ADMINISTRACIÓN Y GESTIÓN DE USUARIOS PARA ACCESO A LA RED INALÁMBRICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS BASADO EN EL PROTOCOLO 802.1x

Fabián G. Cuzme, Carlos P. Bosmediano
fgcuzme@utn.edu.ec, cpbosmedianoc@utn.edu.ec
Universidad Técnica del Norte - Facultad de Ingeniería en Ciencias Aplicadas

***Resumen*— El proyecto planteado consiste en el diseño e implementación de un servidor que proporcione Autenticación, Autorización y Auditoria (AAA) en la red inalámbrica de la Facultad de ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte, para el control de acceso y administración de recursos de red, empleando soluciones basadas en software libre. La autenticación de usuarios se realiza utilizando el método EAP-TTLS basados en el protocolo IEEE 802.1x con dispositivos finales marca Mikrotik, además de contar con un directorio centralizado LDAP en software libre que almacena las credenciales de acceso y permite la asignación de recurso de red.**

***Palabras clave*— AAA, EAP-TTLS, IEEE 802.1X, RADIUS, LDAP, MIKROTIK**

I. INTRODUCCIÓN

Cuando nosotros consideramos un sin número de requisitos de seguridad en aplicaciones distribuidas, la autorización y control aparece como un elemento clave para el diseño del sistema de seguridad completo

Actualmente, la tarea más demandada para administradores de la red es asegurar que todo dispositivo que se conecte a la red por cualquier método de acceso, cumpla con un modelo de seguridad establecido por la entidad, controlando de esta manera el acceso de personal no autorizado; utilizando mecanismos de autentificación que garanticen el acceso solo a usuarios que pertenezcan a la entidad.

Con el planteamiento de este proyecto se pretende elevar los niveles de seguridad en el intercambio de información dentro de la red inalámbrica de la Facultad de Ingeniería en Ciencias Aplicadas, de esta forma se da acceso al usuario que cuente con la debida autorización para que acceda a los diferentes servicios; al mismo tiempo se podrá mantener un control estricto y directo de los usuarios conectados a la red, brindando una correcta distribución de la red inalámbrica y evitando el mal uso del servicio.

II. CONCEPTOS

A. Sistemas AAA

Es una arquitectura de sistema que se utiliza para configurar el trío de funciones de seguridad Autenticación, Autorización y Contabilidad de una forma coherente.

- **Autenticación.** - Proporciona el método de identificación de usuarios, incluyendo nombre de usuario y contraseña, desafío y respuesta, soporte de mensajería, y, dependiendo del protocolo de seguridad que se elija, puede ofrecer cifrado. La autenticación es la manera en la que el usuario se identifica antes de que se le permita acceder a la red y sus servicios [1].

- **Autorización.** - Otorga el método de control de acceso remoto, incluyendo la autorización total o para cada servicio, lista de cuentas y perfil por usuario, soporte para grupos de usuarios. La autorización de AAA trabaja formando el grupo de atributos que describen lo que el usuario tiene permitido usar o a lo que puede acceder. Estos atributos se comparan con la información existente en una base de datos o un directorio para cada usuario; el resultado es devuelto a AAA con el fin de determinar las capacidades reales de los usuarios y sus restricciones. Es posible localizar de forma local dicha base de datos en el servidor de acceso o router, como también puede ser alojado de forma remota en un servidor de seguridad RADIUS.

- **Contabilidad.** - AAA cuenta con un método de recolección y envío de información al servidor de seguridad, la cual inicia cuando el equipo autenticador o NAS autoriza al suplicante acceder a los servicios de red. Contabilidad permite ejecutar el seguimiento de los usuarios con acceso a los servicios, así como la cantidad de recursos que están utilizando. Al activarse AAA contabilidad y según el método de seguridad que se haya implementado, el acceso a la red del servidor informa la actividad del usuario al servidor de seguridad RADIUS a manera de registros contables, permitiendo al administrador de la red gestionar la futura demanda de sus sistemas para planificar su crecimiento.

B. Radius

Remote **A**uthentication **D**ial **I**n **U**ser **S**ervice, que significa: autenticación remota para usuarios de servicio telefónico. Es un protocolo muy utilizado para el control de

acceso a la red, implementado en dispositivos tales como routers, switch y servidores basada en un modelo cliente-servidor. Proporciona autenticación centralizada, autorización y manejo o contabilización de cuentas (AAA). Este sistema de seguridad garantiza el acceso remoto a las redes y sus servicios contra el acceso no autorizado [2].

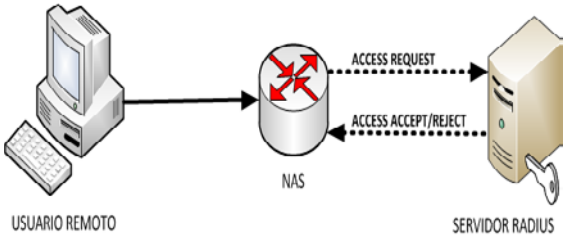


Figura 1. Comunicación RADIUS

RADIUS utiliza el puerto UDP 1812 para el proceso de autenticación y 1813 para el registro de la información (contabilidad).

C. *IEEE 802.1x*

802.1x es el estándar basado en IEEE para gestionar el control de acceso a la red mediante un proceso conocido como autentificación; el cual permite o impide el acceso de cualquier dispositivo que se intente conectar a la red LAN o WLAN. La letra "x" representa el uso obligatorio de protocolo EAP (autentificación extensible) entre cualquier suplicante que pueden ser usuarios de red inalámbrica como cableada, el autenticador como los switches o access point y los servidores de autentificación como el Radius. [3].

Una infraestructura de red 802.1x requiere de tres elementos para operar: suplicante, equipos autenticadores y servidor de autenticación.

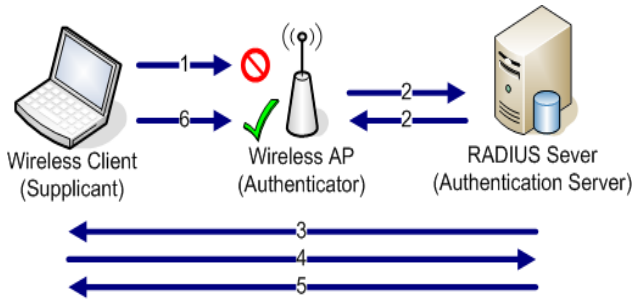


Figura 2. Flujo de autentificación IEE 802.1x

El proceso de autenticación comienza cuando el usuario final intenta conectarse a la WLAN, el autenticador recibe la solicitud y crea un puerto virtual con el solicitante, obligando al autenticador actuar como un proxy para el usuario final el cual garantizara el traspaso de información entre el cliente y el servidor, por tanto:

- El cliente puede enviar un mensaje EAP-inicio.
- El punto de acceso envía un mensaje de identidad de solicitud EAP.
- El servidor de autenticación pide al cliente sus credenciales para demostrar su confiabilidad.
- El servidor de autenticación acepta o rechaza la solicitud del cliente para la conexión.
- Si el usuario final fue aceptado, el autenticador cambia el puerto virtual con el usuario final a un estado autorizado, que permite el acceso de red.
- Al iniciar la sesión inicial, el puerto virtual del cliente se cambia de nuevo al estado no autorizado.

D. *Eap-ttls*

EAP-TTLS es el metodo EAP (Extensible Authentication Protocol) que encapsula una sesión TLS (Seguridad de la capa de transporte), el cual consiste en establecer la conexión segura mediante la creación de un canal cifrado entre el cliente y el servidor para el envío de las credenciales de acceso durante el proceso de autenticación. Durante la fase de datos, el cliente se autentica al servidor (o cliente y el servidor se autentican mutuamente) utilizando un mecanismo arbitrario de encapsulado dentro del túnel seguro (PAP, CHAP, MS-CHAP o MS-CHAP-V2) [4].

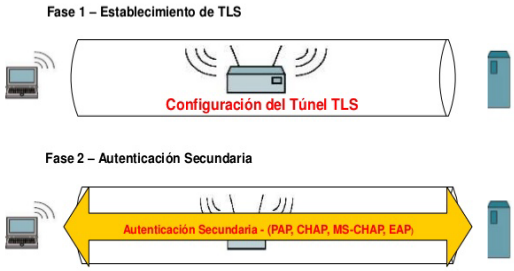


Figura 3. Método EAP-TTLS (2 fases)

Es indescriptible la instalación de un certificado digital en el servidor de autenticación RAIDUS, permitiendo de esta forma reducir la complejidad del sistema, evitando la difusión de certificados a todos los dispositivos de red.

E. *FREERADIUS*

FreeRADIUS es un paquete de distribución en software libre Linux de código abierto, que implementa diversos elementos concernientes con RADIUS, por ejemplo, una biblioteca BSD para clientes, módulos para soporte en apache, y lo más importante, un servidor Radius. [5]

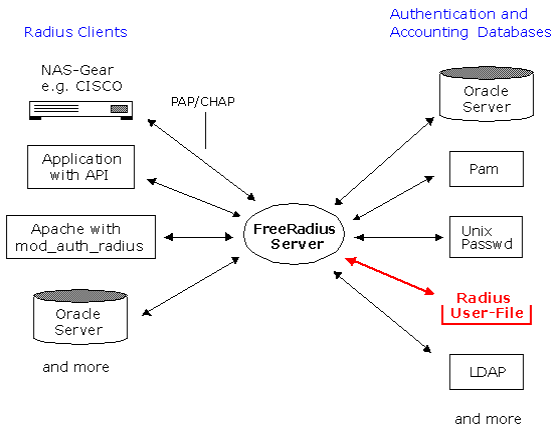


Figura 4. Elementos FREERADIUS

El servicio de FreeRADIUS es modular, para facilitar su extensión; presenta las siguientes características

- Escalable: debido a que se puede ejecutar en múltiples sistemas operativos: Linux (Debian, Ubuntu, Suse, Mandriva, Fedora Core, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin.
- Soporta prácticamente toda clase de clientes Radius (por ejemplo, ChilliSpot, JRadius, mod_auth_radius, pam_auth_radius, Pyrad, extensiones php de RADIUS, etc).
- Realización de trabajos AAA, al cual se podrá almacenar y acceder a la información por medio de múltiples bases de datos: LDAP (AD, OpenLdap,), SQL (Mysql, PostgreSQL, Oracle,) y ficheros de texto (fichero local de usuarios, mediante acceso a otros Reales, fichero de sistema /etc/passwd,).

F. LDAP

Lightweight Directory Access Protocol, o Protocolo Ligero en Acceso a Directorios, es un protocolo de tipo aplicación que permite el acceso a un servicio de directorio ordenado y distribuido, que se utiliza para buscar información diversa en un entorno de red. Entre las ventajas encontramos que una de sus aplicaciones es la autenticación de usuarios basado en Radius controlando el acceso a una red.

Garantiza además una lectura rápida de los registros asegurando que cada uno de ellos sea único, permite crear múltiples directorios independientes y de forma jerárquica para asignación de privilegios, sencillo de instalar y mantener [6].

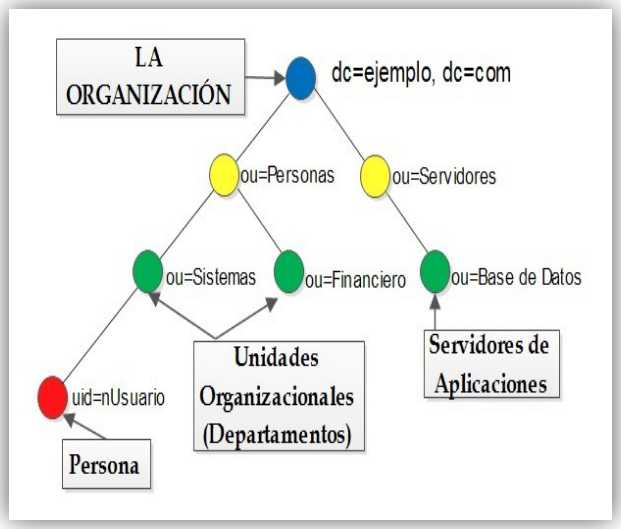


Figura 5. Estructura general de un directorio LDAP

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 5, que muestra algunos objetos reales en una organización.

III. DISEÑO DE LA INFRAESTRUCTURA AAA

El sistema de autentificación y control está basado en el protocolo 802.1x con el método de autentificación EAP-TTLS, el cual se acoplará a los puntos de acceso de la marca Mikrotik.

A. Requerimientos suplicantes (usuarios)

El software necesario con soporte EAP-TTLS que será instalado en los dispositivos del usuario final, para poder acceder a la red inalámbrica

Tabla 1. Requerimientos técnicos para suplicantes

SISTEMA OPERATIVO	EAP-TTLS
Windows 7	SecureW2
Windows 8 / 8.1	Cliente Nativo/ SecureW2
Windows 10	Cliente Nativo
Ubuntu/Debian/Centos Android OS/ IOS (Iphone-OS)	Cliente Nativo

B. Requerimientos de Autenticador (puntos de acceso)

Todo equipo que brinde el acceso a la red; ubicado entre los dispositivos de usuario que requieren ser autenticados y el servidor de autenticación, deben cumplir con los requerimientos técnicos detallados en la Tabla 2.

Tabla 2. Requerimientos técnicos para suplicantes

Requerimiento	Características
RAM	64 MB
10/100 puertos Ethernet	1
Estándares Wireless	802.11b/g/n
OS	RouterOS
Licencia nivel	4
Ganancia de la antena DBI	2
Almacenamiento	16 MB
CAP	SI

C. Requerimientos del servidor autenticación

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 la Tabla 3 se detallan los requerimientos.

Tabla 3. Requerimientos servidor de autenticación

AUTENTICACIÓN	
Servidor	FreeRADIUS
Control de acceso	IEEE 802.1x
Método de autenticación	EAP-TTLS
Conexión	Equipo Autenticador (MIKROTIK)
AUTORIZACIÓN	
Servidor	OpenLDAP
Contraseñas	Algoritmo MD5 o SHA
Conexión	Servidor FreeRADIUS
CONTABILIDAD	
Servidor	FreeRADIUS/MIKROTIK
Conexión	Servidor FreeRADIUS
CRS	
Tamaño RAM	2 GB
10/100/1000 Ethernet puertos	13
PoE	Si
Server DHCP	Si
CAPsMAN	Si
CAP	Si
UEUE	Si

IV. IMPLEMENTACIÓN DEL SERVIDOR AAA

En base al esquema actual de red dentro de las instalaciones de la Facultad de Ingeniería en Ciencias Aplicadas, se implementa el servicio AAA (Figura 6) con equipos de la maca Mikrotik modelo cAP-2n (CAP), RB1100 (CAPsMAN) como autenticadores, server FreeRADIUS Debian 8 como servidor de autenticación, con el fin de garantizar un acceso a la red de la institución.

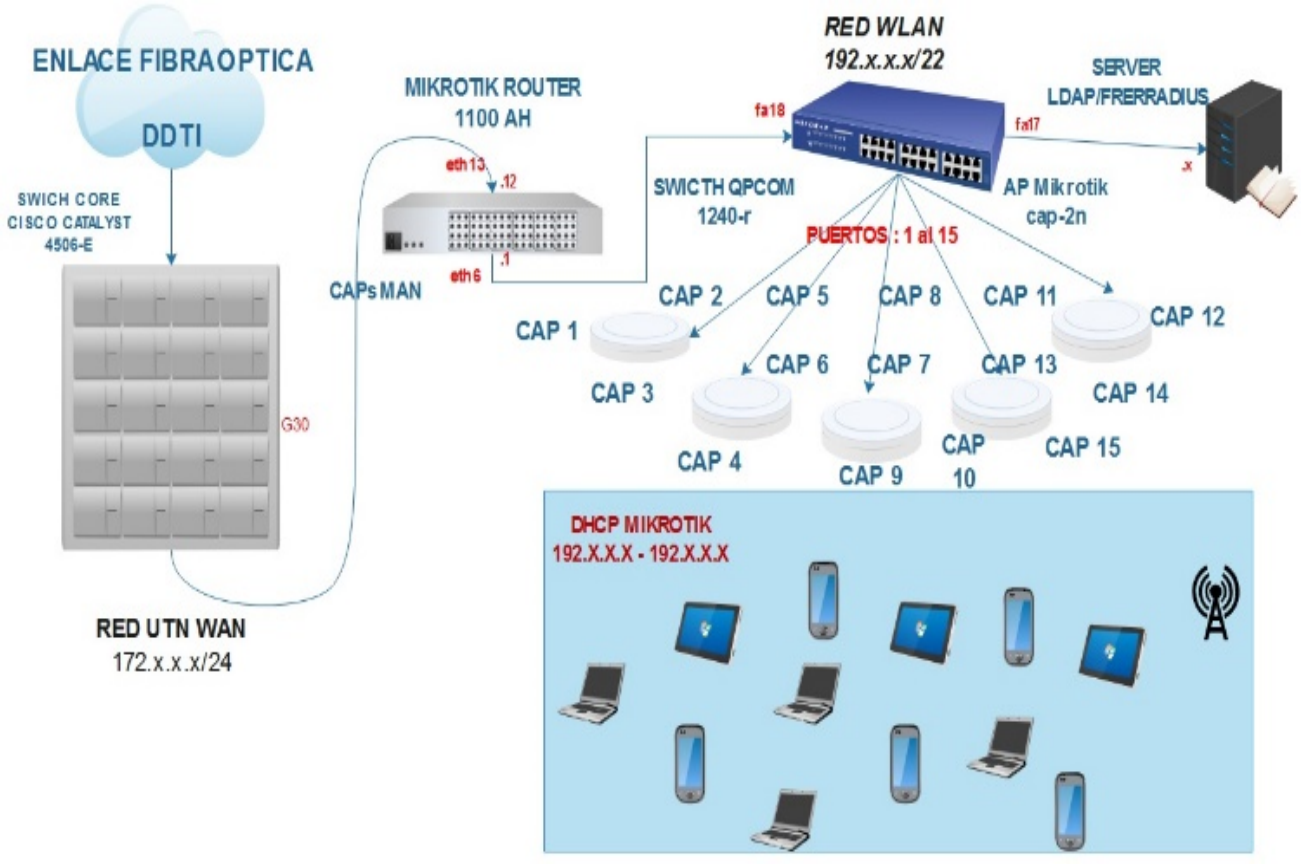


Figura 6. Topología Física y Lógica de la red inalámbrica

A. Sistema AAA

El servicio AAA requiere la instalación de 2 paquetes en el servidor Debian 8: FreeRADIUS para el servicio de autenticación EAP-TTLS, OpenLDAP como directorio de almacenamiento de credenciales de usuario y la base de datos, así como el servicio de Acconunting.

- **Elección de hardware**

Para la implementación del presente proyecto se utilizará el equipo IBM System x3200, debido a que presenta la mayor valoración en requerimientos como muestra la tabla 4.

Tabla 4. Requerimientos de hardware

	Procesamiento 3.5GHz	Almacenamiento 1Tb	Puerto Gigabit Ethernet	Compatibilidad SO libre	Total
IBM System x3250 M3	0	1	0	1	2
IBM System x3200 M2	1	1	1	0	3

Nota: **1 – Cumple**
0 – No Cumple

- **FreeRADIUS**

Todas las dependencias y paquetes se pueden obtener desde sus propios repositorios de datos, utilizando el comando que se muestra en la figura 7. Una ventaja de utilizar el Debian 8 – Jessie como sistema operativo base, es que se encuentra disponible para la mayor parte de arquitecturas tanto en 32 bits como en 64 bits, lo cual agiliza el proceso de instalación de cualquier software y sus dependencias.

```
root@debian:/home/fica# apt-get install  freeradius-ldap
Reading package lists... Done
```

Figura 7. Instalación FreeRADIUS en Debian 8 - Jessie

- **OPENLDAP**

La facultad de Ingeniería en Ciencias Aplicadas (FICA) 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 crea un directorio utilizando OpenLDAP

La estructura de la base de datos que se implementará en la facultad y albergará a los usuarios de la red "ficawifi", se encuentra en un orden jerárquico como muestra la figura 8 usando como referencia las diferentes carreras existentes, cada una con sus respectivos usuarios: Docentes, Estudiantes, personal administrativo, las credenciales de acceso serán difundidas a través del portafolio personal de la institución.

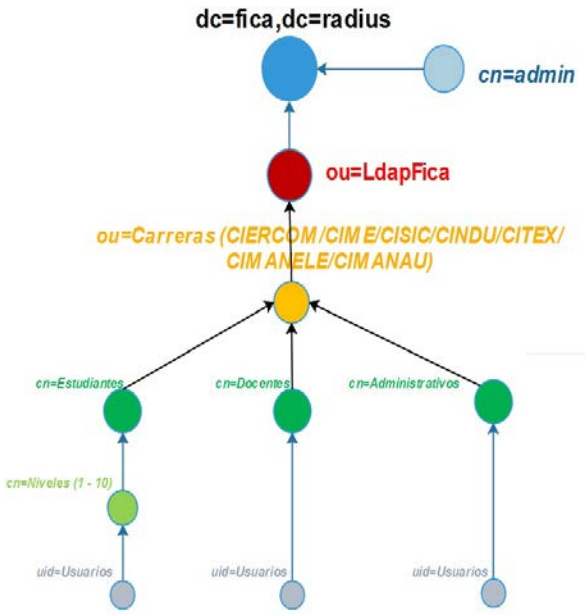


Figura 8. Estructura jerárquica LDAP - FICA

Para la instalación del servicio LDAP se utiliza el comando de la figura 9,

```
root@debian:/home/fica# apt-get install slapd ldap-utils
Reading package lists... Done
```

Figura 9. Instalación OpenLDAP

Una vez que se instalado, procedemos reconfigurar con el comando ***dpkg-reconfigure slapd***; en donde colocaremos los datos que se muestran a continuación

1. Desea omitir la configuración del servidor OpenLdap: **<NO>**
2. Introducimos el nombre del dominio: **utn**
3. Introducimos nombre de la organización: **fica.radius**
4. Introducimos una contraseña para Ldap y la confirmamos: ******
5. Motor de base de datos a utilizar: **MDB**
6. Borrar la base de datos cuando se purgue el paquete slapd: **<SI>**
7. Permitir protocolo LDAPv2: **<NO>**

B. Autenticador (CAP y CAPsMAN)

La implementación del servicio 802.1x para el control de acceso a red inalámbrica se lo hace en el CRS – Mikrotik RB1100 en modo CAPsMAN, operando en capa 2 y capa 3, mientras que la conectividad de usuarios finales se los hace a través del CAP-2n MikroTik.

- **Configuración cAP-2n (CAP)**

Para lograr la comunicación entre todos los equipos de la red, es necesario ubicar a todos nuestros CAP en un mismo segmento de red. Ingresamos a la pestaña IP/ADDRESSES/ADDRESS LIST/NEW ADDRESS y colocamos la dirección IP correspondiente a dicho CAP, repitiendo el proceso en cada access point (figura 10).

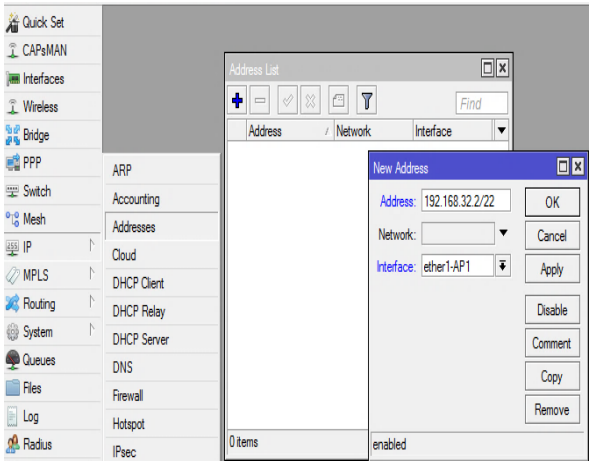


Figura 10. Asignación IP fija CAP1-AP1

A continuación, procedemos a activar el CAP (figura 11) dentro de la pestaña Wireless, el cual permitirá la gestión centralizada del mismo a través del CAPsMAN.

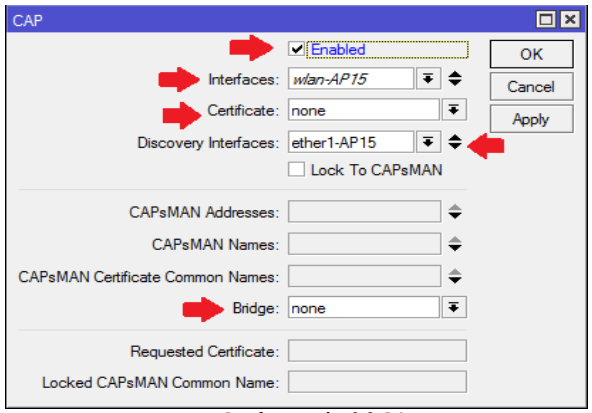


Figura 11. Configuración del CAP

- **Configuración CRS-Mikrotik RB1100 (CAPsMAN)**

Para poder realizar una gestión centralizada habilitamos el Manager en nuestro CAPsMAN en el cual constara con todos los perfiles o configuraciones de redes inalámbricas que serán luego configuradas de forma automática en cada CAP (figura 12). Nos ubicaremos en la pestaña ***CAPsMAN/INTERFACES/MANAGER/ENABLE***, pulsamos aceptar.

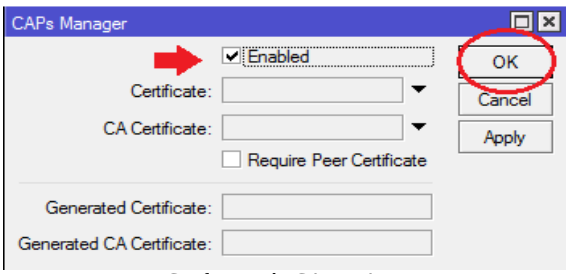
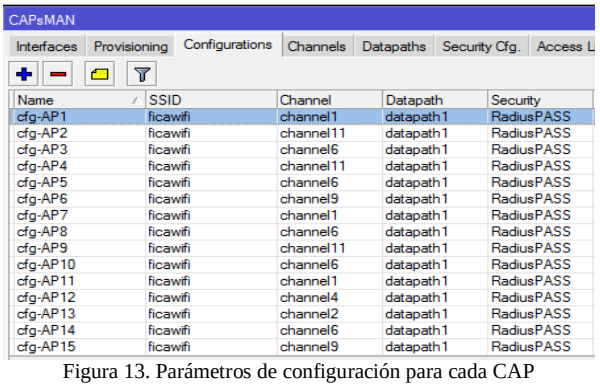


Figura 12. Configuración CAPsMAN

El CAPsMAN puede entregar parámetros de configuración para cada interfaz, dichas configuraciones se encuentran en las pestañas:

1. **Channels**: configuraciones relativas a los canales, como por ejemplo banda, frecuencia y ancho de canal.
2. **Datapaths**: configuración relacionada con el bridge donde se integrará la interfaz de los CAPs. De esta forma se configura el reenvió de tráfico hacia el CAPsMAN
3. **Security Cfg:** configuraciones de autenticación y cifrado. Soporta métodos estáticos (como llaves pre compartidas), EAP y TLS
4. **Configurations:** se encuentran los perfiles principales para cada red inalámbrica. En esta pestaña se configura SSID, se asigna algún canal especifico, el datapath y la correspondiente seguridad.

Una vez creada la configuración (al menos una), se la puede cargar en los diversos CAP (figura 13).



Name	SSID	Channel	Datapath	Security
cfg-AP1	ficawifi	channel1	datapath1	RadiusPASS
cfg-AP2	ficawifi	channel11	datapath1	RadiusPASS
cfg-AP3	ficawifi	channel6	datapath1	RadiusPASS
cfg-AP4	ficawifi	channel11	datapath1	RadiusPASS
cfg-AP5	ficawifi	channel6	datapath1	RadiusPASS
cfg-AP6	ficawifi	channel9	datapath1	RadiusPASS
cfg-AP7	ficawifi	channel1	datapath1	RadiusPASS
cfg-AP8	ficawifi	channel6	datapath1	RadiusPASS
cfg-AP9	ficawifi	channel11	datapath1	RadiusPASS
cfg-AP10	ficawifi	channel6	datapath1	RadiusPASS
cfg-AP11	ficawifi	channel1	datapath1	RadiusPASS
cfg-AP12	ficawifi	channel4	datapath1	RadiusPASS
cfg-AP13	ficawifi	channel2	datapath1	RadiusPASS
cfg-AP14	ficawifi	channel6	datapath1	RadiusPASS
cfg-AP15	ficawifi	channel9	datapath1	RadiusPASS

Figura 13. Parámetros de configuración para cada CAP

- **RADIUS**

Activamos la función RADIUS, para lo cual ingresaremos a nuestro servidor Mikrotik, nos ubicaremos en la pestaña de Radius, crearemos una nueva entrada y configuraremos los siguientes parámetros (figura 14). Activamos la pestaña "Wireless", la cual nos permitirá vincular el servidor LDAP con la tarjeta inalámbrica del router MikroTik.

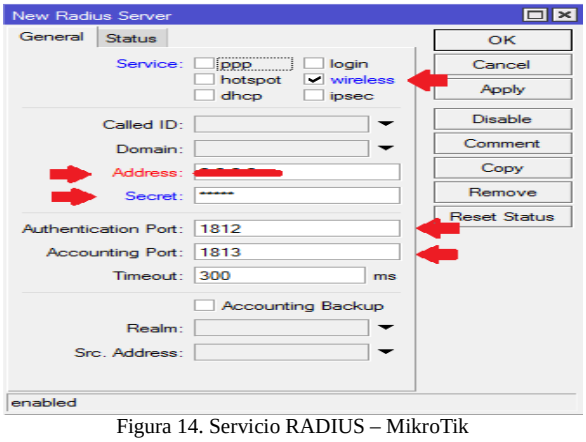


Figura 14. Servicio RADIUS – MikroTik

- **DHCP-SERVER**

El CRS-Mikrotik posee entre sus funciones un servidor DHCP, el cual se encargará de asignar Ip dinámicas a todos los usuarios autorizados en la red. Activamos esta función desde la pestaña IP/DHCP SERVER/ DHCP Setup. (figura 15).

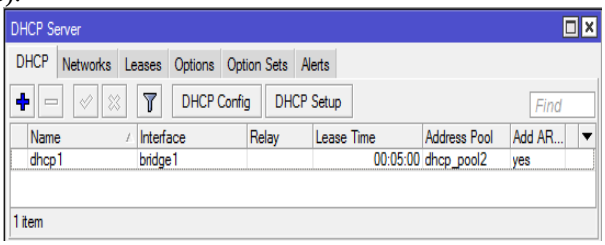


Figura 14. Servidor DHCP

- **SIMPLE QUEUE (ANCHO DE BANDA)**

La forma más sencilla de limitar la velocidad de datos de direcciones y / o subredes específicas, es el uso de colas simples. Para lo cual vamos a crear dos nuevas entradas en la pestaña de QUEUES, una para estudiantes y otra para docentes como se indica en la figura 15.

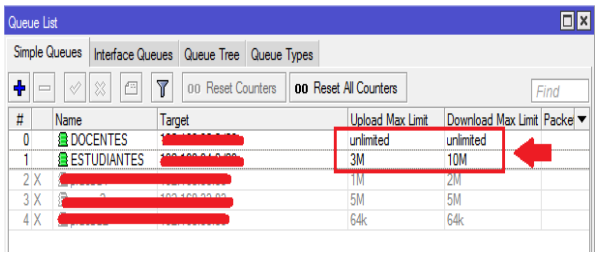


Figura 15. Control de ancho de banda (SIMPLE QUEUE)

C. Usuarios finales – suplicantes

Para poder acceder a la red de datos con el sistema AAA, los usuarios que no poseen el método de autenticación EAP-TTLS requieren de un software adicional (suplicante), 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 7 (figura 16) y en contadas ocasiones Windows 8.1, por otra parte, Windows 10, Linux y MacOS-Appl Android, IOS (iPhone OS) poseen incorporados autentificación EAP-TTLS/PAP de forma nativa.

Figura 16. Configuración SecureW2 – Windows 7 / 8.1

V. CONCLUSIONES

La implementación del servidor de Autentificador Radius en la Facultad de Ingeniería en Ciencias Aplicadas (FICA), logró como resultado una gestión centralizada de usuarios mediante un servidor de autentificación seguro, que a su vez se encuentra apoyada con una distribución equitativa del recurso a través del método de colas simples (QUEUES), para todos los individuos que día a día acceden a los servicios de la universidad a través de la red inalámbrica, garantizando de esta forma una conectividad más estable, confiable y segura ante posibles ataques informáticos, así como también una mejora en la disponibilidad de la red.

El método de autentificación PAP no se suele usar independientemente, ya que se trata de un protocolo inseguro para autenticar un usuario con un servidor de acceso remoto, sin embargo, es utilizado frecuentemente cuando a esta autentificación se asocia EAP-TTLS, cifrando toda la comunicación a través de túneles.

La Facultad de Ingeniería en Ciencias Aplicadas posee una infraestructura de Networking sofisticada, con la integración del servicio de autentificación por separado (base de datos LDAP), se aprovecha al máximo el rendimiento de los dispositivos inalámbricos, logrando autentificar y registrar a diferentes usuarios simultáneamente a través de 802.1x evitando que el servicio caiga por saturación de peticiones en el punto de acceso y otorgando el ingreso solo a usuarios permitidos.

Cabe recalcar que el sistema implementado se encuentra enfocado para todos aquellos dispositivos con soporte del estándar 802.1x, esto debido a que en la actualidad la mayoría de marcas comerciales dan este tipo de soporte nativo, facilitando la integración de seguridad en las redes inalámbricas.

Se eligió el método de autenticación EAP-TTLS como el más

adecuado para el correcto funcionamiento del sistema AAA dentro de las instalaciones FICA, debido a que a través de un canal seguro se garantiza la confidencialidad de los datos en el proceso de autenticación

Para poder manejar los datos registrados en LDAP se hace uso de la herramienta de gestión PhpLdapAdmin, la cual facilita la creación, modificación o eliminación de datos, de esta manera permiten al administrador de la red manejar la enorme cantidad de usuarios de un amanera más sencilla y fácil.

Para realizar las pruebas sobre el correcto funcionamiento del sistema se utilizó el SO Windows 7 debido a que no tiene soporte nativo para el método de autenticación EAP-TTLS, permitiendo de esta forma instalar un suplicante (SecureW2) para poder acceder a la red.

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.

Llegar a tener seguridad al 100% en una red resulta inalcanzable, sin embargo, la mejora continua, adopción de métodos y estándares de seguridad de la información permite mantener un nivel de seguridad aceptable que reduce en cierto grado las vulnerabilidades de la red.

VI. REFERENCIAS

[1] Guiza, J. A. (2010). PROYECTO AAA UD NET. Obtenido de https://proyecto-teleco-2010.wikispaces.com/file/view/Marco+teorico+AAA.pdf

[2] Escalona, S. B. (2011). Protocolos de control de acceso RADIUS. Revista Digital de las Telecomunicaciones. Obtenido de http://revistatelematica.cujae.edu.cu/index.php/tele/article/download/51/50.

[3] Chamorro, J. M. (02 de 2010). SANS Institute InfoSec Reading Room. Obtenido de https://www.sans.org/reading-room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlans-1607

[4] 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

[5] Duran, J. M. (2012). Servidor Radius - FreeRadius.

[6] Acosta, J. A. (2013). Servicio de Directorio LDAP. Obtenido de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=60&ved=0ahUKEwjUg_bIyZzQAhUD5WMKHY10Do44MhAWCFQwCQ&url=http%3A%2F%2Fwww.iesjacaranda-brenes.org%2Fredmine%2Fattachments%2Fdownload%2F66%2FDocumentacion.pdf&usg=AFQjCNHbqqJ2J-KADf_nB_Fh3hHGMy

VII. BIOGRAFÍA

Director – Ing. Fabián Cuzme, Msc.
Nació en Portoviejo provincia de Manabí el 14 de noviembre de 1985. Ingeniero en Sistemas Informáticos, Universidad Técnica de Manabí – Ecuador en 2009. Actualmente es docente en la carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra – Ecuador, obtuvo la Maestría en Redes de Comunicación en la Pontificia Universidad Católica del Ecuador, Quito – Ecuador en 2015.

Carlos P. Bosmediano C
Nació en Atuntaqui-Ecuador el 22 de noviembre de 1992. En el año 2010 obtuvo su título de Bachiller en Ciencias con especialización Físico Matemático en el “Colegio Nacional Teodoro Gómez de la Torre”. Actualmente, obtuvo su título en la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.