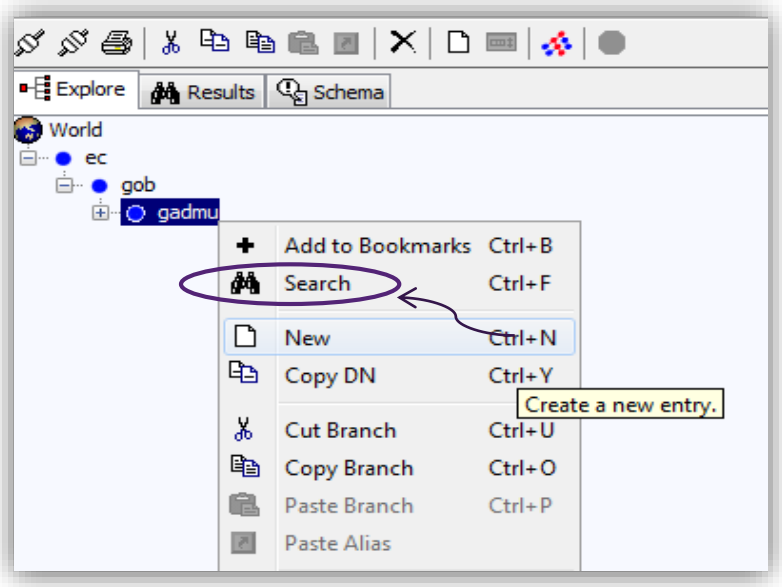


Figura 10. Creación de una nueva Unidad Organizativa

Para completar el proceso de creación de la unidad organizativa haga lo siguiente:

PASO 1. Ingrese un nombre identificativo para el nuevo grupo (RDN).

PASO 2. Agregue las clases de objeto para la nueva entrada.

PASO 3. Haga clic en **ok** para guardar los cambios (Figura 11).

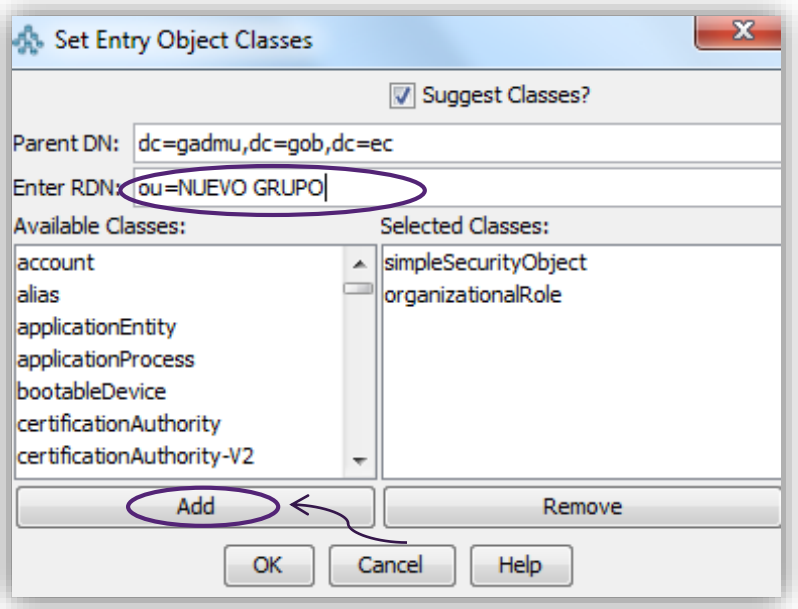


Figura 11. Definición de clases para la nueva OU.

1.4.1.2 Gestión de usuarios

El procedimiento para crear un nuevo usuario del sistema AAA en el directorio LDAP se detalla a continuación:

PASO 1. Haga clic derecho sobre la unidad organizativa a la que pertenece el usuario.

PASO 2. En el menú desplegado seleccione "**new**", para crear una nueva entrada en LDAP (véase Figura 12).

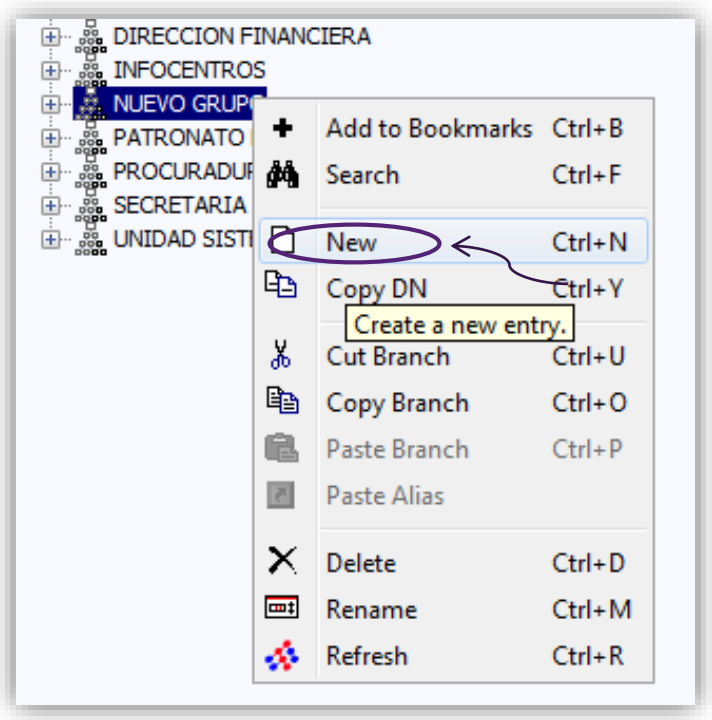


Figura 12. Creación de nuevo usuario en LDAP

Antes de ingresar la información al sistema tome en cuenta las clases y atributos que todo usuario del sistema AAA debe tener.

- ✓ `DN: cn= Nombre Usuario, ou=NUEVO GRUPO, dc=gadmu, dc=gob, dc=ec`
- ✓ `objectClass: person`
- ✓ `objectClass: uidObject`
- ✓ `objectClass: top`
- ✓ `objectClass: radiusprofile`
- ✓ `cn: Nombre del Nuevo Usuario`

- ✓ `description: Nivel de Acceso 2`
- ✓ `radiusTunnelMediumType: IEEE-802`
- ✓ `radiusTunnelPrivateGroupId: 12`
- ✓ `radiusTunnelType: VLAN`
- ✓ `sn: Srta.`
- ✓ `uid: nusuario`
- ✓ `userPassword:: e1NIQX12cEVnTU9JbzR2WnN3UmhBcmRLWUpMSTNUY1k9`

PASO 3. Defina las clases para el nuevo usuario.

Todos los usuarios del sistema AAA tendrán idénticas clases de objeto, para añadir una nueva seleccione de la lista disponible el nombre de la clase de objeto y continuación haga clic en el botón añadir "**Add**" como se muestra en la Figura 13.

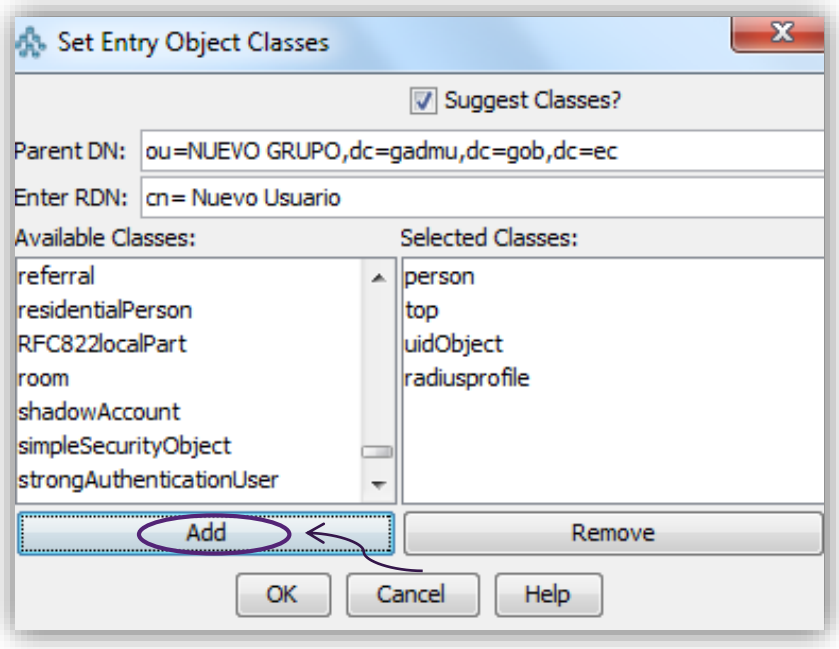


Figura 13. Adición de clases de objeto a un usuario

PASO 4. Finalmente, use el editor de tabla para agregar valores a los atributos de cada objeto (usuario) creado tomando en cuenta la siguiente información (véase Figura 14).

cn: Asignar un nombre representativo de identificación para el usuario.

description: Texto que informa el nivel de acceso del usuario, es decir los privilegios.

radiusTunnelPrivateGroupId: Número usado en la asignación dinámica de VLAN.

uid: Identificador de usuario usado en el proceso de autenticación.

userPassword: Contraseña asignada al identificador de usuario para acceder a la red.

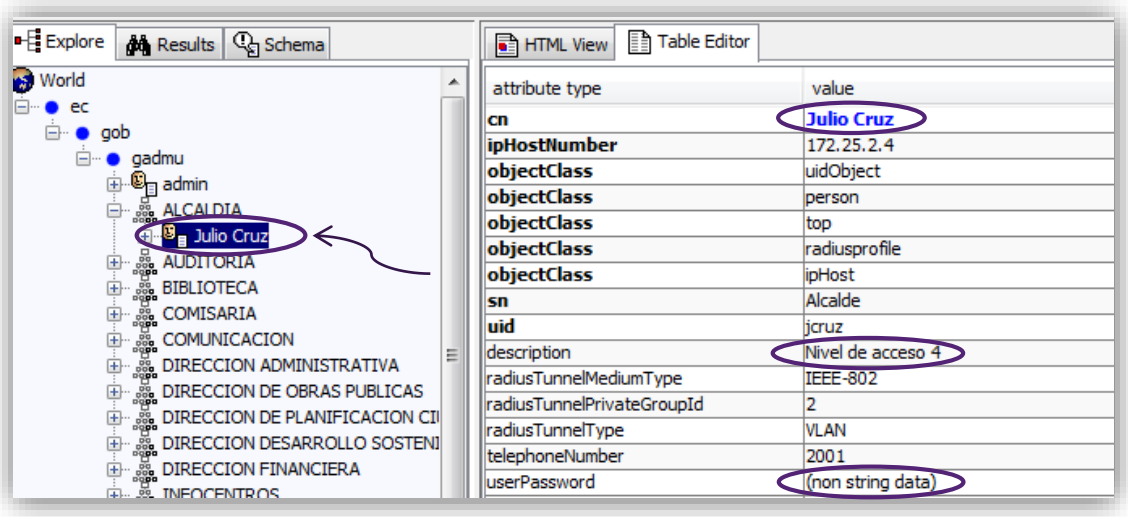


Figura 14. Asignación de valores a los atributos de un usuario

Para modificar los valores asignados a un atributo utilice el editor de tabla mostrada en la Figura 14, en la columna derecha realice la edición y a continuación haga clic en el botón "**submit**" para guardar los cambios hechos.

1.4.1.3 Dar de baja un usuario LDAP.

Para eliminar un usuario del sistema AAA, ubique al usuario dentro de la unidad organizativa al que pertenece y haga clic derecho, posteriormente elija la opción "**Delete**" del menú desplegado para borrarlo definitivamente. El procedimiento se muestra en la Figura 15.

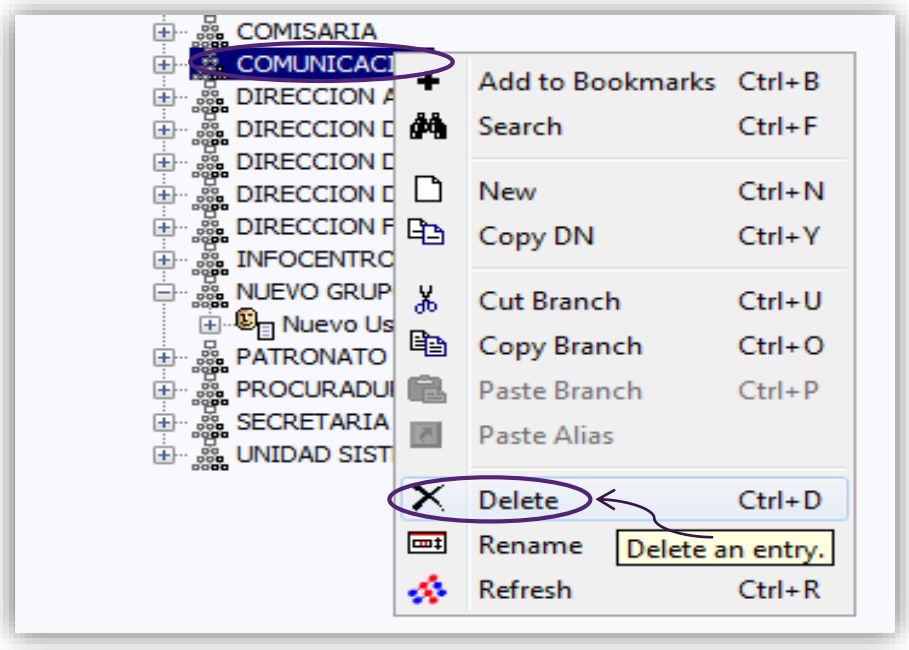


Figura 15. Eliminación de un usuario LDAP

1.5 REGISTRO DE INFORMACIÓN DE ACCESO

La contabilidad es el proceso estadístico y recolección de datos de conexión, estos valores se almacenan en una base de datos.

La información que el servidor MySQL le entregue debe ser manejada y procesada correctamente con la finalidad de gestionar y controlar de manera eficiente el acceso de los usuarios a la red del GAD Municipal San Miguel de Urcuquí.

1.5.1 ACCESO AL SERVIDOR RADIUS

Para ingresar al sistema de registro de información, digite la dirección http://10.10.10.2/daloradius/login.php en la barra de navegación de un explorador web.

Se desplegará una pantalla de autenticación donde se debe ingresar el nombre de usuario **"administrator"** y su correspondiente contraseña **"daloradius"**, en la Figura 16 se muestra la interfaz gráfica de acceso.

Figura 16. Acceso al servidor RADIUS

1.5.2 GESTIÓN: CLIENTES RADIUS

Cliente RADIUS se denomina al dispositivo a través del cual los usuarios del sistema AAA acceden a la infraestructura de red de la institución. Por ejemplo un switch o un router inalámbrico.

Nota. Los clientes radius deben soportar el estándar IEEE 802.1x para permitir el control de acceso a la red. La clave secreta configurada en el cliente RADIUS debe ser la misma del servidor.

El procedimiento requerido para agregar, editar y eliminar una NAS (cliente RADIUS) se detalla a continuación:

PASO 1. En el menú superior de la interfaz web, acceda a la pestaña "**Management**" y de las opciones mostradas, seleccione "**NAS**" (véase Figura 17).

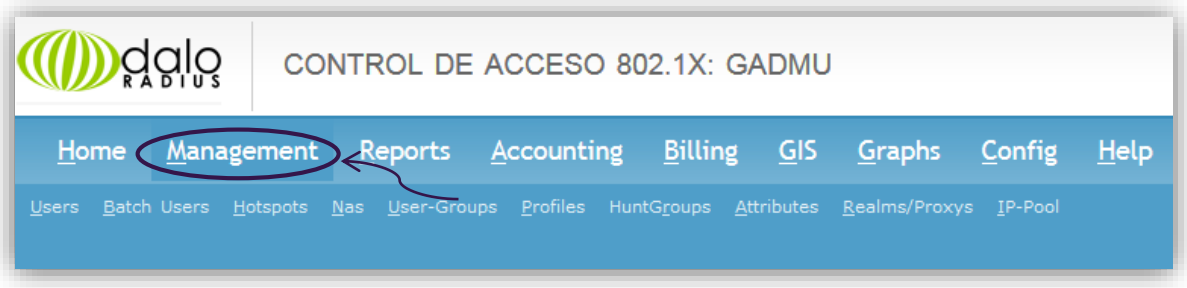


Figura 17. Administración del NAS

A continuación se despliega la sección para gestionar los dispositivos NAS de la infraestructura de red (véase Figura 18).

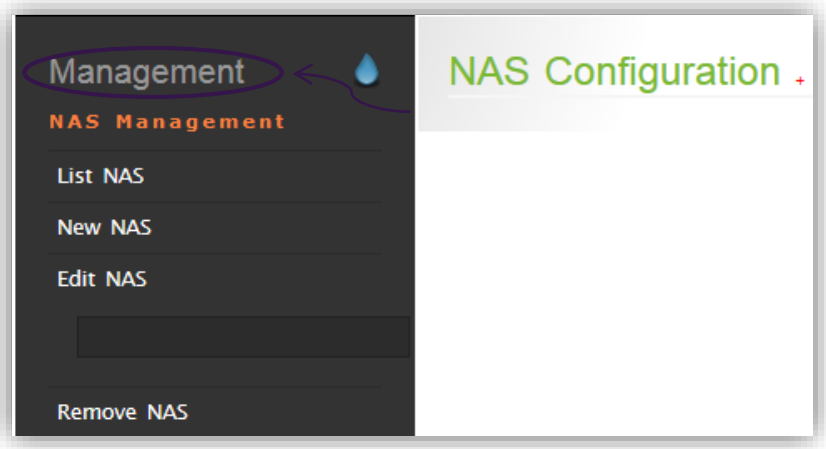


Figura 18. Gestión del NAS

PASO 2. Para **agregar** un nuevo dispositivo NAS a la red, acceda a la opción "**New NAS**" de la sección de administración (véase Figura 18).

En la ventana desplegada (Figura 19) ingrese los valores del nuevo dispositivo NAS:

- ✓ Dirección IP del dispositivo (subred 172.25.1.0/24)
- ✓ Clave secreta compartida (debe ser la misma del dispositivo)
- ✓ Fabricante (opcional)
- ✓ Nombre corto para el cliente RADIUS (descripción)

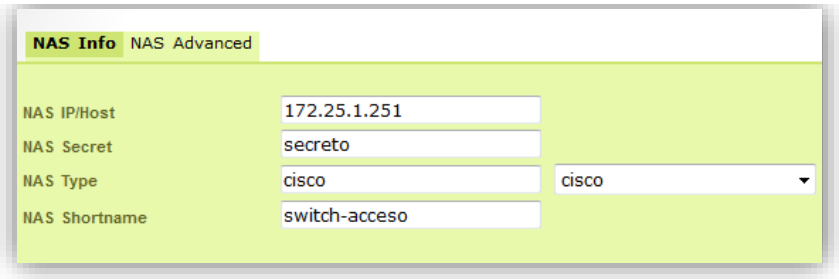


Figura 19. Creación de un NAS

PASO 3. Para **modificar** los valores de un cliente RADIUS creado, ingrese a la sección de gestión "**NAS**" y luego haga clic en el botón "**Edit NAS**" (véase Figura 18). Edite la configuración marcando el ID del dispositivo como se muestra en la Figura 20.

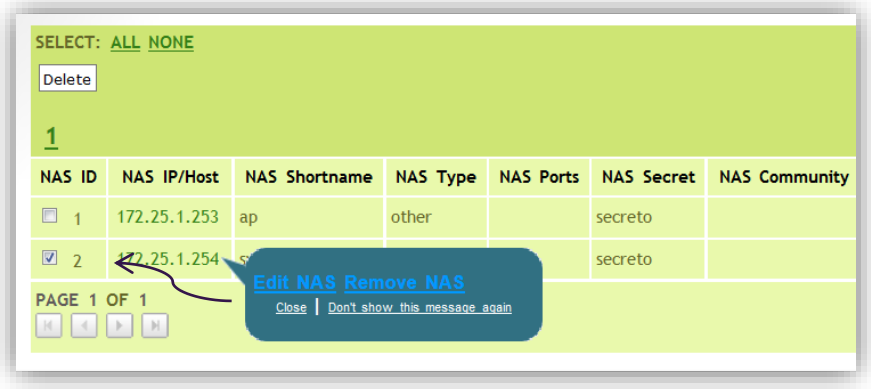


Figura 20. Edición de un NAS

1.5.3 REPORTES: USUARIOS EN LÍNEA

Para verificar los usuarios que se han autenticado correctamente al sistema AAA se accede al menú superior de la interfaz web, en la pestaña "**Reportes**" se elige la opción "**Usuarios en Línea**" (véase Figura 21).

Figura 21. Reportes: usuarios en línea.

1.5.4 REPORTES: ARCHIVOS DE REGISTRO

Un log permite el registro automático de eventos en el sistema, es recomendable monitorear y revisar de forma periódica cada uno de los archivos generados.

El sistema AAA genera mucha información relacionada con la autenticación de usuarios al sistema, en la Figura 22 se observan todos los registros posibles a los que se tiene acceso.

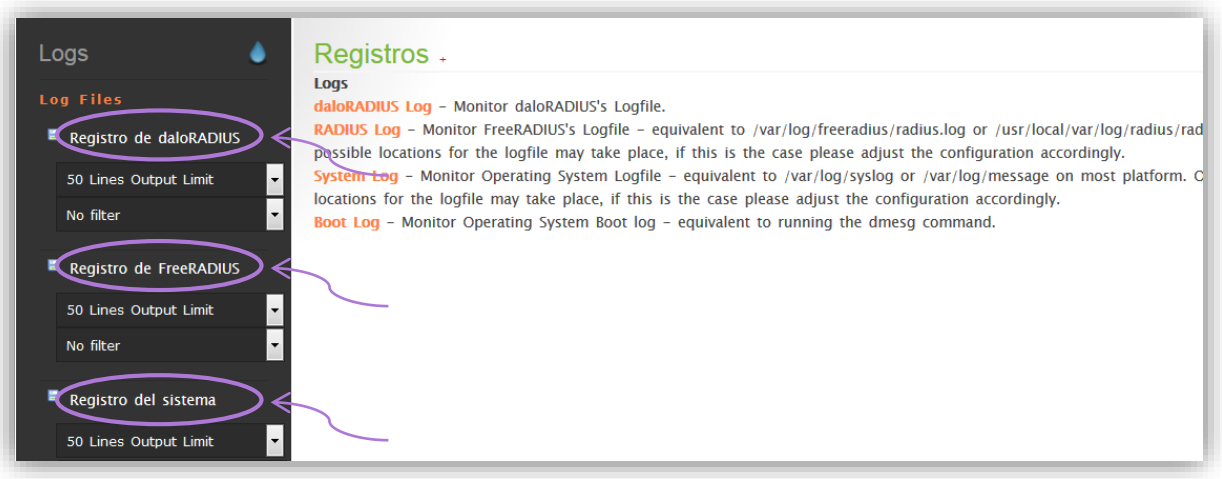


Figura 22. Reportes: Logs del sistema.

1.5.5 ACCOUNTING: REGISTRO DE ACCESOS AL SISTEMA

Cuando un usuario se autentica para acceder al sistema, toda la información generada es registrada en la base de datos. Para acceder a la información, ingrese al menú "**Accounting**", en la sección izquierda de la interfaz web haga clic en la opción "**Users Accounting**" (Figura 23).

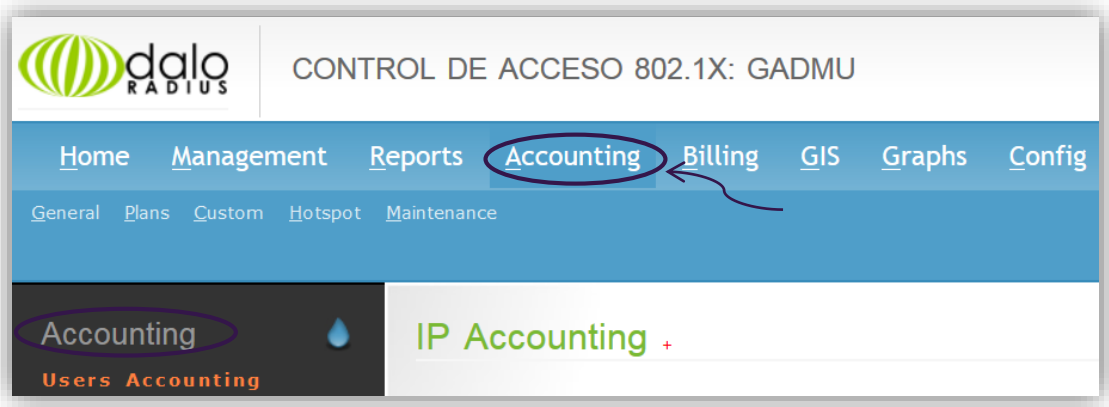


Figura 23. Menú Accounting: Registro de la información de acceso

La información registrada por el sistema entrega datos relevantes como:

- ✓ Nombre de usuario autenticado
- ✓ Dirección física (MAC) del dispositivo conectado
- ✓ Hora de inicio y fin de sesión
- ✓ Cliente RADIUS usado para el acceso a la red.

1 2 3 4 5 6

ID	Hotspot	Usuario	Dirección IP	Hora de inicio	Hora de finalización	Tiempo total	Subida (Bytes)	Descarga (Bytes)	Terminación	Dirección IP del NAS
174		anonymous		2014-07-07 22:52:31	2014-07-07 22:53:57	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254
175		anonymous		2014-07-07 22:54:24	2014-07-07 22:59:00	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254
176		czuleta		2014-07-07 22:56:01	2014-07-07 22:59:38	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254
177		czuleta		2014-07-07 22:59:52	2014-07-07 23:02:33	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254
178		biblioteca		2014-07-07 23:02:57	2014-07-07 23:03:34	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254
179		mfarinango		2014-07-07 23:04:13	2014-07-07 23:05:29	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254
180		fguerrero		2014-07-07 23:05:43	2014-07-07 23:07:39	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254
181		fguerrero		2014-07-07 23:07:56	2014-07-07 23:12:09	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254
182		jegas		2014-07-07 23:13:17	2014-07-07 23:21:30	0 seconds	0 B	0 B	Admin-Reset	172.25.1.254

Figura 24. Registro completo de accesos al sistema AAA

1.5.6 CONFIGURACIÓN: CARACTERÍSTICAS GLOBALES

En la sección configuración (véase Figura 25) se modifica el idioma de la interfaz web y los datos requeridos para establecer la conexión con la base de datos externa MySQL, donde se registra la información de acceso generada por el sistema AAA.

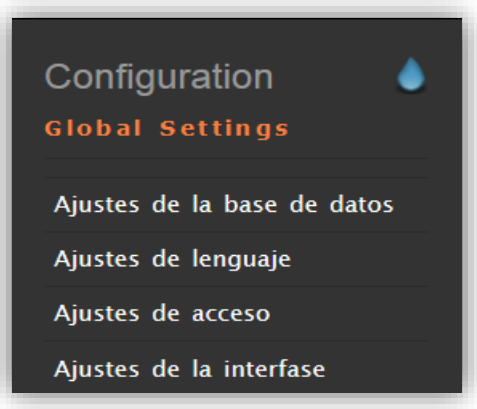


Figura 25. Configuración global

1.5.7 CONEXIÓN CON MYSQL

El servidor FreeRADIUS requiere de la conexión con la base de datos MySQL para registrar los datos de autenticación de los usuarios generados por el NAS. Ingrese los valores requeridos por el servidor RADIUS como se muestra en la Figura 26.

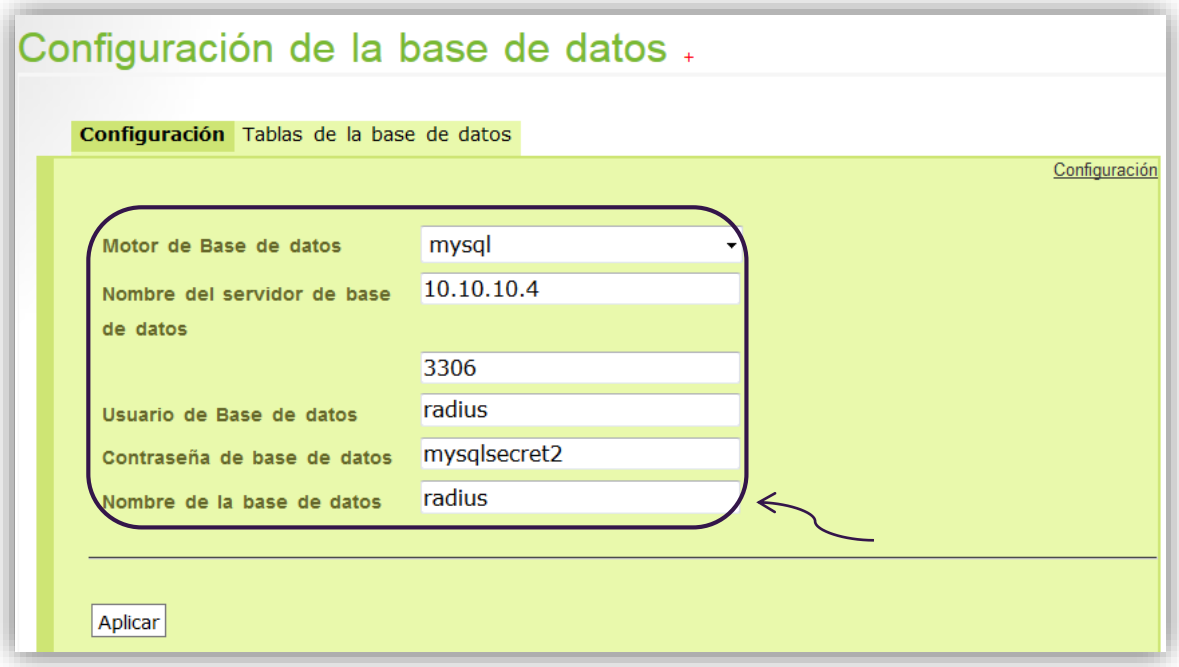


Figura 26. Configuración de la conexión MySQL

2 PUNTO DE POLÍTICAS DE ACCESO A LA RED

Una vez culminado el proceso de autenticación, el servidor RADIUS le asigna un ID de VLAN al usuario, cada subred tendrá acceso a una determinada cantidad de recursos o servicios de red, en base a las actividades que realice el trabajador y las políticas de acceso establecidas por el administrador. Los privilegios y niveles de acceso son controlados por el Firewall o punto de políticas de red.

2.1 ACCESO A LA INTERFAZ WEB

Webmin proporciona una interfaz web para la administración de servidores GNU/Linux basados en consola.

Para ingresar a la interfaz web del Firewall, ingrese la dirección https://10.10.10.1:10000 en la barra de navegación de un explorador de internet (véase Figura 27).

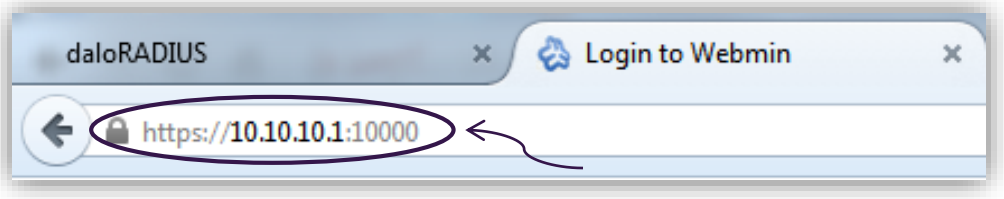


Figura 27. Acceso al Firewall

Se desplegará una ventana de autenticación para acceder a la interfaz de administración, ingrese el nombre de usuario **firewall-aaa** y su correspondiente **contraseña** (véase Figura 28).

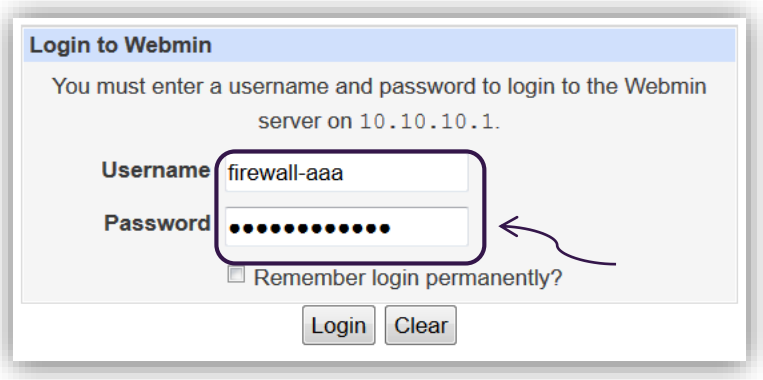


Figura 28. Acceso a Webmin

2.2 CONFIGURACIÓN DE RED

A través de la sección "**red**" de Webmin se accede a la configuración de las interfaces del Firewall (véase Figura 29).

Figura 29. Webmin: sección red

2.2.1 INTERFACES DE RED

Usando el módulo de configuración de red se modifican las interfaces de red, el nombre de la máquina y los servidores de nombres de dominio (véase Figura 30).

Figura 30. Acceso a las interfaces de red del Firewall

2.2.2 INTERFACES DE RED ACTIVAS

Si requiere verificar la cantidad de interfaces activas del firewall, ingrese a la sección "Interfaces de red".

A continuación se despliega una tabla con toda la información (véase Figura 31).

Figura 31. Listado de interfaces de red

2.2.3 EDICIÓN DE UNA INTERFAZ ACTIVA

Para editar una interfaz de red activa, ubique el cursor en la columna "**nombre**" (véase Figura 31), a continuación, haga clic en la interfaz que requiere modificar.

Los parámetros a editar son:

- ✓ Nombre de la interfaz, por ejemplo "**eth10**".
- ✓ Dirección IP
- ✓ Máscara de red
- ✓ Dirección de broadcast.

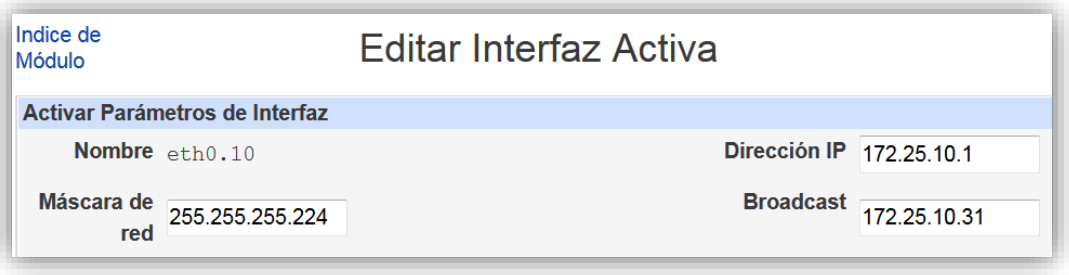


Figura 32. Edición de una interfaz de red

2.3 ADMINISTRACIÓN DEL FIREWALL

Shorewall es una herramienta de alto nivel para configurar filtros de red a través de archivos de configuración.

La estructura de Shorewall se basa en la definición de varios parámetros (Figura 33):

- ✓ Zonas de red
- ✓ Interfaces de red
- ✓ Políticas por defecto
- ✓ Reglas de acceso o negación de servicios
- ✓ Enmascaramiento o NAT.

Figura 33. Estructura de Shorewall - Firewall

2.3.1 ZONAS DE RED

El firewall del sistema AAA está estructurado por tres zonas de red, en la Tabla 1 se muestra el direccionamiento IP utilizado.

Tabla 31. Direccionamiento IP del Firewall

ZONA	DESCRIPCIÓN	SUBRED	INTERFAZ
Red Externa	Acceso a Internet	192.168.8.X	eth1
DMZ	Servidores	10.10.10.1	eth2
Red Interna	Departamentos (VLANs)	172.25.X.X	eth0

La definición de las zonas de red no modifican el funcionamiento del cortafuegos, simplemente define nombres y descripciones.

Para agregar una nueva zona al firewall, se accede al módulo **zonas de red** y luego se elige la opción **Agregar una nueva zona de red** (véase Figura 34).

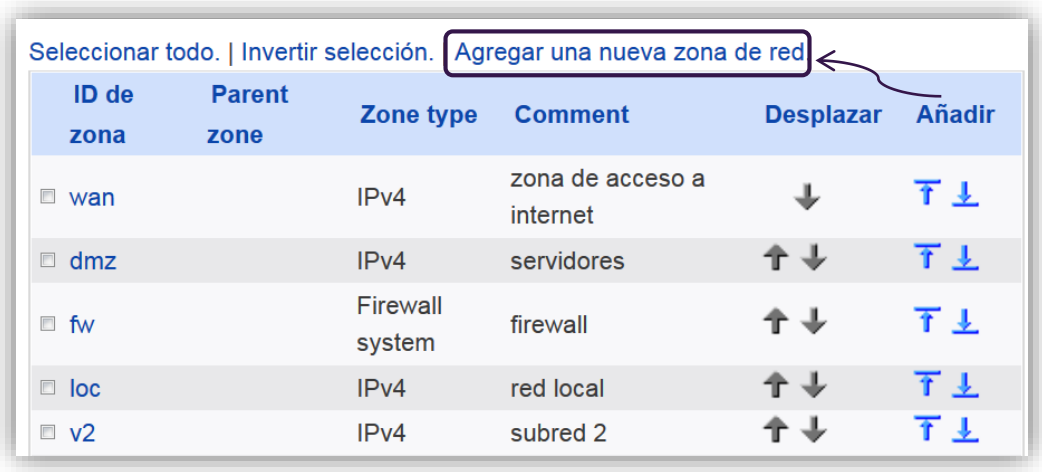


Figura 34. Agregar una nueva zona de red

2.3.2 INTERFACES DE RED

En este módulo se definen todas las interfaces de red del sistema que gestiona el firewall, cada interfaz está asociada o relacionada con una zona de red exclusivamente.

Para agregar una nueva interfaz de red al sistema, haga clic en la opción **Agregar una nueva interfaz de red** y a continuación defina los parámetros requeridos, en la Figura 35 se detallan los valores que debe ingresar.

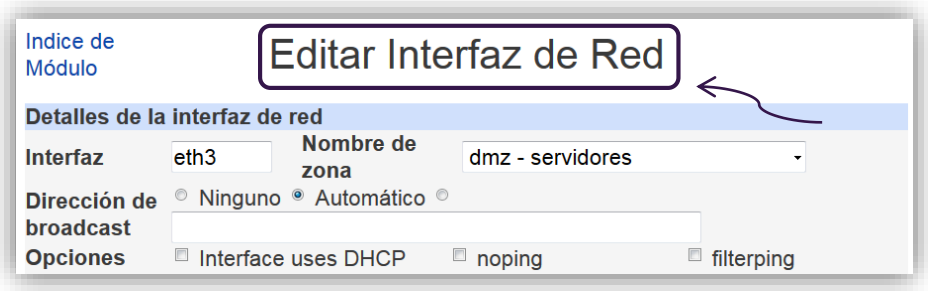


Figura 35. Edición de una interfaz de red

2.3.3 REGLAS DE ACCESO O NEGACIÓN DE SERVICIOS

El módulo está estructurado por una lista de políticas de acceso que permiten o rechazan el tráfico entre las distintas zonas del firewall.

Para crear una nueva regla en el sistema de seguridad haga lo siguiente:

PASO 1. Elija la opción "**Agregar una nueva regla al cortafuegos**".

PASO 2. Ingrese los parámetros:

- **Acción:** controla el establecimiento de las conexiones. Las acciones posibles son: ACCEPT, DROP, REJECT, DNAT, REDIRECT, CONTINUE, LOG, etc.
- **Zona origen:** defina la zona de origen de los paquetes. (DMZ, WAN, LAN, Firewall)
- **Zona o puerto de destino:** defina la zona hacia donde se dirigen los paquetes. Para las acciones DNAT y REDIRECT se debe ingresar la dirección o número de puerto de destino.
- **Protocolo:** defina el protocolo usado para establecer la conexión (TCP o UDP)
- **Puerto de origen:** configure el número de puerto TCP/UDP de origen.
- **Puerto de destino:** configure el número de puerto TCP/UDP de destino.

PASO 3. Haga clic en **salvar** para guardar los cambios realizados.

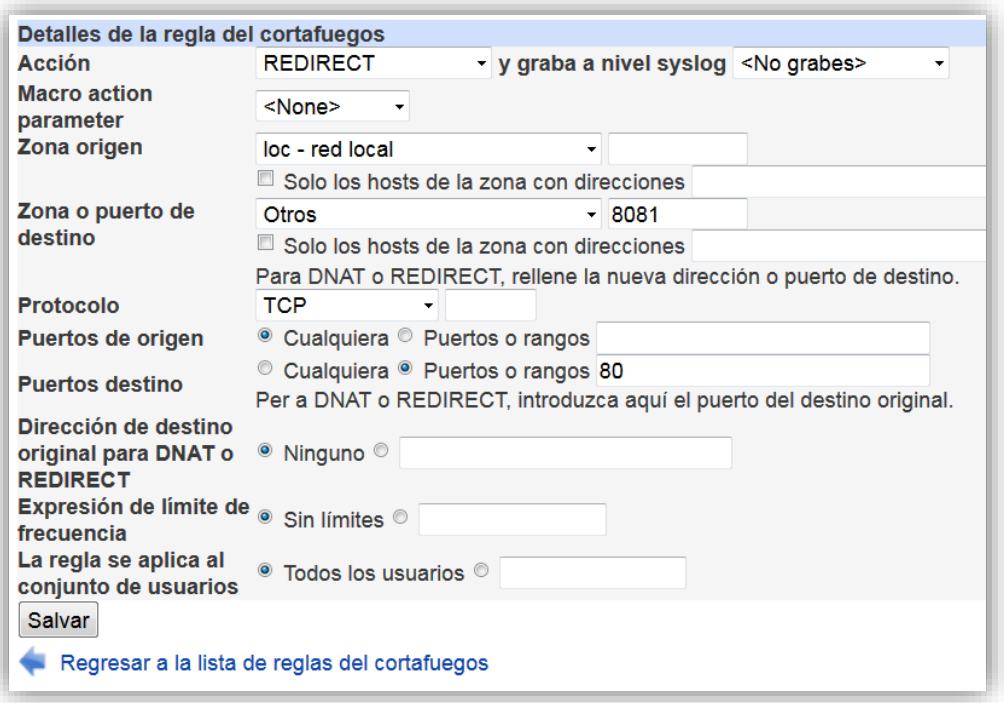


Figura 36. Creación de una nueva regla en el firewall

2.3.4 ENMASCARAMIENTO

El mecanismo de enmascaramiento permite la traducción de direcciones de red para permitir el tráfico entre una red interna y el internet.

Para permitir el acceso a la WAN desde una red interna a través de una interfaz de salida haga lo siguiente:

PASO 1. Haga clic en **Agregar una nueva regla de enmascaramiento**.

PASO 2. Elija la interfaz de salida usada para enmascarar una dirección de red. Por ejemplo **eth1**.

PASO 3. Defina la dirección IP de red o la interfaz a enmascarar.

PASO 4. Haga clic en **salvar** para guardar los cambios realizados.

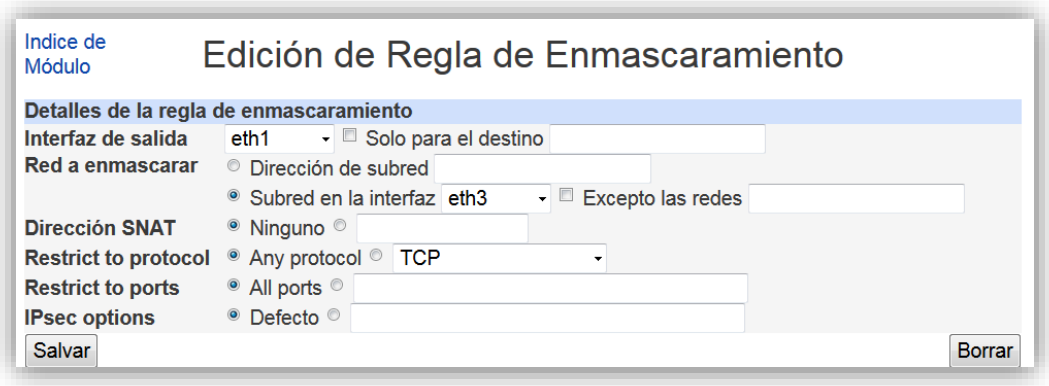


Figura 37. Enmascaramiento de una red

2.3.5 PARÁMETROS PERSONALIZADOS

Los parámetros facilitan la administración y gestión del firewall asignando direcciones de red o hosts a un identificador personalizable.

Para crear un nuevo parámetro realice el siguiente procedimiento:

PASO 1. Haga clic en "**Add a new custom parameter**".

PASO 2. Defina el nombre de identificación para el nuevo parámetro.

PASO 3. Asigne los valores del parámetro (direcciones IP de red o hosts)

PASO 4. Haga clic en **crear** para guardar los cambios realizados.

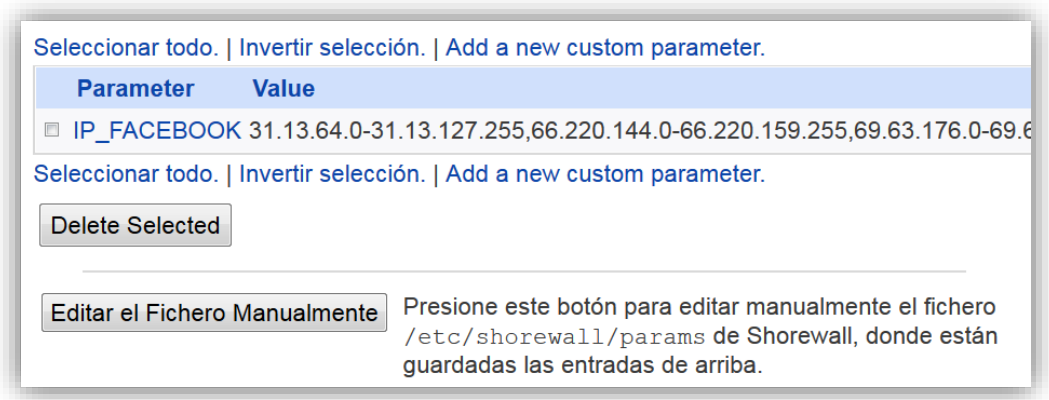


Figura 38. Edición de un parámetro

3 CLIENTE RADIUS: AUTENTICADOR CISCO

En esta sección se describe la configuración del cliente RADIUS (switch Cisco Small Business, serie 300) encargado de controlar el acceso a la red en base a puertos.

3.1 ACCESO AL SWITCH CISCO

Para acceder a la utilidad de configuración basada en web del switch CISCO Small Business, se realiza lo siguiente:

PASO 1. Ingrese la dirección IP del dispositivo **http://172.25.1.254** en la barra de navegación utilizando cualquier explorador web, como se muestra en la Figura 39.

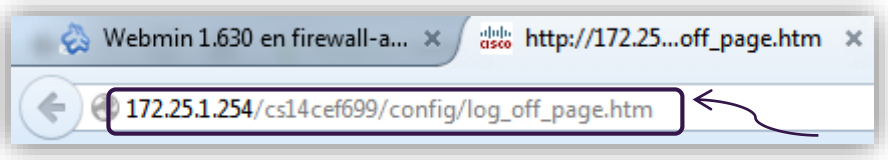


Figura 39. Acceso al switch Cisco Small Business, serie 3000

PASO 2. Ingrese el **nombre usuario** y **contraseña** para autenticarse e iniciar sesión.

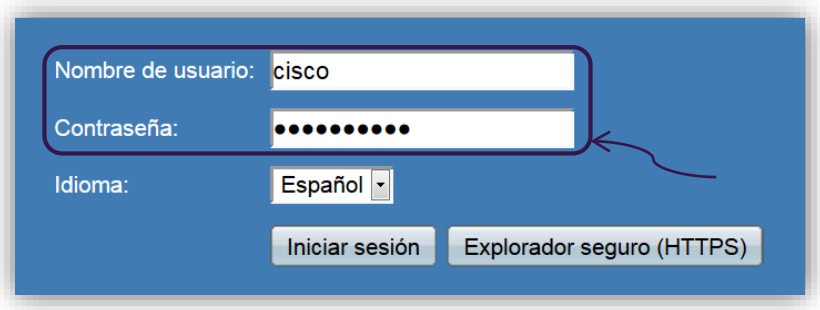


Figura 40. Inicio de sesión switch cisco

Nota. De forma predeterminada, el switch cisco finaliza la sesión después de diez minutos de inactividad.

3.2 ADMINISTRACIÓN DE VLAN

El sistema AAA administra 17 redes virtuales (véase Tabla 2) que representan a cada una de las unidades departamentales de la institución.

Las VLAN son asignadas por el servidor RADIUS de forma dinámica a un puerto, por lo que no debe configurar los puertos en modo acceso.

Tabla 2. VLANs del sistema AAA

VLAN ID	DEPARTAMENTO	SUBRED
100	DATA CENTER	172.25.1.0
2	ALCALDÍA	172.25.2.0
3	PROCURADURÍA SINDICA	172.25.3.0
4	COMISARIA	172.25.4.0
5	DIRECCIÓN DE PLANIFICACIÓN CIUDADANA	172.25.5.0
6	SECRETARÍA GENERAL	172.25.6.0

7	DIRECCIÓN ADMINISTRATIVA	172.25.7.0
8	DIRECCIÓN FINANCIERA	172.25.8.0
9	DIRECCIÓN DE OBRAS PÚBLICAS	172.25.9.0
10	DIRECCIÓN DESARROLLO SOSTENIBLE	172.25.10.0
11	DESARROLLO SOCIAL Y COMUNICACIÓN	172.25.11.0
12	PATRONATO MUNICIPAL	172.25.12.0
13	AUDITORIA	172.25.13.0
14	BIBLIOTECA	172.25.14.0
15	INFOCENTROS	172.25.15.0
16	Wi-Fi	172.25.16.0

3.2.1 CREACIÓN DE VLAN

El procedimiento para agregar una nueva VLAN al sistema AAA es el siguiente:

PASO 1. Acceda a la sección general **Administración de VLAN**.

PASO 2. Haga clic en **Configuración de VLAN** (véase Figura 41).

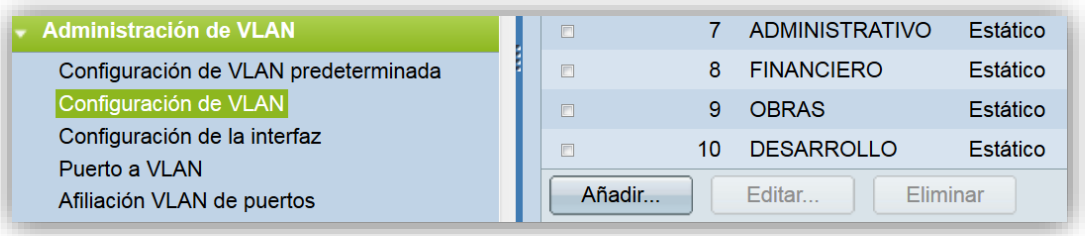


Figura 41. Acceso a la configuración de VLAN

PASO 3. Haga clic en **añadir.**

PASO 4. Ingrese el identificador (1 a 4094) y el nombre de la VLAN, (véase Figura 42).

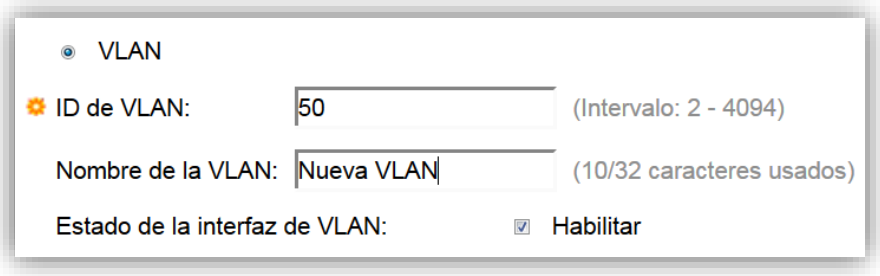


Figura 42. Creación de nueva VLAN

PASO 5. Finalmente, haga clic en **aplicar.**

3.2.2 ASIGNACIÓN DINÁMICA DE VLAN

Para permitir la asignación dinámica de VLAN, el puerto se debe configurar en modo **general** siguiendo el proceso que a continuación se detalla.

PASO 1. Acceda a la sección general **Administración de VLAN**.

PASO 2. Haga clic en la opción **Configuración de la interfaz** (véase Figura 43).

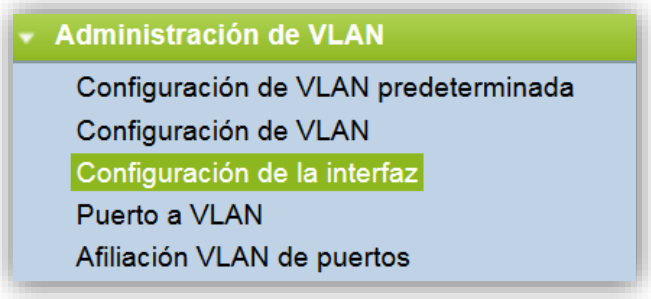


Figura 43. Configuración de la interfaz

PASO 3. Elija la opción **General** en la sección: **Modo de Interfaz de VLAN.**

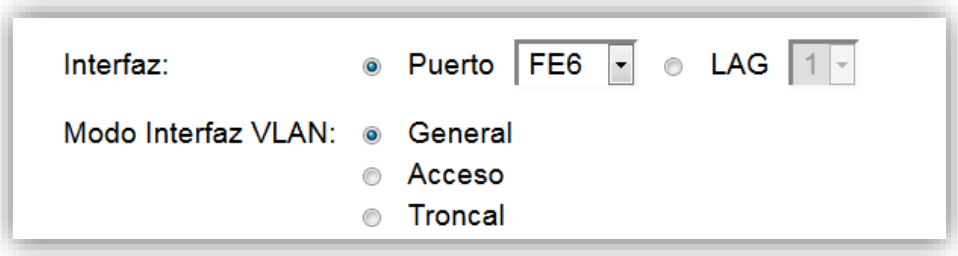


Figura 44. Configuración de puerto en modo General

PASO 4. Como último paso, haga clic en **aplicar** para guardar los cambios.

3.2.3 PUERTO TRONCAL

La nueva VLAN creada debe ser añadida a la interfaz configurada como puerto troncal para permitir el envío de paquetes etiquetados empleando el protocolo IEEE 802.1Q, mecanismo usado para trasportar paquetes IP de diferentes redes usando el mismo medio físico sin interferencias.

Para agregar la nueva VLAN al puerto troncal:

PASO 1. Haga clic en **Administración de VLAN** y luego seleccione la opción **Afiliación VLAN de puertos,** como se muestra en la Figura 45.

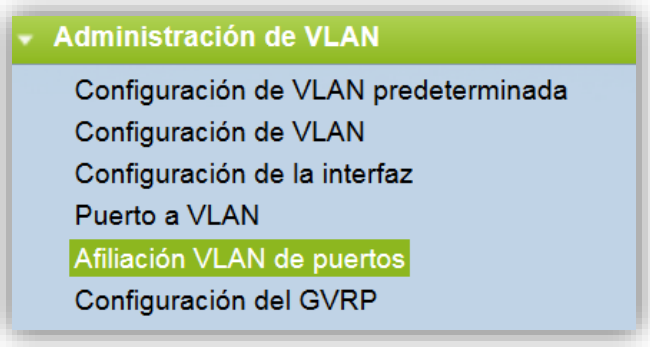


Figura 45. Afiliación de VLAN a puerto troncal.

PASO 2. Seleccione la interfaz configurada como **troncal** (véase Figura 46).

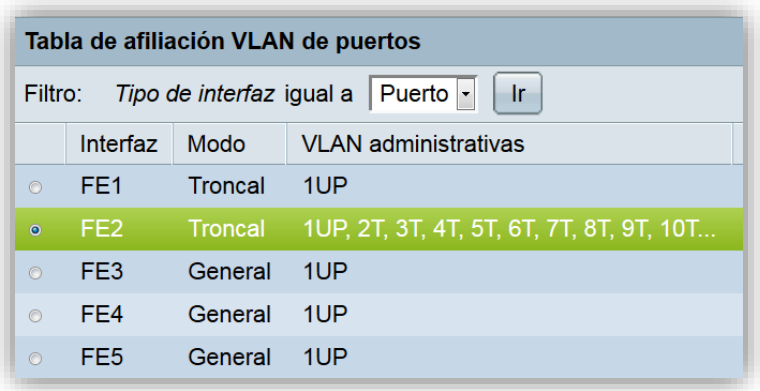


Figura 46. Selección del puerto troncal

PASO 3. Haga clic en el botón **Unir a VLAN** y luego seleccione la VLAN que requiere añadir al puerto troncal del switch (véase Figura 47).

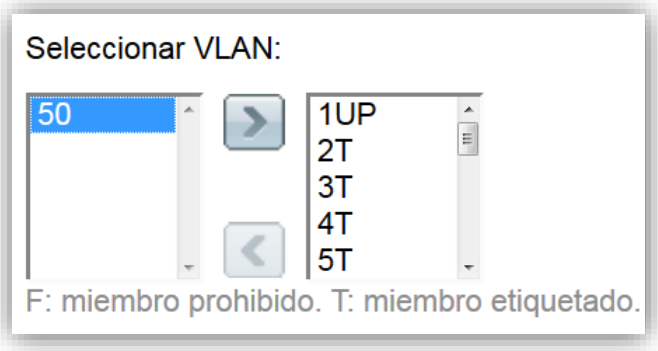


Figura 47. Unión de VLAN al puerto troncal

PASO 4. Haga clic en **aplicar** para guardar los cambios.

3.3 AUTENTICACIÓN 802.1X

El servidor RADIUS proporciona un control de acceso de red centralizado basado en 802.1X. El switch CISCO SMALL BUSINESS, es un cliente RADIUS que utiliza un servidor FreeRADIUS para proporcionar seguridad centralizada empleando EAP-TTLS como método de autenticación.

Cuando un usuario intenta conectarse a la red mediante una solicitud de acceso, el switch habilita el proceso de autenticación y posteriormente, una vez autenticado, le asigna una VLAN de forma dinámica. Para que el dispositivo ejecute las acciones mencionadas siga los pasos que se muestran a continuación:

PASO 1. Acceda a la sección **Seguridad** y luego **Autenticación web/MAC/802.1X.**

PASO 2. Haga clic en la opción **Propiedades**

PASO 3. Seleccione el ID de VLAN para habilitar la autenticación (véase Figura 48).

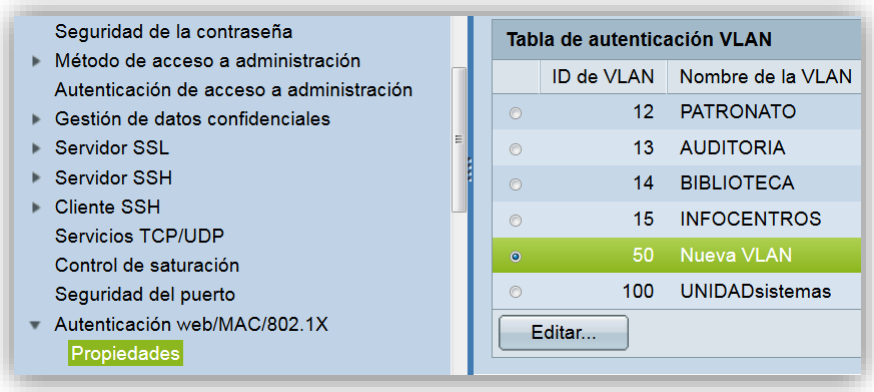


Figura 48. Autenticación web/MAC/802.1x

PASO 4. Seleccione la opción **Habilitado** en la pantalla desplegada, como se muestra en la Figura 49.

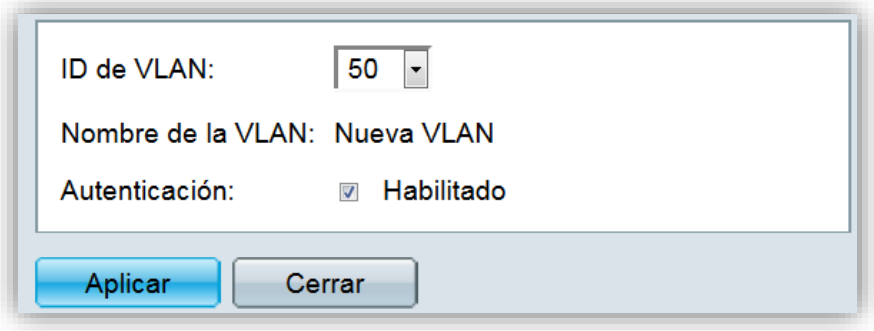


Figura 49. Habilitar autenticación 802.1x en nueva VLAN

PASO 5. Acceda a la opción **Autenticación de puertos** como se muestra en la Figura 50.

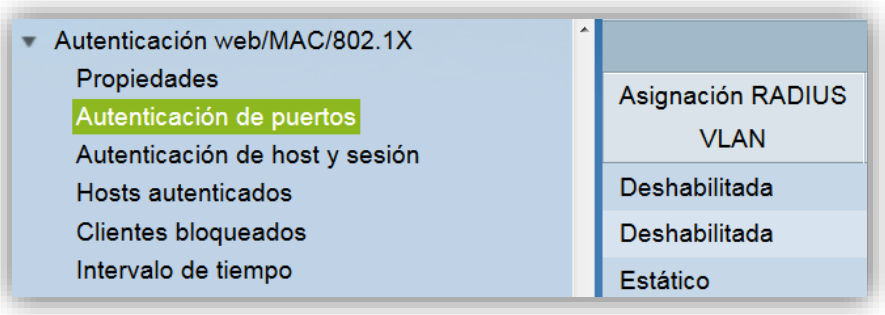


Figura 50. Autenticación de puertos.

PASO 6. Selección una interfaz y a continuación haga clic en la opción **editar**.

PASO 7. En la sección **Control de puerto administrativo** seleccione la opción **Automática**, esto hará que el puerto autorice o no el acceso a un usuario dependiendo del proceso de autenticación.

PASO 8. En la sección **Asignación RADIUS VLAN,** active la opción **Estático** como se muestra en la Figura 51.

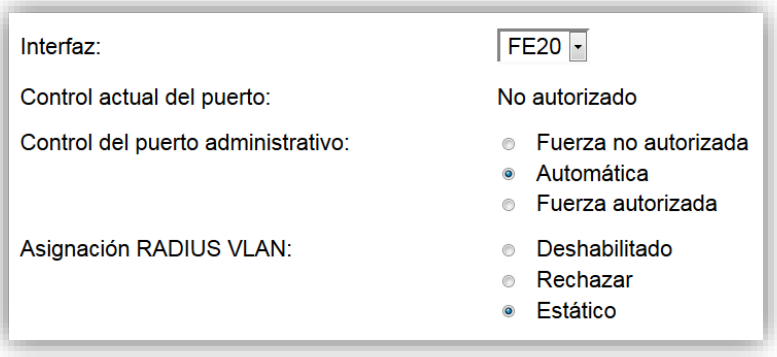


Figura 51. Asignación dinámica de VLAN.

PASO 9. Haga clic en **aplicar** para guardar los cambios realizados.