UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA: INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de: INGENIERO ELECTRÓNICO

TEMA:
IMPLEMENTACIÓN E INTEGRACIÓN DE LA RED WLAN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA (UPS), SEDE QUITO-CAMPUS SUR, AL PROYECTO INTERNACIONAL EDUROAM.

AUTORES:
EDWIN RODRIGO BORJA TACO
JOSÉ RAFAEL JARRÍN PAZ

DIRECTORA:
EMMA VERONICA SORIA MALDONADO

Quito, septiembre de 2014

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE TITULACIÓN

Nosotros, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además, declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Quito, septiembre de 2014

_____
Edwin Rodrigo Borja Taco
CC: 1720062536

_____
José Rafael Jarrín Paz
CC: 1716824089

DEDICATORIA

Este trabajo de titulación lo dedico a mis esfuerzos continuos por lograr llegar a cumplir una de mis metas propuestas a lo largo de toda mi carrera universitaria.

También lo dedico a todas las personas que supieron creer en mí y apoyarme cada día en los buenos y malos momentos que se han presentado, especialmente a mi mami Yolanda, a mi papi José, que gracias a su paciencia me guiaron, inculcándome valores para ser una persona de bien, a mi ñaña querida Estefanía que supo llenar un espacio en mi vida, a mis tíos en especial a mi ñaña Nelly que supo aconsejarme y apoyarme como una madre más, a mis abuelitos Ángel, Iralda y Delia que no dudaron de mis capacidades.

También lo dedico a todas las personas que supieron guiarme y aconsejarme en los momentos difíciles y sobre todo a mi adorable negrita que con su cariñó y amor incomparables me supo valorar, comprender y enseñarme lo maravillosa que es la vida al compartir cada día junto a ti mi amada Jenny. Y a la veci Cecilia que siempre me mostro un lado bueno de la vida que es la alegría, gracias por sus consejos.

Edwin Rodrigo Borja Taco.

El presente trabajo se lo dedico a mis padres ya que con su sacrificio me han concedido que mis metas se cumplan, les estoy muy agradecido y quiero que sepan que este es solo un escalón más, que siempre los hare sentir orgullosos de mí en todo momento, y también mi hermosa abuelita Rosario mi segunda madre, gracias por todo abue; a mis tíos especialmente para mi querido tío TETATO, te quiero agradecer por ser quien me apoyo en seguir adelante cuando más lo necesitaba, por enseñarme a ser humilde, quiero que sepas que me siento orgulloso de tener el mismo título que tu tuviste, gracias TETATO se te extraña full; mi hermana como también a mis primos Mary, Cacho, Nico gracias por estar preocupándote por mí, por sus consejos; A mi personita especial, te has convertido en un ser apoyo incondicional en todo este tiempo.

José Rafael Jarrín Paz.

AGRADECIMIENTO

Agradecemos a nuestra directora de trabajo de titulación Ing. Verónica Soria que nos brindó su tiempo, amistad, consejos, experiencia, paciencia, motivación, conocimientos para lograr terminar nuestros estudios con éxito.

Así mismo agradecemos al Ing. Jorge López lector de nuestro trabajo de titulación, por aportar con su granito de arena, con sus consejos, conocimiento, experiencia, amistad y sobre todo por su valioso tiempo para culminar con este proceso.

Agradecemos a la Universidad Politécnica Salesiana y a nuestros profesores que nos han formado para ser unos grandes profesionales por el resto de nuestras vidas.

A todos les damos unas sinceras gracias.

Edwin Rodrigo Borja Taco.

José Rafael Jarrín Paz.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto contribuirá a la formación académica y al desarrollo de proyectos de investigación de estudiantes, docentes miembros de la Universidad Politécnica Salesiana e invitados que procedan de otras universidades del país como del exterior que están cursando estudios de maestrías y doctorados. Una de las dificultades que tiene la comunidad académica e investigativa es no tener una facilidad y agilidad de acceso a sus recursos necesarios para seguir con el desarrollo de sus investigaciones, como el acceso a equipos, información, papers, etc, ya que no cuentan con un servicio que les permita estar conectado a la red y tener conectividad a Internet automáticamente cuando se desplazan entre universidades o entre organizaciones con afines a la investigación.

Se ha implementado un servidor RADIUS local en la UPS, Sede Quito–Campus Sur y se lo ha integrado al servidor FEDERADO Ecuador para ser un miembro más del proyecto internacional EDUROAM, para a través de la red inalámbrica del Campus Sur y de redes inalámbricas de otras universidades u organizaciones integradas al proyecto pueda la comunidad académica, investigativa miembros de las universidades integrantes al proyecto EDUROAM tener acceso a recursos, acceso autorizado a la red, conectividad a Internet. La realización del presente proyecto ayudará a que la comunidad académica e investigativa pueda desplazarse entre las universidades u organizaciones pudiendo automáticamente estar conectado a la red permitiéndoles tener movilidad a través de sus dispositivos como smartphones, tablets, portátiles y cuidando la seguridad de la red de la universidad.

ABSTRACT

The present proyect will contribute to the academic training and development of investigation proyects of students, teachers members of the University Polytechnic Salesiana and guests that come of other universities of the our country or the foreign that are studying their Masters and PhD. One of the difficulties that have the academic and research community is that does not have an easy and agility access to their resources for continue witch the development of their research as access to equipment, information, papers, etc, they do not have a service that allows them to be connected to the network and have Internet connectivity automatically when these people move between universities or between organizations related to research.

One server RADIUS local was implemented in the UPS, Headquarters Quito, Campus-Sur and was integrated to the server FEDERADO Ecuador for to be a member of the international EDUROAM proyect, for through of the wireless Network Campus south and other wireless Networks universities or organizations that are integrated to the EDUROAM proyect for that have access to resources, access authorized to the network, internet connectivity. The realization of this project will help for that the academic and research community can move into universities or organizations can automatically be connected to the network allowing them to have their mobility through devices smartphones, tablets, laptops and caring the security of the university network.

INTRODUCCIÓN

Hoy en día, el país ha iniciado un cambio trascendental especialmente en la educación puesto a que se propone que las instituciones de educación superior participen con proyectos de investigación para fomentar el aprendizaje de los estudiantes y el desarrollo del país. Es por esta razón que ya existen algunas instituciones, estudiantes de maestrías y doctorados que están orientados en realizar proyectos investigativos.

Por lo cual se ha visto la necesidad de prestarles a estas instituciones y estudiantes la facilidad para que puedan cumplir con sus fines investigativos sea en su misma institución o a su vez de visitantes en otras instituciones ya sea que estén dentro o fuera del país.

El proyecto internacional Eduroam cumple con ciertos estándares necesarios para que la conexión a esta red sea segura, permitiendo tener un espacio único de movilidad a nivel internacional a los estudiantes entre las instituciones integrantes de este proyecto que cuentan con el servicio de Eduroam.

El Internet es un servicio de gran utilidad, utilizado a gran escala para realizar consultas en la web, esto a su vez se vuelve más beneficioso cuando las personas tienen este servicio a través de la red inalámbrica, permitiéndoles acceder a la red desde cualquier sitio y sea desde su laptop, Tablet o Smartphone.

El proyecto permitirá que a través de la red inalámbrica sea en su lugar de origen o como visitantes en otras instituciones, las personas se beneficien de este recurso para acceder a la red con su mismo usuario y password sin que tengan la necesidad de configurar en cada uno de sus dispositivos los parámetros de red.

OBJETIVOS

Objetivo general

Implementar e integrar la red WLAN de la Universidad Politécnica Salesiana (UPS), Sede Quito-Campus Sur, al proyecto internacional Eduroam.

Objetivos específicos

- Analizar los requerimientos del proyecto Eduroam y la Red WLAN de la UPS, Sede Quito-Campus Sur para su integración.

- Implementar e integrar la red WLAN de la UPS, Sede Quito-Campus Sur al proyecto internacional Eduroam.

- Evaluar la integración de la red WLAN de la UPS, Sede Quito-Campus Sur al proyecto internacional Eduroam.

Planteamiento del problema

La UPS siendo miembro de CEDIA no aprovecha ciertos recursos, de los cuales ya algunas instituciones educativas e investigativas del país se están beneficiando, para mejorar y fortalecer su proceso educativo e investigativo, como acceso a publicaciones científicas, bibliotecas digitales, etc. Además, permite la vinculación con investigadores que se encuentran trabajando en temas similares y también participará en el desarrollo de tecnologías de la nueva generación de Internet.

Académicos e investigadores de la UPS, no hacen uso de esta red exclusiva de alta velocidad (1Gbps), para participar en proyectos nacionales e internacionales, por lo que este recurso que les ofrece CEDIA está siendo desperdiciado.

Con frecuencia, la comunidad educativa de la UPS tiene la necesidad de participar en investigaciones y actividades educativas en las instalaciones de otras instituciones

nacionales e internacionales, por lo que se presentan dificultades para acceder a la red inalámbrica de dichas instituciones, creando en el usuario contratiempos para cumplir sus fines investigativos, educativos y sin lograr acceder a todos los recursos de la red.

Investigadores y académicos de otras universidades nacionales e internacionales que han visitado las instalaciones de la UPS encontraron dificultad para acceder a la red inalámbrica, demorando el desarrollo de sus estudios investigativos, generando la necesidad de crear una red provisional y provocando contratiempos tanto para los técnicos que gestionan la red de la UPS como al usuario visitante.

Justificación

Eduroam es un proyecto de la red de investigación europea, coordinada en España por RedIRIS, a la cual están inscritas varias organizaciones de todo el mundo, tal es el caso de CEDIA (Corporación Ecuatoriana para el Desarrollo de Internet Avanzado) que permite al país que sus instituciones académicas y de investigación promuevan el desarrollo de las tecnologías de información, redes de telecomunicaciones e informática con un fin científico, tecnológico y educativo, logrando que puedan participar en proyectos de investigación nacionales e internacionales, haciendo uso de su red de alta velocidad (1Gbps).

Por lo mencionado anteriormente, se pretende integrar a la UPS Sede Quito-Campus Sur a la comunidad investigativa nacional e internacional mediante el proyecto Eduroam, el cual le permitirá obtener varios beneficios como fomentar la investigación y el trabajo conjunto con otras organizaciones del mundo, acceder a nuevas herramientas de investigación, tener movilidad y conectividad sin tener que configurar nuevamente sus equipos cuando se conecten a las distintas redes inalámbricas de investigación del resto de instituciones a nivel mundial afiliadas al proyecto Eduroam.

Alcance

El proyecto propuesto tiene como finalidad prestar el servicio de Eduroam a los docentes y estudiantes que pertenecen a la Universidad Politécnica Salesiana – Sede

Quito, Campus Sur, que están realizando estudios sean estos de investigación o a su vez estudios de maestrías y doctorados dentro y fuera del país.

El proyecto será implementado en la Universidad Politécnica Salesiana – Sede Quito, Campus Sur, con el levantamiento de un servidor RADIUS, una base de Datos la cual será levantada en LDAP, para finalmente integrarles al WLC (Wireless LAN Controller) para dar servicio a través de la red inalámbrica, consiguiendo de esta manera conformar el Proveedor de Identidad (idP). Una vez ya levantado el idP, se le integrará con el federado que se encuentra en CEDIA.

De esta manera la Universidad Politécnica Salesiana – Sede Quito, Campus Sur, aparecerá en el mapa de Eduroam y podrá responder consultas de los usuarios de otras instituciones pertenecientes al proyecto Eduroam y de la misma manera aquellas instituciones puedan responder a consultas de los usuarios de la universidad.

Permitiendo así que aquellos docentes y estudiantes de la Universidad Politécnica Salesiana – Sede Quito, Campus Sur, tenga un fácil acceso a la red para que realicen sus trabajos de investigación desde cualquier institución que también este adscrita al proyecto Eduroam con su mismo usuario y password desde su lugar de origen, sin que tenga la necesidad de que en cada lugar que visite tenga que configurar sus dispositivos y pedir permisos al administrador de esa red para que le deje consumir sus recursos de red.

CAPÍTULO 1
EDUROAM

El capítulo siguiente contiene los temas principales para comprender de una forma completa lo que es Eduroam, incluyendo las organizaciones que la regulan, los tipos de servidores que utilizan, también se explica en una forma general sobre redes inalámbricas incluyendo de una manera importante la seguridad, ya que Eduroam realiza siempre un hincapié en todo lo relacionado a este tema.

1.1 Eduroam, ¿Qué es?

El nombre de Eduroam proviene de dos palabras de origen inglés (Educational Roaming), es una iniciativa de la redIRIS que permite a las instituciones académicas e investigativas de todo el mundo obtener un espacio único de movilidad mundial, disponiendo de servicios que el usuario pueda necesitar en cualquier otra institución a la que este visitando.

Su infraestructura se basa en una red de servidores RADIUS y la utilización de los protocolos 802.1x, EAP, entre otros para brindar al usuario la seguridad necesaria para la movilidad.

1.1.1 Historia de Eduroam.

Esta iniciativa se remonta en el año 2003 en TF-MOBILITY (Task Force on Mobility) de TERENA, siendo esta una organización de colaboración que agrupa a un personal técnico y científico que fomenta el desarrollo de Internet, su infraestructura y servicios para la investigación y educación, su grupo de trabajo realizó pruebas que demostraron la viabilidad de unir la infraestructura basada en RADIUS con la tecnología 802.1x que permitían tener una itinerancia en redes inalámbricas con el fin de proporcionar seguridad y movilidad en redes de investigación y educación.

Estas pruebas se realizaron en varios paises de Europa a las cuales se unieron instituciones y oraganizaciones de investigación y educación que desde ese momento ya se empezó a llamar a esta iniciativa como EDUROAM.

1.1.2 Organismos reguladores de Eduroam.

Al inicio Eduroam solo existía en Europa, pero actualmente se encuentra en varios países del mundo conformando tres confederaciones regionales de Eduroam : América, Asia-Pacífico y Europa.

Figura 1. Mapa de las confederaciones en el mundo.
Fuente: http://wifi.stuba.sk. (2005).

1.1.2.1 Organismo regulador en América.

El organismo encargado de regular Eduroam en América se llama RedCLARA (Corporación Latinoamericana de Redes Avanzadas), esta es una Organización de Derecho Internacional creada el 23 de diciembre de 2003 y su idea inicial de formación apareció en el 2012 en una reunión en España, esta organización está conformada por 15 países latinoamericanos que lo integran y por cada nación existe un representante para la Asamblea internacional en la cual se definen las políticas y líneas de acción para ser implementadas.

1.1.2.2 Organismo regulador en Ecuador.

El organismo encargado de regular Eduroam en Ecuador es Corporación Ecuatoriana de Internet Avanzado (CEDIA), esta se encuentra incorporada a la RedCLARA. CEDIA está constituída por varias instituciones académicas del país, las cuales al estar integradas a esta corporación reciben la facilidad de obtener servicios , recursos y aplicaciones de red avanzada para el desarrollo investigativo y académico.

1.2 Elementos que conforman la red Eduroam

La red Eduroam está conformada por varios servidores RADIUS, los cuales se van diferenciando de sus funciones y características por la jerarquía que ocupen en la red, permitiendo llevar las autenticaciones de una manera segura junto al protocolo 802.1x.

Según la jerarquía de la red Eduroam, se puede diferenciar tres tipos de niveles de servidores RADIUS:

- ORPS o servidor institucional.
- NRPS o servidor nacional (federado).
- TRPS o servidor internacional (confederado).

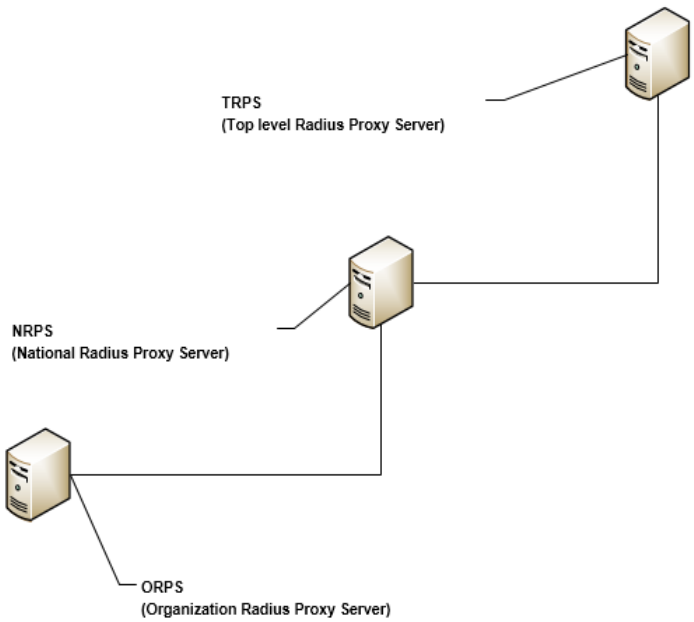

Figura 2. Jerarquía de servidores en la red Eduroam.
Elaborado por: Rodrigo Borja y José Jarrín.

Todos estos servidores utilizan el puerto UDP 1812 para reenviar peticiones RADIUS, y el UDP 1813 para reenviar mensajes de contabilidad.

1.2.1 Servidor RADIUS ORPS (Organization Radius Proxy Server).

Esta clase de servidor es el que está ubicado en el nivel más bajo de la jerarquía de servidores de la red Eduroam, es el encargado de revisar si el dominio del usuario que desea ingresar a la red Eduroam pertenece o no a la institución, en tal caso si fuera de una institución dentro del país solo se realiza la petición al servidor nacional, en otro caso si fuera de otro país se realiza la petición al servidor internacional o TRPS, los cuales envían un mensaje de aceptación y permiten al usuario ingresar a la red Eduroam.

Esta clase de servidores también se encargan de registrar la hora, la fecha o el nombre del usuario para llevar un control.

Todos estos atributos como el dominio, el nombre del usuario, fecha y hora entre otros son enviados en forma transparente utilizando el protocolo EAP (Extensible Authentication Protocol).

1.2.2 Servidor RADIUS NRPS (National Radius Proxy Server).

Esta clase de servidor se ubica en el nivel intermedio de la jerarquía de servidores de la red Eduroam, es el encargado de aceptar y reenviar peticiones que provengan de los servidores ORPS que administra este servidor y de los servidores TRPS; este servidor no se encarga de aceptar las solicitudes de autenticación de esto se encargan los servidores ORPS.

Al igual que un servidor ORPS, también lleva un registro de atributos de los usuarios, con esta clase de servidores se puede añadir subniveles a la red como por ejemplo un nivel regional.

1.2.3 Servidor RADIUS TRPS (Top Level Radius Proxy Server).

Este servidor se encuentra en el nivel más alto en la jerarquía de servidores de la red Eduroam, se encarga de aceptar las solicitudes de cualquier servidor NRPS que proveniente de un usuario que tiene sus atributos de autenticación en otro NRPS, logrando reenviar sus peticiones para una mejor administración, al igual que el NRPS este no acepta solicitudes de autenticación.

1.3 Redes inalámbricas

Las redes inalámbricas actualmente son las más usadas y también son objeto de estudio, ya que todavía la tecnología inalámbrica está en desarrollo debido principalmente a su seguridad, esta tecnología se creó principalmente para lograr comunicar dispositivos que no se encuentran en un sitio fijo permitiendo movilidad o itinerancia, a diferencia de las redes cableadas estas no pueden igualar su velocidad de transmisión debido a varios factores, lo que principalmente genera preocupación en esta clase de redes es la seguridad debido a que su transmisión se realiza en el aire sin ningún medio de transmisión físico, sus datos son objetivos fáciles para un cyber-delincuente, debido a esto se crearon protocolos de seguridad, ya que esta clase de redes exige una seguridad más robusta.

1.3.1 Concepto.

Es un sistema de comunicación inalámbrico, que cubre una área similar a una red cableada es decir una cobertura de casi 100m, su comunicación se lleva mediante ondas radioeléctricas que se propagan en el aire lo que permite que los dispositivos finales o también llamados STAs se comuniquen entre sí y obtengan movilidad entre ellos.

Su historia se remonta en 1986 en donde se dan las primeras redes locales inalámbricas que tienen una velocidad de 860 Kbps y un ancho de banda de 900 MHz.

En el año 1989 se crea el comité de la IEEE el IEEE 802.11 el cual empieza a tratar de estandarizar a las redes WLAN.

En 1997 la IEEE aprueba el estándar 802.11 con una velocidad de 1 Mbps el cual es la velocidad mínima para ser considerada red según la IEEE 802.

En el año 1999 se da por finalizada la norma IEEE 802.11 y también se ponen a prueba suplementos pre estándar como la 802.11a que llega a velocidad de transmisión hasta 54Mbps en una frecuencia de 5 GHZ y también la 802.11b el cual tiene una velocidad de transmisión de 11Mbps en una frecuencia de 2.4 GHz.

En junio del 2003 se hace la publicación del estándar 802.11g el cual trabaja con una velocidad hasta 54 Mbps y 2,4 GHZ de frecuencia.

La Federal Communications Comission (FCC) es una agencia que se encarga de regular y administrar las telecomunicaciones en Estados Unidos y fue la encargada de asignar el uso de las bandas: 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz para las redes inalámbricas.

Tabla 1. Evolución del estándar 802.11.

ESTANDAR	VELOCIDAD	FRECUENCIA	TECNOLOGÍA PHY	OBSERVACIONES
802.1 "legacy"	1-2 Mbps	2,4 GHz	DSSS	Primera aparición del estándar 802.11
802.11a	54 Mbps	5 GHz	OFMD	No puede trabajar con 802.11b
802.11b	11Mbps	2,4GHz	DSSS/CKK	Primero con gran aceptación comercial, no compatible con 802.11ª.
802.11g	54Mbps	2,4GHz	OFMD/DSSS /CKK	Compatible con 802.11b
802.11h	54Mbps	5GHz		Soluciona problemas derivados de la coexistencia de redes 802.11a con sistemas Radares y satelitales.

Continúa…

Tabla 1. Evolución del estándar 802.11. (Continuación…)

802.11i				Creado para mejorar la seguridad, abarca protocolos WEP, WAP WAP2.
802.11e				Mejora el sistema de control y servicio de la 802.11, soporta tráfico en tiempo real con garantía de QoS
802.11n	600 Mbps	2,4-5 GHz	SMD/OFMD	Soporta 802.11a,b,g. utiliza tecnología MIMO (Multiple-input Multiple-output).

Elaborado por: Rodrigo Borja y José Jarrín.

1.3.2 Modos de funcionamiento WLAN.

Su elemento principal es un Basic Service Area (BSA) O CELDA es el área física o la cobertura de un AP (Access Point). Existe dos modos de de funcionamiento:

- Modo infraestructura: sus conexiones involucran un AP, de este modo se derivan las topologías BSS y ESS.
- Modo Ad-hoc: no involucra un AP y de este modo deriva la topología IBSS.

1.3.3 Topologías WLAN.

Existen 3 tipos de topologías en las redes inalámbricas locales o WLAN:

- IBSS: (Independient Basic Service Set).
- BSS: (Basic Service Set).
- ESS: (Exchange Service Set).

1.3.3.1 IBSS.

También conocida como redes de tipo Ad Hoc, y es aquella en la que varios dispositivos están conectados inalámbricamente sin tener un dispositivo intermedio como un AP.

Este tipo de topología se usa cuando se realizan trabajos de forma temporal.

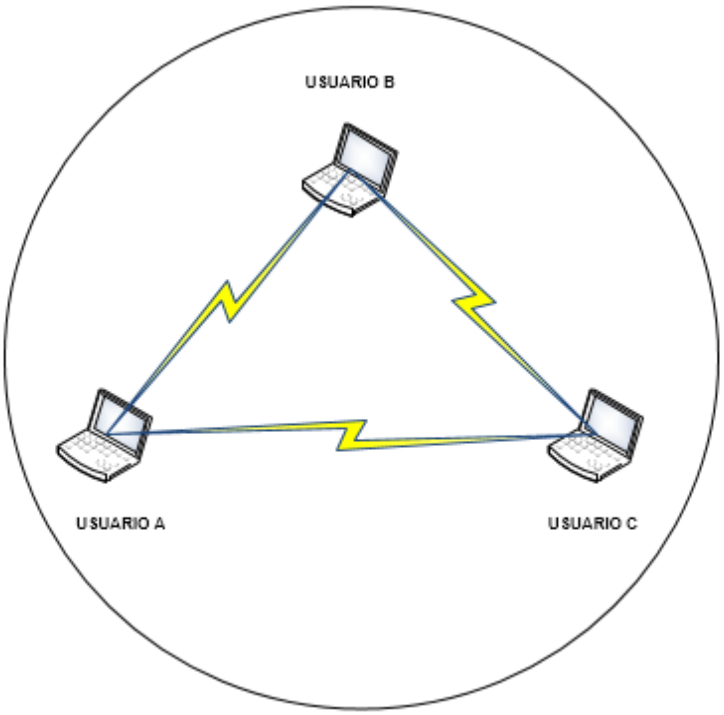

Figura 3. Topología IBSS (Independent Basic Service Set).
Elaborado por: Rodrigo Borja y José Jarrín.

1.3.3.2 BSS.

Es aquella topología en la que todos los STAs o dispositivos finales se asocian a un sólo Ap.

Cada BSS es identificado por BSSID (Basic Service Set Identification) el cual distingue un BSS de otro BSS debido a que este representa la dirección MAC del dispositivo auxiliar por ejemplo un AP, otro término usado en esta topología es el SSID el cual permite al usuario distinguir una red de otra.

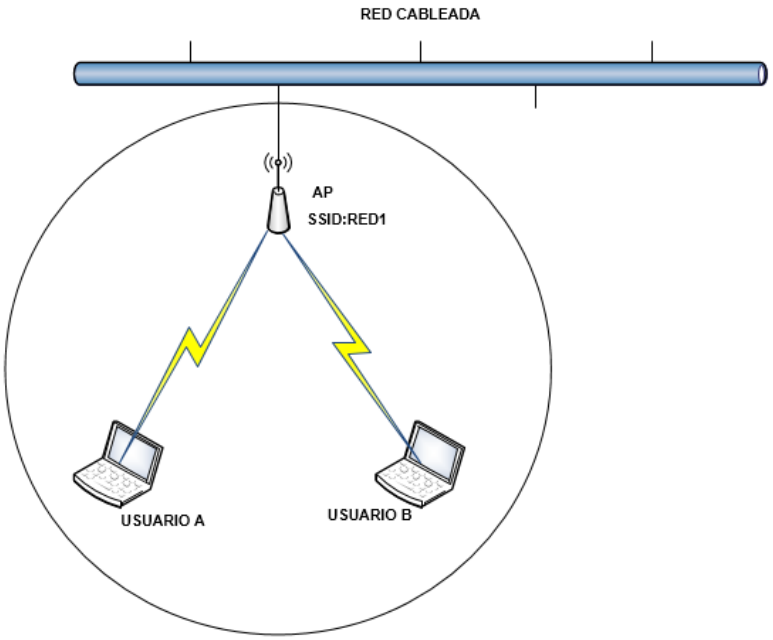

Figura 4. Topología BSS (Basic Service Set).
Elaborado por: Rodrigo Borja y José Jarrín.

1.3.3.3 ESS.

Es un tipo de topología inalámbrica en la cual involucra varias BSS con el mismo SSID.

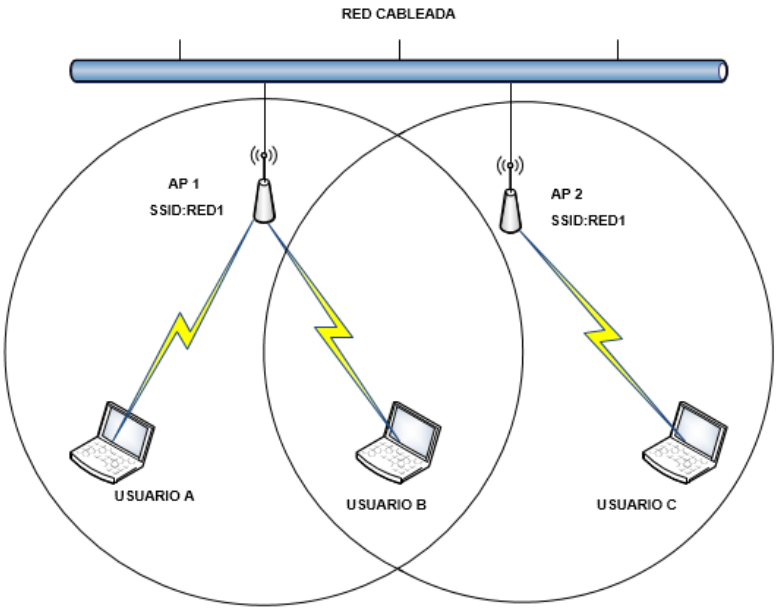

Figura 5. Topología ESS (Extended Service Set).
Elaborado por: Rodrigo Borja y José Jarrín.

1.3.4 Capa enlace de datos.

Según el modelo OSI esta capa le corresponde el segundo puesto, es la encargada de la transferencia de datos de un host a través de una red a la cual se está conectado, esta capa permite la perfecta comunicación entre las otras capas como son aplicación, transmisión y física y el medio que transporte los datos.

Su principal función es que la información viaje libre de errores por el canal físico entre dos host diferentes de una misma red, esto es para un servicio orientado a conexión, la información es transformada en tramas ya que es el PDU de esta capa.

Las principales funciones de la capa de enlace son:

- Identificar tramas.
- Detección de errores.
- Control de flujo.
- Corrección de errores.

La capa enlace de datos tiene dos subcapas primordiales para la comunicación estas son:

- Control de enlace lógico.
- Control de acceso al medio.

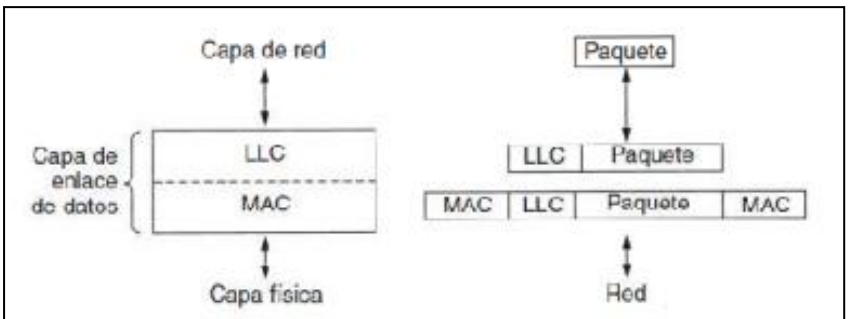

Figura 6. Distribución de las capas de enlace.
Fuente: www.ptolomeo.unam. (2006).

1.3.4.1 Control de enlace lógico (LLC).

La IEEE la define como el protocolo 802.2 el cual está definido para interactuar con todos los demás protocolos de la familia 802, este presenta un mismo interfaz de red y el mismo medio a nivel de capa de red.

1.3.4.2 Control de enlace al medio (MAC).

Se encuentra debajo de la subcapa de enlace lógico y es la que permite el control de acceso de cada dispositivo al medio de transmisión, proporciona el direccionamiento y esta subcapa está representada por la dirección MAC que tiene 48 bits compuestos por 6 bloques hexadecimales que corresponden a un identificador único de cada dispositivo, y es una pieza clave en la transmisión inalámbrica ya que proporciona el control de flujo de datos en el aire.

1.3.5 Capa física.

Sus siglas según el modelo OSI (PHY) que significan capa física, esta capa ha sido objeto de evolución en los últimos años, siendo una de las más relevantes en las redes inalámbricas, así mismo ellas muestran tres tipos de técnicas de transmisión inalámbrica englobando no sólo a la radiofrecuencia sino también la de infrarrojos, estas técnicas son: FHSS, DSSS, OFDM entre otros.

1.3.5.1 FHSS (Frequency Hopping Spread Spectrum).

Es una tecnología de salto de frecuencia que consiste en modular la señal que se va a transmitir con una portadora que salta de frecuencia a otra frecuencia en un intervalo de tiempo, de esta manera la información se transmite en frecuencias distintas en un intervalo de tiempo, este intervalo debe ser menor a 400 ms.

Esta técnica usa una frecuencia de 2,4 GHz organizados en 79 canales con un ancho de banda de 1 MHz cada uno, su número de saltos es regulado por cada país.

1.3.5.2 DSSS (Direct Sequence Spread Spectrum).

Tecnología que se encarga de codificar cada bit con una nueva secuencia de bits de mayor velocidad, creando un patrón de bits, mientras más grande sea este patrón mayor es su resistencia a las interferencias, el nuevo patrón de bits lleva a crear una nueva banda base que es mucho más rápida que la señal original, para obtener la información en el receptor se descodifica la señal.

Esta técnica utiliza el código de Baker que define un tamaño de 11 bits y que según el estándar IEEE 802.11 recomienda que el tamaño mínimo del patrón de bits para cada bit de información debe ser 11bits pero el óptimo es de 100 bits, ya que mientras mayor sea el número de bits en la secuencia, mayor será la resistencia de la señal a las interferencias.

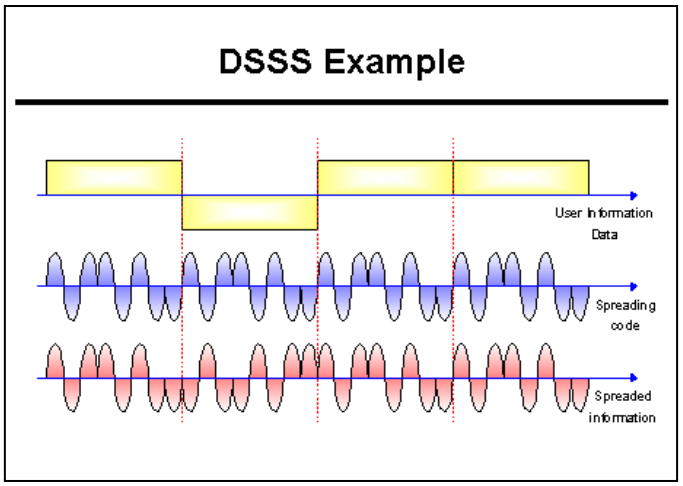

Figura 7. Ejemplo de la modulación DSSS.
Fuente: http://investigaciondsss.blogspot.com. (2012).

1.3.5.3 OFDM (Orthogonal Frecuency Division Multiplexing).

Técnica que se encarga de dividir el ancho de banda en diferentes subportadoras, cada una de ellas están separadas eficientemente ya que cada una es ortogonal al resto, esto permite que no existe interferencia una con otra.

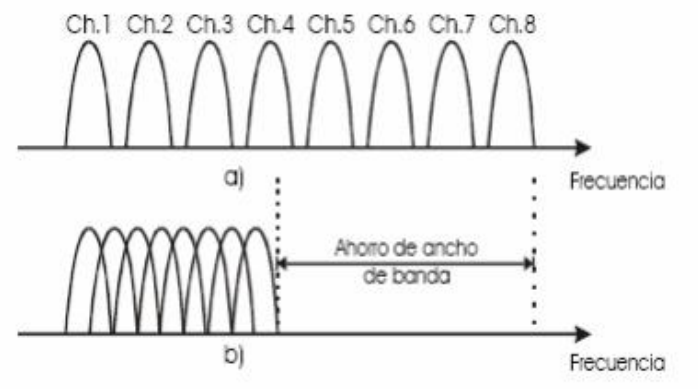

Figura 8. a) Técnica multiportadora convencional,
b) Técnica con portadoras ortogonales

Fuente: León, Esteban, Siguencia, Hernán. (2006). *Normas 802.11a, 802.11b, 802.11g.* Universidad Politécnica Salesiana, Cuenca, Ecuador.

1.3.6 Protocolos y estándares de seguridad inalámbricas.

Eduroam utiliza en toda su estructura de autenticación y verificación del usuario el protocolo RADIUS que al combinarlo con el protocolo de acceso de red 802.1x permite una seguridad en los clientes a nivel de capa 4 del modelo OSI logrando que el usuario se autentique a un nivel muy bajo antes de que el switch abra el puerto.

1.3.6.1 Protocolos WAP y WAP2.

El primer protocolo de seguridad para redes inalámbricas fue WEP, utiliza un algoritmo de cifrado RC4 utilizando claves de 64 bits o de 128 bits tratando de lograr una privacidad equivalente a una red cableada de ahí su siglas en inglés (Wired Equivalence Privacy), debido a fallas que presentó al proporcionar seguridad, en el 2004 fue desaprobada como protocolo de seguridad para una red inalámbrica, esta fue desplazada por el protocolo WAP.

WPA significa (Wi-Fi Protected Access) que surgió para solucionar las fallas que tenía WEP, se la considera como la transición a WPA2 o 802.11i en el estándar IEEE siendo el protocolo que actualmente se usa para redes inalámbricas.

WPA permite a diferencia de WEP cambiar su clave de una manera dinámica logrando que el ingreso a la red inalámbrica sea más complicado, utilizando servidores de

autenticación para identificar a los usuarios que desean ingresar a la red, teniendo una variante menos segura en la cual se tiene una clave pre compartida o TKIP (Temporal Key Integrity Protocol) en la que no se utiliza el servidor de autenticación.

WPA2 es el reemplazo de WPA, considerado por la IEEE en el 2004 como el estándar 802.11i por el cual todos los dispositivos deben de ser compatibles con WPA2, este protocolo puede reconocer una contraseña de al menos 8 hasta 63 caracteres tipo ASCII entre mayúsculas y minúsculas.

Tabla 2. Comparación entre protocolos de seguridad WEP,WPA, WPA2.

		WEP	WPA	802.11i
Autenticación	Autenticación	WEP	802.1x + EAP	802.1x + EAP
	Pre- Autenticación	No	Si	802.1x EAPOL
Cifrado	Negociación de Cifrado	No	Si	Si
	Cifrado	RC4 40-bit o 104-bit	TKIP: RC4 128-bit	CCMP: AES 128-bit
	Vector de Inicialización	24 bits	48 bits	48bits
	Integridad de la cabecera	No	MIC	CCM
	Integridad de los Datos	CRC-32	MIC	CCM
	Protección de Respuesta	No	Forza secuencia de IV	Forza secuencia de IV
	Gestión de Claves	No	Basada en EAP	Basada en EAP
	Distribución de Clave	Manual	802.1x (EAP)	802.1x (EAP)
	Clave asignada	Red	Paquete, sesión y usuario	Paquete, sesion y usuario
	Clave por paquete	Concatenación de IV	Mezclado TKIP	No necesario

Fuente: Muñoz, Diego. (2006). *Seguridades en redes Wlan*.
Universidad Politécnica Salesiana, Cuenca, Ecuador.

1.3.6.2 Protocolo RADIUS.

RADIUS (Remote Authentication Dial-In User Service) es un tipo de protocolo que maneja los servicios AAA (Authentication Autorization Accoutig) y utiliza el puerto UDP 1812 para establecer conexiones.

Una de sus principales características es que puede ser utilizado como servidor, para lo cual se encarga de administrar todas las autenticaciones y autorizaciones enviadas por el usuario la cual el servidor verifica si la información es correcta dando acceso a la red.

Esta verificación se realiza mediante protocolos de acceso a la red como EAP, PAP, además una de las características sobresalientes de este protocolo es que permite llevar un registro de la actividad que se realice en la red por medio del usuario, este registro se lleva acabo al inicio y al final de una sesión entre cliente y servidor.

Otra de sus características es que puede trabajar como un cliente Proxy con otros servidores RADIUS permitiendo una administración centralizada de autenticación.

1.3.6.3 Protocolo 802.1X.

Protocolo creado por la IEEE para control acceso en la capa 2 del modelo OSI, se basa en la arquitectura cliente-servidor creando una restricción de conexión a los usuarios que no están autorizados para ingresar a la red, fue fundamentado en el protocolo EAP el cual es usado para enviar toda la información del usuario.

Este protocolo fue creado para redes cableadas pero actualmente está disponible para las redes inalámbricas, está presente en los puntos de acceso que hoy en día son compatibles con 802.1x.

En el protocolo están involucrados tres elementos en su sistema de autentificación:

- **Cliente:** Es el que realiza la petición para conectarse a la red.
- **Autenticador:** Dispositivo de red (switch, router) que proporciona acceso al solicitante cuando el servidor de autenticación y autorización acepte la solicitud.
- **Servidor de autenticación y autorización:** Dispositivo que contiene toda la información del solicitante para permitir el ingreso a los usuarios autorizados para ingresar a la red. Generalmente se utiliza servidores tipo RADIUS para estos sistemas.

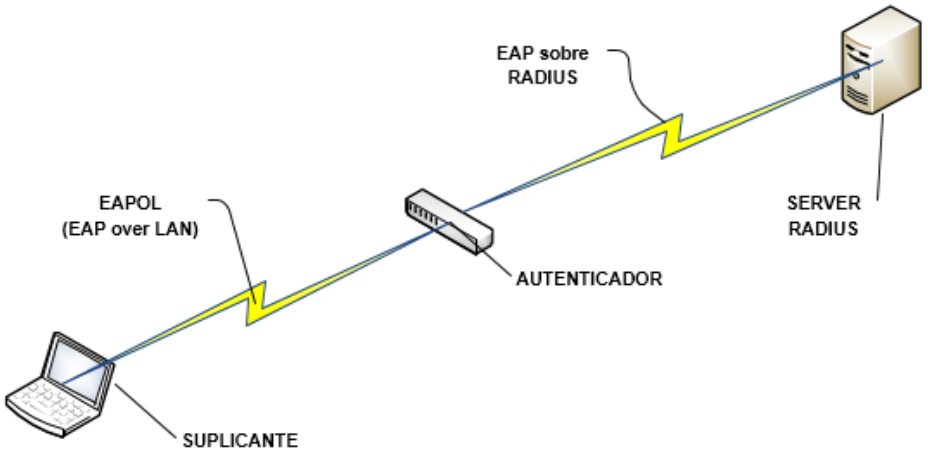

Figura 9. Sistema de autenticación del protocolo 802.1x.
Elaborado por: Rodrigo Borja y José Jarrín.

La autenticación se realiza mediante el protocolo EAP (Extensible Authentication Protocol), esto se efectúa mediante una comunicación entre el suplicante, el autenticador y el servidor, entre ellos se envían mensajes EAP para dar acceso al usuario, este diálogo de autenticación se muestra en la siguiente figura:

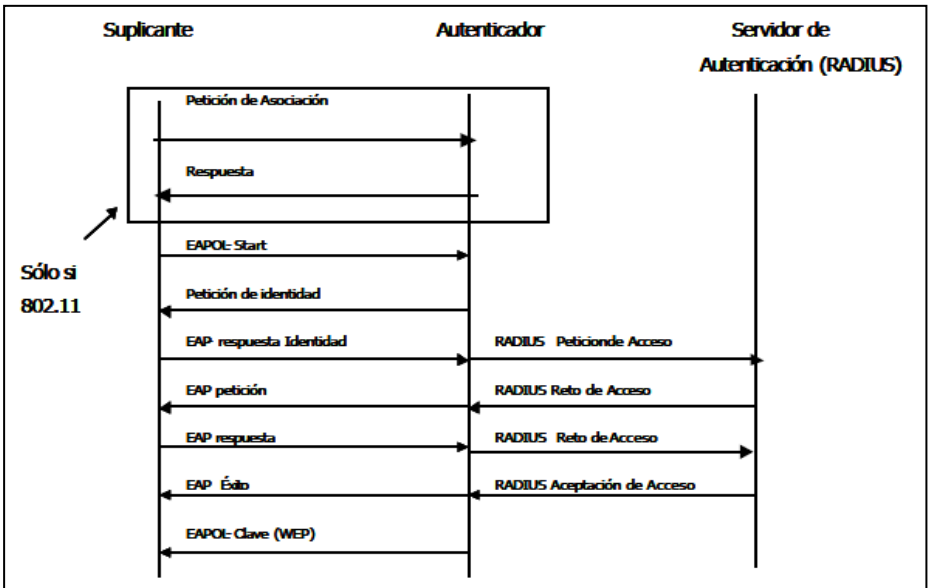

Figura 10. Diálogo de autenticación.
Fuente: http://cita2003.fing.edu.uy. (2003).

La figura 3 muestra el diálogo típico de autenticación realizada por un suplicante, este proceso comienza con la detección del suplicante en la red mediante un autenticador, el cual permite solo tráfico 802.1x y bloqueando todo el tráfico TCP y UDP.

El primer mensaje que se envía es un "EAPOL-START" por parte del suplicante al autenticador que indica que desea realizar una autenticación, este responde al suplicante que se identifique mediante una petición de identidad, que es respondida con el mensaje "EAP respuesta-identidad" en el contiene la identidad del suplicante, una vez conseguida la ID se envía un mensaje "RADIUS petición de acceso" al servidor RADIUS.

El servidor responde a esta solicitud con un mensaje "RADIUS Reto de acceso", este reto creado por el servidor implica una serie de desafíos que el suplicante debe realizarlos para obtener el acceso, este mensaje llega al autenticador que a su vez hace llegar al suplicante mediante un "EAP petición".
El suplicante cumple el desafío y lo envía con un "EAP respuesta", el cual pasa por el autenticador y este lo hace llegar al servidor mediante el mensaje "RADIUS reto de acceso".

Si todo está correcto el servidor envía el mensaje de aceptación "RADIUS Aceptación de acceso" permitiendo al autenticador otorgar el acceso completo al suplicante, se envía un mensaje "EAP Éxito" al suplicante.

En este diálogo también el autenticador envía el mensaje "EAPOL Clave (WEP)" que lleva la clave WEP indicando al suplicante que el acceso se ha realizado correctamente.

1.3.6.4 Protocolo EAP.

EAP (Extensible Authentication Protocol), protocolo que sirve para realizar intercambios de información de autenticación entre el cliente y el servidor para el acceso a la red.

Este protocolo es una extensión del protocolo PPP debido a que existe una gran demanda en sistemas de autenticación y también dispositivos como tarjetas de identificación.

Este protocolo tiene algunas variantes en cuanto a autenticación y se clasifican en dos grupos: autenticación por certificados y por contraseñas.

1.3.6.5 Protocolo EAP-TLS.

Es una variante del EAP, fue desarrollado por Microsoft, y puede proporcionar una fuerte autenticación mutua entre cliente-servidor previamente instalando los certificados en cada uno de ellos sino el protocolo no funcionará, es capaz de aceptar claves WEP dinámicas para evitar que se ingrese a la red mediante la misma clave. Su sesión de autenticación es realizada por el protocoló TLS (Transparent Layer Substrate) de ahí el nombre que se le da a esta variación.

1.3.6.6 Protocolo EAP-TTLS.

Variación del protocolo EAP, fue desarrollado por Funk Software y Certicom, lo cual su autentificación se realiza mediante certificados instalados solo en el servidor permitiendo la autenticación del servidor por parte del cliente garantizando una robusta autenticación de parte del ser servidor, por otro lado la autenticación del cliente por parte del servidor se realiza solo cuando existe una sesión TLS mediante otro protocolo de autenticación como CHAP, CHAP-2 entre otros.

1.3.6.7 Procolo PEAP.

Variación del protocolo EAP, fue desarrollado por CISCO, Microsoft y RSA Security, usa TLS para crear un túnel seguro entre el cliente y el autenticador, al igual que EAP-TTLS sólo requiere la instalación de un certificado en el servidor para autenticar.

Tabla 3. Comparación de las variantes EAP.

PROTOCOLO	EAP-TLS	EAP-TTLS	PEAP
Certificados en cliente	SÍ	NO	NO
Certificados en servidor.	SÍ	SÍ	SÍ
Credenciales de seguridad.	BUENA	BUENA	BUENA
Soporta autenticación en base de datos.	Acrive Directory, NT Domains,	Acrive Directory, NT DOmains, Tokens Systems, SQL, LDAP.	Acrive Directory
Intercambio de llaves dinámicas.	SÍ	SÍ	SÍ
Autenticación cliente servidor	SÍ	SÍ	SÍ

Elaborado por: Rodrigo Borja y José Jarrín.

Con lo contemplado anteriormente se tiene un conocimiento básico para comprender una parte de las redes inalámbricas, como por ejemplo su funcionamiento básico y la seguridad, entre otros temas, mismos que son necesarias ya que estos a su vez se aplican en la implementación de Eduroam en la UPS.

CAPÍTULO 2
SITUACIÓN ACTUAL DE LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO-CAMPUS SUR

En este capítulo se detallará como actualmente se encuentra distribuída la infraestructura de red de la Universidad Politécnica Salesiana – Sede Quito, Campus Sur, tanto a nivel de topología física como de topología lógica de la infraestructura alámbrica e inalámbrica. También se mostrará la cobertura de la red inalámbrica del mencionado campus.

2.1 Descripción del área física de la UPS, Sede Quito - Campus Sur

El Campus Sur de la UPS – Sede Quito se encuentra conformado por 7 bloques, los cuales están nombrados como bloque A, bloque B, bloque C, bloque D, bloque E, bloque F y recientemente construido el bloque G.

Figura 11. Área física de la UPS, Sede Quito – Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

2.2 Topología física de la red

2.2.1 Data Center.

El data center de la UPS – Sede Quito, Campus Sur se encuentra ubicado en el quinto piso del bloque A, en el mismo que se encuentran instalados los equipos principales que componen la infraestructura de red.

Se encuentran instalados 5 armarios de rack de 42 unidades de rack (UR) cada uno, en cada uno de estos se encuentran instalados los siguientes equipos.

2.2.1.1 Armario 1.

Tabla 4. Distribución del armario 1.

Item	Equipo	Número de Puertos	Modelo	Unidad de Rack (UR)	Posición UR
1	Distribuidor de Fibra Óptica modular (ODF)	18 puertos	Siemon	1 UR	42
2	Distribuidor de Fibra Óptica (ODF)	24 puertos	Hubbell	1 UR	41
3	Distribuidor de Fibra Óptica (ODF)	24 puertos	Hubbell	1 UR	40
4	Organizador de FO			2 UR	39 - 38
5	Patch Panel de cable Ethertnet modular	24 puertos	Siemon	1 UR	37
6	Patch Panel de cable Ethertnet modular	24 puertos	Siemon	1 UR	36
7	Organizador de cableado estructurado			2 UR	35 - 34
8	Distribuidor de Fibra Óptica modular (ODF)	18 puertos	Siemon		
9	Organizador de cableado estructurado			2 UR	30 - 29
10	Router		Cisco 2851	2 UR	26 - 25
11	Redundant Power System		Cisco RPS 675	1 UR	23
12	Router		Cisco 7604	5 UR	22 - 18
13	Router		Cisco 2800 Series	1 UR	17
14	Wireless Lan Controller (WLC)		Cisco 2504	1 UR	16
15	Switch Core		Cisco WS-C 6506-E	12 UR	12 - 1

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.1.2 Armario 2.

En este armario se encuentran ubicados dos servidores, uno se encuentra operando con el antivirus del CECASIS, mientras que el segundo servidor fue recientemente instalado para el desarrollo del proyecto internacional EDUROAM.

2.2.1.3 Armario 3.

En este armario se encuentra instalado el sistema de enfriamiento para controlar la temperatura de los equipos que se encuentran en el data center.

2.2.1.4 Armario 4.

Tabla 5. Distribución del **a**rmario 4

Item	Equipo	Número de Puertos	Modelo	Unidad de Rack (UR)	Posición UR
1	Patch Panel de cable Ethertnet modular	24 puertos	Siemon	1 UR	40
2	Organizador de cableado estructurado			2 UR	38 - 37
3	Sistema de almacenamiento		IBM	1 UR	18
4	File Server	2 puertos	IBM System X3650	2 UR	17 – 16
5	Active Directory	2 puertos	IBM System X3650	2 UR	15 - 14
6	VMware UIOS (Antivirus f-swcurity)	2 puertos	IBM System X3550 M2	1 UR	13
7	Centos (Proxy)	2 puertos	IBM System X3550 M2	1 UR	12
8	CIMA	2 puertos	HP Proliant DL380G7	2 UR	10 - 9

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.1.5 Armario 5.

Tabla 6. Distribución del armario 5.

Item	Equipo	Número de Puertos	Modelo	Unidad de Rack (UR)	Posición UR
1	Patch Panel de cable Ethertnet	24 puertos	Siemon	1 UR	40
2	Organizador de cableado estructurado			2 UR	38 - 37
3	Servidor	2 puertos	IBM System X3650 M3	2 UR	24 - 23

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2 Cuartos de Comunicaciones.

En el bloque A se encuentran ubicados los cuartos de comunicaciones, en donde están instalados los equipos de acceso y en los demás bloques solamente se encuentran instalados los rack de pared con sus respectivos equipos de acceso.

A continuación se detallan los equipos que conforman la parte de acceso por cada bloque del Campus.

2.2.2.1 Bloque A.

En este bloque los cuartos de comunicaciones se encuentran ubicados en el cuarto piso, quinto piso y en la planta baja ubicados en la sala de profesores y en la biblioteca, a continuación se detallan los equipos instalados en los cuartos de comunicaciones mencionados anteriormente.

2.2.2.1.1 Quinto Piso.

Tabla 7. Cuarto de Comunicación, piso quinto, CECASIS.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	48 puertos ethernet, 4 puertos fibra óptica	Cisco 2960-S Series
5	Switch	48 puertos	3com

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.1.2 Cuarto Piso.

Tabla 8. Cuarto de Comunicación, piso cuarto, CECASIS.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	48 puertos ethernet, 4 puertos de fibra óptica	Cisco 2960-S Series
1	Switch	48 puertos ethernet, 4 puertos de fibra óptica	Cisco 3750 PoE-48
1	Switch	50 puertos ethernet, 2 puertos de fibra óptica	Cisco 2960
2	Switch	50 puertos ethernet	3com 3250

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.1.3 Administración.

Tabla 9. Cuarto de Comunicación, planta baja, Administración.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	24 puertos ethernet	Cisco Catalyst 3750 v2 Series PoE-24
1	Switch	48 puertos ethernet	Cisco Catalyst 3750G Series PoE-48

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.1.4 Biblioteca.

Tabla 10. Cuarto de Comunicación, planta baja, Biblioteca.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	24 puertos ethernet, 2 de fibra óptica	Cisco Catalyst 3750G Series PoE-24

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.2 Bloque B.

En este bloque se encuentran instalados dos racks de pared ubicados en el segundo piso en la sala de profesores y en el primer piso en bienestar estudiantil, a continuación se detallan los equipos instalados.

2.2.2.2.1 Bienestar Estudiantil.

Tabla 11. Cuarto de Comunicación, Bienestar Estudiantil, Sala de profesores.

Cantidad	Equipo	Número de puertos	Modelo
1	Switch	48 puertos ethernet, 4 de fibra óptica	Cisco Catalyst 3750 Series

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.2.2 Sala de Profesores.

Tabla 12. Cuarto de Comunicación, Bienestar Estudiantil, Sala de profesores.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	48 puertos ethernet, 4 de fibra óptica	Cisco Catalyst 2960 Series
1	Switch	48 puertos ethernet, 4 de fibra óptica	Cisco Catalyst 3750 Series PoE-48

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.3 Bloque C.

En este bloque se encuentra instalado el rack de pared ubicado en el segundo piso en el departamento de idiomas, a continuación se detallan los equipos instalados.

2.2.2.3.1 Idiomas.

Tabla 13. Cuarto de Comunicación, Idiomas.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	48 puertos ethernet, 4 de fibra óptica	Cisco Catalyst 3750 Series
1	Switch	48 puertos ethernet, 4 de fibra óptica	Cisco Catalyst 3750 Series PoE-48

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.4 Bloque D.

En este bloque se encuentra instalado el rack de pared ubicado en el primer piso en el laboratorio 3 de CISCO, a continuación se detallan los equipos instalados.

2.2.2.4.1 CISCO.

Tabla 14. Cuarto de Comunicación, CISCO.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	48 puertos ethernet, 4 de fibra óptica	Cisco Catalyst 2960 Series

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.5 Bloque E.

En este bloque se encuentra instalado el rack de pared ubicado en el primer piso en el laboratorio de suelos, a continuación se detallan los equipos instalados.

2.2.2.5.1 Laboratorio de Suelos.

Tabla 15. Cuarto de Comunicación, Laboratorio de Suelos.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	24 puertos ethernet, 4 de fibra óptica	3com Series 3226

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.6 Bloque H.

En este bloque se encuentra instalado el rack de pared ubicado en el primer piso en el departamento de pastoral, a continuación se detallan los equipos instalados.

2.2.2.6.1 Pastoral.

Tabla 16. Cuarto de Comunicación, Pastoral.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	48 puertos ethernet, 4 de fibra óptica	Cisco Catalyst 3750 Series PoE-48

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.7 Bloque F.

En este bloque se encuentra instalado el rack de pared ubicado en el primer piso en el lado posterior del edificio, a continuación se detallan los equipos instalados.

2.2.2.7.1 Ambiental.

Tabla 17. Cuarto de Comunicación, Ambiental.

Cantidad	Equipo	Número de puertos	Modelo
1	Distribuidor de Fibra Óptica (ODF)	24 puertos	
1	Switch	48 puertos ethernet, 4 de fibra óptica	Cisco Catalyst 3750 Series PoE-48

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.2.8 Bloque G.

En este bloque se encuentran en la fase de instalación tres cuartos de comunicaciones para cubrir los cinco pisos, los mismos que se van a encontrar ubicados en el subsuelo, en el segundo piso y en el cuarto piso.

2.2.3 Diseño de la LAN.

El diseño de la red del Campus Sur de la UPS, está conformada por tres tipos de servicio de distribución:

1. MDF (Main Distribution Facility).
2. IDF (Intermediate Distribution Facility).
3. SDF (Sub-Distribution Facility).

Estos sistemas de distribución se han instalado en cada uno de los bloques de acuerdo a las diferentes necesidades demandadas por los usuarios.

El MDF es el punto central de la red del Campus Sur de la UPS, ubicado en el data center, desde este punto se derivan los IDFs y los SDFs ubicados en los demás sitios.

Existen dos IDFs, uno de ellos está ubicado en el quinto piso del bloque A, y el segundo IDF se encuentra ubicado en el cuarto piso del mismo bloque.

Los SFDs están ubicados en cada uno de los departamentos y bloques que se describen a continuación.

Tabla 18. Sistema de distribución SDFs.

SDF	DEPARTAMENTO	BLOQUE
SDF-A-PB	Administración	Bloque A
SDF-A-PB	Biblioteca	Bloque A
SDF-B-P1	Sala de profesores	Bloque B
SDF-C-P1	Idiomas	Bloque C
SDF-D-PB	CISCO	Bloque D
SDF-E-PB	Laboratorio Suelos	Bloque E
SDF-F-PB	Ambiental	Bloque F
SDF-H-PB	Pastoral	Bloque H

Elaborado por: Rodrigo Borja y José Jarrín.

2.2.4 Comunicación de los servicios de distribución.

Los servicios de distribución se encuentran interconectados de la siguiente manera:

Desde el MDF que se encuentra instalado en el Data Center ubicado en el bloque A se derivan los enlaces hacia los dos IDFs que se encuentran ubicados en el cuarto y quinto piso del mismo bloque y hacia los SDFs ubicados en los diferentes departamentos del Campus Sur, tal y como se detalló en la tabla 18.

La interconexión entre estos diferentes tipos de distribución se realiza por medio de fibra óptica y a su vez con una configuración Etherchannel para brindar un mayor ancho de banda, cabe destacar que no existe un backbone.

La forma en cómo se encuentran interconectados los equipos describe una topología en estrella, a continuación se ilustra la topología y en la misma se muestra la conexión de todos los Access Point desde los switch.

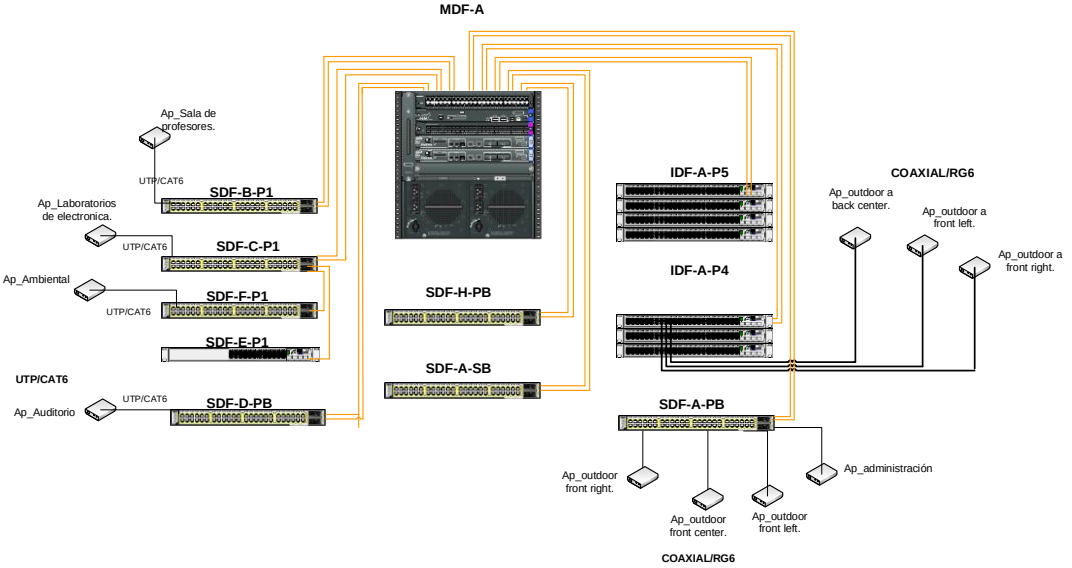

Figura 12. Comunicación de los servicios de distribución.
Elaborado por: Rodrigo Borja y José Jarrín.

2.2.5 Dispositivos que conforman la WLAN.

Los dispositivos que integran la WLAN se encuentran ubicados tanto en la parte exterior de los bloques como en la parte interior de cada uno de estos.

El WLC que está especificado en la tabla 4, es el manager de los Access Point que permiten tener acceso a la red a través de la red inalámbrica. En este caso el WLC instalado en el Campus Sur de la UPS, se encuentra configurado para que soporte 25 Access Points. Los Access Points se encuentran conectados desde los switchs que se sitúan en cada cuarto de comunicación de acuerdo a la necesidad donde se requiere de red inalámbrica, la ubicación de los Access Points donde se localizan instalados y desde donde están conectados se detallan en los site surveys y en la figura 12 respectivamente.

A continuación se detallan los diferentes tipos de Access Point que brindan el servicio de red inalámbrica en el campus.

- 13 Access Point, los cuales están conformados por tres familias o series:
  - 2 Access Point de la serie 1252
  - 2 Access Point de la serie 1131
  - 9 Access Point de la serie 1310

2.2.6 Cobertura inalámbrica en el Campus Sur.

La UPS, Sede Quito-Campus Sur, para proporcionar red inalámbrica a los usuarios de la UPS a través de los APs, dispone de un Wirelles Lan Controller, el cual permite concentrar configuraciones en un mismo punto brindando rapidez, confiabilidad y seguridad en la administración de los APs ubicados en el campus Sur.

Figura 13. Modelo del Wireless Controler de la UPS, Sede Quito – Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

El modelo con que cuenta el campus Sur es el 2504 con licencias para soportar 25 access points.

2.2.6.1 Distribución de los puntos de acceso en el Campus Sur.

Los Access Points permiten el acceso inalámbrico a la red, se encuentran distribuidos en diferentes puntos del Campus Sur, la ubicación de los Access Points de acuerdo a la necesidad se indica en la siguiente tabla.

Tabla 19. Distribución de los Access Points.

	UBICACIÓN	MODELO
Bloque A	AP_Outdoor frontal izquierdo	Cisco 1310 Series
	AP_Outdoor frontal Central	Cisco 1310 Series
	AP_Outdoor frontal derecho	Cisco 1310 Series
	AP_Outdoor posterior izquierdo	Cisco 1310 Series
	AP_Outdoor posterior Central	Cisco 1310 Series
	AP_Outdoor posterior derecho	Cisco 1310 Series
	AP_Biblioteca	Cisco 1131 Series
	AP_Administración	Cisco 1131 Series
Bloque B	AP_Sala de Profesores	Cisco 1310 Series
Bloque C	AP_Laboratorios de Electrónica	Cisco 1252 Series
Bloque D	AP_Auditorio	Cisco 1131 Series
Bloque E	No existe	No existe
Bloque F	AP_Ambiental	Cisco 1310 Series
Bloque H	AP_Pastoral	Cisco 1310 Series

Elaborado por: Rodrigo Borja y José Jarrín.

2.3 Análisis de cobertura

El software que se ha utilizado para el análisis de cobertura de la red inalámbrica de la UPS en la Sede Quito – Campus Sur fue el Covera Zone. Este software lo que ha permitido a diferencia de otros programas para el análisis de cobertura ha sido obtener una mejor apreciación gráfica del nivel de intensidad de la señal en cada uno de los puntos situados sobre el plano, también identificó y mostró en el plano aproximadamente en qué lugar se encontraba el punto de acceso que estaba propagando la señal.

En las siguientes gráficas se muestra el análisis de cobertura realizado en la UPS, Sede Quito – Campus Sur. En las gráficas se muestran cinco diferentes colores, cada uno de estos colores muestran cada nivel de intensidad de señal que se tiene en cada lado del Campus dependiendo a qué distancia esté el usuario de la antena que esté irradiando, ya que entre más cerca esté el usuario de la antena que irradia mejor será el nivel de señal con la que cuente en el dispositivo móvil.

En el análisis de cobertura realizado se puede apreciar cinco niveles distintos de intensidad de la señal caracterizados cada uno por un tipo de color diferente, en el que el color azul muestra una intensidad de señal fuerte, el color verdoso muestra una intensidad de señal menos fuerte, el color verde claro muestra una intensidad de señal muy baja y el color rojo muestra una intensidad de señal bien baja con poca opción de poder acceder a la red.

2.3.1 Exteriores.

2.3.1.1 Bloque A.

En las figuras 14 y 15 se ilustra el análisis de cobertura realizado en la parte exterior, frontal, posterior y laterales del bloque A, en la cual se puede visualizar cinco niveles de intensidad de señal propagados por los 3 AP_Outdoor que se encuentran ubicados en la parte superior del poste de luz eléctrica situado a la entrada y en el sector posterior del bloque A.

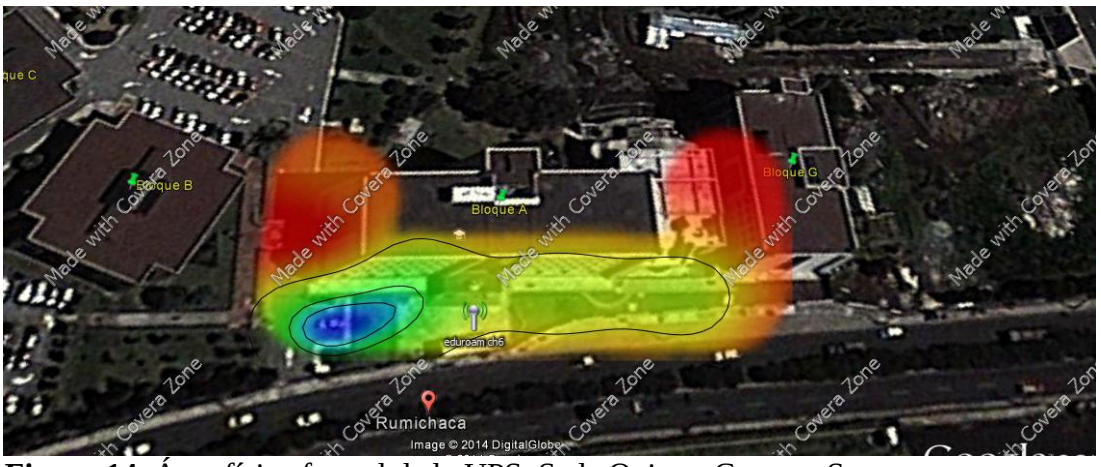

Figura 14. Área física frontal de la UPS, Sede Quito – Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

En la siguiente tabla se detalla la potencia de cada una de las intensidades de señal que se adquirió en el análisis de cobertura para la parte exterior, frontal y laterales del bloque A.

Tabla 20. Intensidades de las señales de la figura 14.

Color de la Intensidad de la Señal	Potencia
Azul	-47dBm
Verde	-51dBm
Verde claro	-56dBm
Amarillo	-73dBm
Rojo	-91dBm

Elaborado por: Rodrigo Borja y José Jarrín.

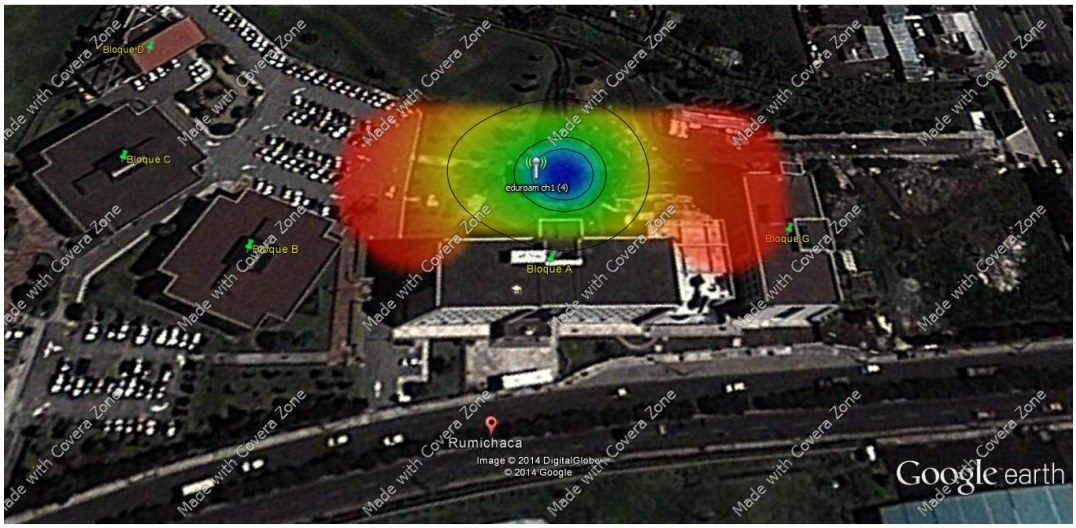

Figura 15. Área física trasera de la UPS, Sede Quito – Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

En la siguiente tabla se detalla la potencia de cada una de las intensidades de señal que se adquirió en el análisis de cobertura para la parte exterior, posterior y laterales del bloque A.

Tabla 21. Intensidades de las señales de la figura 15.

Color de la Intensidad de la Señal	Potencia
Azul	-64dBm
Verde	-66dBm
Verde claro	-68dBm
Amarillo	-75dBm
Rojo	-82dBm

Elaborado por: Rodrigo Borja y José Jarrín.

2.3.1.2 Bloque B.

En las figuras 16 y 17 se ilustra el análisis de cobertura realizado en la parte exterior, frontal, posterior y laterales del bloque B, en la cual se puede visualizar cinco niveles de intensidad de señal propagados por el AP_Outdoor dirigido hacia estos sectores que se encuentra ubicado en la parte superior del poste de luz eléctrica situado a la entrada y en sector posterior del bloque A.

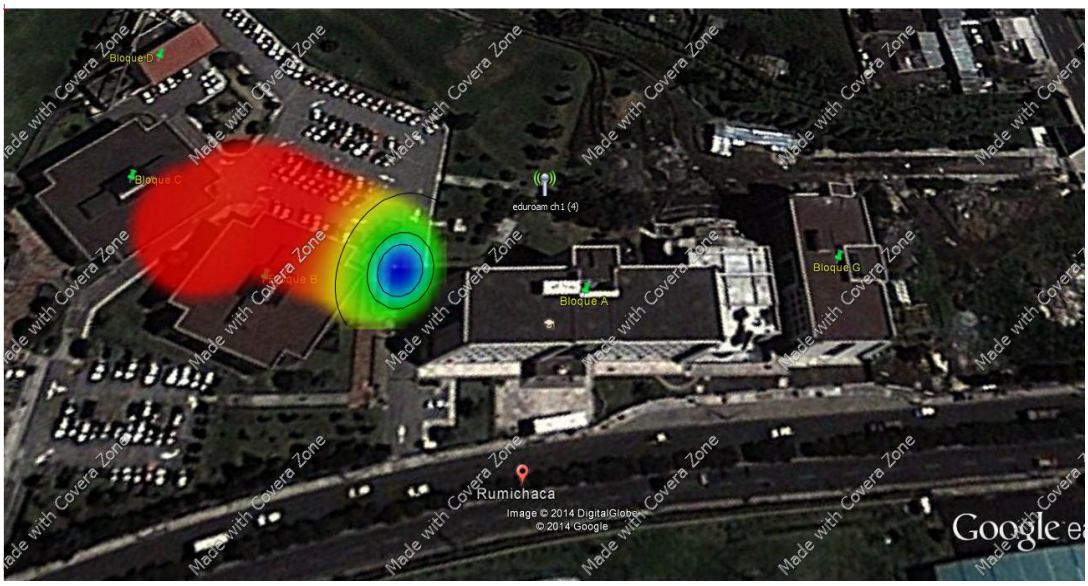

Figura 16. Área física del bloque B de la UPS, Sede Quito – Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

En la siguiente tabla se detalla la potencia de cada una de las intensidades de señal que se adquirió en el análisis de cobertura para la parte exterior, posterior y lateral sur del bloque B.

Tabla 22. Intensidades de las señales de la figura 16.

Color de la Intensidad de la Señal	Potencia
Azul	-69dBm
Verde	-70dBm
Verde claro	-71dBm
Amarillo	-75dBm
Rojo	-80dBm

Elaborado por: Rodrigo Borja y José Jarrín.

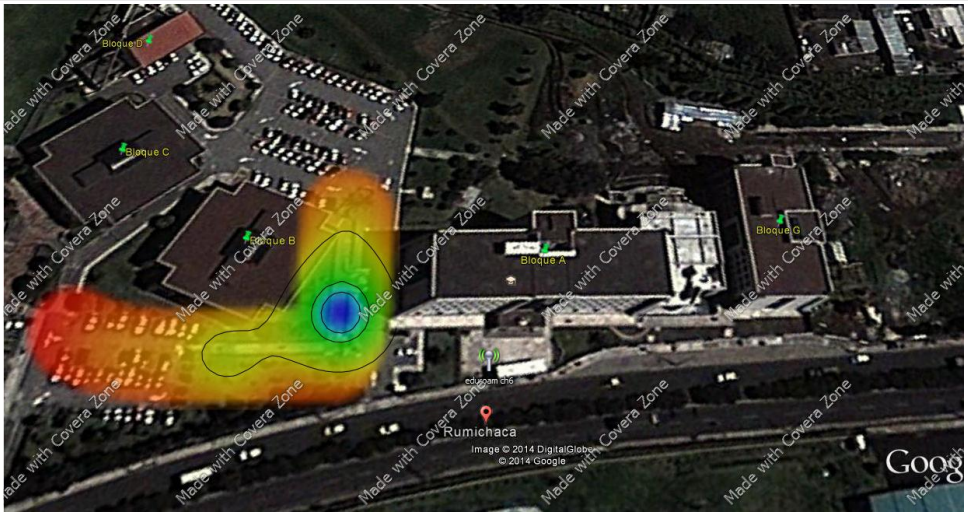

Figura 17. Área física del bloque B de la UPS, Sede Quito – Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

En la siguiente tabla se detalla la potencia de cada una de las intensidades de señal que se adquirió en el análisis de cobertura para la parte exterior, posterior y lateral norte del bloque B.

Tabla 23. Intensidades de las señales de la figura 17.

Color de la Intensidad de la Señal	Potencia
Azul	-55dBm
Verde	-58dBm
Verde claro	-62dBm
Amarillo	-75dBm
Rojo	-89dBm

Elaborado por: Rodrigo Borja y José Jarrín.

2.3.2 Interiores.

2.3.2.1 Administración.

En la figura 18 se ilustra el análisis de cobertura realizado en la planta baja del bloque A en el área de: sala de profesores, pasillos, en la cual se puede visualizar *cinco niveles* de intensidad de señal propagados por el AP_Indoor ubicado en la parte superior de la pared en la sala de profesores.

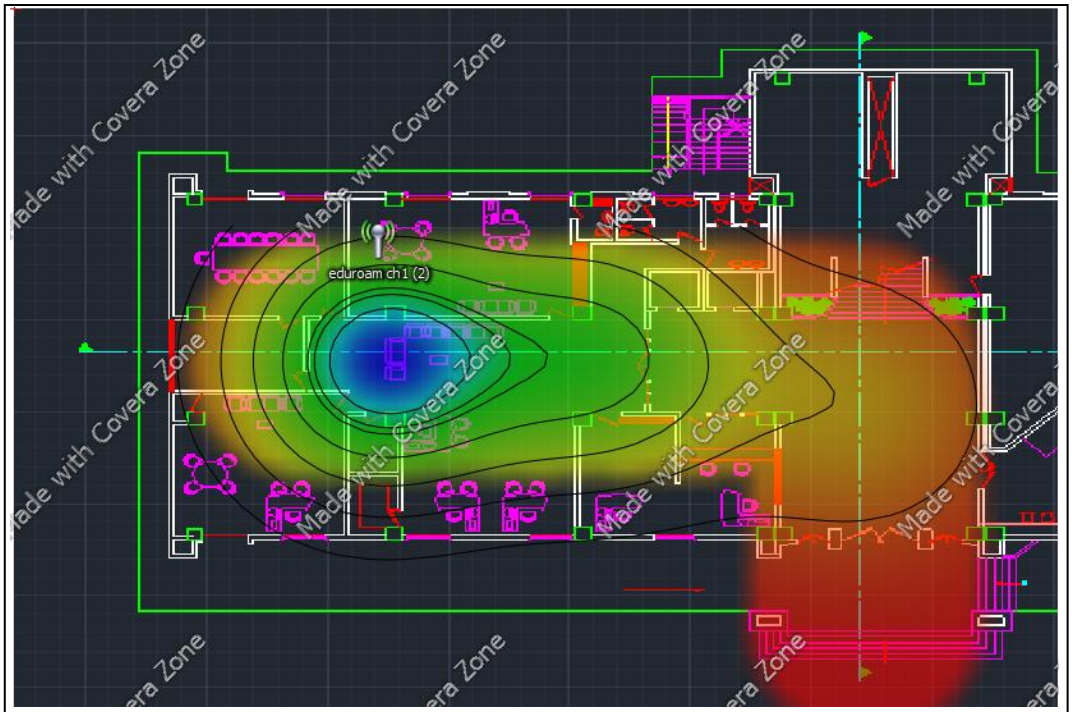

Figura 18. Interior del Bloque A.
Elaborado por: Rodrigo Borja y José Jarrín.

En la siguiente tabla se detalla la potencia de cada una de las intensidades de señal que se adquirió en el análisis de cobertura realizado en la planta baja del bloque A, área de sala de profesores, administración.

Tabla 24. Intensidades de las señales de la figura 18.

Color de la Intensidad de la Señal	Potencia
Azul	-27dBm
Verde	-32dBm
Verde claro	-37dBm
Amarillo	-58dBm
Rojo	-78dBm

Elaborado por: Rodrigo Borja y José Jarrín.

2.3.2.2 Biblioteca.

En la figura 19 se ilustra el análisis de cobertura realizado en la planta baja del bloque A en el área de biblioteca, en la cual se puede visualizar cinco niveles de intensidad de señal propagados por el AP_Indoor ubicado en la parte superior de la pared en la sala de profesores.

Figura 19. Área interna de la biblioteca de la UPS, Sede Quito – Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

En la siguiente tabla se detalla la potencia de cada una de las intensidades de señal que se adquirió en el análisis de cobertura realizado en la planta baja del bloque A, área de biblioteca.

Tabla 25. Intensidades de las señales de la figura 19.

Color de la Intensidad de la Señal	Potencia
Azul	-27dBm
Verde	-32dBm
Verde claro	-37dBm
Amarillo	-55dBm
Rojo	-74dBm

Elaborado por: Rodrigo Borja y José Jarrín.

El análisis de cobertura que fue realizado permite conocer que en ciertos lugares del campus se posea una muy buena intensidad de señal inalámbrica como también en ciertos otros lugares se carece de una pobre y en ocasiones una nula intensidad de señal, tanto en la parte interna y externa del campus.

2.4 Topología lógica de la red

2.4.1 Redes.

El Switch Core se encuentra configurado con 32 VLANs, las mismas que permiten tener un tipo de acceso dedicado y distribuido de acuerdo a la necesidad de cada

usuario. Cada VLAN tiene una configuración diferente de políticas como: ancho de banda, permisos de acceso.

Las 32 VLANs que se encuentran configuradas en el Switch Core son:

Tabla 26. Vlans creadas en Switchcore.

VLAN	Name	Status
1	Default	Active
2	DMZ	Active
3	ADMINISTRATIVA	Active
4	ESTUDIANTES	Active
5	CISCO	Active
6	SUN	Active
7	SALAPROF	Active
8	SALA-INTERNET	Active
9	MICROSOFT	Active
10	WIRELESS	Active
11	IPT	Active
12	SALA-CECASIS	Active
13	VLAN-VIDEO	Active
14	VLAN-HP	Active
15	ELECTRÓNICA	Active
16	VLAN-TELCONET	Active
17	WLAN-IPCAM-CECASIS	Active
18	WLAN-IPCAM-ELECTRÓNICA	Active
19	INVESTIGACIÓN	Active
20	INTERNET-LOCAL	Active
21	CIMA-SRV	Active
22	RUI	Active
23	LAB-IDIOMAS	Active
24	WLAN-SUR	Active
25	CÁMARAS-IP-UIOS	Active
26	EVENTOS	Active
27	LAB-FÍSICA-UIO	Active
28	INTERNET-CECASIS	Active
29	GIETEC	Active
30	DOCENTES-TIEMP-COMP	Active
31	EDUROAM	Active
32	CÁMARAS-APS	Active

Elaborado por: Rodrigo Borja y José Jarrín.

Las redes WLANs se encuentran creadas en el *Switch Core*, para por medio del WLC y las antenas puedan ser difundidas en el medio teniendo así la red inalámbrica, los SSIDs (nombres) que se ha asignado para cada WLAN son los siguientes:

1. ADM
2. VLAN GIETEC
3. VLAN CIMA
4. VLAN LABORATORIO FÍSICA
5. VLAN ESTUDIANTES
6. VLAN DOCENTES
7. VLAN BIBLIOTECA

La concurrencia que se tiene del acceso a la red inalámbrica de los usuarios en la hora pico es de aproximadamente 230 usuarios.

2.4.2 Seguridades.

El WLC se encuentra configurado con dos protocolos para brindar la adecuada seguridad de los usuarios en la red inalámbrica. Estos dos protocolos son:

- LWAPP
- CAPWAP

2.4.2.1 Protocolo LWAPP.

Es el protocolo ligero de punto de acceso, mediante el cual se puede controlar múltiples puntos de acceso a la vez. Mediante la utilización del protocolo se puede reducir la cantidad de tiempo dedicado a la configuración, la supervisión o la solución de problemas de una red grande. El sistema también permite a los administradores de red analizar de cerca la red.

Este sistema se instala en un servidor central que recoge datos de los dispositivos de RF de diferentes marcas y configuraciones. El servidor puede ordenar a un grupo seleccionado de los dispositivos para aplicar los ajustes dados simultáneamente.

2.4.2.2 Protocolo CAPWAP.

El protocolo de Control y Aprovisionamiento de Puntos de Acceso Inalámbrico, es una norma para el control de los puntos de acceso inalámbrico, siendo este un protocolo de red interoperable que permite administrar a un conjunto de puntos acceso.

La RFC 5415 especifica que la intención del protocolo CAPWAP es facilitar el control, la gestión de los puntos de terminación de una WLAN.

Para el acceso a la WLAN ADM, CIMA y DOCENTES, se utiliza el protocolo de seguridad WPA2 con el modo PSK para la autenticación del usuario.

2.4.3 Conexión hacia el Internet.

El Campus Sur de la Sede Quito, tiene su propia salida hacia el internet a través de CEDIA TELCONET con un ancho de banda de 162.5 Mbps.

El enlace que tiene el Campus Sur con el Campus el Girón es solamente de datos, este servicio prestan los ISP CNT y TELCONET con un ancho de banda de 6 Mbps por cada uno, en la figura 20 se muestran las respectivas conexiones de salida hacia al internet del Campus Sur de la Sede Quito.

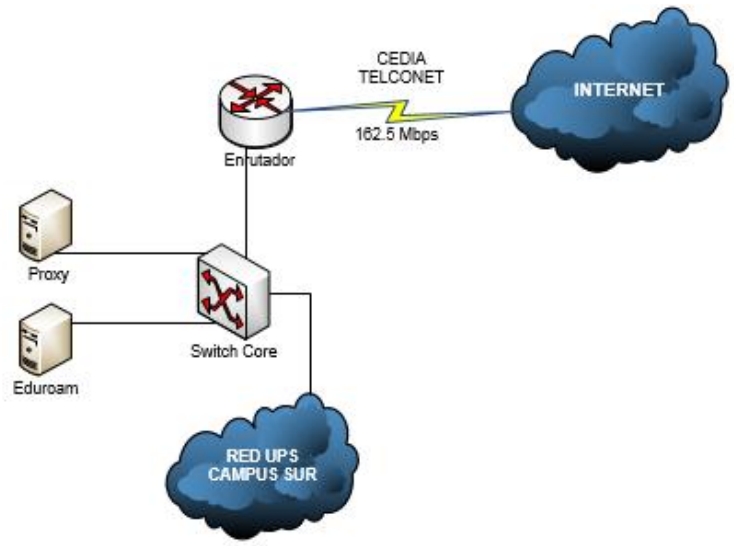

Figura 20. Conexión hacia el Internet.
Elaborado por: Rodrigo Borja y José Jarrín.

CAPÍTULO 3

IMPLEMENTACIÓN E INTEGRACIÓN DE LA RED EDUROAM

En este capítulo se mostraran todos los pasos necesarios para la implementación y la integración del servidor RADIUS local con la red inalámbrica de la UPS, Sede Quito-Campus Sur.

También se puede observar de una manera general la creación de una base de datos realizada mediante el software Apache OpenLdap para Linux.

3.1 Funcionamiento de Eduroam

Eduroam es un servicio que permite a un usuario con su respectiva contraseña ingresar a la red Eduroam en cualquier parte de mundo de una forma segura usando RADIUS y el protocolo 802.1x.

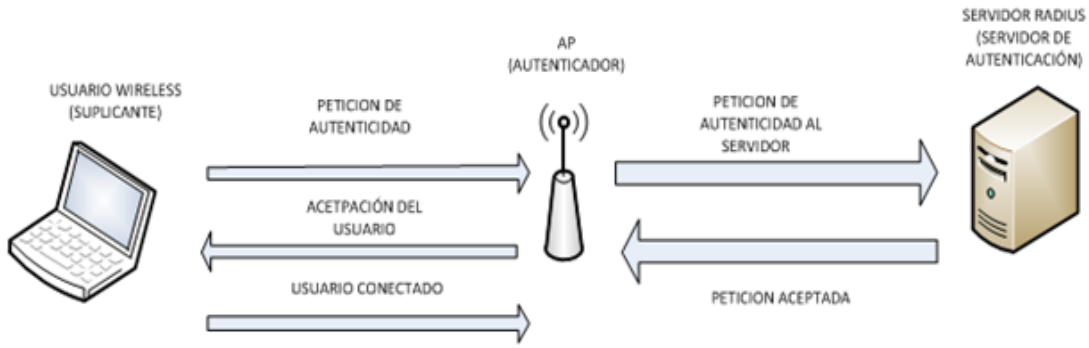

Figura 21. Modelo de autenticación de la red Eduroam.
Elaborado por: Rodrigo Borja y José Jarrín.

3.2 Implementación del servidor IDP (RADIUS) e integración a la red wlan de la UPS Campus Sur sede Quito

Para la instalación del servidor se requiere una máquina con las siguientes características mínimas:

- 4Gb de memoria RAM
- 120 Gb de memoria
- Soporte de 64 y 32 bits para el OS.

Como primer paso para la creación del servidor RADIUS, se instala el sistema operativo, lo cual para este proyecto es "DEBIAN 6.07 - SQUEZEE" debido a que es un requerimiento dispuesto por CEDIA Y Eduroam el uso de este sistema operativo al cual se lo instala por defecto, esto quiere decir sin nada opcional solo lo necesario como son:

- Particiones del disco.
- Escritorio.
- Claves para root y de usuario.

A continuación de la instalación se procede a editar las interfaces de red para que exista conexión con todos los dispositivos necesarios para la red Eduroam, y para descargar los diferentes paquetes necesarios para la implementación del servidor.

Se ingresa al fichero **/etc/network/interfaces** y se procede a editar la interfaz eth0 con la IP Pública para poder tener conexión con el servidor Federado de CEDIA.

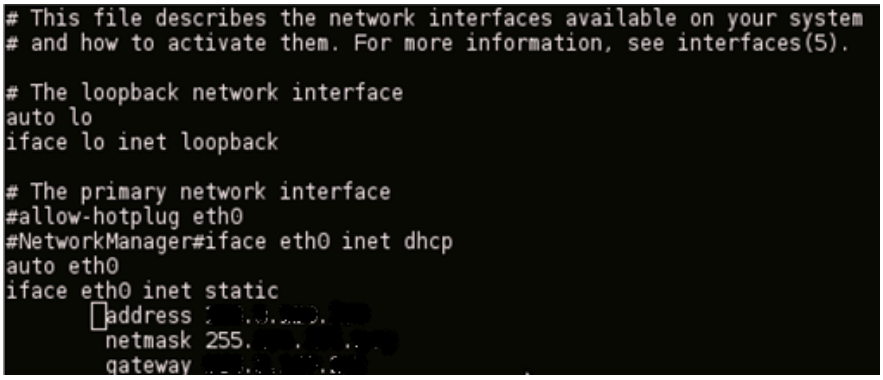

Figura 22. Configuración del fichero **/interfaces.**
Elaborado por: Rodrigo Borja y José Jarrín.

Al finalizar la edición de este fichero se procede a reiniciar la interfaz de red mediante el comando **service networking restart.**

Como siguiente paso se edita el fichero **sources.list**, este se encuentra localizado en la dirección **/etc/apt/sources.list**, esto permite una actualización de repositorio para realizar un **update** y **upgrade** al IOS del servidor.

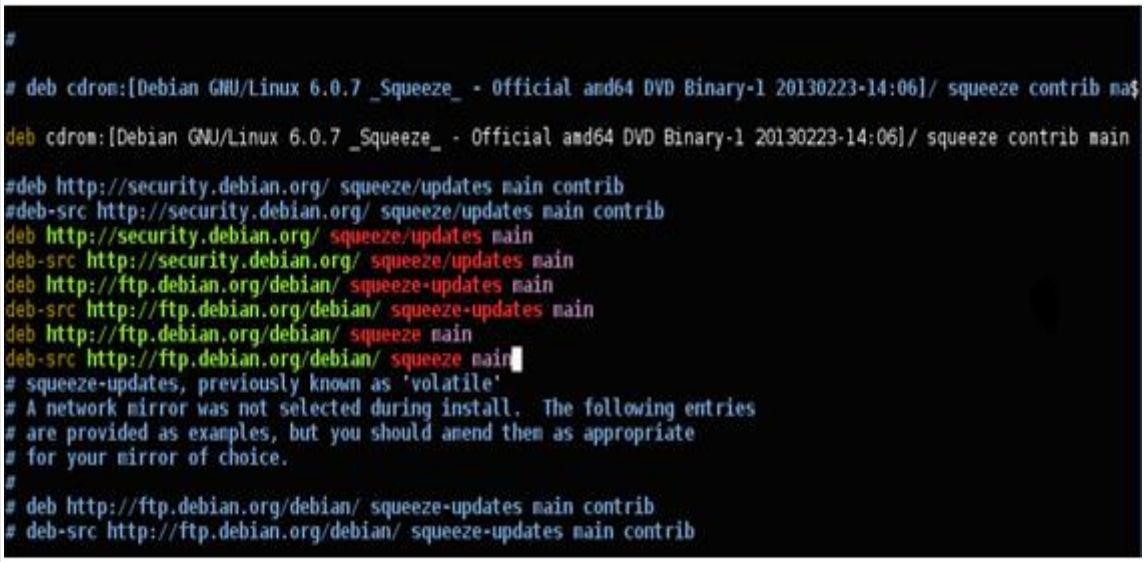

Figura 23. Configuración del fichero **/sources.list.**
Elaborado por: Rodrigo Borja y José Jarrín.

Una vez editado el fichero **sources.list** se graban los cambios realizados y se procede a realizar un **update** que actualizara el sistema operativo.

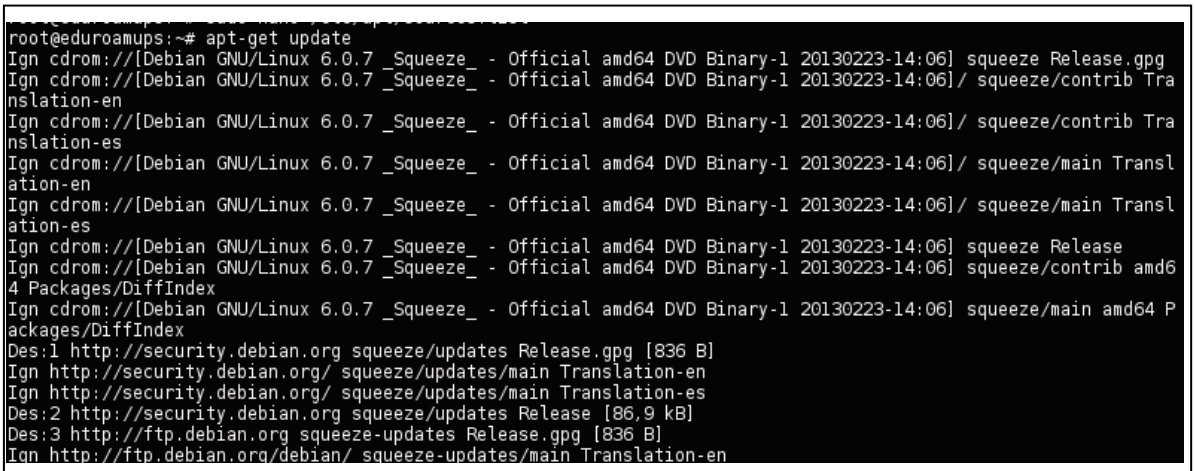

Figura 24. Ejecución del comando **apt-get update.**
Elaborado por: Rodrigo Borja y José Jarrín.

Después de realizar un update se efectuará un upgrade al servidor de la misma manera que se efectuó el update mediante el comando **apt-get upgrade**.

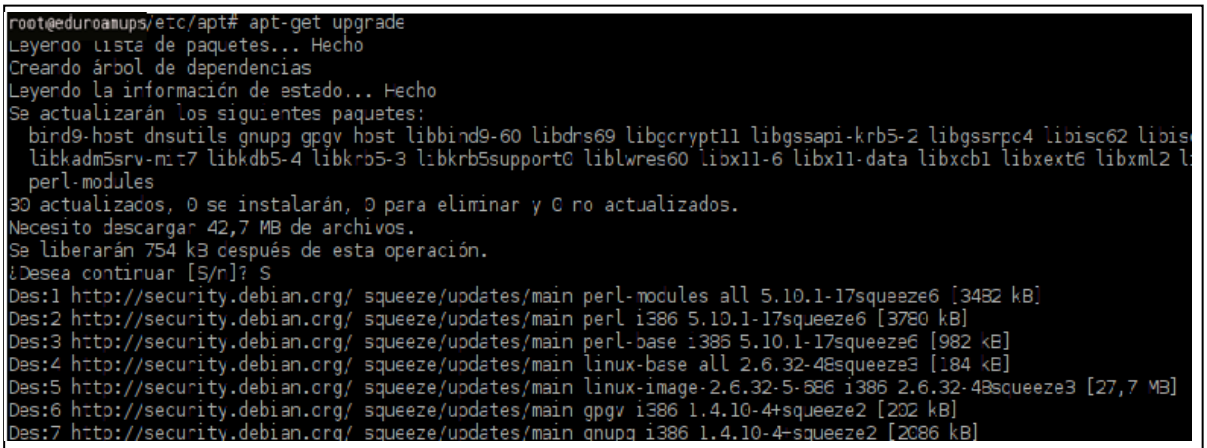

Figura 25. Ejecución del comando **apt-get upgrade.**
Elaborado por: Rodrigo Borja y José Jarrín.

Al finalizar se procede a instalar los paquetes requeridos por Eduroam con el comando **apt-get install** para el servidor RADIUS, estos paquetes son: **freeradius freeradius-ldap freeradius-mysql make pkg-config vim nmap mysql-server mysql-client libssl-dev libgnutls-dev libsnmp-dev libmysqlclient-dev libldap-dev libtool.**

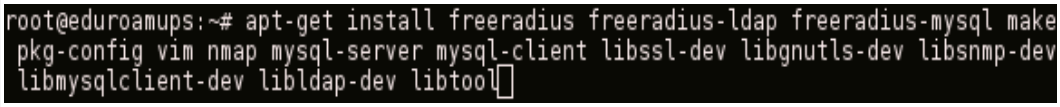

Figura 26. Instalación de paquetes.
Elaborado por: Rodrigo Borja y José Jarrín.

Los siguientes pasos que se realizan tienen que ver con la configuración de los ficheros para que el servidor ya sea incluido a la red Eduroam y al servidor Federado de CEDIA.

El primer paso es editar el fichero **/etc/freeradius/client.conf**, que permite crear un nuevo cliente para la autenticación a nivel federado y confederado. Para esto se procede a escribir los datos del servidor Federado de CEDIA incluyendo la clave creada para que se pueda autenticar CEDIA con el servidor institucional.de la UPS.

Figura 27. Configuración del fichero **/clients.conf.**
Elaborado por: Rodrigo Borja y José Jarrín.

Se prosigue con la configuración del fichero **/etc/freeradius/proxy.conf**, para que el servidor tenga la información de los proveedores de autenticación Eduroam, para esto se solicita a CEDIA una clave de autentificación para solicitar peticiones a su servidor Federado, también se ingresa los datos respectivos del servidor Federado.

Figura 28. Configuración del fichero **/proxy.conf.**
Elaborado por: Rodrigo Borja y José Jarrín.

Para finalizar se crea un usuario con el fin de comprobar que se esté realizando la autenticación que se requiere en Eduroam, para integrar la red inalámbrica de la UPS. Este usuario se crea en el fichero **/etc/freeradius/users**, el nombre del usuario es "**usuarioprueba**" y su clave "**prueba**".

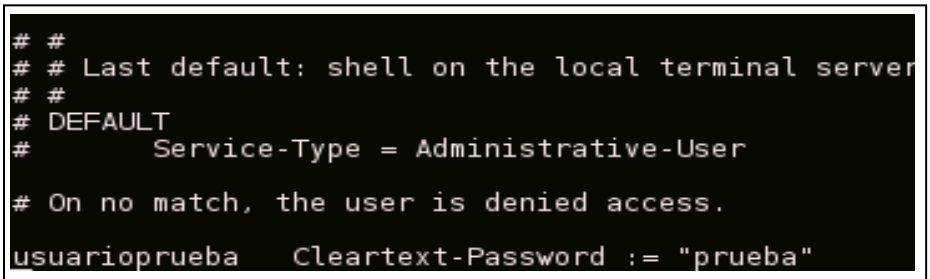

Figura 29. Configuración del fichero **/users.**
Elaborado por: Rodrigo Borja y José Jarrín.

Verificado todos las configuraciones anteriores se procede a realizar una prueba a al servidor mediante la inicialización en modo debug ejecutando el comando "**freeradius -X**" para comprobar dentro del servidor la aceptación de solicitudes de autentificación.

Figura 30. Mensaje de inicialización del deamon de freeradius.
Elaborado por: Rodrigo Borja y José Jarrín.

Ver en el capítulo 4 sección 4.1 las pruebas realizadas para esta sección.

En esta fase de la implementación del servidor se necesita una base de datos como requisito, para la instalación del servidor esta base es creada mediante el protocolo LDAP (Lightweight Directory Access Protocol), que se maneja a nivel de capa aplicación para permitir el acceso a un directorio, este directorio está constituido y organizado por varios elementos de una forma lógica y jerárquica.

El LDAP que se instala a continuación es **Apache Directory Studio** una versión libre para Linux, es una aplicación Eclipse RPG destinado a ser utilizado como una plataforma LDAP.

Figura 31. Página web de Apache Directory Studio.
Elaborado por: Rodrigo Borja y José Jarrín.

Esta herramienta de LDAP puede ser instalada como plug-in de Eclipse, esta es la forma más rápida para instalarla, primero hay que ingresa en Ayuda- actualizaciones de software-Buscar e instalar.

Seleccionar **Search for new features to install** y presionar la opción como se muestra en la siguiente figura:

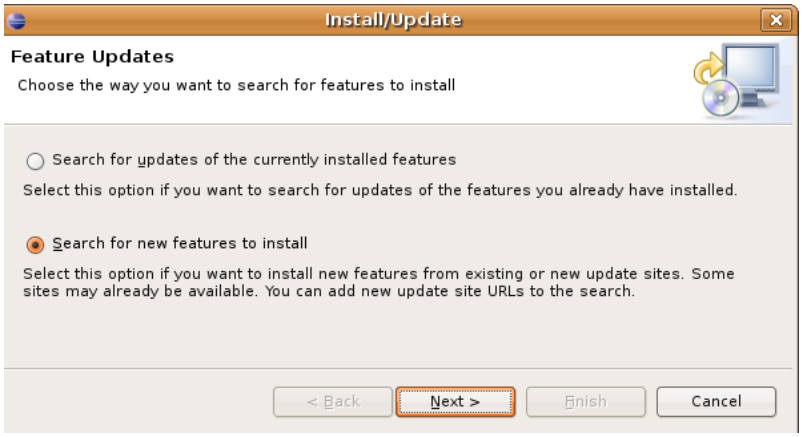

Figura 32. Ventana de elección de la aplicación Apache Directory Studio.
Elaborado por: Rodrigo Borja y José Jarrín.

Lo siguiente es indicar el sitio de actualización de Apache Directory Studio, ingresar a sitio remoto pulsar nuevo e ingresar el nombre del sito de actualización y la siguiente URL: http://directory.apache.org/studio/update/1.x.

Figura 33. Ventana de actualización de aplicación.
Elaborado por: Rodrigo Borja y José Jarrín.

Seleccionar la aplicación Apache Dierctory Studio Update Site para poderla instalar y pulsar Finalizar.

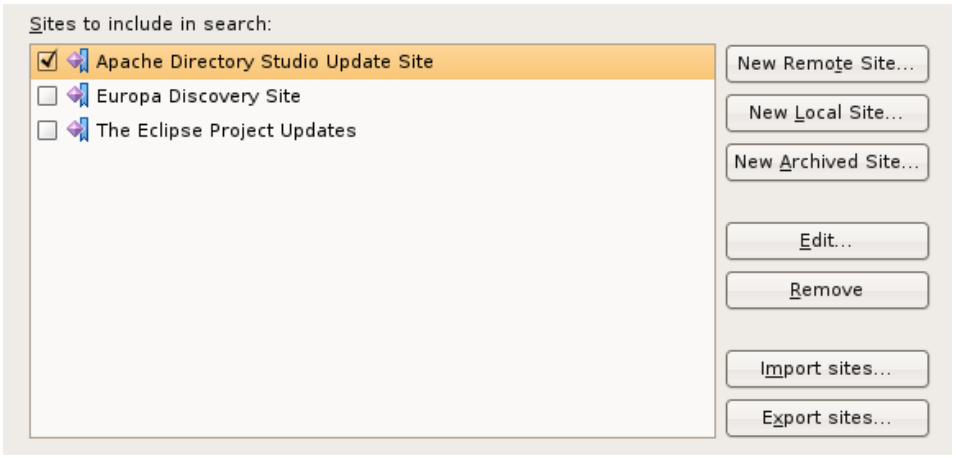

Figura 34. Selección de Apache Directory Studio Update Suite.
Elaborado por: Rodrigo Borja y José Jarrín.

En este momento el gestor de actualización comprueba el sitio para actualizar y presenta varias alternativas de las que se escoge la opción que se muestra en la siguiente figura.

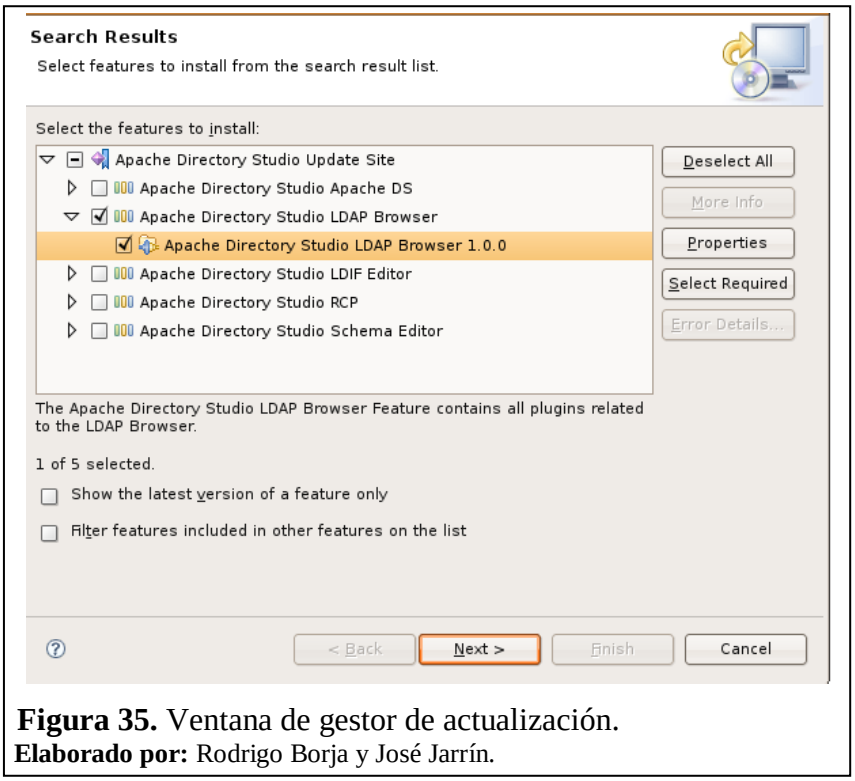

Figura 35. Ventana de gestor de actualización.
Elaborado por: Rodrigo Borja y José Jarrín.

Se acepta los términos de licencia y se oprime la opción siguiente para visualizar las otras opciones de la instalación.

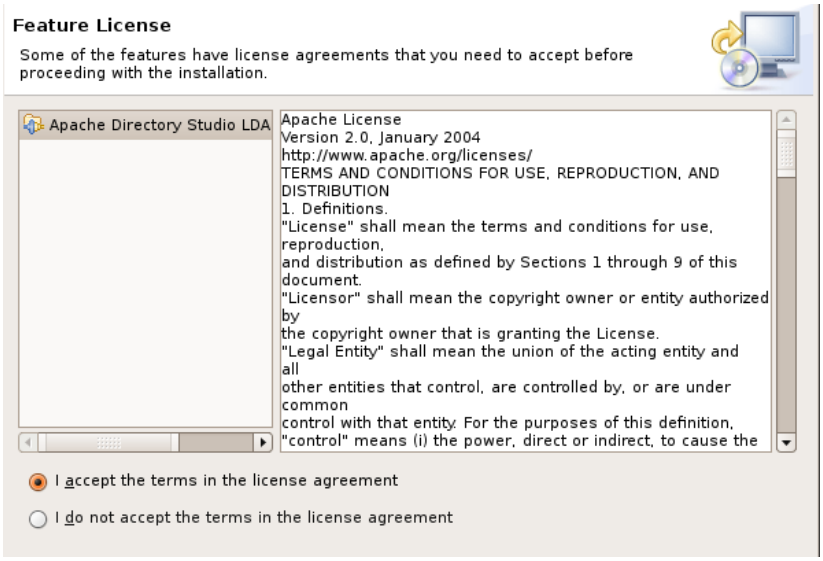

Figura 36. Ventana de instalación de Apache Directory Studio.
Elaborado por: Rodrigo Borja y José Jarrín.

Se observa que el paquete que se va a instalar sea Apache Directory Studio LDAP Browser y se pulsa siguiente.

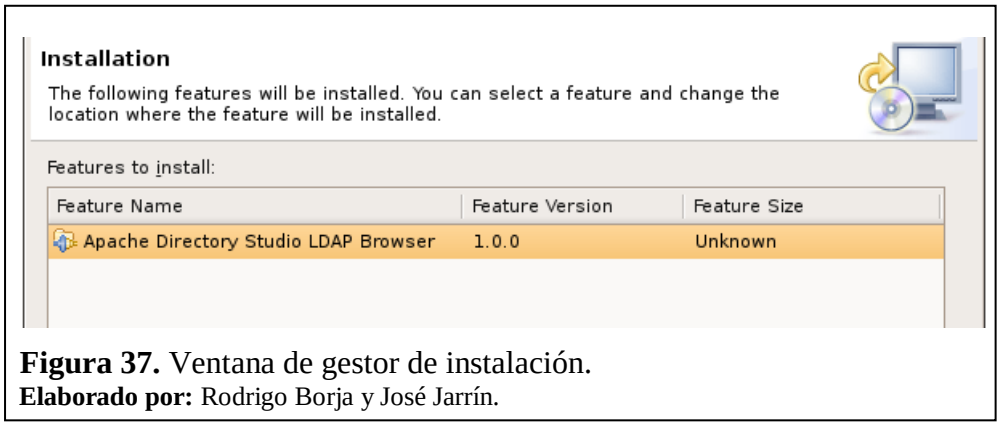

Figura 37. Ventana de gestor de instalación.
Elaborado por: Rodrigo Borja y José Jarrín.

Cuando haya finalizado el paso anterior empezará a descargar el programa con su respectiva actualización y al final pulsar Install.

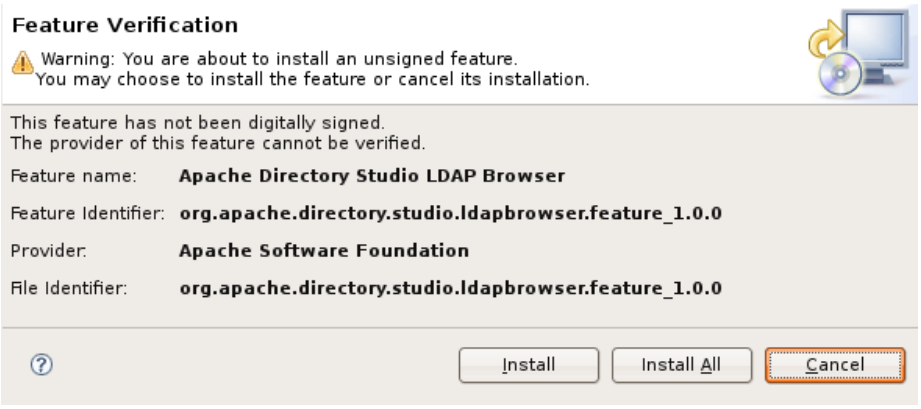

Figura 38. Ventana de verificación de la instalación.
Elaborado por: Rodrigo Borja y José Jarrín.

Después de la instalación se procede a crear una nueva conexión, para esto dirigirse a la esquina izquierda para crear una nueva ventana.

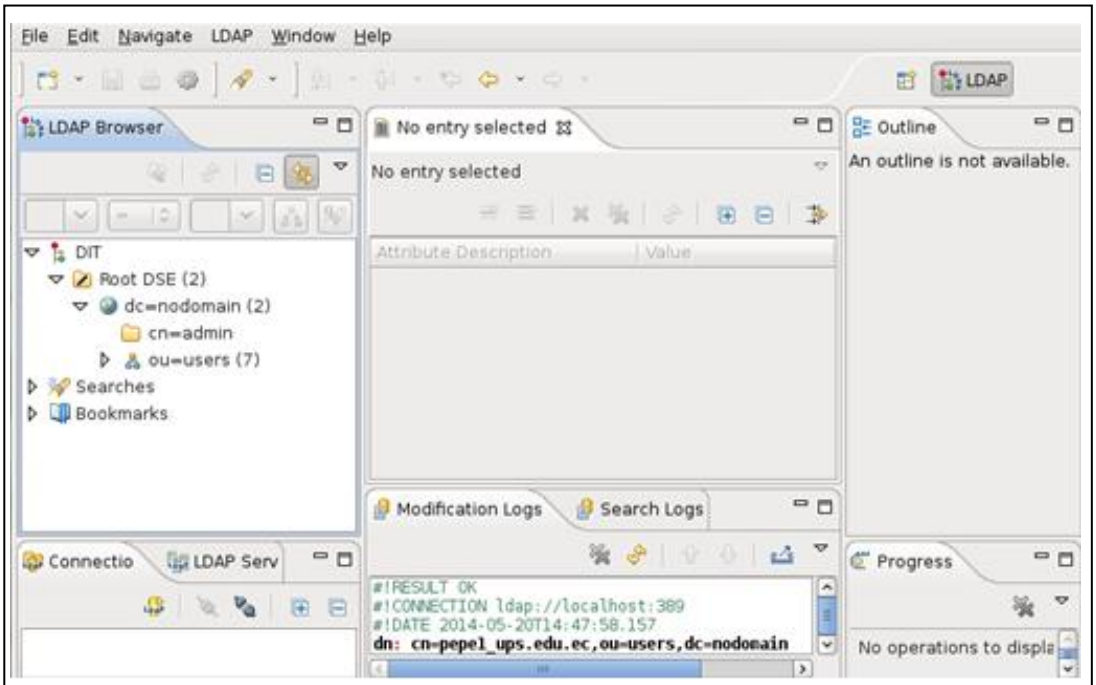

Figura 39. Pantalla de Apache Directory Studio.
Elaborado por: Rodrigo Borja y José Jarrín.

Escoger la opción LDAP Connection para crear una nuevo directorio LDAP que permitirá crear los usuarios que van hacer autenticados con el servidor RADIUS.

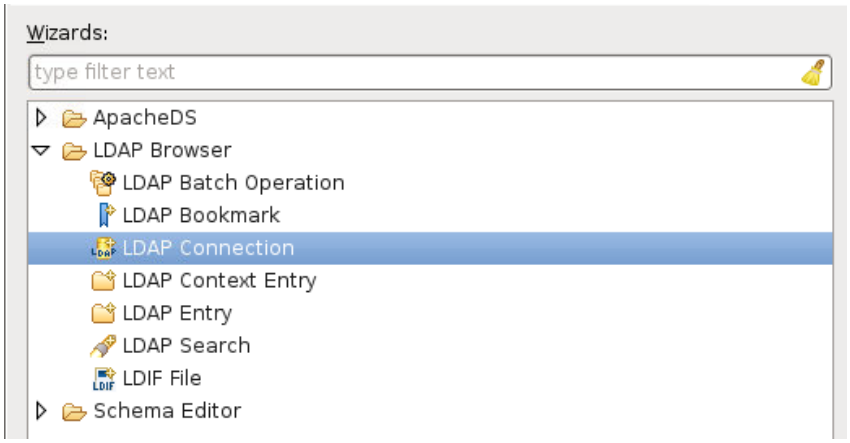

Figura 40. Gestor de conexión LDAP con servidor.
Elaborado por: Rodrigo Borja y José Jarrín.

En la ventana ingresar el nombre de la nueva conexión para este caso se llamará Freeradius, el hostname será el localhost de la máquina y el puerto predeterminado es 389.

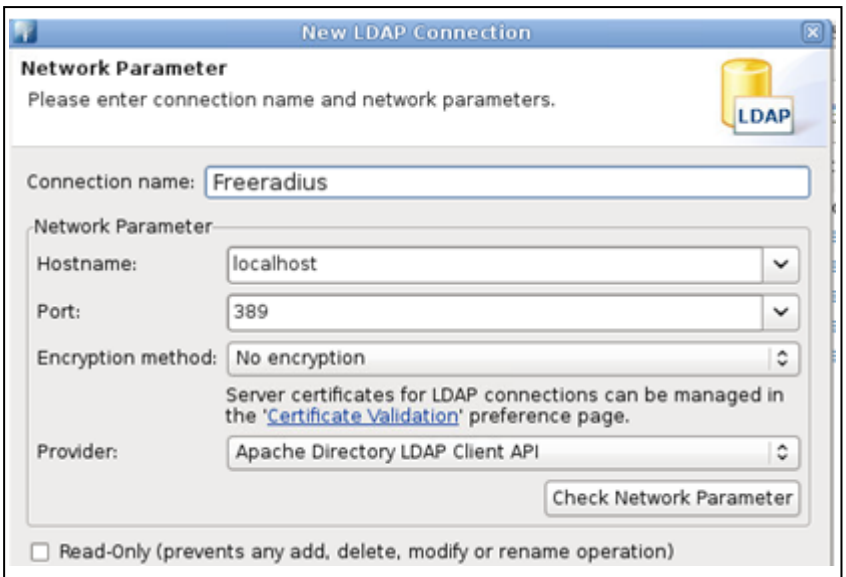

Figura 41. Ventana de ingreso de datos de la conexión.
Elaborado por: Rodrigo Borja y José Jarrín.

En la siguiente ventana se procede a ingresar los directorios de los servidores, este se especifica en el fichero **/slapd.conf** por lo cual se mantiene con esa misma configuración y también se ingresa la contraseña para que exista conexión entre el RADIUS y el OpenLdap.

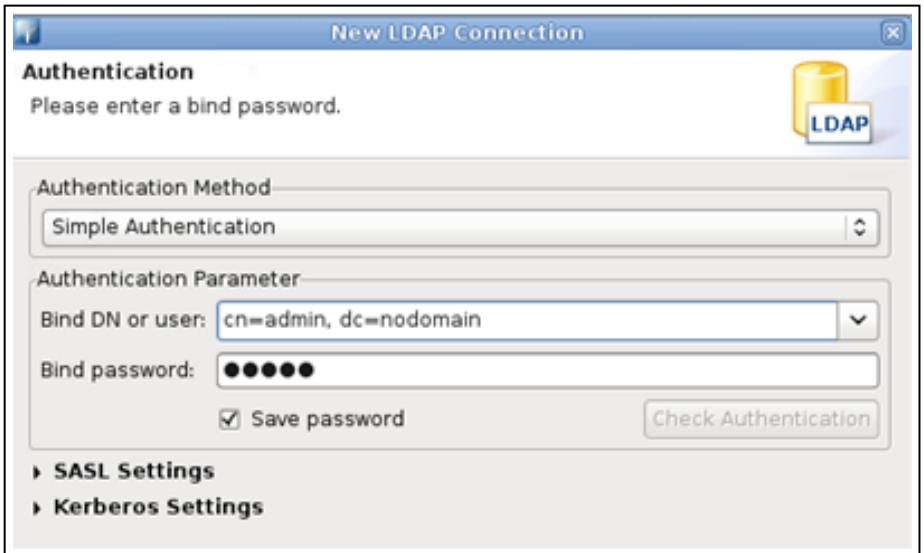

Figura 42. Ventana de atributos para el directorio.
Elaborado por: Rodrigo Borja y José Jarrín.

Como se muestra en la figura 42 ya se creó la conexión entre el servidor y el directorio llamado Freeradius, ahora se procede a crear los nuevos usuarios para que sean autenticados con el servidor.

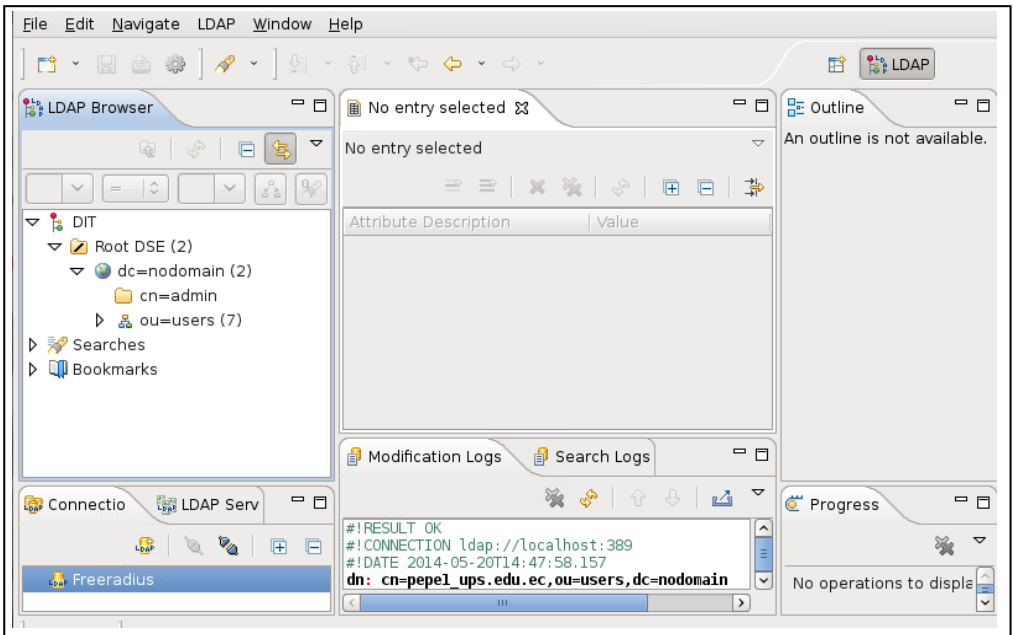

Figura 43. Conexión creada entre el servidor y el directorio LDAP.
Elaborado por: Rodrigo Borja y José Jarrín.

En la creación de usuarios se deben especificar los atributos LDAP para identificar a los usuarios en el directorio, la siguiente tabla muestra los atributos más importantes que se usan en un directorio LDAP.

Tabla 27. Atributos LDAP.

ATRIBUTOS	ALIAS	OBSERVACIÓN
Dn	distinguishedName	Se refiere al componente del dominio, en él está contenido los atributos cn, ou, dc.
Dc	domainComponent	Identifica los componentes de un dominio.
Ou	organisationalUnitName	Identifica el grupo o el directorio, representa también organizaciones internas dentro del directorio.
Cn	Common name	Almacena un nombre en el directorio.
Sn	Surname	Identifica el apellido.
Uid	userid	Identifica el usuario con un único valor en específico.

Elaborado por: Rodrigo Borja y José Jarrín.

Para la creación de usuarios se da click derecho dentro del directorio LDAP en la opción **ou=users** y seleccionar **New-New Entry**, aparecerá la siguiente ventana como se muestra en la figura, dar click en siguiente.

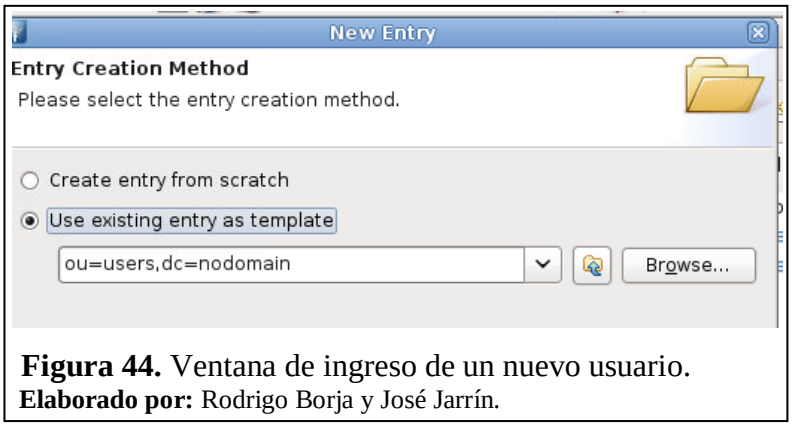

Figura 44. Ventana de ingreso de un nuevo usuario.
Elaborado por: Rodrigo Borja y José Jarrín.

Dar click en siguiente ya que se encuentra con todos los atributos necesarios para crear el usuario, por lo tanto no se modifican ni se agregan otros atributos.

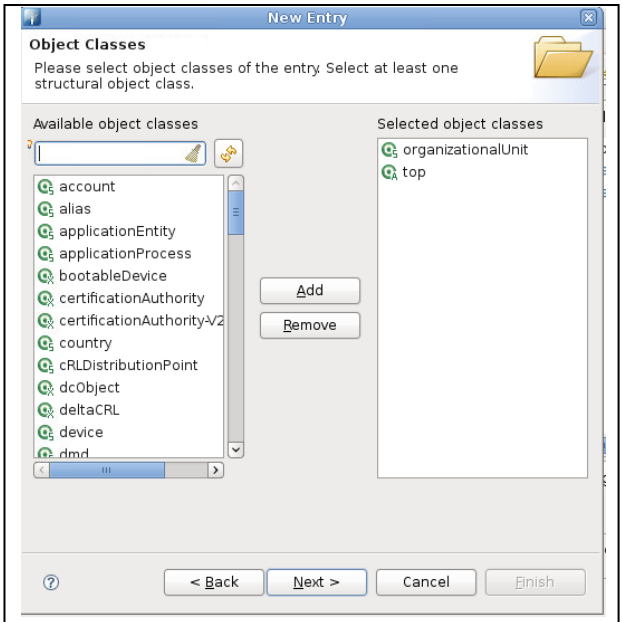

Figura 45. Ingreso de atributos del usuario.
Elaborado por: Rodrigo Borja y José Jarrín.

En la opción RCN ingresar el mail de usuario sin el signo (@) en su lugar usar el símbolo (_), con el domino de la UPS.

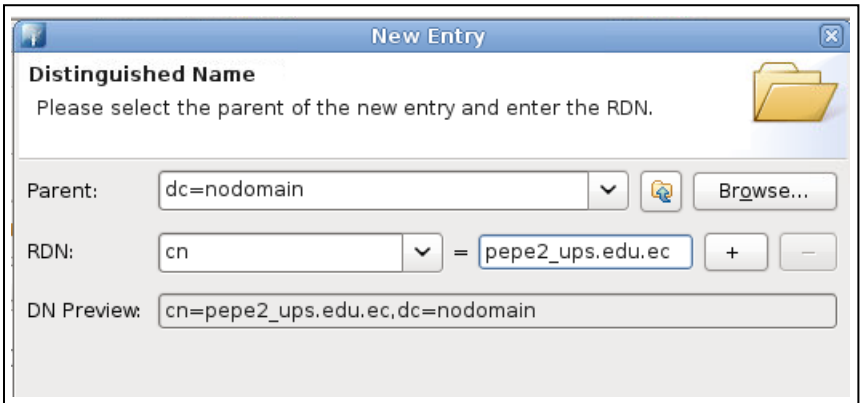

Figura 46. Ingreso de usuario con su respectivo dominio.
Elaborado por: Rodrigo Borja y José Jarrín.

Ingresar el atributo ou que esta descrito en el directorio para este caso es users, y como se observa en la figura 46 ya está ingresado el usuario en el directorio.

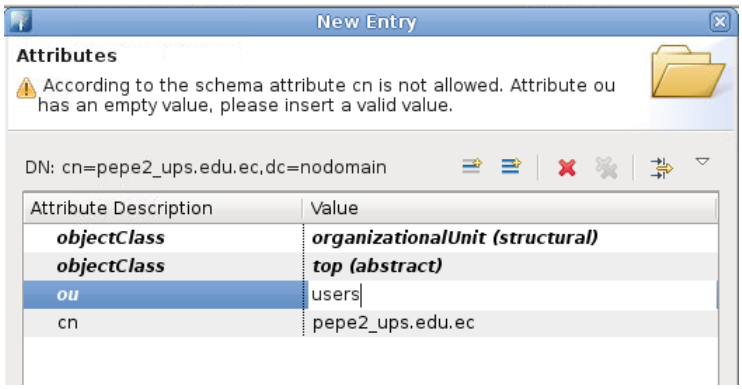

Figura 47. Ingreso del atributo **ou=users** para la conexión.
Elaborado por: Rodrigo Borja y José Jarrín.

Como se visualiza en la figura 47 el usuario pepe2 con dominio ups.edu.ec ya está creado en el directorio LDAP con sus atributos, lo último que se modifica es la contraseña del usuario.

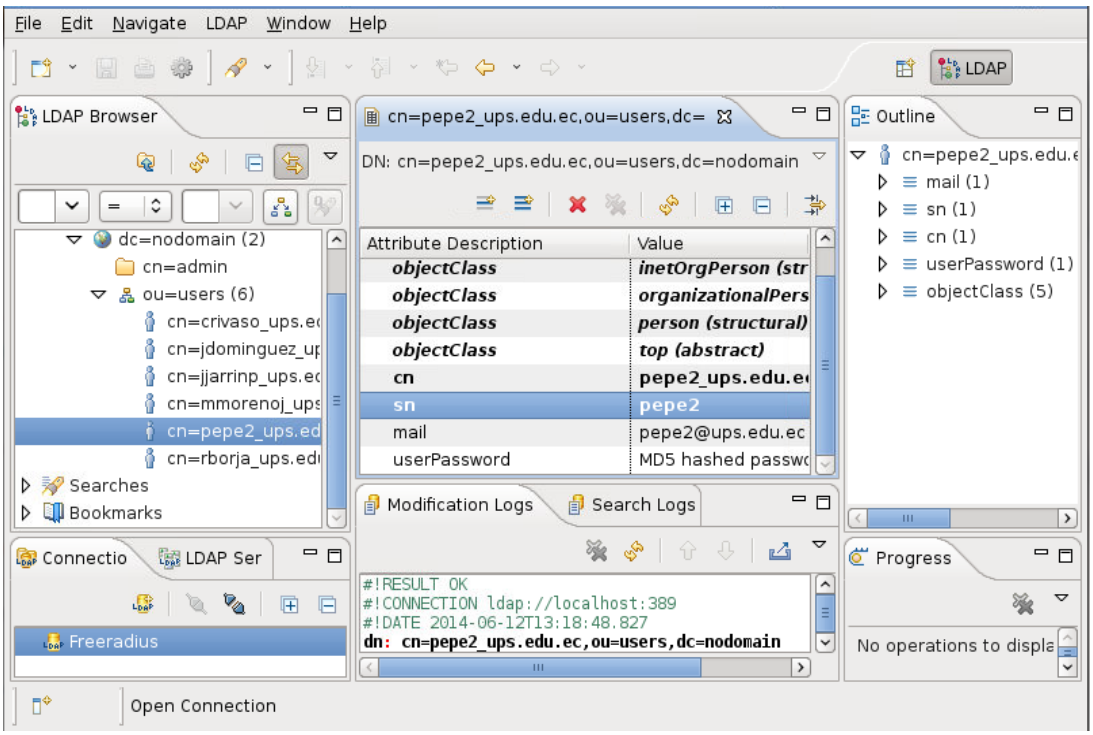

Figura 48. Verificación del usuario con sus respectivos atributos.
Elaborado por: Rodrigo Borja y José Jarrín.

Para la edición de la contraseña dar click derecho en la opción **userPassword** y seleccionar la opción **Edit Value**, se muestra una ventana como en la figura 48 y se procede a editar la contraseña que se otorgará al usuario.

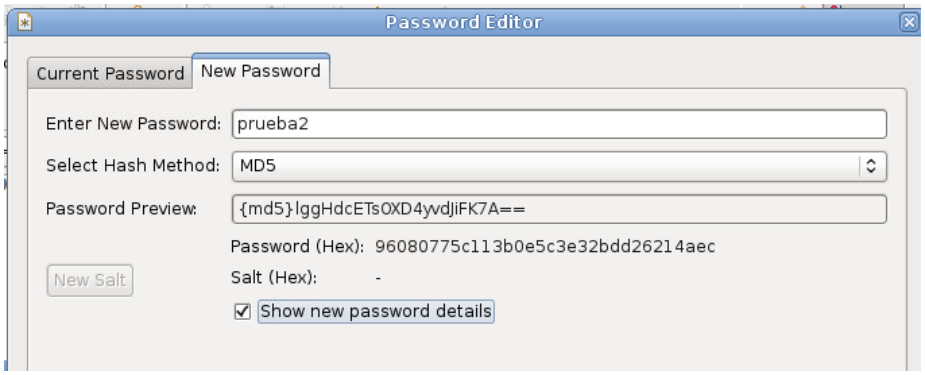

Figura 49. Ingreso de la contraseña para el usuario.
Elaborado por: Rodrigo Borja y José Jarrín.

Ahora es momento de integrar la base de datos de la institución con el servidor Radius, para esta actividad se ingresa al fichero **/etc/freeradius/sites-enabled/default** para que la base de datos autentifique los usuarios con el servidor, luego dirigirse dentro del fichero a la sección **authorize** y descomentar **ldap**.

```
        #  See "Authorization Queries" in sql.conf
#       sql

        #
        #  If you are using /etc/smbpasswd, and are also doing
        #  mschap authentication, the un-comment this line, and
        #  configure the 'etc_smbpasswd' module, above.
#       etc_smbpasswd

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

        #
        #  Enforce daily limits on time spent logged in.
```

Figura 50. Configuración del fichero **/etc/freeradius/sites-enable/default** sección **authorize.**
Elaborado por: Rodrigo Borja y José Jarrín.

También dentro del mismo fichero dirigirse a la sección **autenticate** y descomentar **Auth-Type Ldap**.

```
# 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
}

#
#  Allow EAP authentication.
eap
```

Figura 51. Configuración del fichero **/etc/freeradius/sites-enable/default** sección **autenticate.**

Elaborado por: Rodrigo Borja y José Jarrín.

El mismo procedimiento para el fichero **/etc/freeradius/sites-enabled/inner-tunnel**, ya que contienen las mismas secciones.

El último paso es ingresar al fichero **/etc/freeradius/modules/ldap**, e ingresar los datos del servidor LDAP institucional.

```
ldap {
        #
        #  Note that this needs to match the name in the LDAP
        #  server certificate, if you're using ldaps.
        server = "localhost"
        identity = "cn=admin,dc=nodomain"
        password = admin
        basedn = "ou=users,dc=nodomain"
        #filter = "(mail=%{%{Stripped-User-Name}:-%{User-Name}})"
        filter = "(mail=%{User-Name})"
        #base_filter = "(objectclass=radiusprofile)"

        #  How many connections to keep open to the LDAP server.
        #  This saves time over opening a new LDAP socket for
        #  every authentication request.
        ldap_connections_number = 5
```

Figura 52. Configuración del fichero **/etc/freeradius/modules/ldap.**

Elaborado por: Rodrigo Borja y José Jarrín.

Ingresar al servidor en modo debug o prueba, y realizar el test correspondiente para verificar la conexión entre el LDAP y el servidor RADIUS.

Ver en el capítulo 4 sección 4.2 las pruebas realizadas para esta sección.

Para el siguiente nivel se debe solicitar los certificados a CEDIA para la navegación a Internet, porque con ellos se evita el robo de la información, también la confirmación de las identidades del usuario y encriptar la información cuando se va a salir a Internet.

Lo primero es mover los dos certificados facilitados por CEDIA al fichero **/etc/freeradius/certs**, hay que tener en cuenta que los dos archivos terminan en el formato **.pem** y **.key** para ser considerados certificados de navegación en el servidor.

Mover los archivos con el comando **mv** al fichero **/etc/freeradius/certs** tal y como muestra la figura.

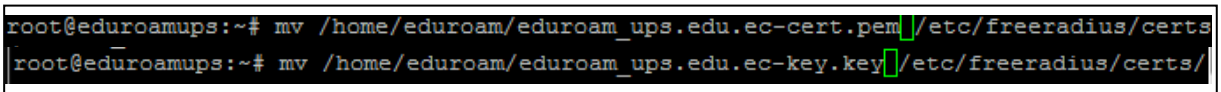

Figura 53. Cambio de ubicación del los certificados.
Elaborado por: Rodrigo Borja y José Jarrín.

Comprobar que los dos archivos se encuentren en el fichero **/etc/freeradius/certs** para poder ser usados en el servidor.

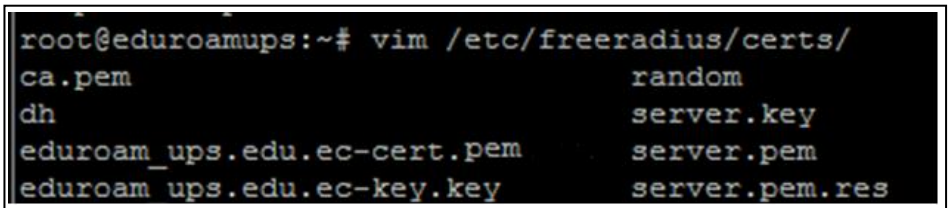

Figura 54. Verificación del fichero **/certs.**
Elaborado por: Rodrigo Borja y José Jarrín.

Se ingresa al fichero **/etc/freeradius/eap.conf**, para configurar el protocolo de autentificación EAP el cual en este caso es TTLS.

```
eap {
        #  Invoke the default supported EAP type when
        #  EAP-Identity response is received.
        #
        #  The incoming EAP messages DO NOT specify which EAP
        #  type they will be using, so it MUST be set here.
        #
        #  For now, only one default EAP type may be used at a time.
        #
        #  If the EAP-Type attribute is set by another module,
        #  then that EAP type takes precedence over the
        #  default type configured here.
        #
        default_eap_type = ttls
```

Figura 55. Configuración del protocolo de autenticación.
Elaborado por: Rodrigo Borja y José Jarrín.

También modificar los certificados por defecto e ingresar los que CEDIA otorgó, lo demás no se cambia.

```
certdir = ${confdir}/certs
cadir = ${confdir}/certs

private_key_password = UpS.Ui0AA2o14
private_key_file = ${certdir}/eduroam_ups.edu.ec-key.key



#  If Private key & Certificate are located in
#  the same file, then private_key_file &
#  certificate_file must contain the same file
#  name.
#
#  If CA_file (below) is not used, then the
#  certificate_file below MUST include not
#  only the server certificate, but ALSO all
#  of the CA certificates used to sign the
#  server certificate.
certificate_file = ${certdir}/eduroam_ups.edu.ec-cert.pem
```

Figura 56. Ingreso del los certificados en el fichero **/eap.conf.**
Elaborado por: Rodrigo Borja y José Jarrín.

Guardar los cambios e iniciar el servicio de RADIUS en el servidor con el comando **/etc/init.d/freeradius start**.

Ahora el servidor ya está en funcionamiento con lo cual se lo puede integrar a la red inalámbrica de la UPS Campus Sur esta integración del servidor con el WLC (Wireless Lan Controler) de la UPS permite a las antenas irradiar la red inalámbrica Eduroam dentro del campus.

El primer paso es ingresar en el servidor RADIUS al fichero **/etc/freeradius/clients.conf**, para agregar al WLC como otro cliente para permitir la autenticación, se procede a ingresar la ip del WLC, una clave para que permitir el acceso al WLC, un shortname o un alias para el dispositivo y el nastype el cual define el nombre de la tecnología de almacenamiento para compartir información de un servidor con los clientes a través de la red.

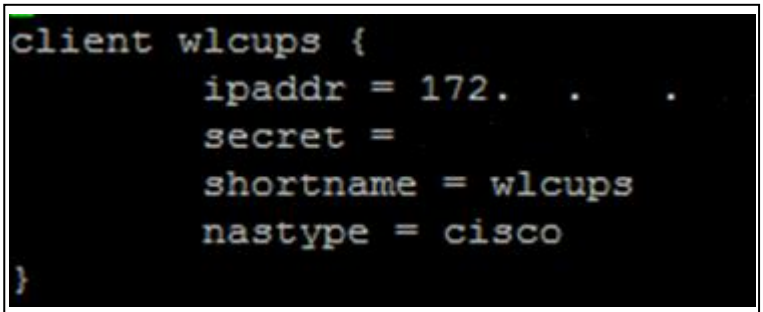

Figura 57. Creación del cliente WLC.
Elaborado por: Rodrigo Borja y José Jarrín.

Se ingresa al interfaz gráfico del WLC de la UPS, y se crea la red inalámbrica Eduroam la cual va a ser propagada mediante todas las antenas de campus, a su vez se le realizará modificaciones para que junto al servidor RADIUS puedan realizar las peticiones de autentificación inalámbrico.

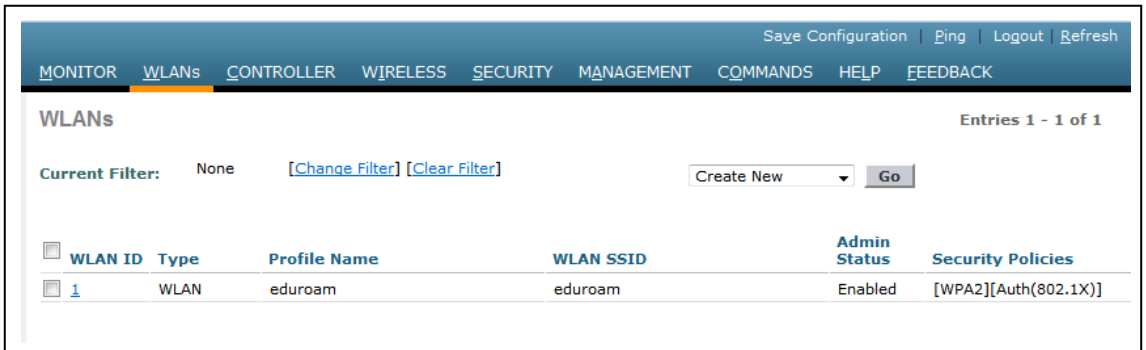

Figura 58. Creación del cliente WLC.
Elaborado por: Rodrigo Borja y José Jarrín.

Se procede a ingresar a la pestaña **SECURITY** y se selecciona la opción Authentication se hace click en **NEW** y se modifican los siguientes literales, se ubica la IP del servidor RADIUS y también la clave que se ingresó en el fichero **/clients.conf**, y se guardan las configuraciones.

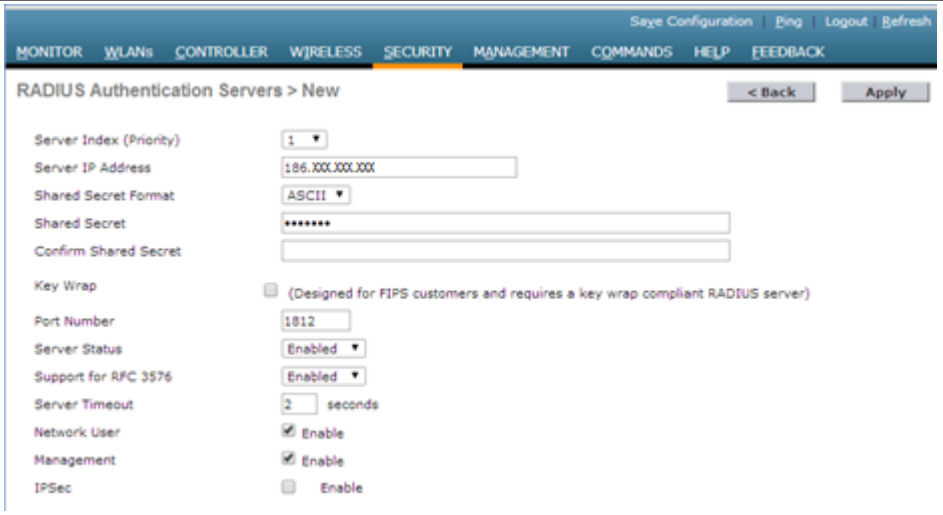

Figura 59. Ingreso del servidor en el WLC de la UPS Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

Se aplican los cambios y se procede a realizar la configuración de la comunicación entre el WLC de la UPS y el servidor RADIUS, se puede observar en la figura 59 que ya se ha creado la comunicación entre los dos dispositivos dichos anteriormente.

Figura 60. Verificación de la comunicación entre el servidor y el WLC de la UPS Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

Seleccionar la pestaña WLANs e ingresar en la opción **Edit**, para modificar la red Eduroam, después se ingresa a Security y se escoge como opción las opciones WPA+WPA2 como método de autentificación y también se selecciona el protocolo 802.1x lo demás se deja por defecto.

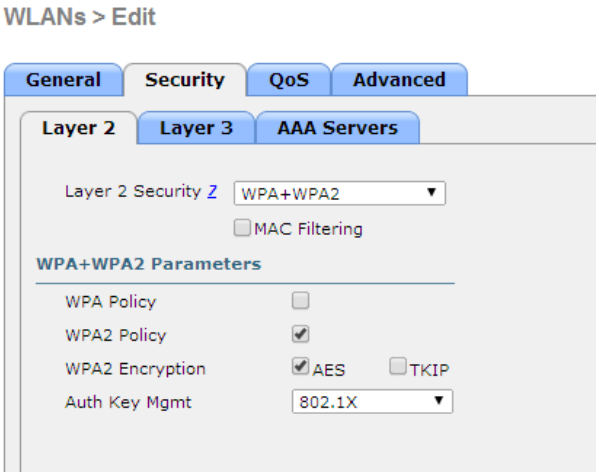

Figura 61. Edición del método de autenticación en el WLC de la UPS Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

Dentro de esta misma pestaña seleccionar la pestaña AAA Server y elegir la opción "Server 1"que contiene la información del servidor de autenticación, guardar los cambios.

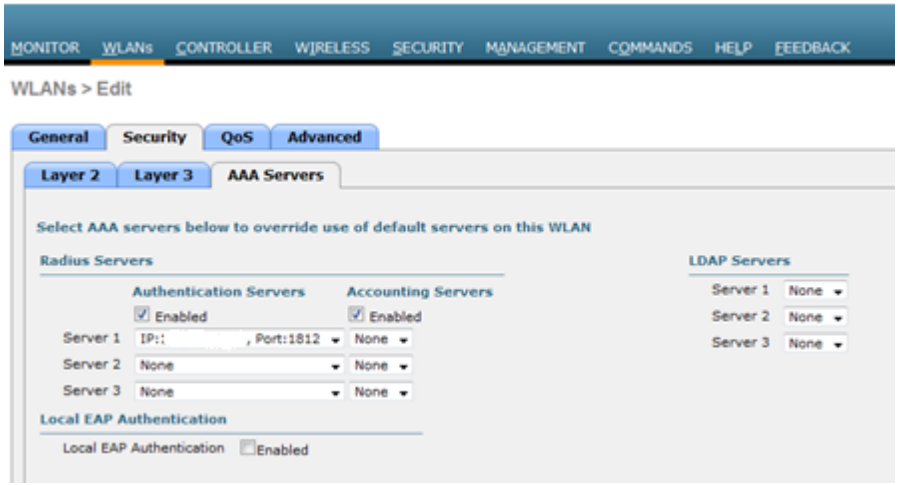

Figura 62. Ingreso de la información del servidor en el WLC de la UPS Campus Sur.
Elaborado por: Rodrigo Borja y José Jarrín.

Para finalizar se observa que la red Eduroam ya se está propagando y está lista para usarse con los dispositivos de los usuarios que tiene el acceso a este proyecto internacional, cabe mencionar que aquellos beneficiarios de esta red deben de tener ciertos parámetros para ingresar y utilizar este servicio.

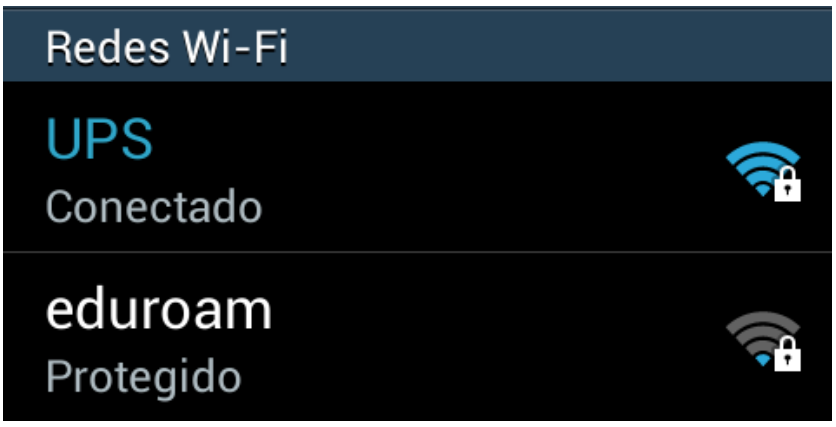

Figura 63. Verificación de la red Eduroam.
Elaborado por: Rodrigo Borja y José Jarrín.

Este capítulo mostró la instalación del servidor, su integración con la red dando como resultado el servicio de Eduroam en la UPS Campus Sur, incluyendo también los servicios que posteriormente se otorgarán a la universidad con la integración a este proyecto.

CAPÍTULO 4

PRUEBAS Y RESULTADOS

En el presente capitulo se describen las pruebas realizadas de autenticación entre el usuario y la red inalámbrica Eduroam creada la UPS Campus-Sur con dispositivos móviles que soportan el protocolo 802.1x. También se incluyen las conclusiones y recomendaciones con respecto al proyecto que se ha realizado en los anteriores capítulos.

4.1 Prueba de autenticación al localhost del servidor

Esta prueba se realiza después de haber configurado todo lo referente a la conexión entre el servidor de la UPS y CEDIA, ya que con esta prueba se verifica que el servidor RADIUS este autentificando con usuarios internos y también este consultando al servidor Federado tal es el caso de CEDIA.

Para la prueba se envía un mensaje a al localhost con las siguientes características.

- radtest usuario clave localhost 0 testing123

En este mensaje de prueba, la palabra radtest simboliza el mensaje de prueba al servidor RADIUS local, el número 0 significa que no exista encriptación en la consulta al localhost, y testing123 es la clave por defecto para realizar consultas al servidor local.

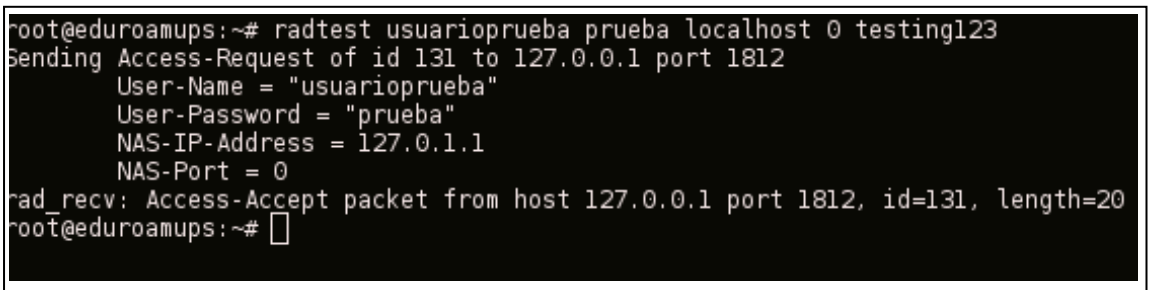

Figura 64. Realización de un radtest al localhost.
Elaborado por: Rodrigo Borja y José Jarrín.

Después de haber realizado la prueba se procede a enviar la IP pública del servidor y la clave que se escribió en el fichero "**clients.conf**" y también el usuario creado en el fichero **"/users"** para que realice las consultas a al servidor el servidor Federado de CEDIA.

La respuesta positiva por parte del administrador de CEDIA, señala que el servidor de la UPS ya es parte del dominio de Eduroam y que ya está disponible para toda la red Eduroam.

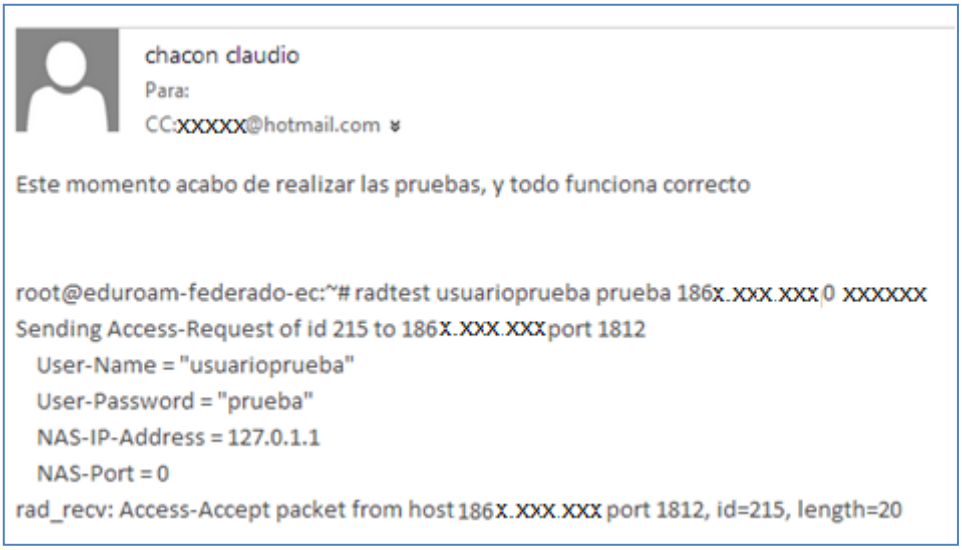

Figura 65. Configuración del fichero **/proxy.conf.**
Elaborado por: Rodrigo Borja y José Jarrín.

4.2 Prueba de autenticación con la base de datos y con usuario de prueba internacional

Para esta prueba se tuvo que ingresar anteriormente los datos del OpenLdap de la institución en el servidor RADIUS para que pueda autenticar a los usuarios creados en la base de datos, y también se demostrará que el servidor ya puede autenticar beneficiarios que no estén registrados en la UPS sino que estén en otra institución en este caso CEDIA.

Primero se ingresa en modo debug al servidor y se procede a realizar un radtest con un beneficiario creado en el OpendLdap al localhost con contraseña testing123.

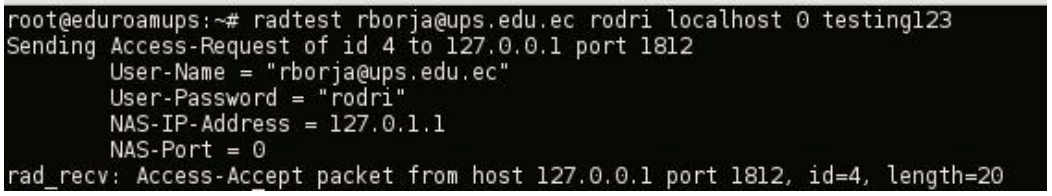

Figura 66. Prueba de conexión entre del usuario en el directorio LDAP y servidor RADIUS.
Elaborado por: Rodrigo Borja y José Jarrín.

En la figura 66 se muestra el proceso de autenticación, verificando la contraseña, el nombre de usuario y el dominio entre el usuario creado en el directorio LDAP y el servidor RADIUS.

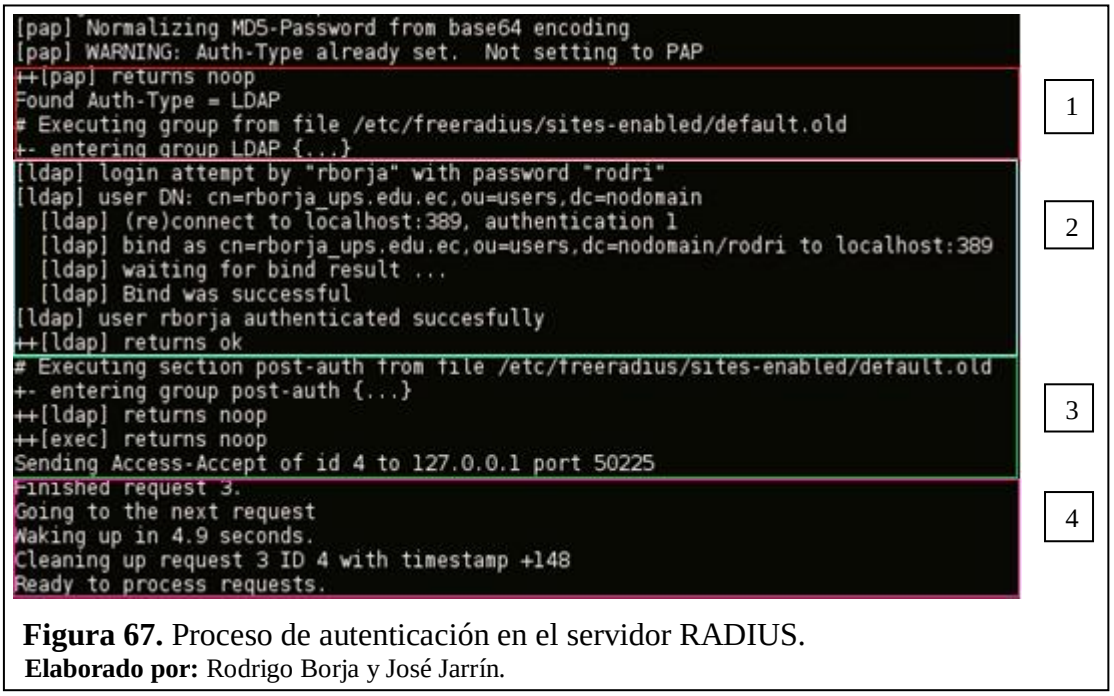

Figura 67. Proceso de autenticación en el servidor RADIUS.
Elaborado por: Rodrigo Borja y José Jarrín.

Mediante la figura 66 se pueden visualizar algunas gestiones en el proceso de autenticación que realiza en el servidor, en el paso número (1) se observa que la autenticación se la va a realizar al LDAP, en el paso (2) se verifica la contraseña y el usuario que va a ingresar el cual se lo compara con el que está registrado en el LDAP, en el paso (3) se ejecuta el fichero /default.old en el cual permite que todas las decisiones que tome el servidor en la autenticación de un usuario se la haga por LDAP, y si es correcta acepta la solicitud de autenticación, en el paso (4) el servidor se restaura y está listo para escuchar otra petición.

Por último se verifica que exista autenticación entre el usuario prueba otorgado por CEDIA para esta prueba, al igual que la anterior prueba realizarla al local host con la contraseña que se ingresó en el fichero **/clients.conf** para el servidor Federado de CEDIA.

Figura 68. Prueba de usuario CEDIA y el servidor RADIUS institucional de la UPS.
Elaborado por: Rodrigo Borja y José Jarrín.

4.3 Conectividad con el usuario local

Para que exista conectividad entre el usuario y la red inalámbrica Eduroam se debe de crear un usuario en la base de datos para que al final el servidor RADIUS pueda proceder la autentificación.

Se crea en la base de datos un usuario prueba con su respectiva contraseña el cual mantenga el dominio de la universidad en este caso es rborja@ups.edu.ec, y se usa un dispositivo móvil para conectarse a la red.

Eduroam contiene diferentes manuales que permiten la conexión de dispositivos móviles como laptops, iPads, Smartphone, ya que ellos tienen diferentes métodos de conexión para soportar el protocolo 802.1x.

En la prueba de conexión el dispositivo móvil primero identifica la red inalámbrica Eduroam, a la cual se la escoge, y se procede a configurar los diferentes parámetros para ingresar a ella.

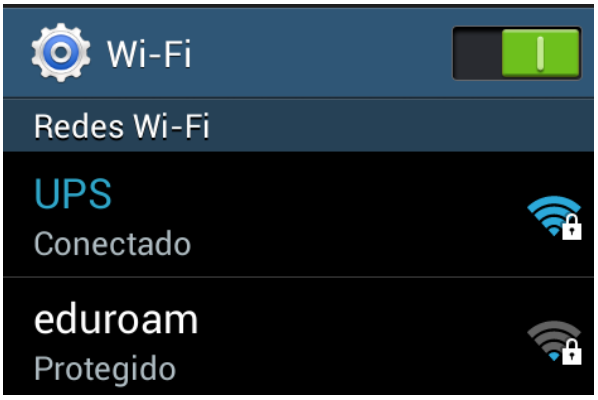

Figura 69. Red Eduroam propagada inalámbricamente.
Elaborado por: Rodrigo Borja y José Jarrín.

Primero se configura el método EAP que da como opción en el dispositivo Android y se escoge como método TTLS, después se prosigue a cambiar el método de autenticación el cual será PAP, no se escoge ningún tipo de certificado.

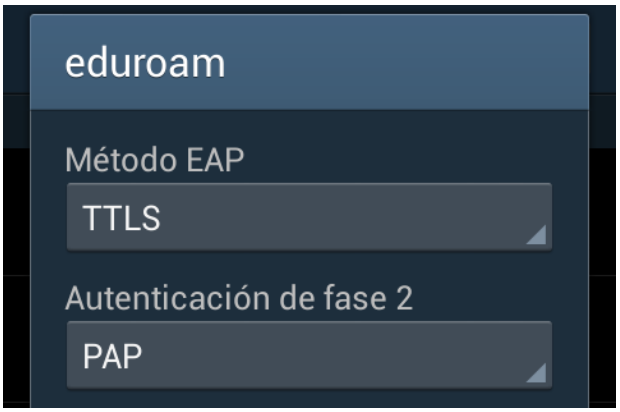

Figura 70. Configuración del método EAP y autenticación.
Elaborado por: Rodrigo Borja y José Jarrín.

La identidad es el nombre del usuario creado en la base de datos para esta prueba el cual ya se mencionó anteriormente al igual que su contraseña, para finalizar se selecciona "Establecer conexión".

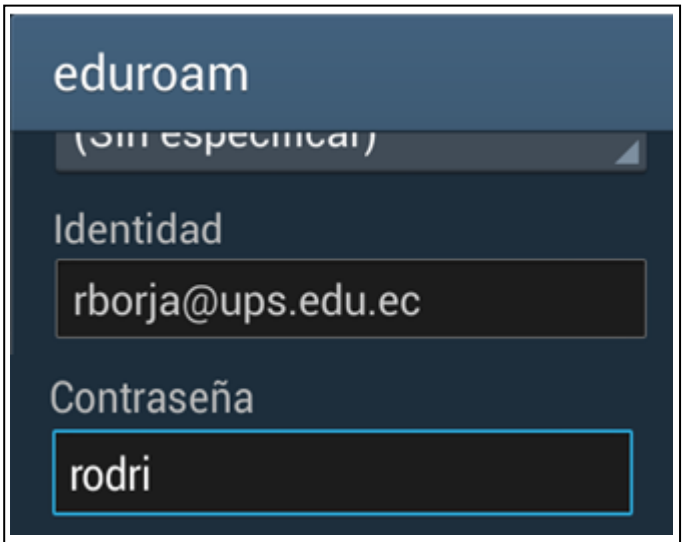

Figura 71. Ingreso del usuario y contraseña.
Elaborado por: Rodrigo Borja y José Jarrín.

Se observa que el dispositivo solicita una dirección IP que es otorgado por el servidor DHCP de la institución, lo que significa que la autenticación ya se ha realizado y está dando los últimos pasos para establecer una conexión.

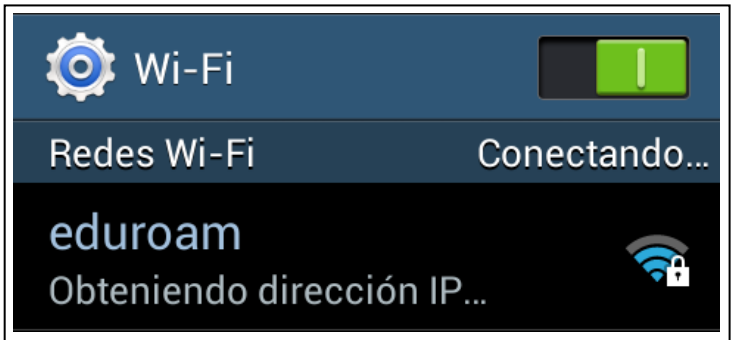

Figura 72. Obtención de dirección IP.
Elaborado por: Rodrigo Borja y José Jarrín.

Como parte final se observa que se estableció conexión entre el dispositivo móvil y la red inalámbrica Eduroam, dando como conclusión que el servidor RADIUS está autentificando de una manera correcta y su integración a la red está funcionando.

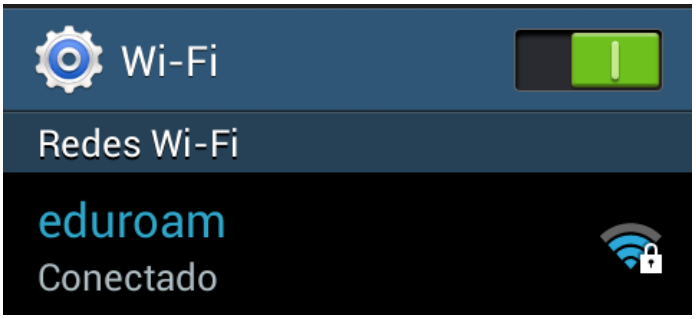

Figura 73. Conexión del dispositivo a la red Eduroam.
Elaborado por: Rodrigo Borja y José Jarrín.

Para comprobar la conexión entre el usuario y el servidor se realiza un ping a la ip del cliente para esta prueba se identifica la dirección del cliente.

Figura 74. Verificación de conexión a la red Eduroam.
Elaborado por: Rodrigo Borja y José Jarrín.

Con esta prueba se verifica que la autenticación y la conexión se realizaron correctamente como muestra la siguiente figura.

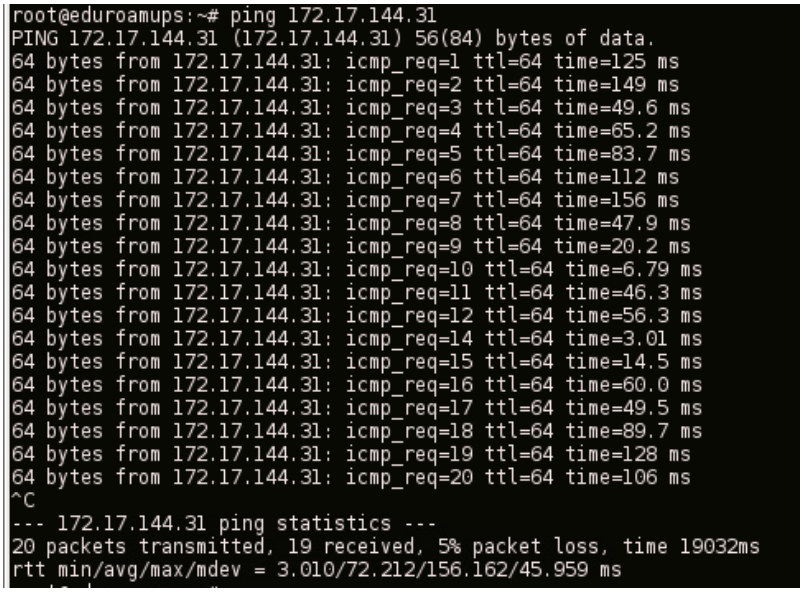

Figura 75. Verificación de conectividad del dispositivo.
Elaborado por: Rodrigo Borja y José Jarrín.

Como prueba final se verifica la navegación del dispositivo del usuario en Google, para comprobar que si existe navegación.

Figura 76. Navegación dentro de la red Eduroam.
Elaborado por: Rodrigo Borja y José Jarrín.

En este capítulo se mostró las pruebas de conectividad con la red Eduroam y también con el usuario final, verificando el proceso de autentificación para ingresar a la red.

CONCLUSIONES

La situación actual de la red en la Universidad Politécnica Salesiana, Sede Quito-Campus Sur tanto en la parte lógica como física, ha permitido la implementación e integración de la red WLAN al proyecto internacional Eduroam de una manera viable y satisfactoria, debido a que la infraestructura de la red WLAN cuenta con los dispositivos necesarios para la integración cumpliendo de esta manera la UPS con los requerimientos establecidos por CEDIA para la integración al proyecto Eduroam.

La validación de la integración de la red WLAN, Sede Quito-Campus Sur al proyecto internacional Eduroam se lo realizó desde dos lugares, se validó el acceso a la red inalámbrica desde el Campus Sur con el usuario creado en nuestra base de datos local con el realm @ups.edu.ec y con un usuario prometeo con el realm @ucuenca.ec y también desde la Universidad de Cuenca con el usuario @ups.edu.ec, obteniendo como resultados satisfactorios por parte de los usuarios al establecerse la conexión.

El uso de software libre para los servidores permite a los administradores obtener confiabilidad y estabilidad del sistema operativo que se vaya usar, así para la implementación del servidor se usó Debian GNU/Linux en su versión Squeeze o 6.0.9 debido a su versatilidad y seguridad, su configuración se la realiza por línea de comandos y también admite herramientas que ayudaron a la ejecución del proyecto como Apache Directory Studio que se usó para realizar la base de datos.

El servidor RADIUS trabaja de acuerdo a los parámetros establecidos por Eduroam para su configuración y la realización de la autenticación de los usuarios con sus respectivas contraseñas creadas en la base de datos de la institución como también a los que se encuentran en otros establecimientos que pertenecen a Eduroam.

El estándar 802.1x implementado en el servidor permite varios métodos de autenticación, cada uno con diferente nivel de seguridad para el caso del servidor institucional de la UPS se usa el método TTLS y autenticación PAP debido a que Eduroam precisa a utilizar de estos métodos para mantener de una forma general la seguridad en toda su red de servidores.

El uso de certificados SSL para Eduroam proporcionan más seguridad al servicio, ya que se consigue con ellos evitar el robo de la información notificando al usuario que la página web a la que se va a ingresar es confiable, también se incluye como ventajas en la confirmación de las identidades del usuario y además la encriptación de la información.

RECOMENDACIONES

En el proceso de la obtención de los certificados por parte de CEDIA los dos archivos se los puede editar mediante el comando **gedit** copiando toda la información de los archivos originales a los archivos que están por defecto en la carpeta **/certs** que se encuentran en el servidor.

Cuando están ingresados los dos certificados al servidor, hay que ingresar al modo debug para visualizar si el servidor aceptó estos dos certificados como parte de su configuración.

Para la edición de tarjetas siempre hay que apagar el interfaz que se va a editar ya que no se guarda la configuración sin el interfaz apagado, después de ello guardar los cambios y realizar un restart a las interfaces.

En la edición del fichero **/eap.conf** si se registra algún error del tipo random que se visualiza en el modo debug, es debido a que no se tiene ningún dato en el fichero /**random** el cual permite sesiones SSL para ello ingresar al fichero **/etc/freeradius/certs/random** e ingresar el siguiente código:

- dd if=/dev/urandom of=./random count=10

Con esto se soluciona el problema de las sesiones SSL y la inicialización del servidor junto con los dos certificados.

Ingresar correctamente las contraseñas que se ingresan en el fichero **/poxy.conf**, y también enviar a CEDIA estas mismas debido a que si se ingresa de una forma incorrecta en el fichero no podrá existir comunicación ni tampoco peticiones a los servidores federados.

Es recomendable que las instituciones, organizaciones, aeropuertos, etc., que se encuentren integradas al proyecto internacional Eduroam, cubran buena parte de sus instalaciones con equipos que permitan tener una muy buena y estable cobertura de señal inalámbrica para el acceso a la red de los usuarios pertenecientes a las instituciones, etc., o sean visitantes.

LISTA DE REFERENCIAS

Chávez, C. N. (2009). *Evaluación de la tecnología IEEE 802.11n con la plataforma OPNET.* Universidad Politécnica de Catalunya, Catalunya. Recuperado de 15 de mayo de 2014 http://upcommons.upc.edu/pfc/bitstream/2099.1/7834/1/memoria.pdf

DSSS. (31 de octubre de 2012). Recuperado de Espectro ensanchado por secuencia directa:

http://investigaciondsss.blogspot.com/

Evolución del estándar 802.11. (s.f.). Recuperado de 15 de mayo de 2014 http://guimi.net/monograficos/G-Redes_de_comunicaciones/G-RCnode33.html

Filip , A., & Vázquez, E. (2010). *Seguridad en redes WiFi, Eduroam.* Escuela Técnica Superior de Ingenieros. Recuperado de 02 de junio de 2014 http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20redes%20Wifi%20Eduroam.pdf

GEANT2. (2008). *Inter-NREN Roaming Infrastructure and Service Support Cookbook* .

GLOSARIO

WLAN: La Wireless Local Area Network, usa ondas de radio para transmitir datos y a su vez conectar dispositivos móviles tanto a Internet como a la red y aplicaciones de su empresa.

LAN: La Local Area Network, es la interconexión de varios equipos.

WPA: El Wireless Application Protocol es una especificación para un conjunto de protocolos de comunicación para estandarizar la forma en que los dispositivos inalámbricos, tales como teléfonos celulares y los transceptores de radio, se pueden utilizar para el acceso a Internet.

EAP: El Extensible Authentication Protocol es un protocolo para redes inalámbricas que se expande sobre los métodos de autenticación que utiliza el protocolo punto a punto (PPP), un protocolo de uso frecuente al conectar un ordenador a Internet.

CEDIA: Corporación Ecuatoriana De Internet Avanzado.

EDUROAM: Educational Roaming.

RedCLARA: La Corporación Latinoamericana de Redes Avanzadas, es el organismo encargado de regular Eduroam en América.

CEDIA: La Corporación Ecuatoriana De Internet Avanzado, es el organismo encargado de regular Eduroam en Ecuador.

ORPS: El Organization Radius Proxy Server, es el servidor institucional que se implementa en la universidad que se integrará al servidor federado, CEDIA en este caso.

NRPS: El National Radius Proxy Server, es el servidor nacional (federado) al cual el ORPS se encuentra enlazado, este se encarga de aceptar y reenviar peticiones que provengan de los servidores ORPS.

TRPS: El Top Level Radius Proxy Server, es el servidor internacional (confederado), se encarga de aceptar las solicitudes de cualquier servidor NRPS.

WLC: Wireless Lan Controller.

BSA: Basic Service Area.

BSS: Es el Basic Service Set en español conjunto de servicios básicos, es la jerga de estándares IEEE para una red inalámbrica que contiene sólo un único punto de acceso inalámbrico.

ESS: Es el Exchange Service Set en español conjunto de servicios de servicios extendido, es la jerga de estándares IEEE para una red inalámbrica que contiene dos puntos de acceso, pero ambos tienen el mismo SSID.

IBSS: El Independient Basic Service Set está simplemente formado por una o más estaciones que se comunican directamente entre sí.