UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES.

Ingeniería en Sistemas

Tema:

IMPLEMENTACIÓN DEL SISTEMA FEDERADO EDUROAM EN LA UNIVERSIDAD NACIONAL DE LOJA Y CONFIGURACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA COMO INICIATIVA PARA EL DESPLIEGUE EN LAS UNIVERSIDADES DEL ECUADOR

Tesis previa a la obtención del Título de Ingeniero en Sistemas

Autores: Jennifer Jomaira Loayza Castro

José Fernando Castillo Alba

Director: Ing. Luis Antonio Chamba Eras, Mg. Sc.

Loja – Ecuador

2014

CERTIFICACIÓN DEL DIRECTOR

Ing. Luis Antonio Chamba Eras, Mg. Sc.

DIRECTOR DE PROYECTO DE FIN DE CARRERA
DOCENTE INVESTIGADOR DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA UNIVERSIDAD NACIONAL DE LOJA

CERTIFICA:

Que los Egresados **José Fernando Castillo Alba** y **Jennifer Jomaira Loayza Castro** desarrollaron cabalmente el proyecto de fin de carrera titulado **"IMPLEMENTACIÓN DEL SISTEMA FEDERADO EDUROAM EN LA UNIVERSIDAD NACIONAL DE LOJA Y CONFIGURACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA COMO INICIATIVA PARA EL DESPLIEGUE EN LAS UNIVERSIDADES DEL ECUADOR",** dicho proyecto cumple con los requisitos establecidos en las normas generales tanto en el aspecto de forma como de contenido bajo las sugerencias de mi dirección, supervisión y asesoramiento.

Loja, 24 de junio del 2014.

Ing. Luis Antonio Chamba Eras, Mg. Sc.
DIRECTOR DE TESIS

AUTORÍA

Nosotros José Fernando Castillo Alba, Jennifer Jomaira Loayza Castro declaramos ser autores del presente trabajo de tesis y eximimos expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente aceptamos y autorizamos a la Universidad Nacional de Loja, la publicación de nuestra tesis en el Repositorio Institucional-Biblioteca Virtual.

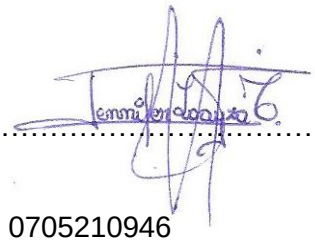
Autor: José Fernando Castillo Alba

Firma: ……

Cédula: 1104742703

Fecha: 24 de Junio del 2014

Autora: Jennifer Jomaira Loayza Castro



Firma: ……

Cédula: 0705210946

Fecha: 24 de Junio del 2014

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL LOS AUTORES, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO

Nosotros José Fernando Castillo Alba y Jennifer Jomaira Loayza Castro, declaramos ser autores de la tesis titulada: **"IMPLEMENTACIÓN DEL SISTEMA FEDERADO EDUROAM EN LA UNIVERSIDAD NACIONAL DE LOJA Y CONFIGURACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA COMO INICIATIVA PARA EL DESPLIEGUE EN LAS UNIVERSIDADES DEL ECUADOR",** como requisito para optar al grado de **Ingeniero en Sistemas**; autorizamos al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 24 días del mes de junio del dos mil catorce, firman los autores.

Autor: José Fernando Castillo Alba

Firma: ……

Cédula: 1104742703
Dirección: Cdla. Electricista Alto **Correo Electrónico:** jfcastillo@unl.edu.ec
Teléfono: 3 060-061 **Celular:** 0986161365

Autora: Jennifer Jomaira Loayza Castro

Firma: ……

Cédula: 0705210946
Dirección: Cdla. La Argelia **Correo Electrónico:** jloayza@unl.edu.ec
Teléfono: 2 913-769 **Celular:** 0989453047

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Luis Antonio Chamba Eras, Mg. Sc.
Tribunal de Grado: Ing. Hernán Leonardo Torres Carrión, Mg. Sc.
Ing. Fredy Patricio Ajila Zaquinaula, Mg. Sc.
Ing. Mario Enrique Cueva Hurtado, Mg. Sc.

AGRADECIMIENTO

Una vez terminado el proyecto de fin de carrera expresamos nuestro agradecimiento principalmente a Dios por darnos salud, vida, ganas de superación y por rodearnos de seres maravillosos como nuestros padres, familiares y amigos. Gracias a todas aquellas personas que con su ayuda, consejo, paciencia y cariño nos apoyaron para su desarrollo.

De igual forma un agradecimiento sincero a la Universidad Nacional de Loja que nos acogió para formarnos como profesionales, a la Unidad de Telecomunicaciones e Información (UTI) por darnos la apertura necesaria que permitió llevar a cabo dicho proyecto, al Ing. Luis Antonio Chamba Eras, Mg. Sc. director de tesis que con su dirección supo guiarnos para llegar al objetivo propuesto.

José Fernando Castillo Alba

Jennifer Jomaira Loayza Castro

DEDICATORIA

Dedico todo el esfuerzo de mi vida académica y este proyecto de fin de carrera a mi Dios Bendito porque en los momentos difíciles he buscado su sosiego, por la fé que tengo en él he cumplido con mis objetivos. Lo dedico de manera especial a mi mamá, Lcda. Braulia Castro, que con su amor ha dado todo de sí para darme lo mejor y construir una persona de bien, a mi bebé, Ían Leonel, que ahora se ha convertido en mi razón de ser, mi vida, mi todo, a mi padre, Sgto. Mario Loayza, que con su apoyo me ayudó a superar todos los obstáculos y alcanzar mis metas, mi hermano, Tnlgo. Eduardo Loayza, que con sus palabras me supo aconsejar en los momentos que necesité y a todos mis familiares que siempre me aconsejaron, me incentivaron a ser una profesional, a mis amigos que siempre estuvieron en los buenos y malos momentos y de forma desinteresada me ayudaron y me escucharon cuando lo necesité.

Jennifer Jomaira Loayza Castro

Con toda la humildad de mi corazón, dedico principalmente mi trabajo a Dios, por haberme dado la vida y la fuerza necesaria para superar obstáculos que se han ido presentando en el transcurso del camino y así poder llegar hasta este momento tan importante de mi formación profesional, ya que sin él nada es posible.

A mi madre, Magdalena Alba quien con su esfuerzo y apoyo incondicional he logrado culminar mi carrera con éxito, las palabras quedan cortas para agradecer una vida entera, este logro es enteramente tuyo.

A mis hermanas Erika y Maite les agradezco mucho por su presencia en mi vida y el amor brindado en todo momento. Un agradecimiento especial a mi abuelita quien me ha inculcado sus valores y ha sabido guiarme por el camino del bien, mil gracias por toda tu dedicación.

Así mismo a amigos y demás familiares, gracias por el apoyo manifestado, por esa gran calidad humana que me han demostrado.

José Fernando Castillo Alba

CESIÓN DE DERECHOS

José Fernando Castillo Alba y **Jennifer Jomaira Loayza Castro,** declaramos ser autores intelectuales del presente proyecto de fin de carrera y autorizamos a la Universidad Nacional de Loja, al Área de Energía, las Industrias y los Recursos Naturales No Renovables y por ende a la Carrera de Ingeniería en Sistemas a hacer uso del mismo en lo que estime sea conveniente.

Para constancia firmamos a continuación.

……..
José Fernando Castillo Alba
CI: 1104742703

……..
Jennifer Jomaira Loayza Castro
CI: 0705210946

A. TÍTULO

"IMPLEMENTACIÓN DEL SISTEMA FEDERADO EDUROAM EN LA UNIVERSIDAD NACIONAL DE LOJA Y CONFIGURACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA COMO INICIATIVA PARA EL DESPLIEGUE EN LAS UNIVERSIDADES DEL ECUADOR"

B.RESUMEN

Actualmente, la movilidad en la conexión a internet es un servicio que ofrece varias ventajas en las universidades principalmente al realizar eventos académicos con gran afluencia de visitantes cuya petición frecuente es el acceso a internet por medio de la red inalámbrica, generando como consecuencia la divulgación innecesaria de claves secretas.

Para resolver dicha inconsistencia, en el presente proyecto de fin de carrera (PFC) se detalla la integración de la Universidad Nacional de Loja (UNL) dentro de la arquitectura Eduroam mediante la implementación de servidores RADIUS, para formar parte del espacio único de movilidad entre organizaciones participantes, cuyo propósito radica en proveer acceso a los recursos y servicios inalámbricos de la institución visitada y así crear un entorno virtual de trabajo con acceso al servicio de internet sin límite de tiempo.

La implementación de los servidores RADIUS se la realizó en el S.O GNU/Linux en la distribución Debian versión Squeeze 6.0, principalmente por su estabilidad para un servidor con alto rendimiento y en constante producción, además que es utilizado como estándar en las implementaciones del proyecto. Para el protocolo de autenticación y autorización RADIUS se utilizó el software de distribución libre freeRADIUS, que es administrado mediante la aplicación web daloRADIUS, el cual permite visualizar de forma amigable la actividad de los usuarios, además con la utilización de certificados digitales, llaves públicas y privadas proveerán del servicio de movilidad. Se tiene configurado parámetros de redireccionamiento para las peticiones de acceso de usuarios itinerantes hacia el servidor FEDERADO EDUROAM para Ecuador que se encuentra implementado en el Consorcio Ecuatoriano de Internet Avanzado (CEDIA) en la ciudad de Cuenca.

Para la autenticación/validación de los usuarios de la UNL se implementó un servidor LDAP en la distribución libre OpenLDAP, gestionado por la aplicación web phpLDAPadmin, considerado un directorio de almacenamiento y consulta optimizada de usuarios. Finalmente para evaluar la infraestructura implementada, se procedió a realizar las pruebas pertinentes del servicio EDUROAM en el Área de Energía, las Industrias y los Recursos Naturales no Renovables, así como también se dispuso de las credenciales de usuarios de prueba de otras instituciones evidenciando movilidad.

SUMMARY

Nowadays, the mobility in the connection to the Internet is a service that offers several benefits in the universities primarily to perform events academic which large numbers of visitors whose frequent request is the access to Internet through the wireless network generating as consequence in the unnecessary divulgation of secret keys.

To resolve this inconsistency, in this final career project (PFC) detailed the integration of the Universidad Nacional de Loja within Eduroam architecture by implementing RADIUS servers, to be part of the single space of mobility between participating organizations, the aim being to provide access to resources and the visited wireless service institution and create a virtual work environment with access to the internet service without time limit.

The implementation of the RADIUS servers are performed in the OS GNU / Linux in the distribution Debian Squeeze version 6.0, mainly for its stability for a server with high performance and constant production, also being used as a standard in project implementations. For the protocol RADIUS authentication and authorization was used the free distribution software freeRADIUS which is administered by daloRADIUS web application, which allows to display od form friendly the user activity, also with the use of digital certificates, public and private keys provide service mobility. It has set parameters redirection requests for roaming users access to the server to EDUROAM FEDERAL Ecuador that is deployed in the Consorcio Ecuatoriano de Internet Avanzado (CEDIA) in the Cuenca City.

For authentication / validation of users de la Universidad Nacional de Loja is implemented an LDAP server in the free distribution OpenLDAP, managed by the web application phpLDAPadmin, considered directory storage and optimized users query. Finally, to evaluate all the infrastructure applied in the project, we proceeded to carry out the relevant tests EDUROAM service in the area of Energy, Industries and Non-Renewable Natural Resources, as well as set out the credentials of test users of other institutions evidencing mobility.

ÍNDICE DE CONTENIDOS

Índice de Figuras

Índice de Tablas

C. INTRODUCCIÓN

La rapidez que tiene el movimiento actual de la sociedad exige el máximo de su capacidad a las redes inalámbricas y la exigencia aumenta de forma progresiva debido a la introducción de dispositivos móviles en la vida cotidiana, mayor aún en el ámbito de la educación/investigación donde es de vital importancia disponer de una infraestructura que permita tener conexión durante el tiempo que se necesite y en el lugar que se necesite; sin restar calidad a la seguridad que la red inalámbrica ofrece.

Por lo tanto, en el presente proyecto de fin de carrera cuyo entorno de desarrollo son las redes informáticas, se describe la implementación en la Universidad Nacional de Loja, de un sistema federado llamado Eduroam para proveer a estudiantes, docentes e investigadores de una red inalámbrica segura en todo el campo universitario y a su vez en cualquier institución que disponga del mismo sistema.

El proyecto empieza con el análisis del estado actual de la red inalámbrica que determina las condiciones que pueden ser aprovechadas como punto de partida, dentro de la cuales se evidenció el método de autenticación que luego de un estudio se realizó el establecimiento de un método estandarizado para la autenticación en el servicio de conectividad móvil, que en conjunto al desarrollo de la configuraciones a los servidores RADIUS dio paso a la fase de pruebas de movilidad en diferentes plataformas y dispositivos móviles con usuarios tanto locales como itinerantes; para finalmente terminar con el proceso de documentación de todo el proyecto.

Durante el desarrollo de este proyecto se estudiaron protocolos de autenticación tales como RADIUS y su funcionamiento conjunto con EAP y el estándar 802.1x, se describe la instalación de certificados digitales, creación de autoridades certificadoras con su respectivas firmas digitales, uso de credenciales como mecanismo de autenticación además se especifica los pasos a seguir para poner en marcha un servidor RADIUS y complementar su proceso de autenticación con la instalación de un servidor LDAP.

Para que el usuario pueda tener acceso a la red inalámbrica tendrá que configurar su dispositivo móvil o instalar un software, dependiendo de la plataforma, que se enlazará a

los puntos de acceso inalámbricos previamente configurados, y éstos a su vez realizarán el proceso de solicitud de servicio a los servidores determinados.

A continuación de la revisión literaria se empieza con la instalación y configuración de los servidores RADIUS que mediante sus configuraciones específicas serán los servidores LOCAL y FEDERADO, además de las configuraciones del servidor que hará las veces de directorio de autenticación.

Los lineamientos establecidos por la Universidad Nacional de Loja y el Área de la Energía, las Industrias y los Recursos Naturales No Renovables rigen la estructura de éste proyecto de fin de carrera, el cual tiene el siguiente orden: RESUMEN contiene un extracto del contenido general de la investigación del proyecto de fin de carrera, ÍNDICE describe la ubicación de los temas tratados con sus respectivas figuras y tablas indicando su perteneciente número de página, INTRODUCCIÓN relata lo relevante que es el tema y su aplicabilidad en el campus universitario, METODOLOGÍA se realiza una descripción de los principales métodos y técnicas de investigación científica usados además de especificar las fases secuenciales que se desarrollaron, REVISIÓN DE LA LITERATURA que comprende la sustentación teórica de las temáticas que ayudan a la comprensión del proyecto de tesis, RESULTADOS tiene como propósito la evaluación y el cumplimiento de los objetivos planteados, DISCUSIÓN se plantea la propuesta alternativa basada en los objetivos planteados además de presentar la valoración técnica, económica y ambiental de la investigación realizada, CONCLUSIONES detalla las ideas a las que los autores llegaron, el proyecto finaliza con sus respectivas RECOMENDACIONES, BIBLIOGRAFÍA y ANEXOS.

D. REVISIÓN DE LITERATURA

CAPÍTULO I: EDUROAM

1. EDUROAM

1.1. Definición

Eduroam (contracción de education roaming) es el servicio mundial de movilidad segura desarrollado para la comunidad académica y de investigación. Eduroam persigue el lema *"abre tu portátil y estás conectado"*.

El servicio permite que estudiantes, investigadores y personal de las instituciones participantes tengan conectividad a Internet a través de su propio campus y cuando visitan otras instituciones participantes [1].

1.2. Filosofía

"El objetivo es que estos usuarios al llegar a otra organización dispusieran, de la manera más transparente posible, de un entorno de trabajo virtual con conexión a Internet, acceso a servicios y recursos de su organización origen, así como acceso a servicios y recursos de la organización que en ese momento les acoge…"

EDU referente a educación y ROAM que viene de la palabra en inglés ROAMING que significa "*capacidad de un dispositivo de moverse de una zona de cobertura a otra, sin pérdida de la conectividad*" [2].

1.3. Antecedentes de EDUROAM

La iniciativa EDUROAM surgió en 2003 dentro de la TF-Mobility de TERENA. Este departamento creó un banco de pruebas para mostrar la viabilidad de combinar una infraestructura basada en RADIUS con la tecnología del estándar 802.1x para proporcionar movilidad entre las redes educativas y de investigación.

Las pruebas iniciales se llevaron a cabo entre cinco instituciones situadas en Los Países Bajos, Finlandia, Portugal, Croacia y Reino Unido. Más tarde, otras instituciones y organizaciones educativas y de investigación empezaron a unirse a esta infraestructura. Fue en este momento cuando se le dio el nombre de EDUROAM.

Actualmente EDUROAM es una federación de federaciones (confederación); federaciones individuales se dirigen a nivel nacional y todas ellas están conectadas a una confederación regional [3].

1.4. Servicio de Movilidad

En este servicio se distingue la responsabilidad del usuario para respetar las políticas de uso, tanto de la institución visitada como de la de origen. Algunas de las políticas para este servicio son [2]:

- El servicio de movilidad será prestado solamente al personal y a las organizaciones dedicadas a proyectos de investigación que pertenezcan al espacio de movilidad internacional.
- Los usuarios móviles deberán autenticarse en su organización de origen con el fin de tener acceso a la organización visitada.
- Los usuarios móviles son responsables de sus claves y deben respetar las políticas de uso de la organización de origen.
- Las organizaciones visitadas deberán ofrecer servicios de acceso, los usuarios podrán aceptarlas y hacer uso de ellas.
- La organización visitada debe garantizar la transferencia segura de las claves de los usuarios móviles.
- La organización visitada tiene la autoridad de impedir el acceso a cualquier usuario móvil, institución o red de investigación que no cumpla con las políticas de uso de la organización visitada.
- Las organizaciones visitadas establecerán el permiso para el acceso de servicios prestados a los usuarios móviles.
- La organización de origen será la encargada de brindar soporte a sus usuarios, incluyendo información en tecnologías de acceso y políticas de uso.

1.5. Funcionamiento

Fundamentalmente EDUROAM se basa en los protocolos estándar de autenticación inalámbrica como 802.11, 802.1x, y RADIUS.

Cuando un usuario se asocia con el SSID EDUROAM (802.1x protegidas o cualquier SSID o cable de conexión para el caso) el equipo cliente no es capaz de pasar todo el tráfico que no sea 802.1x hasta que concede el acceso por el punto o interruptor del cable de acceso.

El software del cliente en el equipo se llama el *suplicante* (aunque es posible que se refieran a la computadora del cliente así mismo como el suplicante también); El hardware de red a la que el equipo esté asociado o conectado físicamente se llama el *autenticador*, y el autenticador dirige la comunicación con la infraestructura de autenticación, conocido como el " servidor de autenticación". El servidor de autenticación puede ser en realidad múltiples servidores y / o componentes de autenticación tales como LDAP, (o Samba actuando como un controlador de dominio principal y la interacción con LDAP detrás de las escenas) [2]. En la Fig. 1 se puede visualizar el proceso de autenticación básica con 802.1x.

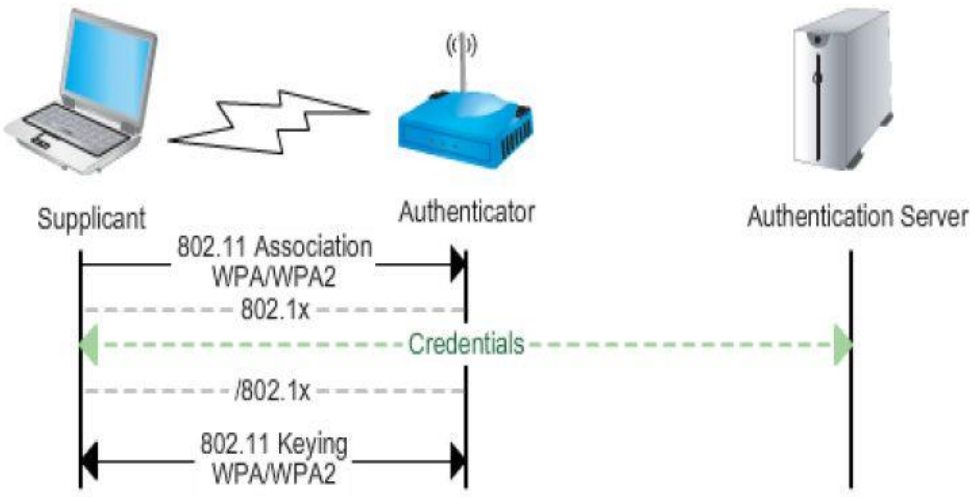


Figura 1. Autenticación básica con 802.1x

1.6. Beneficios

La disponibilidad del servicio de movilidad Eduroam, ofrece muchos beneficios tanto para los usuarios como a las instituciones, a continuación se enumeran los principales [4]:

1.6.1. Beneficios para los Usuarios

- **Movilidad Global.** Conexión a internet inalámbrica en todos los puntos de acceso disponibles en más de 10.000 instituciones a nivel mundial.
- **Cuenta única de acceso.** Acceso con la cuenta institucional.
- **Fácil.** Se configura una sola vez y luego será tan simple como "enciende tu dispositivo y estás conectado".
- **Multiplataforma.** Conéctese desde cualquier dispositivo (laptop, smartphone u otro dispositivo móvil).

1.6.2. Beneficios para las Instituciones

- **Autenticación segura y estable** para usuarios visitantes e institucionales.
- **Adaptable** a las normas de uso aceptable de la institución.
- **Servicio recíproco.** Los usuarios de su institución tendrán acceso a internet en todas las instituciones adheridas al servicio a nivel global. Del mismo modo, los usuarios de dichas instituciones tendrán acceso a internet en su institución.
- **Facilidad de administración de usuarios.** No es necesario tener cuentas especiales para los usuarios visitantes, ya que ellos utilizan su propia cuenta institucional.

1.7. Implementación

Para implementar esta red es necesario contar con una serie de servidores RADIUS, que dependiendo del lugar que ocupen en la jerarquía contarán con las siguientes características y funciones [3]:

1.7.1. Servidores Proxy RADIUS de las organizaciones

Deben:

- Resolver las peticiones de su propio dominio.
- Reenviar las peticiones de otros dominios al servidor RADIUS nacional.

- Todos los atributos RADIUS se deben reenviar de forma transparente para asegurar la trasparencia EAP.
- Aceptar peticiones que vengan del servidor RADIUS nacional. Por lo tanto, los servidores RADIUS deben intercambiarse sus direcciones IP y se tiene que determinar un RADIUS Secret que se usará entre cada servidor RADIUS de cada organización y el servidor
- RADIUS nacional de mayor nivel. El puerto será el 1812.
- Reenviar mensajes de contabilidad de forma transparente al puerto 1813.
- Prevenir bucles no reenviando peticiones al servidor del que proceden.
- Ser implementados en parejas: un primario y un secundario. El secundario se utilizará cuando el primero se caiga. Después de un tiempo se debe intentar alcanzar el primario otra vez. El tiempo de espera y los reintentos deben ser ajustados para que sean óptimos.
- Registrar, al menos, la hora, la fecha, el nombre de usuario, el dominio y la aceptación o denegación de cada petición.
- (Opcional) La comunicación con un servidor RADIUS nacional puede ser encriptada con SSL o IPSEC para conseguir seguridad adicional.
- Pueden eliminarse atributos opcionales de mensajes entrantes que sólo tengan relevancia en el contexto del dominio local del visitante.
- Se necesita contabilizar las pruebas que se realizan sobre los dominios del ORPS.

Es posible conectar directamente ciertos servidores RADIUS de organizaciones cuando están estrechamente relacionados y van a intercambiar muchas peticiones como puede ser el caso de dos organizaciones que se encuentren en el mismo campus y muchos de los empleados de una organización visiten las instalaciones de la otra.

1.7.2. Servidores Proxy RADIUS Nacionales

Deben:

- Reenviar peticiones basadas en un dominio de segundo nivel.
- Todos los atributos RADIUS se deben reenviar de forma transparente para asegurar la trasparencia EAP.
- Aceptar peticiones que provengan de servidores RADIUS de confianza de mayor nivel y servidores RADIUS de las organizaciones. Por lo tanto, los servidores

RADIUS deben intercambiarse sus direcciones IP y se tiene que determinar un RADIUS Secret que se usará entre cada servidor RADIUS Nacional y el servidor RADIUS Europeo de mayor nivel. El puerto será el 1812.

- Reenviar mensajes de contabilidad de forma transparente al puerto 1813.
- Prevenir bucles no reenviando peticiones al servidor del que proceden.
- Ser implementados en parejas: un primario y un secundario. El secundario se utilizará cuando el primero se caiga. Después de un tiempo se debe intentar alcanzar el primario otra vez. El tiempo de espera y los reintentos deben ser ajustados para que sean óptimos.
- Registrar, al menos, la hora, la fecha, el nombre de usuario, el dominio y la aceptación o denegación de cada petición.
- (Opcional) La comunicación con un servidor RADIUS nacional puede ser encriptada con SSL o IPSEC para conseguir seguridad adicional.
- Se necesita contabilizar las pruebas que se realiza sobre los dominios del NRPS. Se puede tomar la decisión de permitir que el Servidor Proxy RADIUS Nacional se encargue también de subdominios. También es posible añadir cualquier número de subniveles, con su servidor proxy RADIUS correspondiente, por ejemplo a nivel regional.

1.7.3. El Servidor Proxy RADIUS de mayor Nivel

Debe:

- Reenviar peticiones basadas en el dominio de mayor nivel.
- Todos los atributos RADIUS se deben reenviar de forma transparente para asegurar la trasparencia EAP.
- Aceptar peticiones que provengan de los Servidores Proxy RADIUS Nacionales. Por lo tanto, los servidores RADIUS deben intercambiarse sus direcciones IP y se tiene que determinar un RADIUS Secret que se usará entre cada Servidor Proxy RADIUS Nacional y el servidor RADIUS Europeo de mayor nivel. El puerto será el 1812.
- Reenviar mensajes de contabilidad de forma transparente al puerto 1813.
- Prevenir bucles no reenviando peticiones al servidor del que proceden.
- Ser implementados en parejas: un primario y un secundario. El secundario se utilizará cuando el primero se caiga. Después de un tiempo se debe intentar

alcanzar el primario otra vez. El tiempo de espera y los reintentos deben ser ajustados para que sean óptimos.

- Registrar, al menos, la hora, la fecha, el nombre de usuario, el dominio y la aceptación o denegación de cada petición.
- (Opcional) La comunicación entre un servidor RADIUS nacional y el Servidor Proxy RADIUS Europeo de mayor nivel puede ser encriptada con SSL o IPSEC para conseguir seguridad adicional.

  Como se ha podido observar esta red proporciona la suficiente seguridad, una solución sencilla de implementar y sobre todo la una forma de desplegar fácilmente una red que permita el roaming entre instituciones tanto nacionales como internacionales [2].

En la Fig. 2 se visualiza los servidores RADIUS en orden jerárquico para que tenga lugar el roaming internacional, y en la Fig. 3 se presenta la jerarquía real de los servidores RADIUS con las instituciones encargadas del despliegue a nivel regional y con las instituciones que hacen uso del servicio de movilidad.

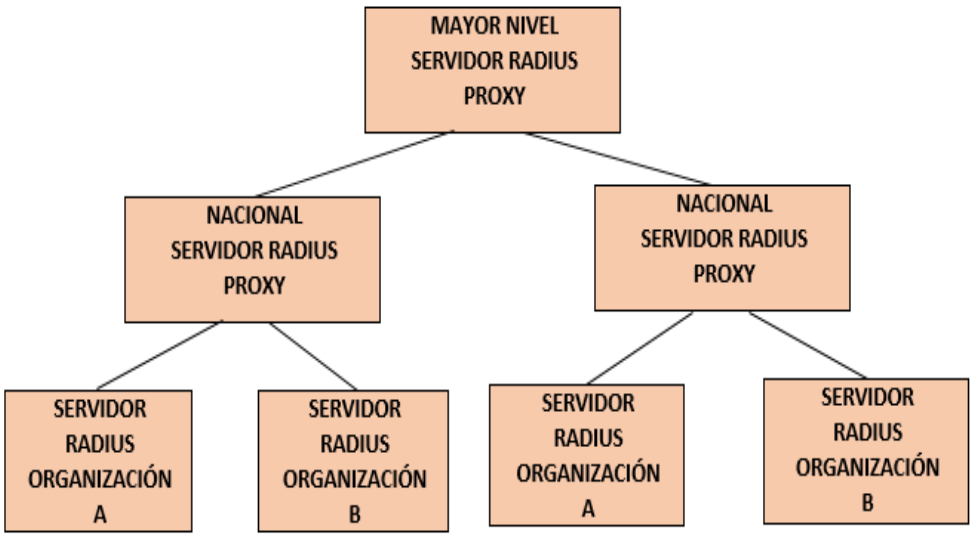


Figura 2. Jerarquía de Servidores Eduroam

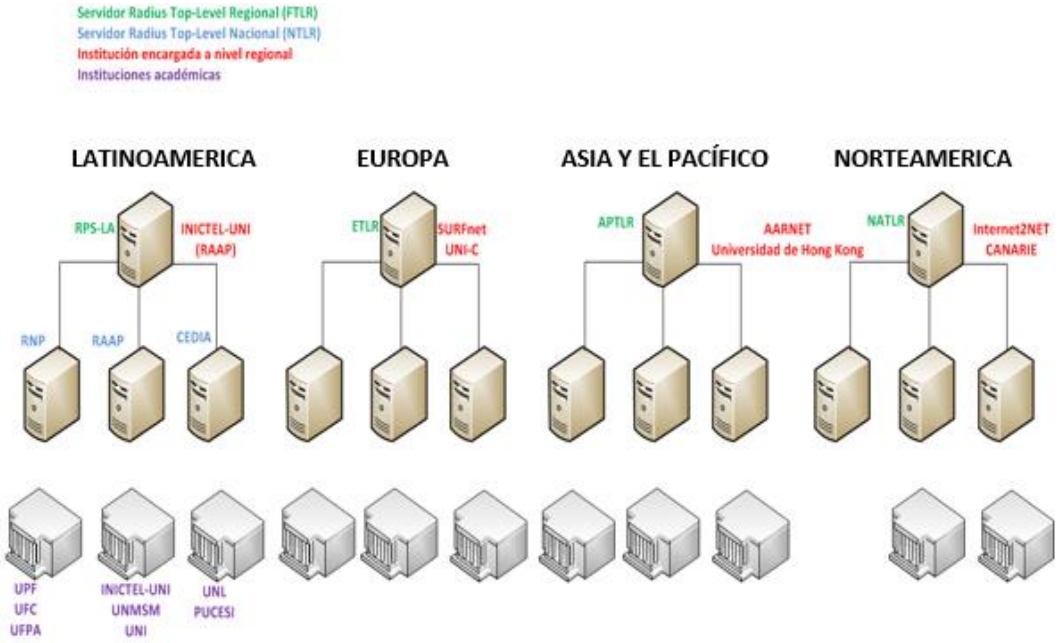


Figura 3. Servidores en orden Jerárquico

En la Fig. 4 se puede visualizar como está desplegado Eduroam a nivel de Latinoamérica, donde el operador encargado del servicio y por ende del Servidor Federado es Red Académica Peruana (RAAP).

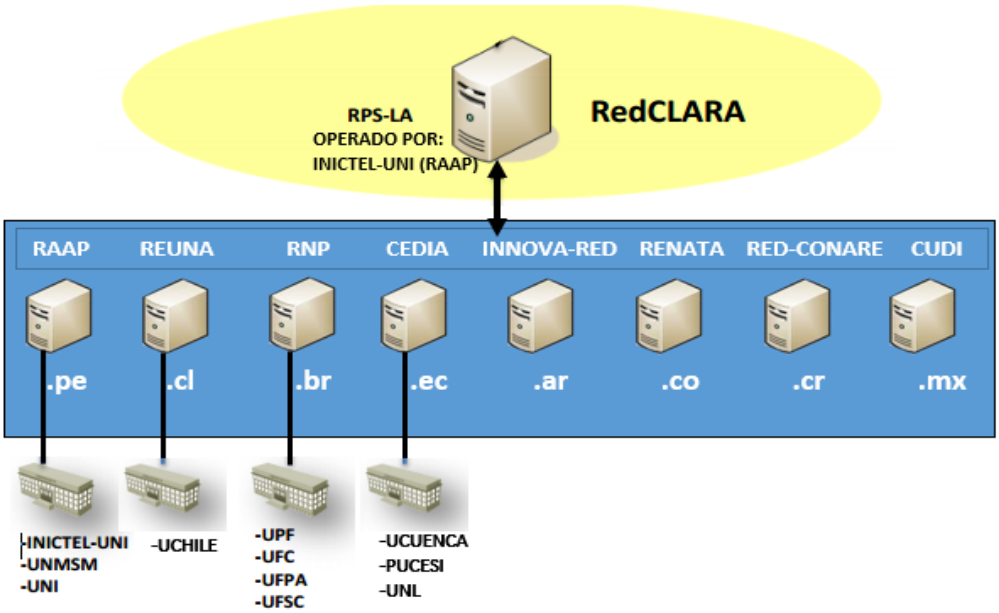


Figura 4. Despliegue a Nivel de Latinoamérica

CAPÍTULO II: SEGURIDAD EN REDES INALÁMBRICAS

2. Seguridad en Redes Inalámbricas

2.1. Seguridad

Definir el concepto de seguridad no es algo fácil, pero podemos empezar a partir de la frase citada por el Dr. Eugene Spafford: “El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto y cuidado por guardias muy bien armados... y aun así tengo mis dudas”

Se puede decir que la seguridad consiste en que un sistema se comporte como el usuario espera que lo haga, y a su vez mantenerlo libre de amenazas y riesgos. Por más de dos décadas se ha manejado que la seguridad se logra a partir de tres conceptos, conocidos como la triada de la seguridad: confidencialidad, integridad y disponibilidad (Fig.5) [5].

Figura 5. Triada de la Seguridad

2.2. Confidencialidad

Consiste en mantener la información secreta a todos, excepto a aquellos que tienen autorización para verla. Cuando la información de naturaleza confidencial ha sido accedida, usada, copiada o revelada por una persona que no estaba autorizada, entonces se presenta una ruptura de confidencialidad. La confidencialidad es un requisito para mantener la privacidad de las personas [5].

2.3. Integridad

Significa que se debe asegurar que la información no ha sido alterada por medios no autorizados o desconocidos. Un atacante no debe ser capaz de sustituir información legítima por falsa [5].

2.4. Disponibilidad

Significa que todos aquellos elementos que sirven para el procesamiento de la información, así como los que sirven para facilitar la seguridad, estén activos y sean alcanzables siempre que se requiera. Dicha característica puede perderse a través de ataques de DoS (Denial of Service -Denegación de Servicio-) [5].

2.5. Autenticación con IEEE 802.1X

El 802.1X es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.

Este protocolo permite la autenticación de equipos y/o usuarios antes de que éstos puedan conectarse a una red cableada o inalámbrica. La autenticación se realiza con el Protocolo de Autenticación Extensible (EAP, *Extensible Authentication Protocol*) y con un servidor de tipo RADIUS (*Remote Authentication Dial In User Services*) [7].

El protocolo 802.1X involucra tres elementos [7]:

- El suplicante o equipo del cliente, que desea conectarse con la red. Es una aplicación cliente que suministra las credenciales del usuario.
- El servidor de autorización/autenticación (RADIUS), que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red.
- El autenticador, que es el equipo de red (Punto de Acceso, *switch*, *router*, etc.) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación; solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

La autenticación 802.1X es un proceso de múltiples pasos que involucra al cliente o suplicante, un Punto de Acceso o autenticador, un servidor RADIUS o de autenticación y generalmente una base de datos (Fig. 6) [6].

Figura 6. Estándar 802.1x

2.5.1. Ventajas

Entre las ventajas que ofrece el estándar 802.1x se menciona las siguientes [7]:

- **Nivel de Seguridad alto:** Se trata de un esquema de autenticación de seguridad elevado porque puede emplear certificados de cliente o nombres de usuarios y contraseñas.
- **Autenticación de usuarios y de equipos:** Permite la autenticación por separado de usuario y de equipo. La autenticación por separado de un equipo permite administrarlo incluso cuando ningún usuario ha iniciado la sesión.
- **Transparencia:** Proporciona una autenticación y una conexión a la WLAN transparentes.
- **Cifrado más seguro:** Permite un cifrado muy seguro de los datos de la red.
- **Bajo coste:** Bajo coste del hardware de red.
- **Alto rendimiento:** Dado que el cifrado se lleva a cabo en el hardware de WLAN y no en la CPU del equipo cliente, el cifrado de WLAN no influirá en el nivel de rendimiento del equipo cliente.

2.5.2. Desventajas

Sin embargo, el estándar presenta ciertas desventajas que es preciso mencionar [7]:

- **Interoperabilidad:** Aunque 802.1x disfruta de una aceptación casi universal, el uso de distintos métodos de EAP implica que la interoperabilidad no siempre está garantizada.
- **Disponibilidad:** Por ser compleja la configuración en lo que respecta a la seguridad de WLAN, muchas de las empresas no disponen del estándar 802.1x.

2.5.3. WPA (WI-FI Protected Access)

Los mecanismos de encriptación WPA y WPA2 se desarrollaron para solucionar las debilidades detectadas en el algoritmo de encriptación WEP. El nombre de WPA (*Wi-Fi Protected Access*, Acceso Protegido *Wi-Fi*) es el nombre comercial que promueve la *Wi-Fi Alliance*, las especificaciones y consideraciones técnicas se encuentran definidas en el estándar IEEE 802.11i [6].

Para solucionar los inconvenientes de WEP la *Wi-Fi Alliance* decidió implementar dos soluciones de seguridad [6]:

- Una solución rápida y temporal para todos los dispositivos inalámbricos ya instalados hasta el momento, especificando al estándar comercial intermedio WPA.
- Una solución más definitiva y estable para aplicar a nuevos dispositivos inalámbricos, especificando al estándar comercial WPA2

2.5.3.1. WPA Versión 1 (WPA)

WPA se fundamenta en el protocolo de cifrado TKIP, este protocolo se basa en el tercer borrador de 802.11i publicado a mediados del 2003.

TKIP se encarga de cambiar la clave compartida entre el Punto de Acceso y el cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.

TKIP utiliza el algoritmo RC4 para realizar la encriptación, que es lo mismo que el WEP. Sin embargo, una gran diferencia con el WEP es que el TKIP cambia las claves temporales cada 10.000 paquetes. Esto proporciona un método de distribución dinámico, lo que mejora significativamente la seguridad de la red [6].

Las mejoras a la seguridad introducidas en WPA son [6]:

- Se incrementó el Vector de Inicialización (IV) de 24 a 48 *bits*.
- Se añadió la función MIC (*Message Integrity Check*, Chequeo de Integridad de Mensajes) para controlar y detectar manipulaciones de los paquetes de información.
- Se reforzó el mecanismo de generación de claves de sesión.

2.5.3.2. WPA Versión 2 (WPA2)

WPA2 es el nombre comercial de la *Wi-Fi Alliance* a la segunda fase del estándar IEEE 802.11i dando una solución de seguridad de forma definitiva. WPA2 utiliza el algoritmo de encriptación AES (*Advanced Encryption Standard*, Estándar de Encriptación Avanzado) el cual es un código de bloques que puede funcionar con muchas longitudes de clave y tamaños de bloques.

WPA2 se fundamenta en el protocolo de seguridad de la capa de enlace basado en AES denominado CCMP, el cual es un modo de funcionamiento combinado en el que se utiliza la misma clave en el cifrado para obtener confidencialidad, así como para crear un valor de comprobación de integridad criptográficamente segura. Para la implementación de CCMP se realizaron algunos cambios en los paquetes de información como por ejemplo en las tramas *beacon2*, tramas de asociación e integración, etc [6].

2.5.4. Modalidades de Operación

Según la complejidad de la red, un Punto de Acceso compatible con WPA o WPA2 puede operar en dos modalidades [6]:

- Modalidad de Red Empresarial, para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El Punto de Acceso emplea entonces 802.1X y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.
- Modalidad de Red Personal o PSK (*Pre-Shared Key*), tanto WPA como WPA2 operan en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el Punto de Acceso y en los dispositivos móviles. Solamente podrán acceder al Punto de Acceso los dispositivos móviles cuya contraseña coincida con la del Punto de Acceso. Una vez

lograda la asociación, TKIP entra en funcionamiento para garantizar la seguridad del acceso

2.5.5. Métodos de Autenticación EAP

EAP (Protocolo de autenticación Extensible, Extensible Authentication Protocol) nació de la necesidad de tener un mecanismo de autenticación más robusto para las conexiones PPP (Punto a Punto, Point-to-Point). El EAP está definido en RFC 3748 y al ser "Extensible" (o tener estatus de framework) se le permite que pueda ser modificado para incluir nuevos métodos de autenticación (como en su momento hizo CISCO Systems con la autenticación LEAP).

En el caso de las transmisiones inalámbricas, el EAP es utilizado por el 802.1x para realizar la comunicación entre los dispositivos que intervienen en la autenticación del cliente [5].

2.5.5.1. EAP-TLS

EAP-TLS (*Extensible Authentication Protocol with Transport Layer Security, RFC 2716*) se trata de una variante de EAP en la cual se realiza una negociación SSL con autenticación basada en certificados X.509 para autenticar tanto usuario como servidor. En el caso de TLS, las credenciales corresponden al certificado de cliente, mientras que en otros tipos de EAP la conexión segura se realiza a partir exclusivamente del certificado del servidor. El certificado del usuario se puede almacenar en algún dispositivo hardware como Smart Card o USB para aumentar aún más la seguridad de la red, aunque también hace más difícil la implementación y la gestión de ésta. Además, hay que tener en cuenta que algunos usuarios necesitan extensiones específicas para certificados digitales [3].

2.5.5.2. EAP-TTLS

En la línea de EAP-TLS se encuentran otros métodos que resuelven los problemas de éste. EAP-TTLS (*Extensible Authentication Protocol with Tunneled Transport Layer Security),* desarrollado por Funk Software, está orientado a trabajar con servidores RADIUS. Puede emplear métodos de autenticación EAP adicionales o métodos como PAP y CHAP. Está integrado con una gran variedad de formatos de almacenamiento de contraseñas y sistemas de autenticación basados en contraseñas, así como con múltiples

bases de datos de seguridad. Además, en el mercado existen un gran número de usuarios TTLS disponibles.

Hay dos etapas de autenticación:

- Primera fase: identificación del servidor por el cliente mediante un certificado (validado por una autoridad de certificación).
- Segunda fase: identificación del cliente por el servidor mediante usuario y contraseña [3].

En un sistema EAP-TTLS se autentica al usuario en el sistema con las credenciales basadas en nombre de usuario y contraseña, y se cifran las credenciales de usuario para garantizar la protección de la comunicación inalámbrica

CAPÍTULO III: RADIUS

3. RADIUS

3.1. Descripción

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza los puertos 1812 y 1813 UDP para establecer sus conexiones (para autentificar/autorizar y contabilizar, respectivamente).

Cuando se realiza la conexión con un ISP mediante un módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Network Access Server o Servidor de Acceso a la Red) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS.

RADIUS consta de tres componentes: un protocolo con un formato de trama que utiliza el protocolo de datagramas de usuario (UDP), un servidor y un cliente.

Los paquetes que se envían a través de la red manejan un formato propio del protocolo RADIUS, los mismos que contienen un campo denominado código que indica el tipo de paquete, como se muestra en la Tabla I [8]:

Tabla I. MENSAJES ENVIADOS POR EL SERVIDOR RADIUS

Valor	Nombre del Campo	Descripción
1	Access-Request	Cliente: Petición de acceso
2	Access-Accept	Servidor: Petición aceptada
3	Access-Reject	Servidor: Petición rechazada
4	Accounting-Request	Cliente: Petición de registro
5	Accounting-Response	Servidor: Respuesta de registro
11	Access-Challenge	Servidor: Desafío para autenticación
12	Status-Server	Reservado (experimental)
13	Status-Client	Reservado (experimental)
255	Reserved	Reservado

3.2. Características

Principales características [8]:

- Funciona bajo el modelo cliente-servidor.
- Ofrece nivel limitado de seguridad en la red ya que aunque las comunicaciones entre el cliente y el servidor son validadas mediante un secreto compartido que no se envía por la red, solo se encripta la clave del usuario en los paquetes de solicitudes de acceso desde el cliente al servidor, utilizando el método de encriptación MD5. El resto del paquete no está encriptado pudiendo ser objeto de captura el nombre de usuario, servicios autorizados y la contabilización de estos.
- Los servidores RADIUS soportan varios esquemas de autentificación de usuario como: EAP, PAP y CHAP y soportan varios orígenes de información como: una base de datos del sistema (/etc/passwd), o una base de datos interna (del propio servidor RADIUS), mecanismos PAM y otros como Active Directory, LDAP y Kerberos
- Capacidad para el manejo de sesiones, notificando inicio/cierre de conexión, lo que permite que al usuario se le pueda determinar su consumo y facturar en consecuencia; esta constituye una de las características fundamentales de este protocolo.

3.3. Descripción del Protocolo

RADIUS es un servicio o daemon que se ejecuta en una de las múltiples plataformas que permite (Unix, GNU/Linux, Windows, Solaris…) y que permanece de forma pasiva a la escucha de solicitudes de autenticación hasta que estas se producen. Para ello utiliza el protocolo UDP y permanece a la escucha en los puertos 1812 ó 1645 para la autenticación y 1813 ó 1646 para el arqueo. En un principio se utilizaban los puertos 1645 y 1646 para RADIUS, pero tras la publicación de la RFC 2865 se utilizan por acuerdo 1812 y 1813 debido a que el 1645 estaba siendo utilizado por otro servicio “datametrics”. Algunos servidores como Freeradius utilizan el puerto UDP 1814 para la escucha de respuestas Proxy RADIUS de otros servidores.

RADIUS está basado en un modelo cliente-servidor, ya que RADIUS escucha y espera de forma pasiva las solicitudes de sus clientes o NAS, a las que responderá de forma inmediata. En este modelo el cliente es el responsable del envío y de la correcta recepción de las solicitudes de acceso, y es el servidor

RADIUS el responsable de verificar las credenciales del usuario y de ser correctas, de enviar al NAS los parámetros de conexión necesarios para presentar el servicio.

El motivo por el cual RADIUS justifica el uso de UDP sobre TCP en su RFC (Petición De Comentarios, Request for Comments) es por el aprovechamiento de las normativas del protocolo UDP, que mantiene una copia del paquete de solicitud sobre la capa de transporte a fin de poder recuperarlo para reenviarlo, si fuera necesario, a otro servidor RADIUS si el primero no estuviera disponible. De esta manera se simplifica el diseño del protocolo, evitando tener que hacerse cargo del control de llegada de esos paquetes a su destino. Para aprovechar esta simplicidad se utiliza la característica de UDP de ser "sin cable". Las retransmisiones se pueden hacer más rápidamente hacia otros servidores, ya que el puerto no quedará colapsado por el control de la conexión, evitándose las esperas necesarias en el protocolo TCP.

Dispone de una muy extensa variedad de módulos de autenticación, encargados de completar un proceso de autenticación con todo lo que ello conlleva. En una comunicación RADIUS nunca se enviarán las contraseñas en texto claro, incluso en sus versiones más antiguas se utilizaba un sistema de cifrado, aunque este sistema primitivo se ha quedado ya obsoleto. Estos módulos de autenticación se han ido desarrollando a medida que el mercado ha ido demandado nuevos sistemas más seguros y fiables para la autenticación. La idea predominante es la de sustituir los métodos que se van quedando obsoletos por vulnerabilidades o problemas de seguridad por otros más actuales que ofrezcan más confianza y más posibilidades de servicio [5].

3.4. Protocolo AAA

3.4.1. Autenticación

Consiste en el proceso de validar la petición de un usuario, el cual quiere hacer uso de los recursos de la red inalámbrica. El proceso de autenticación se realiza mediante la presentación de identidad y credenciales por parte del usuario.

La identidad del usuario viene a ser el nombre o alias con el cual está registrado en la base de datos del servidor de autenticación, mientras que las credenciales se implementarán mediante contraseñas, aunque también podría incluirse el uso de certificados digitales [9].

Existen varios métodos de autenticación que son soportados por el servidor FreeRADIUS, algunos de los cuales se detallan a continuación [9]:

- EAP-MD5
- EAP-TLS
- EAP-PEAP MSCHAPv2
- EAP-TTLS
- Kerberos

3.4.2. Autorización

El proceso de autorización es el siguiente paso luego de la autenticación. Este proceso consiste en determinar si un usuario se encuentra autorizado para hacer uso de ciertas tareas, operaciones o recursos de la red. Usualmente el proceso de autorización se realiza en conjunto con el de autenticación, de esta manera una vez que el usuario es autenticado como válido, este podrá hacer uso de ciertos recursos de la red [9].

3.4.3. Contabilidad

La contabilidad es la última característica de un servidor AAA, y consiste en el proceso de medición y almacenamiento de consumo de recursos de red. Esto permite el monitoreo y reporte de eventos y uso de la red inalámbrica para varios propósitos, entre los cuales se encuentran: tarifación de usuarios, análisis de recursos de red, capacidad de la red.
Este proceso también hace uso de la base de datos para poder registrar el comportamiento de los usuarios en la red inalámbrica [9].

3.5. Mensajes RADIUS

Los mensajes RADIUS se envían como mensajes de datagramas de usuario UDP. El puerto UDP 1812 se utiliza para los mensajes de autenticación RADIUS y el 1813 para los mensajes de administración de cuentas RADIUS. La carga UDP de un paquete RADIUS sólo incluye un mensaje RADIUS [10].

- ***Access-Request*** **(solicitud de acceso)**
  Enviado por un cliente RADIUS para solicitar autenticación y autorización de un intento de conexión, y contiene información que el servidor RADIUS utiliza para determinar si a dicho usuario se le permite o no el acceso [10].

Los atributos que mínimo debe contener este paquete son los siguientes:

- User-Name.- El atributo User-Name debe llegar al servidor RADIUS de cliente como: usuario@dominio
- User-Password.- Contraseña del usuario.

- ***Access-Accept*** **(aceptación de acceso)**
  Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. En él se informa al cliente RADIUS de que se ha autenticado y autorizado el intento de conexión [10].

- ***Access-Reject*** **(rechazo de acceso)**
  Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. En él se informa al cliente RADIUS de que se ha rechazado el intento de conexión. Un servidor RADIUS envía este mensaje si las credenciales no son auténticas o si no se ha autorizado el intento de conexión [10].

- ***Access-Challenge*** **(desafío de acceso)**
  Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. Este mensaje es un desafío al cliente RADIUS que exige una respuesta [10].

- ***Accounting-Request*** **(solicitud de administración de cuentas)**
  Enviado por un cliente RADIUS para especificar información de administración de cuentas de una conexión que se ha aceptado [10].

- **Accounting-Response (respuesta de administración de cuentas)**

  Enviado por el servidor RADIUS como respuesta a un mensaje de Solicitud de administración de cuentas. En este mensaje se confirman la recepción y el procesamiento correctos del mensaje de Solicitud de administración de cuentas [10].

3.6. Aplicaciones e implementaciones del servidor RADIUS

3.6.1. FreeRADIUS

FreeRADIUS es un paquete de software de código abierto y libre distribución que implementa diversos elementos relacionados con RADIUS, tales como una biblioteca BSD para clientes, módulos para soporte en apache y un servidor de RADIUS.

- El servidor de FreeRADIUS es modular, para facilitar su extensión, y es muy escalable. Soporta prácticamente toda clase de clientes Radius (por ejemplo, ChilliSpot, JRadius, etc.).
- Se puede ejecutar en múltiples sistemas operativos: Linux (Debian, Ubuntu, Suse, Mandriva, FedoraCore, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin.
- Soporta el uso de proxies y la replicación de servidores [8].

3.6.2. El proyecto EDUROAM

Eduroam (EDUcation ROAMing) es un proyecto internacional creado para facilitar el acceso a Internet a los miembros de las instituciones científico-académicas asociadas, desde cualquiera de estas instituciones. Infraestructura de roaming basada en RADIUS. La conexión a Internet se hace habitualmente mediante un punto de acceso inalámbrico (cuyo identificador SSID es “eduroam”) que conecta al usuario directamente a una red IEEE 802.11 local. El proceso de autentificación se hace mediante el protocolo EAP, esta autentificación la hace siempre el centro al que pertenece el usuario (y no el centro al que se quiere conectar), y para llevar a cabo este proceso de manera segura y escalable se emplea el protocolo RADIUS [8].

3.7. DaloRADIUS

Es una plataforma de RADIUS web avanzada dirigida a la gestión de puntos de acceso y de uso general despliegues ISP. DaloRADIUS está escrito en PHP y JavaScript, y utiliza una capa de abstracción de base de datos de lo que significa que es compatible con muchos sistemas de bases de datos, entre ellos el popular MySQL, PostgreSQL, SQLite, MSSQL, y muchos otros.

Se basa en una implementación FreeRADIUS con un servidor de base de datos que sirve como el backend. Entre otras características se implementa ACLs, integración de Google Maps para localizar puntos de acceso / puntos de acceso visual y muchas más características. DaloRADIUS es esencialmente una aplicación web para administrar un servidor Radius lo que en teoría se puede gestionar cualquier servidor Radius, pero específicamente gestiona FreeRADIUS y su estructura de base de datos [11].

CAPÍTULO IV: CRIPTOGRAFÍA

4. Criptografía

4.1. Definición

La palabra Criptografía proviene del griego "kryptos" que significa oculto, y "graphia", que significa escritura, y su definición según el diccionario es "el arte de escribir con clave secreta o de un modo enigmático".

Esta definición puede ser muy interesante y llamativa, pero resulta muy poco ajustada para los tiempos actuales [12].

Una definición más técnica de Criptografía sería la siguiente [12]:

Rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Esto dará lugar a diferentes tipos de sistemas de cifra, denominados criptosistemas, que nos permiten asegurar al menos tres de los cuatro aspectos básicos de la seguridad informática: la confidencialidad o secreto del mensaje, la integridad del mensaje y autenticidad del emisor, así como el no repudio mutuo entre emisor (cliente) y receptor (servidor).

4.2. Protocolo SSL

4.2.1. Introducción

El protocolo SSL (Secure Sockets Layer, Capa de Sockets Seguro) fue desarrollado por Netscape, el principal objetivo de este protocolo es proveer de privacidad y confiabilidad a la comunicación entre aplicaciones cliente servidor. Este protocolo fue diseñado con un propósito general y es por esta razón se adapta fácilmente a varias aplicaciones como son transmisión segura, copia segura, acceso remoto en forma segura, correo seguro, comercio electrónico entre otras

El protocolo SSL se divide en cuatro protocolos: El protocolo Handshake, el protocolo Change Cipher Spec, y el protocolo Alert que están ubicados en la capa de Aplicaciones, y el ultimo protocolo Record que se encuentra sobre la capa TCP del modelo TCP/IP.

El protocolo SSL Handshake es donde se realiza la negociación, en esta fase el cliente y el servidor intentan consensuar los parámetros básicos de la sesión y de la conexión si ambos interlocutores no se pone de acuerdo en lo que se refiere al cifrado y autenticación no se podría producir ninguna transferencia de la información.

En la negociación se define la versión del protocolo usada y los algoritmos de cifrado que se van a aplicar, además cualquiera de los interlocutores pueden solicitar la autenticación del otro como parte del proceso de negociación por último la fase de negociación crea un conjunto de claves que se comparten usando técnicas de cifrado de clave pública (cifrado asimétrico).

El Protocolo SSL Change Cipher Spec se usa para señalizar cambios de estrategia de cifrado es decir se puede cambiar entre un algoritmo de cifrado y otro.

Se podría usar por ejemplo en transacciones HTTP críticas en cualquier momento cuando uno de los dos interlocutores estima que la seguridad puede estar comprometida es posible volver a negociar la utilización de una nueva especificación de seguridad.

El protocolo de Alerta que permite informar al interlocutor sobre circunstancias excepcionales: Mensajes no esperados, MAC incorrecto, Error de descompresión, Error de negociación, Certificado corruptos o caducados, etc. Usando mensajes de alerta para cada una de los casos mencionados anteriormente.

La capa de registros de SSL o protocolo record recibe datos no interpretados en bloques de tamaño arbitrario y lleva a cabo las siguientes operaciones: Fragmentación, compresión y Cifrado.

Un sitio web se puede identificar que es seguro si su URL comienza con https:// en lugar del http://. SSL proporciona servicios de cifrado de datos, autenticación de servidores, Integridad de mensajes, y opcionalmente autenticación del cliente en conexiones TCP/IP [13].

4.2.2. Funcionamiento básico del Protocolo SSL

El funcionamiento del protocolo SSL se podría dividir en dos fases, la fase de negociación y la fase de transmisión de datos.

4.2.2.1. Fase de Negociación

La fase de negociación, handshake o también conocido como apretón de manos inicia el cliente al solicitar al servidor una comunicación segura enviándole un mensaje con

parámetros como la versión del protocolo, una lista de algoritmos de cifrado y de igual forma una lista de algoritmos de compresión que el cliente soporta.

El servidor responde al cliente igualmente con un mensaje que contiene los siguientes parámetros: Un certificado otorgado por alguna Autoridad Certificadora (CA) y los algoritmos de cifrado y compresión seleccionados de la lista enviada por el cliente y adicionalmente envía la clave pública del servidor.

El cliente verifica el certificado enviado por el servidor, y si este es correcto responde con un mensaje que contiene la posible clave secreta para la transmisión de los datos, toda esta información se envía al servidor de forma cifrada con la clave pública del servidor.

Tanto el servidor como el cliente comparten la información que se ha enviado con la clave secreta acordada y están listos para transmitir los datos de manera segura mediante el uso del protocolo Record.

El algoritmo que se usa en la fase de negociación es asimétrico y se usa las claves públicas para cifrar la información y las claves privadas para descifrar en cada uno de los extremos.

Si la comunicación se suspende no es necesario realizar otra vez todo este proceso, únicamente se comprueba los datos de la sesión y la conexión actual [13].

4.2.2.2. Fase de Transmisión de Datos

El protocolo Record es el encargado de transmitir los datos entre el cliente y el servidor usando los parámetros acordados en la fase de negociación.

Para la transmisión de datos en este protocolo se usan algoritmos de encriptación simétricos con claves que van modificándose para cada siguiente paquete transmitido [13].

4.2.3. Fundamentos del Protocolo SSL

El Protocolo SSL para cumplir con su objetivo principal que es el de brindar una comunicación segura entre dos aplicaciones y en especial en una red tan grande e insegura como es la red del Internet se fundamenta en las siguientes tecnologías [13]:

- Criptografía de claves simétricas y asimétricas
- Códigos de autenticación de mensajes (MACs).
- Certificados digitales X.509

4.3. Cifrado Asimétrico

La criptografía asimétrica utiliza un par de claves para cifrar la información, este par de claves son únicos, la una clave es de dominio público por lo que cualquier persona puede saber pero la otra es privada y únicamente debe conocer su propietario. Los métodos criptográficos garantizan que estos pares de claves no se repitan.

Una vez que el remitente utiliza la clave pública para cifrar el mensaje solo el destinatario poseedor de la clave privada puede descifrar el mensaje y de esta forma se consigue la confidencialidad. Si el propietario de la clave privada utiliza esta para cifrar el mensaje todos los que poseen la pública pueden descifrar el mensaje y de esta forma se consigue la identificación y autenticación del remitente. En esta idea se basa la firma electrónica.

Las desventajas que estos sistemas presentan es la gran cantidad de tiempo que se necesita para cifrar un mensaje en comparación con los sistemas simétricos, además que la longitud de sus mensajes cifrados es mayor a la del mensaje original.

Algunos algoritmos que utilizan claves públicas son: RSA, DHE, SRP, PSK, DSA, Curvas Elípticas (CEE), etc [13].

4.3.1. Algoritmo de cifrado Asimétrico RSA

El algoritmo RSA realiza un cifrado en bloques y es el más popular y utilizado de los algoritmos asimétricos gracias a su facilidad para el entendimiento y la implementación, básicamente se basa en la teoría de los números primos, este algoritmo fue creado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977 [13].

RSA se basa en la dificultad para factorizar grandes números. Las claves pública y privada se calculan a partir de un número que se obtiene como producto de dos primos grandes. El atacante se enfrentará, si quiere recuperar un texto claro a partir del criptograma y la llave publica, a un problema de factorización [14].

4.3.1.1. Funcionamiento

Los cálculos matemáticos de este algoritmo emplean un numero denominado Modulo Publico, N, que forma parte de la clave pública y que se obtiene a partir de la multiplicación de dos números primos, p y q, diferentes y grandes (del orden de 512 bits) y que forman parte de la clave privada. La gran propiedad de RSA es que, mientras que N

es público, los valores de p y q se pueden mantener en secreto debido a la dificultad de la factorización de un número grande [13].

4.3.1.2. Seguridad

La seguridad del criptosistema RSA está basado en dos problemas matemáticos: el problema de factorizar números grandes y el problema RSA. El descifrado completo de un texto cifrado con RSA es computacionalmente intratable, no se ha encontrado un algoritmo eficiente todavía para ambos problemas. La longitud de la clave puede tener una longitud variable y puede ser tan grande como se desee [13].

4.4. Función de hash SHA-1

Secure Hash Algorithm, desarrollado como parte integrante del Secure Hash Standar (SHS) y el Digital Signature Standar (DSS) por la Agencia de Seguridad Nacional Norteamericana, NSA. Sus creadores afirman que la base de este sistema es similar a la de MD4 de Rivest, y ha sido mejorado debido a ataques nunca desvelados. La versión actual se considera segura (por lo menos hasta que se demuestre lo contrario) y es muy utilizado como algoritmo de firma, como en el programa PGP en sus nuevas claves DH/DSS (Diffie-Hellman/Digital Signature Standar). Existen cuatro variantes cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (llamándose SHA-2 a todos ellos) [13].

4.4.1. Utilización

La función hash SHA-1 tiene diferentes usos [15], entre los cuales se menciona:

- Uno de los algoritmos más usados para firmar documentos electrónicos, guardar contraseñas encriptadas, y en general cualquier tipo de huella digital.
- Se puede utilizar en el correo electrónico, transferencia electrónica de fondos, distribución de software, almacenamiento de datos y otras aplicaciones que requieren la garantía de integridad de datos y la autenticación del origen de datos.
- SHA-1 requerido por la ley para el uso en el Gobierno de los EE.UU, para las aplicaciones, incluyendo el uso en otros algoritmos criptográficos y protocolos para la protección de la información no confidencial sensible.
- SHA-1 es usado por las organizaciones privadas y comerciales.

4.5. Autoridad Certificadora

En criptografía una Autoridad de certificación, certificadora o certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea el cifrado de clave pública. Jurídicamente es un caso particular de Prestador de Servicios de Certificación [13].

4.5.1. Definición

La Autoridad de Certificación, por si misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad. Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están firmados electrónicamente por la Autoridad de Certificación utilizando su clave privada. La Autoridad de Certificación es un tipo particular de Prestador de Servicios de Certificación que legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública. La confianza de los usuarios en la CA es importante para el funcionamiento del servicio y justifica la filosofía de su empleo, pero no existe un procedimiento normalizado para demostrar que una CA merece dicha confianza.
Un certificado revocado es un certificado que no es válido aunque se emplee dentro de su periodo de vigencia. Un certificado revocado tiene la condición de suspendido si su vigencia puede restablecerse en determinadas condiciones [13].

4.5.2. Certificados Digitales

Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El certificado contiene usualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación [13].

4.5.3. Certificado x.509

El formato de certificados X.509 es un estándar del ITU-T (International Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (International Standards Organization / International Electrotechnical Commission) que se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios. Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996 [16]. Los elementos del formato de un certificado X.509 v3 son [16]:

- **Versión**. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- **Número de serie del certificado**. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- **Identificador del algoritmo de firmado**. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- **Nombre del emisor**. Este campo identifica la CA que ha firmado y emitido el certificado.
- **Periodo de validez**. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
- **Nombre del sujeto**. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- **Información de clave pública del sujeto**. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- **Identificador único del emisor**. Este es un campo opcional que permite reutilizar nombres de emisor.

- **Identificador único del sujeto**. Este es un campo opcional que permite reutilizar nombres de sujeto.

4.6. OpenSSL

El proyecto OpenSSL es un esfuerzo conjunto para el desarrollo de una implementación robusta y segura de nivel comercial, con todas las características y de tipo Open Source de los protocolos SSL y TLS, además de bibliotecas con propósitos de cifrado. Su principal diferencia con un paquete SSL se puede apreciar en el eslogan presente en su página web:

"¿Porque comprar un paquete SSL como una caja negra, cuando puede obtener una abierta y gratis?".

OpenSSL es una implementación Open Source de los protocolos SSL y TLS y librerías de cifrado para desarrollo de algoritmos de cifrado y descifrado, certificados x.509, firmas digitales además ofrece la posibilidad de programar con C/C++ aplicaciones de seguridad y autoridades de certificación utilizando OpenCA. La aplicación OpenSSL es multiplataforma adaptándose a una gran variedad de sistemas operativos Unix, Linux, Windows, etc.

La principal herramienta de OpenSSL es la herramienta de línea de comandos openssl que nos permite administrar autoridades certificadoras, certificados digitales, claves públicas y claves privadas. La herramienta openssl nos provee de una gran cantidad de comandos y opciones para el desarrollo de las funciones mencionadas anteriormente [13].

E. MATERIALES Y MÉTODOS

Durante el proceso de desarrollo del presente PFC, se recurre a diferentes técnicas de recolección de información, métodos científicos y procedimientos que la investigación científica ofrece y que son de mucha utilidad. Entre los métodos de investigación científica principales se manejaron:

Método Inductivo:

La utilización del método permitió determinar el problema general de investigación del PFC a partir de una lista de problemas que se presentan en el campus universitario. Analizando de forma particular las conexiones inalámbricas del campus en los diferentes puntos de acceso inalámbrico.

Método Deductivo:

Mediante este método se logró conocer los beneficios y el proceso de desarrollo de los sistemas federados de manera particular sobre EDUROAM y a partir de aquello determinar los problemas que se generan por la falta de movilidad entre universidades y construir la problemática a resolver.

Método Analítico:

La utilización de este método permitió determinar el análisis actual de la red inalámbrica de la UNL, permitiendo conocer y describir los diferentes equipos de hardware y software que forman la infraestructura inalámbrica (*ver sección Resultados en el apartado Análisis de requerimientos*).

Método Bibliográfico:

Este método se utilizó para la recolección de información acerca de las temáticas que comprenden el funcionamiento del servicio de movilidad mundial EDUROAM, constituyéndose la base teórica del PFC (*ver sección Revisión de Literatura*).

Así mismo, es fundamental apoyarse en técnicas que permitirán extraer información para sustentar el PFC, entre las utilizadas se mencionan a continuación:

- **Lectura Científica,** proporcionó el conocimiento y comprensión metódica y secuencial de los temas que constituyen la sustentación del proyecto.
- **Observación Directa,** permitió palpar el problema de forma personal y que se puede percibir acerca del proceso que se lleva para conectarse a la red inalámbrica universitaria.

Metodología de desarrollo del PFC.

Puesto que no se dispone de una metodología estandarizada para la implementación de proyectos referentes a temáticas que gestionen las redes inalámbricas, se determina usar una metodología creada por los autores, dicha metodología está basada en las fases de desarrollo del PFC mencionadas a continuación:

Fase 1: Análisis de requerimientos

El análisis de requerimientos comprende el estudio de la situación existente de la red inalámbrica de la Universidad, conociendo así aspectos generales como la unidad que gestiona las Tecnologías de la Información y de forma particular puntos de la administración de la red inalámbrica. En este análisis se muestra el backbone de la Universidad y la simbología de los elementos que la componen, haciendo énfasis en detallar los principales dispositivos networking y el direccionamiento tanto de la intranet como de la extranet. Para luego examinar la Red Mesh con su respectivo proceso de autenticación y los equipos que usa.

En esta fase, igualmente, se realizó un estudio minucioso de los requisitos, restricciones y exigencias del proyecto EDUROAM que incluye estándares, protocolos, métodos de autenticación, etc. Para cumplir con esta fase, además, se realizó el estudio teórico de los temas incluidos en la revisión de literatura (*ver sección Resultados, Fase 1: Análisis de Requerimientos*).

Fase 2: Desarrollo

En esta fase se enfoca de forma objetiva en la configuración, funcionamiento, y validación de los servidores Radius, así como la asignación del ente encargado para el despliegue de Eduroam a nivel nacional y finalmente alternar con el análisis para elegir el método de autenticación adecuado y posterior configuración. El primer servidor a configurar fue el servidor Radius Local Eduroam UNL, en el que se manipulan archivos de configuración que permiten adaptar los requerimientos de acuerdo al servicio, posteriormente se inicia la creación de certificados digitales para garantizar la seguridad de la información. Seguidamente, se empieza con la implementación del servidor federado Ecuador de prueba donde se manejan archivos de configuración para el enlace con el servidor Radius Local Eduroam UNL y posterior despliegue nacional. Terminadas las configuraciones, se pone a prueba los servidores demostrando la vinculación entre ellos. Luego, se determina

cual será el ente encargado del despliegue nacional de Eduroam, el cual emitirá los certificados necesarios. Así mismo se trabaja en el servidor LDAP, que previamente se analizó como método de autenticación, empezando desde la instalación y configuración del servidor, seguido de la carga de usuarios divididos en 3 grupos: personal administrativo y de servicios, estudiantes, y personal docentes e investigador (*ver sección Resultados, Fase 2: Desarrollo*).

Fase 3: Pruebas de movilidad

Las pruebas de movilidad, es la fase crucial dentro de la implementación de Eduroam, puesto que esta fase evidencia de forma contundente la movilidad en la UNL. Se inicia por determinar el escenario en el que se llevaría a cabo el proceso en cuestión, por lo que el usuario tiene acceso a la red inalámbrica mediante la topología especificada. Para comprobar el rendimiento del servidor RADIUS se realizó la simulación de muchas solicitudes simultáneas con la ayuda de RADIUS test client, Una vez terminada esta comprobación, se enuncia las plataformas a evaluarse donde eduroam.ec@unl.edu.ec será el usuario de prueba, demostrando conexión a la red mediante figuras tanto de la plataforma evaluada como con capturas del registro del usuario en el sistema de monitoreo DaloRADIUS. De igual forma se evalúa la movilidad con el usuario de prueba en el campus de otra universidad (*ver sección Resultados, Fase 3: Pruebas de movilidad*).

Fase 4: Difusión de los Resultados de la Investigación

Para presentar los resultados de la investigación se toma como instrumentos de difusión los siguientes:

- Se redactó un Artículo Técnico cuyo título versa “Implementation of Eduroam as Wirelless Infraestructure on the Campus of National University of Loja”, este tipo de documento sigue las normas para la presentación de artículos en IEEE Latin America Transactions; para ser presentado a la comunidad científica en la Revista **“Energía”** Edición N° 2 Junio 2014. (*ver sección Resultados Fase 4: Difusión de los Resultados de la Investigación*)
- Se participó en las charlas de antesala al FLISOL 2014 (Festival Latinoamericano de Instalación de Software Libre) con la exposición cuyo tema versa **“Servicio de Movilidad mundial Eduroam en la Universidad Nacional de Loja con FreeRADIUS, OpenSSL y OpenLDAP”.** Para la participación en dicho evento se

persiguió con énfasis las normas y requerimientos establecidos por los organizadores. (*ver sección Resultados Fase 4: Difusión de los Resultados de la Investigación*)

- Con el ánimo de proponer un alcance de difusión mayor se decide crear un portal web con información introductoria del proyecto, los manuales de configuración en diferentes plataformas, los participantes de Eduroam a nivel nacional y los contactos de Eduroam en la UNL. El portal web fue creado, por petición del Director de la UTI, con el mismo CMS debido a que es necesario seguir con el estándar con el que fueron gestionados los demás portales de la UNL. (*ver sección Resultados Fase 4: Difusión de los Resultados de la Investigación*)
- Finalmente, se procede a la redacción del informe final que plasma los resultados obtenidos, cuyo documento sigue la normativa de presentación del proyecto de fin de carrera establecido por las autoridades de la Carrera de Ingeniería en Sistemas. (*ver sección Resultados Fase 4: Difusión de los Resultados de la Investigación*)

F. RESULTADOS

Durante la implementación del sistema federado Eduroam se crearon fases esenciales para su desarrollo. En la fase de requerimientos se constató el manejo de la red inalámbrica para tomar lo necesario como punto de partida, para luego demostrar las configuraciones de los servidores a implementar las mismas que se detallan en la fase de desarrollo. La fase de movilidad indica las pruebas realizadas en los diferentes dispositivos y plataformas, lo cual se traslada en un proceso de documentación en la fase de resultados de la investigación.

1. Fase 1: Análisis de requerimientos

1.1. Generalidades

La Universidad Nacional de Loja en el trascurso de los años ha ido mejorando en cuanto a infraestructura física y tecnológica, dando cabida a una actualización constante en las tecnologías de la información y así poder cumplir con las necesidades que se presentan en la institución, donde tanto estudiantes, docentes e investigadores se ven en la necesidad de utilizar servicios cada vez más avanzadas acorde a los cambios que van presentando en el mundo de la tecnología.

Al mejorar estos servicios se pretende mantener una infraestructura tecnológica sólida y moderna. Además logra establecer iniciativas futuras de investigación acorde a los cambios que se van dando y así garantizar la privacidad e integridad de la información.
En la actualidad la Universidad Nacional de Loja cuenta con la UTI, encargada de la infraestructura tecnológica y su respectiva ubicación física; que está dividida en tres secciones: mantenimiento y equipos informáticos, desarrollo de software, y sección redes y equipos informáticos.

La sección de redes y equipos informáticos es la encargada de administrar y proveer que todo el campus universitario disponga todo el tiempo de red inalámbrica siempre y cuando garantice la seguridad de la información que se transmite a través de este medio.

El Proveedor de Servicios de Internet (ISP) con el que cuenta la UNL es el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA), quienes en convenio con la empresa TELCONET S.A, provee un ancho de banda de 99Mbps.

1.2. Cuarto de Telecomunicaciones

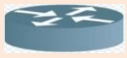
El Cuarto de Telecomunicaciones es el lugar definido como el espacio donde residen los equipos de telecomunicaciones. Solo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones, tales como routers, switchs, y servidores, que son manejo exclusivo del administrador de red y personal autorizado.

Cabe mencionar que el Cuarto de Telecomunicaciones se encuentra en el Departamento de la Unidad de Telecomunicaciones e Información, ubicado en el cuarto piso del Edificio de Administración Central bloque 2.

1.3. Simbología de los elementos de la Red de Datos de la Universidad Nacional de Loja

En la Tabla II se detalla la simbología de los principales dispositivos y equipos que forman la red de datos de la Universidad Nacional de Loja.

Tabla II. DISPOSITIVOS Y EQUIPOS QUE FORMAN LA RED DE DATOS

SIMBOLOGÍA	DESCRIPCIÒN
	Router
	Switch de Acceso
	Servidor
	PC Personales

	WIreless Controller
	Packet Shaper
	Access Point Inalàmbricos
	Antena
	Torre
	Conexión Inalámbrica
	Cable UTP
	Fibra Óptica

1.4. Backbone de la Universidad Nacional de Loja

En la Fig. 7 se muestra el backbone de la infraestructura de la red de datos, donde se observan las principales conexiones troncales de la intranet como de la extranet.

El backbone de la Universidad está compuesto de un gran número de switch interconectados, los cuales llevan los datos a través de las distintas dependencias, utilizando como medio de transmisión fibra óptica, cable UTP y ondas electromagnéticas.

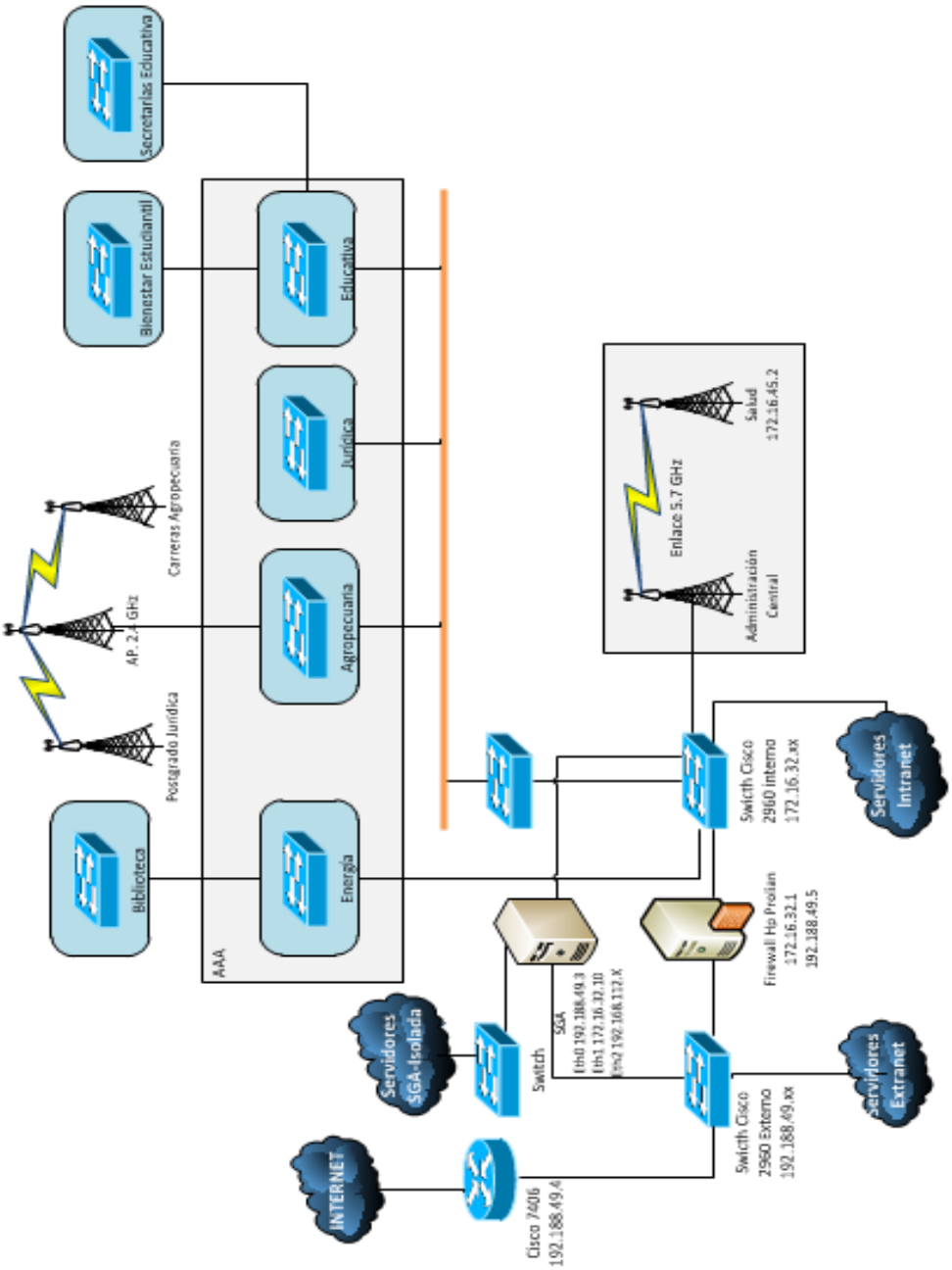


Figura 7. Backbone de la Universidad Nacional de Loja

1.5. Detalle de los principales dispositivos Networking

En la Tabla III se detalla los principales dispositivos networking que forman parte de la red de la Universidad Nacional de Loja con su descripción y funcionamiento.

Tabla III. DISPOSITIVOS NETWORKING PRINCIPALES

DISPOSITIVOS	DESCRIPCIÓN
Router Cisco 7604	Tiene asignado la dirección IP pública 192.188.xx.xx/24, permite acceder al internet comercial proporcionado por CEDIA y a su vez establecer la conexión internamente a la red de la universidad.
Switch Cisco 2960 externo	Tiene asignado la dirección IP pública 192.188.xx.xx/24, aquí se encuentra configurado una de las interfaces Fast Ethernet se conecta al router cisco 7604 y el puerto 10/100 Mbps con los servidores públicos de la Universidad.
Switch Cisco 2960 interno	Tiene asignado la dirección IP privada 172.16.xx.xx/19, en este swich se encuentra conectado al Firewall por la interfaz Fast Ethernet 10/100, como también están los servidores internos de la red de datos de la Universidad
Firewall HP Proliant	Tiene asignado la dirección IP pública 192.188.49.5 y la dirección IP privada 172.16.xx.xx, se encuentra conectado al Switch Cisco 2960 externo y externo por cada una de las interfaces Fast Ethernet 10/100. Además está configurado con NAT permitiendo que equipos con direcciones Ip privadas puedan salir con IP públicas (enrutamiento)

1.6. Direccionamiento IPv4 de la Intranet

La Universidad actualmente posee un direccionamiento IPv4 privado de clase B que se usa en los dispositivos de networking, equipos finales, servidores, puntos de acceso inalámbrico, etc. En la Tabla IV se detalla el direccionamiento IPv4 de la UNL.

Tabla IV. DIRECCIONAMIENTO IPV4 DE LA INTRANET

DESCRIPCIÓN	ESPECIFICACIÓN
Red de Clase B	172.16.0.0/16
Dominio	unl.edu.ec
Subred	172.16.32.0/19
Mascara de Subred	255.255.224.0
Dirección de Broadcast	172.16.63.255
Puerta de Enlace	172.16.32.1
Sistema de Nombres de Dominio	172.16.32.2

1.7. Direccionamiento IPv4 Público

La Universidad posee un rango de direcciones IPv4 públicas que ha sido asignada por NIC.EC (Registro de Nombres de Dominio del Ecuador), estas direcciones permiten a la universidad brindar sus servicios de internet al personal docente, estudiantes y administrativos. En la Tabla V se detalla el direccionamiento IPv4 público de clase C

Tabla V. DIRECCIONAMIENTO IPV4 PÚBLICO

DESCRIPCIÓN	ESPECIFICACIÓN
Red de Clase C	192.188.49.0/24
Dominio	unl.edu.ec
Mascara de Subred	255.255.255.0
Dirección de Broadcast	192.188.49.255
Puerta de Enlace	192.188.49.4

1.8. Red Mesh de la Universidad Nacional de Loja

La Universidad Nacional de Loja en la actualidad tiene implementado la Red Mesh (Red Inalámbrica Mallada) con la finalidad de proveer del servicio de internet inalámbrico a todos los usuarios que sean parte de la institución y posean de una computadora portátil o dispositivo móvil.

1.8.1. Descripción de Red Mesh Inalámbrica

Una Red Mesh Inalámbrica (WMN) es una de red compuesta por nodos organizados en una topología mesh (malla). El área de cobertura, de todos los nodos actuando como uno sólo, se llama nube de la malla (mesh cloud).

La forma de operar que tienen éstas redes consiste en que los datos van a saltar de un nodo a otro hasta que llegue a su destino [17].

En la Fig. 8 se muestra el funcionamiento de una red Mesh de 7 nodos los cuales se encuentran distribuidos para cubrir toda el área de red. Se puede observar que cada nodo establece comunicación con todos los demás.

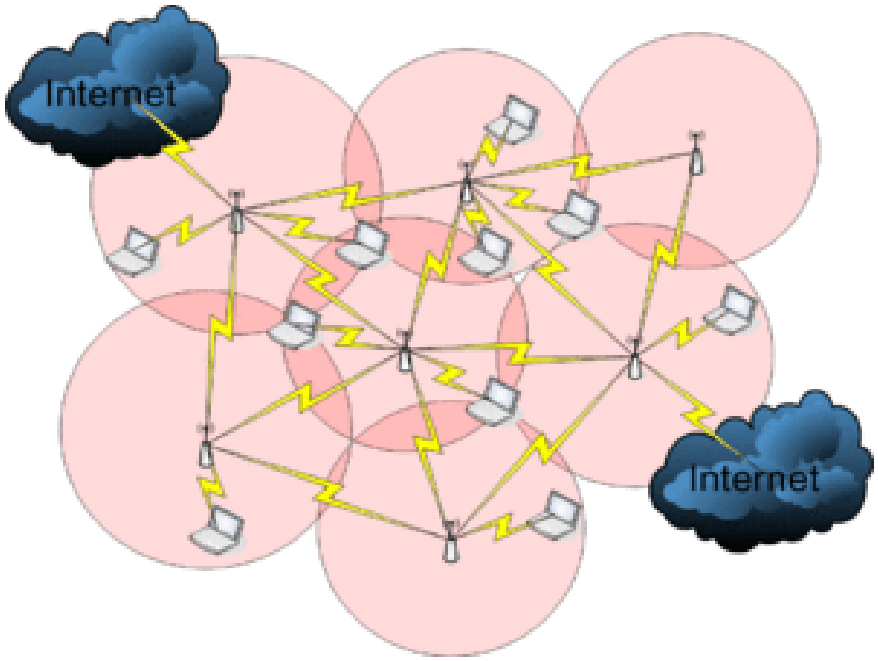


Figura 8. Esquema del funcionamiento de una Red MESH

1.8.2. Proceso de Autenticación a la Red Mesh Inalámbrica de la UNL

En la actualidad los usuarios que requieran disponer de internet de forma inalámbrica deben realizar el siguiente procedimiento:

a) El usuario debe detectar en su portátil o dispositivo móvil la red con el SSID **S.I. UNL** y dar clic en conectar como se muestra en la Fig. 9.

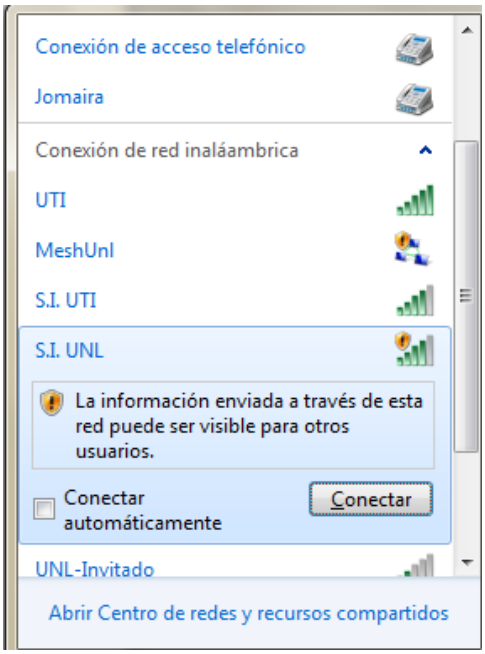


Figura 9. Dispositivo portátil detectando la red con el SSID S.I. UNL

b) Posteriormente el usuario abre un navegador web y accede a una dirección web, donde se redirecciona a la página de inicio de sesión o portal cautivo. Si en caso el usuario ingresa por primera vez, el navegador lanza una excepción donde se debe añadir dicha excepción como se muestra en la Fig.10.

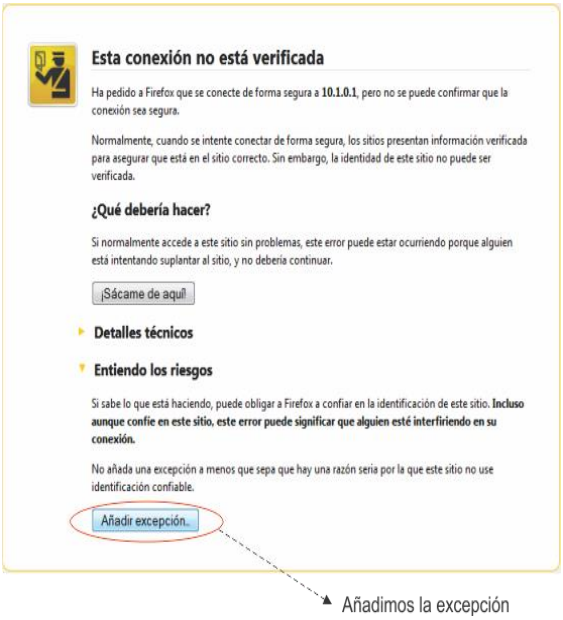


Figura 10. Interfaz web de añadir excepción

c) Se visualiza una ventana donde se obtiene el certificado de seguridad y se confirma la excepción de seguridad como se muestra en la Fig. 11.

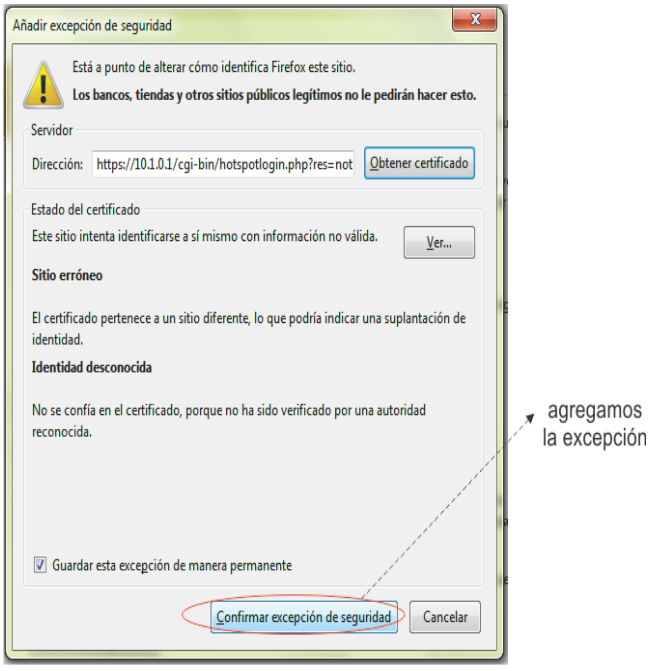


Figura 11. Ventana de confirmación de excepción

d) Finalmente se muestra la página de inicio de sesión, donde se ingresa las credenciales de usuario que están establecidas por la Cédula de Identidad y contraseña como se muestra en la Fig. 12.

Figura 12. Página de Inicio de Sesión

Para validar las credenciales ingresadas por el usuario, son consultadas al Web Services del Sistema de Gestión Académica de la Universidad Nacional de Loja que proporciona métodos para obtener datos personales, como lo es en este caso cédula y clave.

1.8.3. Equipos principales de la Red Mesh

1.8.3.1. Wireless Lan Controller (WLC)

1.8.3.1.1. Descripción General

La Red Mesh cuenta con un equipo Wireless Lan Controller (WLC) cuya arquitectura permite visualizar de forma centralizada a través de una interfaz web los diferentes puntos de acceso que forman la Red Mallada como se muestra en la Fig.13.

AP Name	AP Model	AP MAC
AP_Postgrado_Salud	AIR-CAP1552E-A-K9	54:78:1a:0c:55:20
AP_Adm_Central	AIR-CAP1552E-A-K9	1c:e6:c7:2a:8d:e0
AP_Bloque5_Educativa	AIR-CAP1552E-A-K9	20:3a:07:98:49:60
AP_Electromecanica_energia	AIR-CAP1552E-A-K9	54:78:1a:0c:72:60
AP_Biblioteca_Agropecuaria	AIR-CAP1552E-A-K9	1c:e6:c7:2a:09:c0
AP_Bloque14_Juridica	AIR-CAP1552E-A-K9	1c:e6:c7:2a:91:e0
AP_ComunicacionSocial_Educati	AIR-CAP1552E-A-K9	20:3a:07:98:2c:60
AP_Colegio_Educativa	AIR-CAP1552E-A-K9	54:78:1a:0c:75:60
AP_Post_Educativa	AIR-CAP1552E-A-K9	1c:e6:c7:2a:97:40
AP_Idiomas_Educativa	AIR-CAP1552E-A-K9	1c:e6:c7:2a:97:60
AP_Forestal_Agropecuaria	AIR-CAP1552E-A-K9	54:78:1a:0d:b8:20
AP_Artes_Educativa	AIR-CAP1552E-A-K9	34:a8:4e:51:d5:60
AP_Economia_UNL	AIR-CAP1552E-A-K9	54:78:1a:0d:95:80
AP_Torre_Salud	AIR-CAP1552E-A-K9	54:78:1a:0c:71:00
AP_Salud	AIR-CAP1552E-A-K9	1c:e6:c7:2a:c9:00
AP_Med_Unl	AIR-CAP1552E-A-K9	54:78:1a:0c:7a:c0

Figura 13. Diferentes puntos de acceso que forman la Red Mallada

En la Tabla VI se detalla las características principales y ubicación del Wireless Lan Controller (WLC)

Tabla VI. CARACTERÍSTICAS PRINCIPALES Y UBICACIÓN DEL WLC

WIRELESS LAN CONTROLLER	
Serie	Cisco 5500
Modelo	5508
Escalable	Soporta 12, 25, 50,100, 250, o 500
Administración RF	Provee información en tiempo real e histórico sobre las interferencia de RF
Ubicación	Unidad de Telecomunicaciones e Información
Dirección IP	172.16.xx.xx

1.8.3.1.2. Características de Hardware

En la Fig. 14 se muestra un esquema general del WLC que en conjunto con la Tabla VII indica los diferentes puertos de conexión del equipo.

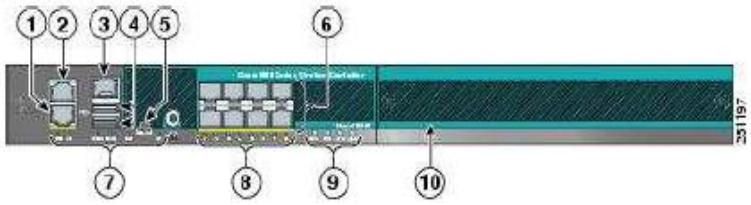


Figura 14. Esquema general del WLC

Tabla VII. PUERTOS DE CONEXIÓN DEL WLC

PUERTOS DE CONEXIÓN			
1	**Puerto redundante para un uso futuro (RJ-45)**	**6**	**SFP (transceptor) Puertos de distribucion1-8**
2	Servicio de puerto (RJ-45)	**7**	LED de gestión del puerto
3	Puerto de Consola (conector RJ-45)	**8**	LED de actividad de los puertos de distribución
4	Puertos USB 0 y1 (Tipo A)	**9**	LED de Fuente de alimentación (PS1 y PS2), sistema (SYS), y de alarma (ALM)
5	Puerto de consola (mini USB TIPO B)	**10**	Ranura de expansión del modulo

A continuación se presenta una descripción rápida de cada uno de los puertos que tiene el equipo para su funcionalidad de acuerdo a la Tabla VII.

1. **Puerto Redundante:** Este puerto sirve como Backup cuando se requiere otro camino para llegar a la LAN, se puede decir que es otro puerto de distribución, pero este puerto tiene un conector RJ-45.
2. **Puerto de Servicio:** Este puerto está destinado a brindar un acceso al equipo cuando todos los otros caminos para ingresar al controlador han fallado, por eso este puerto debe estar en una subred diferente a los demás.
3. **Puerto de Acceso a Consola:** Se tiene un puerto de consola estándar al igual que el de un Switch; lo que se puede recalcar es que este controlador tiene dos puertos de consola tipo USB uno tipo A y otro Tipo B.
4. **Puertos de Distribución:** Los controladores Cisco de la serie 5500 tienen 8 puertos Giga Ethernet para el sistema de distribución, con los cuales el controlador puede administrar los Access Point.

1.8.3.1.3. Interfaces Principales del WLC

En la Fig. 15 se muestra información básica del WLC referente a su dirección IP, nombre descriptivo, versión del software y estándares de autenticación, etc.

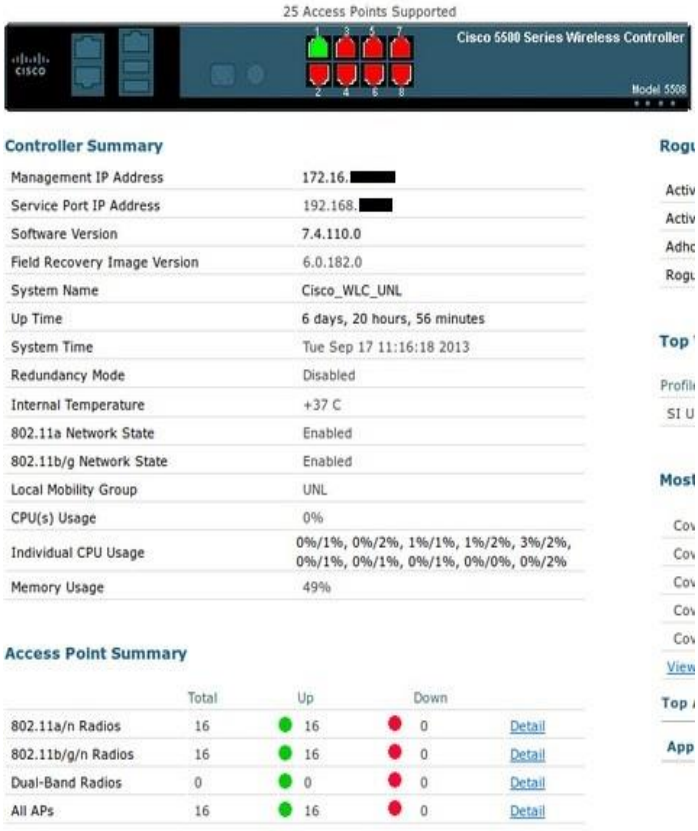


Figura 15. Información básica del WLC

En la Fig. 16 se muestra la WLAN 1 con el **SSID S.I. UNL** que provee del servicio de red inalámbrica en el campus universitario para los usuarios que forman parte de la Universidad Nacional de Loja.

Figura 16. WLAN SSID creados en el WLC

En la Fig. 17 se muestra las direcciones MAC de cualquier dispositivo que pueda engancharse a la red, estos pueden ser computadoras portátiles, Smartphone, tablets, etc. Están asociados a los diferentes AP's y al WLAN SSID S.I.UNL

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID
00:01:da:f0:05:04	AP_Colegio_Educativa	SI UNL	S.I. UNL
00:08:22:f6:0f:70	AP_Bloque5_Educativa	SI UNL	S.I. UNL
00:0c:e7:00:00:00	AP_Economia_UNL	SI UNL	S.I. UNL
00:13:02:6f:28:fa	AP_Forestal_Agropecuaria	SI UNL	S.I. UNL
00:13:e8:1c:22:f5	AP_Salud	SI UNL	S.I. UNL
00:18:de:2c:29:7f	AP_Forestal_Agropecuaria	SI UNL	S.I. UNL
00:1b:77:5e:9d:73	AP_Artes_Educativa	SI UNL	S.I. UNL
00:1c:bf:6a:54:1b	AP_Economia_UNL	SI UNL	S.I. UNL
00:1d:e0:37:21:53	AP_Post_Educativa	SI UNL	S.I. UNL
00:1e:52:76:96:4a	AP_ComunicacionSocial_Educativa	SI UNL	S.I. UNL
00:1e:64:76:78:2c	AP_Forestal_Agropecuaria	SI UNL	S.I. UNL
00:1f:3a:5d:ab:f2	AP_Artes_Educativa	SI UNL	S.I. UNL
00:1f:3c:dd:d9:46	AP_Electromecanica_energia	SI UNL	S.I. UNL
00:1f:e2:a5:ee:3a	AP_Post_Educativa	SI UNL	S.I. UNL
00:21:00:ca:40:da	AP_Electromecanica_energia	SI UNL	S.I. UNL
00:21:5c:74:8c:73	AP_Post_Educativa	SI UNL	S.I. UNL
00:21:91:94:70:33	AP_Torre_Salud	SI UNL	S.I. UNL
00:22:5f:8e:1e:5e	AP_Economia_UNL	SI UNL	S.I. UNL
00:23:15:71:e7:9c	AP_Bloque5_Educativa	SI UNL	S.I. UNL
00:24:7e:ff:e5:a4	AP_Electromecanica_energia	SI UNL	S.I. UNL
00:25:56:3c:36:b4	AP_Economia_UNL	SI UNL	S.I. UNL
00:26:08:e1:b9:b6	AP_ComunicacionSocial_Educativa	SI UNL	S.I. UNL
00:26:82:80:e3:01	AP_Economia_UNL	SI UNL	S.I. UNL
00:26:ff:34:76:7d	AP_Bloque5_Educativa	SI UNL	S.I. UNL
00:34:00:a0:17:6f	AP_Economia_UNL	SI UNL	S.I. UNL
00:8b:0e:01:16:6b	AP_Colegio_Educativa	SI UNL	S.I. UNL
00:cf:05:00:73:50	AP_Colegio_Educativa	SI UNL	S.I. UNL

Figura 17. Direcciones MAC de los dispositivos inalámbricos conectados

1.8.3.2. AP de la Red Mesh

1.8.3.2.1. Descripción General

La red mallada (mesh) implantada en la UNL se encuentra diseñada con dispositivos networking Aironet 1552E que se encuentran distribuidos en las diferentes infraestructuras físicas del campus universitario, dichos dispositivos están a una altura máxima de 10 metros que fueron ubicados de acuerdo al criterio de los proveedores.

Una práctica es instalar su antena de 5 a 10 pies (1,5 a 3 m) por encima de la línea del techo y lejos de todas las líneas eléctricas y las obstrucciones [18].

El Cisco Aironet 1552E/1552EU puntos de acceso al aire libre son los modelos estándar, el sistema de radio dual con puertos de antena externos que cumplen con los estándares IEEE 802.11b/g/n (2,4 GHz) y 802.11a / n (5 GHz). El 1552E tiene tres conexiones de la antena externa para dual-band omni o antenas direccionales. Estos modelos también tienen un puerto PoE de salida que puede alimentar una cámara de vigilancia de vídeo u otros dispositivos. Modelos muy flexibles, el Cisco Aironet 1552E están bien equipadas para despliegues municipales y de la escuela, las aplicaciones de video vigilancia, entornos mineros, y descarga de datos [19].

1.8.3.2.2. Características del AP Aironet 1552E

En la Tabla VIII se realiza una descripción rápida de las características principales del dispositivo utilizado en la Red Mesh Inalámbrica de la Universidad.

Tabla VIII DESCRIPCIÓN DE LAS CARACTERÍSTICAS DEL AIRONET 1552E

DESCRIPCIÓN	ESPECIFICACIÓN
Diseño Resistente	Exteriores
Temperatura min. /máx. de funcionamiento	-40°C/55°c
Cantidad de Canales	13
Cantidad de Antenas	3
Tasa de Transferencia (máx.)	300Mbps
Anchura	30.5cm
Profundidad	19.8cm
Altura	16.3cm
Peso	7.8kg
Protocolo de interconexión de Datos	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n
Algoritmo de Seguridad	802.1x RADIUS, EAP-TLS
Frecuencia de Banda	2.4GHz, 5GHz

1.8.3.2.3. Ubicación y Direccionamiento IP de los Aironet

Los dispositivos están ubicados en todo el campo universitario, incluyendo el área de la salud humana e instituto de idiomas. En la Tabla IX se detalla el área, ubicación dentro del área, dirección IP y su MAC.

Tabla IX. UBICACIÓN DE LOS AIRONET

ÁREAS	UBICACIÓN	IP	MAC
Adm. Central	Bloque 2	172.16.xx.xx	1c:e6:c7:2a:8d:e0
A.E.A.C.	Col. Manuel Cabrera L.	172.16.xx.xx	54:78:1a:0c:75:60
	Bloque 5	172.16.xx.xx	20:3a:07:98:49:60
	Posgrado	172.16.xx.xx	1c:e6:c7:2a:c9:00
	Carrera de CC.SS	172.16.xx.xx	20:3a:07:98:2c:60
	Carrera de CC.FF: Estadio	172.16.xx.xx	54:78:1a:0c:55:20
	Biblioteca Artes Plásticas	172.16.xx.xx	34:a8:4e:51:d5:60
A.J.S.A.	Bloque 14	172.16.xx.xx	1c:e6:c7:2a:91:e0
	Plaza de la Cultura Universitaria	172.16.xx.xx	54:78:1a:0d:95:80
A.E.I.R.N.N.R.	Biblioteca	172.16.xx.xx	1c:e6:c7:2a:97:40
A.A.R.N.R.	Biblioteca	172.16.xx.xx	1c:e6:c7:2a:09:c0
	Carrera de Medio Ambiente	172.16.xx.xx	54:78:1a:0c:72:60
A.S.H.	Torre	172.16.xx.xx	54:78:1a:0d:b8:20
	Postgrado	172.16.xx.xx	54:78:1a:0c:71:00
M.E.D.	Edificio MED	172.16.xx.xx	54:78:1a:0c:7a:c0
Instituto de Idiomas	Edificio Principal	172.16.xx.xx	1c:e6:c7:2a:97:60
Bakup		172.16.xx.xx	34:a8:4e:51:ed:00

1.8.3.2.4. Cobertura de los AP Aironet 1550

El diseño de la red inalámbrica implementa varios Puntos de Acceso y antenas Omnidireccionales, llegando a satisfacer los requerimientos para que cada uno de los usuarios pueda acceder sin ningún problema a la red mediante un enlace inalámbrico.

Las Fig. 18 y 19 muestran las áreas de cobertura de los Puntos de Acceso, distribuidos de forma que pueda ser utilizado por el mayor número de usuarios.

Se determinaron las áreas de cobertura y la posición para cada equipo, con Puntos de Acceso Cisco Aironet 1552e con antenas Omnidireccionales, ya que estos equipos poseen las mejores características para la implementación de la red mesh inalámbrica dentro del campus universitario. Todos los equipos utilizan antenas omnidireccionales dual band, los cuales están ubicados en distintos lugares estratégicos, ofreciendo la mayor cobertura y rendimiento de la Red inalámbrica [20].

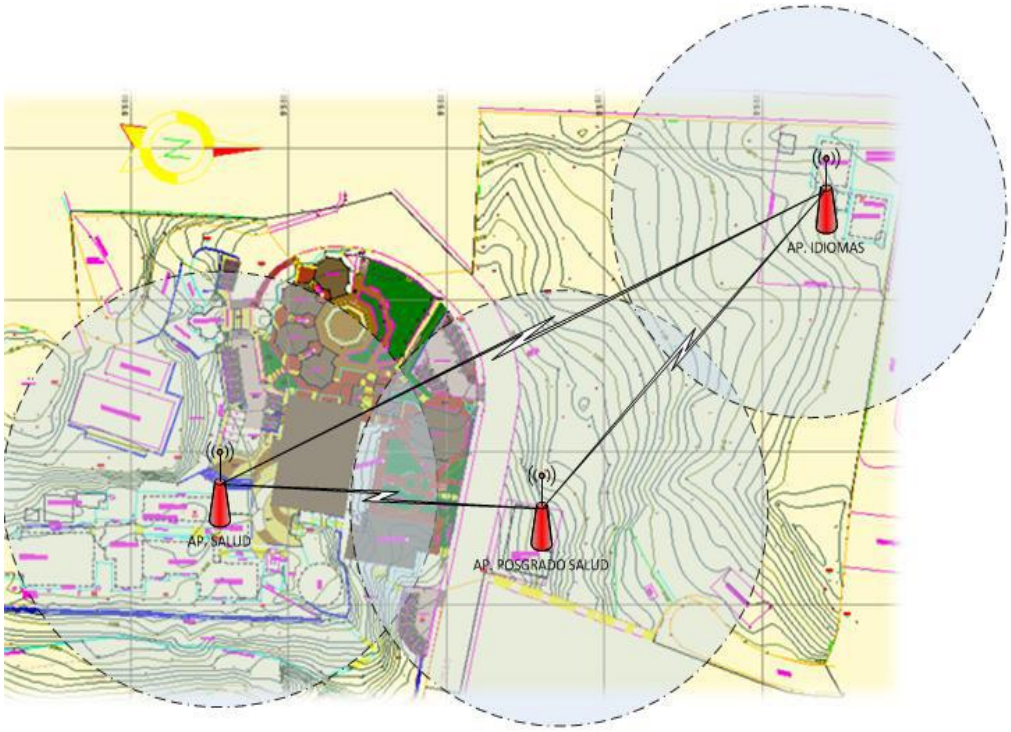


Figura 18. Cobertura de los AP en el Área de la Salud e Instituto de Idiomas

Figura 19. Cobertura de los AP en el Campus Universitario

1.9. Lineamientos de EDUROAM frente a la Red Mesh UNL

El proyecto EDUROAM posee algunos requerimientos específicos que no pueden pasar por desapercibido y que son necesarios llevarlos a cabo para su implementación en cualquier institución que desee forma parte la iniciativa.

Se ha creído preciso realizar una comparativa en cuanto a los requerimientos de EDUROAM frente a lo que se posee en la Universidad Nacional de Loja. Para su mejor compresión se procedió a dividirlo en 3 puntos primordiales que son hardware, software y los usuarios finales que se detalla en los puntos que más adelante se mencionan.

Cabe mencionar que la información detallada de Eduroam fue proporcionada por el representante de Eduroam en Latinoamérica a través de su correo personal: jlquiroza62@gmail.com (Anexo 1), así como información recolectada del sitio web Eduroam España (http://www.eduroam.es/).

De la misma forma cabe indicar que la información detallada sobre la Red Mesh de la UNL fue recolectada de la Tesis cuyo tema versa: “Implantación de un sistema de seguridad para el acceso inalámbrico a la red de la Universidad Nacional de Loja utilizando Software Libre” que nos proporciona ciertos indicadores para su comparación.

1.9.1. Hardware

En la Tabla X se realiza una comparativa de hardware entre el Servidor que posee actualmente la Universidad Nacional de Loja frente a lo que requiere la Iniciativa Eduroam.

Tabla X. COMPARATIVA DE HARDWARE ENTRE SERVIDORES

HARDWARE	RADIUS EDUROAM	RADIUS SI UNL
Procesador	Core i3	Core 2 Duo
Memoria RAM	4 GB	2 GB
Disco Duro	80 GB	120 GB

En la Tabla XI muestra con un visto lo requiere Eduroam en la configuración de los Access Point y lo que dispone la Red Mesh UNL.

Tabla XI. PROTOCOLO ACCESS POINT

RED	AP's(soporte protocolo 802.1x)
Eduroam	✓
Red Mesh UNL	✓

1.9.2.Software

En la Tabla XII se realiza una comparativa de software entre el Servidor que posee actualmente la Universidad Nacional de Loja frente a los requerimientos de la Iniciativa Eduroam.

Tabla XII. COMPARATIVA DE SOFTWARE ENTRE SERVIDORES

SOFTWARE	RADIUS EDUROAM	RADIUS SI UNL
Sistema Operativo	Debian 6.0 Squeeze	Ubuntu Server 12.04
RADIUS	Freeradius 2.1.10	Freeradius 2.1.10
Protocolo EAP	SSL/TTLS	MD5
Consulta de Credenciales	LDAP	WebService

1.9.3.Usuario Final

En la Tabla XIII se realiza una comparación en cuanto a los usuarios permitidos tanto en la Red S.I. UNL como en el proyecto Eduroam, para el uso de los recursos tecnológicos como es el servicio de internet.

Tabla XIII. USUARIOS

USUARIOS	DEFINICIÓN	CONECTIVIDAD	
		Eduroam	S.I. UNL
Locales	Usuarios que pertenecen a su institución	✓	✓
Itinerantes	Usuarios visitantes de otra institución, cuya entidad pertenece a la Comunidad Eduroam	✓	x

En la Tabla XIV se plasma una comparativa del proceso de logeo que deben realizar los usuarios al momento de enlazarse a la red S.I. UNL y como lo realizarían en la red Eduroam.

Tabla XIV PROCESO DE CONECTIVIDAD Y LOGEO

CONECTIVIDAD	EDUROAM	S.I. UNL
Forma de Conectividad	Interfaz Manager	Portal Cautivo
Logeo (credenciales del usuario)	La primera vez	Cada vez que requiera del servicio

En la Tabla XV se realiza una comparativa de los sistemas operativos permitidos para establecer conectividad tanto en la red S.I. UNL y cuales serían permitidos en la red Eduroam.

Tabla XV SISTEMAS OPERATIVOS

RED	SISTEMAS OPERATIVOS			
	Windows	Linux	Android	Mac OS
S.I. UNL	✓	✓	✓	✓
Eduroam	✓	✓	✓	✓

A continuación en la Tabla XVI muestra el tiempo de sesión permitido para cada usuario al momento de conectarse a una de las redes detalladas en la tabla.

Tabla XVI TIEMPO DE SESIÓN

RED	TIEMPO DE SESIÓN
S.I. UNL	7200 seg (2 horas)
Eduroam	Indefinido

2. Fase 2: Desarrollo

2.1. Servidores Radius

2.1.1. Servidor Radius Local Eduroam UNL

2.1.1.1. Funcionalidad

El Servidor Radius Local Eduroam UNL que forma parte de la infraestructura inalámbrica de la institución, tiene como funciones principales realizar lo siguiente:

- Resolver solicitudes de conexión de su propio dominio *(@unl.edu.ec):* Es decir si un usuario local identifica el SSID eduroam dentro del campus universitario, deberá resolverlo.
- Reenviar al servidor RADIUS Federado de Ecuador las solicitudes de otros dominios distintos al *(@unl.edu.ec):* Se trata de un usuario visitante o itinerante, el cual es identificado por su dominio que no pertenece a la UNL, para lo cual debe reenviar la solicitud al servidor RADIUS Federado Ecuador.
- Aceptar solicitudes del servidor RADIUS Federado Ecuador: Si un usuario con dominio *@unl.edu.ec* se encuentra en otra institución y esta forma parte de la iniciativa Eduroam, se remite la solicitud a través del servidor RADIUS Federado Ecuador hacia el servidor RADIUS Local Eduroam UNL.

2.1.1.2. Características

Las configuraciones del servidor se desarrollaron en un equipo BLADE HP PROLIANT BL460c G7 con tecnología KVM. Cuyas características son las que se muestran en la Tabla XVII y Tabla XVII.

2.1.1.2.1. Hardware

Tabla XVII. CARACTERÍSTICAS DE HARDWARE

HARDWARE	DESCRIPCIÓN
Disco Duro	43.5 GB
Memoria RAM	4 GB
Procesador	Amd64

2.1.1.2.2. Software

Tabla XVIII. REQUERIMIENTOS DE SOFTWARE

SOFTWARE	DESCRIPCIÓN
Sistema Operativo	GNU/Linux
Distribución	Debian 6.0 Squeeze
Radius	Freeradius 2.1.10
SSL	OpenSSL O.9.8º
Paquetes y librerías	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, libpcap0.8-dev, gnutls-bin

2.1.1.3. Desarrollo de las configuraciones

2.1.1.3.1. Autoridad Certificadora

La autoridad certificadora es la entidad encargada de emitir los certificados digitales con la clave privada del usuario solicitante que hará pareja con su respectiva clave pública. La Universidad Nacional de Loja emitirá para el Servidor Radius Local Eduroam UNL el certificado digital, desempeñando el rol de autoridad certificadora, en la Fig. 20 se muestra la creación de la CA.

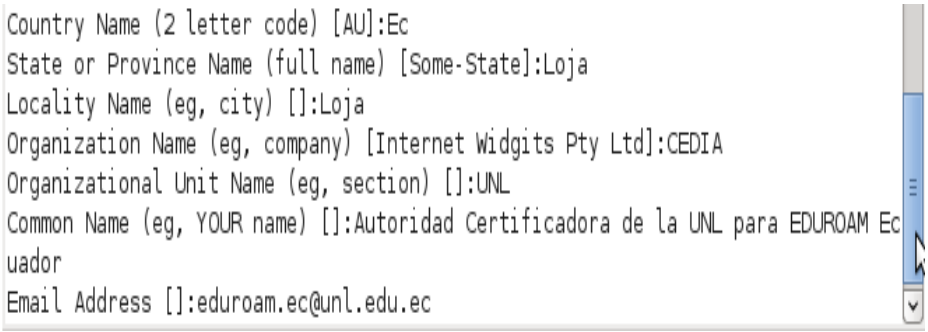


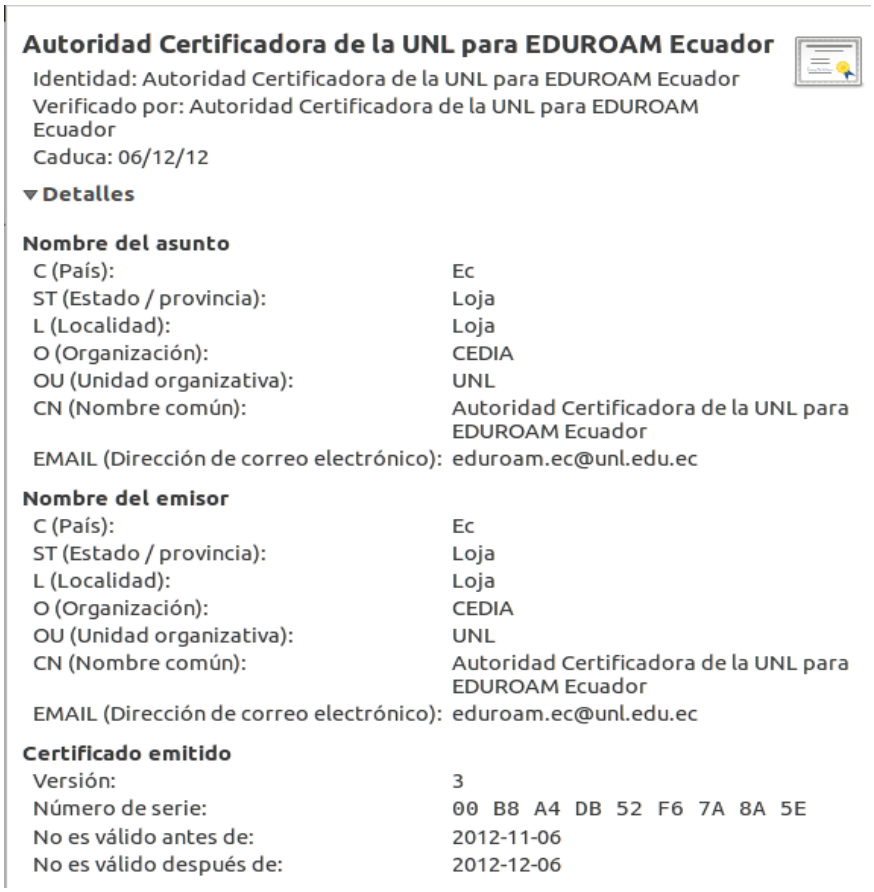
Figura 20. Creación de la CA, indicando a la UNL como CA

2.1.1.3.1.1. Llaves de la Autoridad Certificadora

Mediante la siguiente línea de comando openssl req -new -x509 -extensions v3_ca -keyout private/ca.key -out ca.crt se crean la llave pública y privada, haciendo una petición en formato X509 con la herramienta openssl cuya clave privada para la AC se guardará en el archivo ca.key y su llave pública en el archivo ca.crt.

2.1.1.3.1.1.1. Llave pública

La llave pública sirve para cifrar las credenciales que el usuario está ingresando al momento de acceder al servicio de red inalámbrica, dicha llave se la comparte con las demás personas. La llave pública contiene información relevante tal como: datos de la CA, llave pública y tipo de algoritmo; tal como se presenta en la Fig. 21, 22 y 23 respectivamente



Autoridad Certificadora de la UNL para EDUROAM Ecuador

Identidad: Autoridad Certificadora de la UNL para EDUROAM Ecuador
Verificado por: Autoridad Certificadora de la UNL para EDUROAM Ecuador
Caduca: 06/12/12

▼ **Detalles**

Nombre del asunto

C (País):	Ec
ST (Estado / provincia):	Loja
L (Localidad):	Loja
O (Organización):	CEDIA
OU (Unidad organizativa):	UNL
CN (Nombre común):	Autoridad Certificadora de la UNL para EDUROAM Ecuador
EMAIL (Dirección de correo electrónico):	eduroam.ec@unl.edu.ec

Nombre del emisor

C (País):	Ec
ST (Estado / provincia):	Loja
L (Localidad):	Loja
O (Organización):	CEDIA
OU (Unidad organizativa):	UNL
CN (Nombre común):	Autoridad Certificadora de la UNL para EDUROAM Ecuador
EMAIL (Dirección de correo electrónico):	eduroam.ec@unl.edu.ec

Certificado emitido

Versión:	3
Número de serie:	00 B8 A4 DB 52 F6 7A 8A 5E
No es válido antes de:	2012-11-06
No es válido después de:	2012-12-06

Figura 21. Datos de la CA

Información de la clave pública

Clave del algoritmo:	RSA
Parámetros de la clave:	05 00
Tamaño de la clave:	1024
Huella de la clave SHA1:	AC E4 05 0D 10 84 51 D5 38 02 41 A9 D3 AC E5 E0 09 90 D9 79
Clave pública:	30 81 89 02 81 81 00 AC 8A 9A 86 12 79 26 8B FC CD EA 36 D9 E2 93 82 6F 6C A4 BF 53 FD 3C 4D 09 A6 21 6F 8C 70 63 70 C5 92 BC 1C AF DA 93 EC 0B 5C 4C DB E3 48 06 96 A3 7C B5 7D 58 EB 54 0B 92 C8 BE 49 99 D6 12 4E 1C 24 CA 9F 6F 13 C0 79 91 C8 81 47 E4 9A DB 65 C0 9C AF E7 48 D9 1D F8 06 50 A6 DD 61 F9 C1 E8 58 55 4E 8B 40 6A 99 D8 25 94 16 3A 14 00 48 2F 14 A6 D4 EE EF 7E 21 9B 87 D2 BE F7 C8 18 19 E7 02 03 01 00 01

Identificador del asunto de la clave

Identificador de clave:	72 DF EB FF 05 19 27 A3 41 F3 FA A4 89 EE 9D 47 36 B7 A0 37
Crítico:	No

Extensión

Identificador:	2.5.29.35
Valor:	30 81 DA 80 14 72 DF EB FF 05 19 27 A3 41 F3 FA A4 89 EE 9D 47 36 B7 A0 37 A1 81

Figura 22. Información de la Clave Pública

Restricciones básicas

Autoridad de certificación:	Sí
Longitud máxima de la ruta:	Sin límite
Crítico:	No

Firma

Algoritmo de firma:	SHA1 con RSA
Parámetros de la firma:	05 00
Firma:	3A AF F4 9E E2 A2 5C 68 DF 08 2B EC 38 A9 08 7F 0B 7B A3 2F 02 FA 3C 7D 3F 08 A6 1F DE FE 6A E6 AE 2B 9D FD 9C 8F 5B C8 21 56 9B E1 0A AB 2F A8 AE 16 15 C3 FD D8 D0 16 6F 02 D3 E8 83 D7 26 FA B6 CF 17 3D 47 22 C5 EE 92 20 24 6E 98 A6 99 FF 96 CD 0C 65 96 98 18 C5 84 21 95 BF DD B5 D5 65 E7 52 B8 F6 26 13 51 9E EB 19 94 BB A5 A3 C2 90 14 11 D1 3C A6 4C EC 5D A6 BD 1B 5E 62 F1 51 AE

Figura 23. Algoritmo de Firma

2.1.1.3.1.1.2. Llave privada

En la Fig. 24 se muestra el contenido del archivo ca.key que contiene la llave privada la cual firmará las peticiones de los certificados, motivo por el cual se presenta cifrada con el algoritmo sha-1.

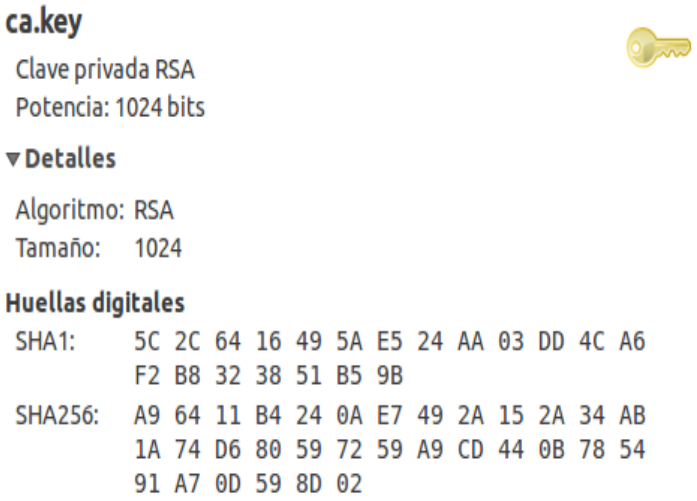


Figura 24. Llave privada del CA

2.1.1.3.2. Certificado de Consulta para el Servidor Radius

El certificado de consulta se crea para el servidor Radius con la finalidad de solicitar un certificado de tipo SSL para el dominio @unl.edu.ec.

2.1.1.3.2.1. Creación del Certificado

Para la creación del certificado de consulta se realiza la petición (radius.unl.edu.ec.csr, ver Fig. 25) a la CA para creación de la llave privada (radius.key, ver. Fig. 26) del servidor RADIUS Local UNL. Para dicha petición se ejecuta la siguiente línea de comando openssl req -new -keyout radius.key -out radius.<dom_institución>.csr -days 1460 la cual se realiza con openssl, el certificado tendrá una duración de un tiempo establecido de 4 años.

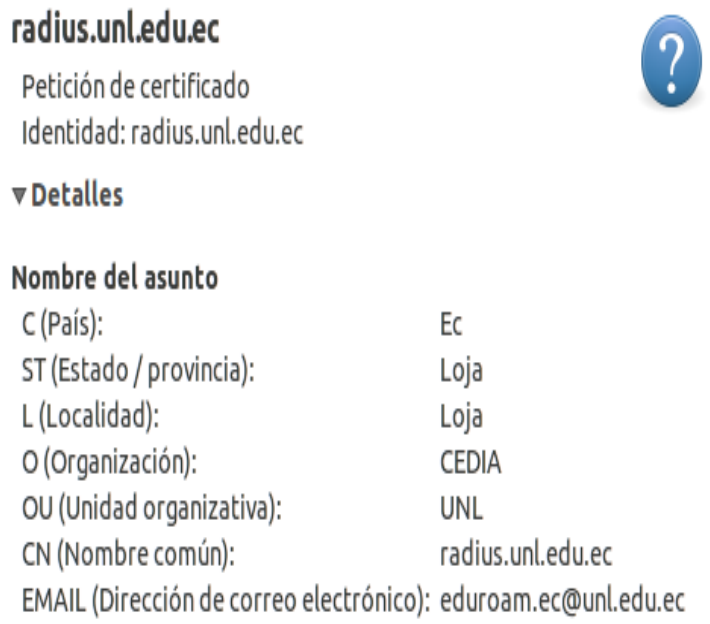


Figura 25. Petición de Certificado

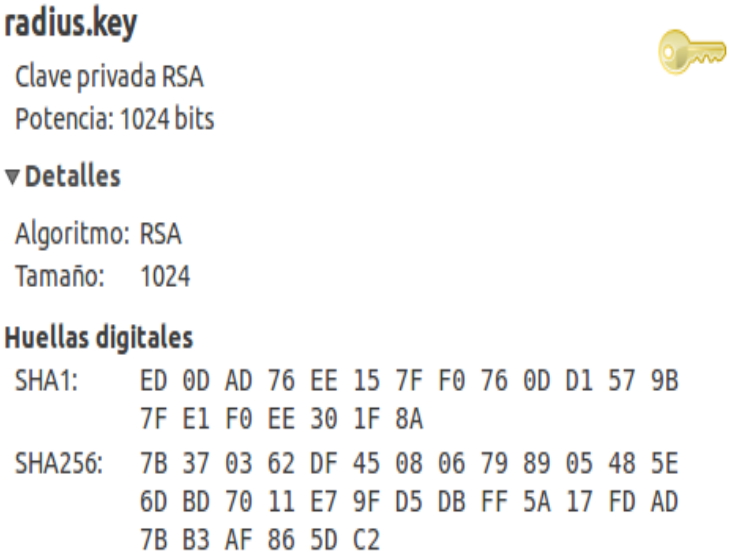


Figura 26. Llave privada del Radius Local Eduroam

2.1.1.3.2.2. Firma del Certificado

Mediante la línea de comando *openssl ca -policy policy_anything -out radius.<dom_institución>.crt -extensions xpserver_ext -extfile xpextensions -infiles radius.<dom_institución>.csr* se realiza una petición al CA para que firme el certificado de consulta del servidor RADIUS Local UNL, la información que contiene hace referencia a la CA, clave pública y algoritmo de firma, la cual se alojará el archivo radius.unl.edu.ec.crt que viene constituirse la llave pública, en la Fig. 27 y 28 se visualizan los detalles.

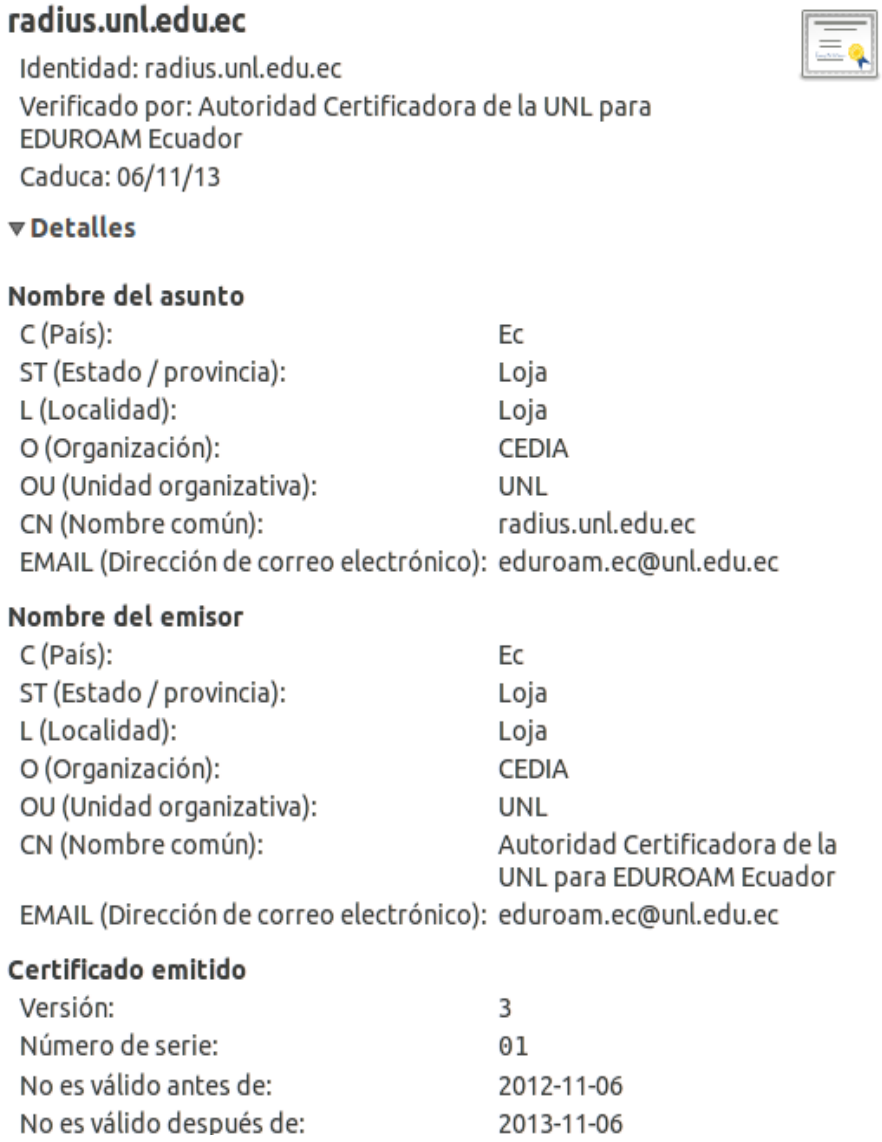
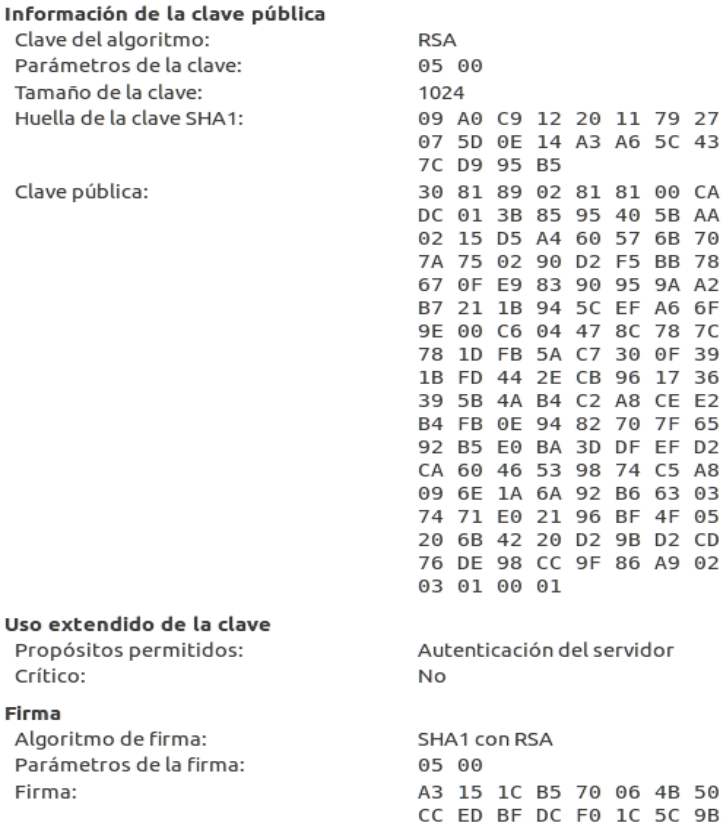


Figura 27. Llave pública Radius Local Eduroam-1



Información de la clave pública

Clave del algoritmo:	RSA
Parámetros de la clave:	05 00
Tamaño de la clave:	1024
Huella de la clave SHA1:	09 A0 C9 12 20 11 79 27 07 5D 0E 14 A3 A6 5C 43 7C D9 95 B5
Clave pública:	30 81 89 02 81 81 00 CA DC 01 3B 85 95 40 5B AA 02 15 D5 A4 60 57 6B 70 7A 75 02 90 D2 F5 BB 78 67 0F E9 83 90 95 9A A2 B7 21 1B 94 5C EF A6 6F 9E 00 C6 04 47 8C 78 7C 78 1D FB 5A C7 30 0F 39 1B FD 44 2E CB 96 17 36 39 5B 4A B4 C2 A8 CE E2 B4 FB 0E 94 82 70 7F 65 92 B5 E0 BA 3D DF EF D2 CA 60 46 53 98 74 C5 A8 09 6E 1A 6A 92 B6 63 03 74 71 E0 21 96 BF 4F 05 20 6B 42 20 D2 9B D2 CD 76 DE 98 CC 9F 86 A9 02 03 01 00 01

Uso extendido de la clave

Propósitos permitidos:	Autenticación del servidor
Crítico:	No

Firma

Algoritmo de firma:	SHA1 con RSA
Parámetros de la firma:	05 00
Firma:	A3 15 1C B5 70 06 4B 50 CC ED BF DC F0 1C 5C 9B

Figura 28. Llave pública Radius Local Eduroam-2

2.1.1.3.3. Archivo clients.conf

En el archivo *clients.conf* se registra los clientes del servidor RADIUS Local Eduroam UNL, tal es el caso del servidor Radius Federado Ecuador como se muestra en la Fig.29 y el Wireless Lan Controller (WLC) visualizado en la Fig. 30; donde cada cliente contiene su correspondiente dirección IP y su contraseña.

```
#
client cedia_federado_ftlr {
        #  Allowed values are:
        #       dotted quad (1.2.3.4)
        #       hostname    (radius.example.com)
        ipaddr = ftlr.cedia.org.ec
        secret = F3dera.UNL-EC
        shortname= org-federado.cedia.org.ec
        nastype= other
```

Figura 29. Cliente Servidor Radius Federado Ecuador

```
client WLC {
  ipaddr =172.16.[redacted]
  secret= [redacted]
  shortname= AP-UNL
  nastype=other
}
```

Figura 30. Cliente Wireless Lan Controller (WLC)

2.1.1.3.4. Archivo eap.conf

En este archivo se determina el tipo de protocolo de autenticación eap-ttls que es utilizado en la comunidad del servicio de movilidad EDUROAM, además se especifica las direcciones de los certificados creados anteriormente como se aprecia en la Fig. 31.

```
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 31. Archivo eap.conf

2.1.1.3.5. Archivo users

Se determina que el tipo de repositorio donde se va a consultar los usuarios, que en este caso es el servidor de directorio LDAP; el cual contiene los diferentes usuarios de la Universidad Nacional de Loja. En la Fig. 32 se muestra el directorio que se ha descomentado para su uso.

```
DEFAULT
        User-Name=  `%{User-Name}`,
        Fall-Through = yes
user Cleartext-Password := "pass"
DEFAULT Auth-Type = LDAP
    Fall-Through = 1
#DEFAULT Auth-Type = SQL
#    Fall-Through = 1
```

Figura 32. Archivo users

2.1.1.3.6. Archivo proxy.conf

En el archivo proxy.conf se crea dos bloques que permitirán el redireccionamiento tanto hacia el servidor Local Eduroam UNL como el servidor Federado Ecuador.

En la Fig. 33 se muestra el bloque donde se especifica que los usuarios que posean el realm (dominio) unl.edu.ec se autenticarán en el servidor Local.

```
realm unl.edu.ec {
        type=radius
        authhost=LOCAL
        accthost=LOCAL
}
```

Figura 33. Bloque con el realm unl.edu.ec

En la Fig. 34 se muestra el bloque donde se especifica que los usuarios que posean un realm (dominio) distinto al servidor Local, serán redireccionados al servidor Radius Federado el cual se encargará de enviar la solicitud al servidor que posea el dominio correspondiente.

```
home_server ftlr {
    type = auth+acct
    ipaddr = ftlr.cedia.org.ec
    port = 1812, 1813
    secret = [redacted]
    response_windows = 20
    zombie_period = 40
    revive_interval = 60
    status_check = status-server
    check_interval = 30
    num_answers_to_alive = 3
 }

home_server_pool EDUROAM-FTLR {
        type=fail-over
        home_server=ftlr
}
```

Figura 34. Bloque de redireccionamiento al Servidor Federado

2.1.2.Servidor Federado Ecuador de Prueba

2.1.2.1. Funcionalidad

El Servidor Radius Federado Ecuador forma parte del servicio de movilidad EDUROAM a nivel de Ecuador, cuyas funcionalidades son las siguientes:

- Aceptar y a su vez reenviar solicitudes de servidores RADIUS de las instituciones a nivel de Ecuador que formen parte de Eduroam, tomando en cuenta el dominio al cual pertenece.
- Aceptar solicitudes que provengan del servidor RADIUS de mayor nivel, a la vez reenviarlas al servidor RADIUS institucional correspondiente de acuerdo al dominio.
- Aceptar solicitudes que provengan de servidores RADIUS institucionales que no pertenezcan a ninguna institución a nivel nacional para reenviarla al servidor RADIUS de Mayor Nivel.

2.1.2.2. Características

Las configuraciones del servidor se desarrollaron en un equipo BLADE HP PROLIANT BL460c G7 con tecnología KVM. Cuyas características son las que se muestran en la Tabla XIX y Tabla XX.

2.1.2.2.1. Hardware

Tabla XIX. CARACTERÍSTICAS DE HARDWARE

HARDWARE	DESCRIPCIÓN
Disco Duro	82 GB
Memoria RAM	4 GB
Procesador	Amd64

2.1.2.2.2. Software

Tabla XX. REQUERIMIENTOS DE SOFTWARE

SOFTWARE	DESCRIPCIÓN
Sistema Operativo	GNU/Linux
Distribución	Debian 6.0 Squeeze
Radius	Freeradius 2.1.10
Paquetes y librerías	freeradius, freeradius-utils

2.1.2.3. Desarrollo de las configuraciones

2.1.2.3.1. Archivo clients.conf

En la Fig. 35 Se muestra un ejemplo de configuración de un cliente para el Servidor Federado Ecuador el cual detalla la dirección IP del servidor cliente y una clave que será compartida. Los clientes pueden ser Servidores Radius Local a nivel nacional y Servidores Radius Confederados que son parte del servicio de movilidad de EDUROAM.

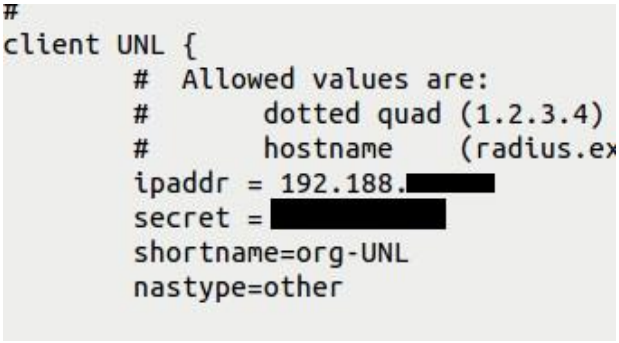


Figura 35. Archivo clients.conf

2.1.2.3.2. Archivo proxy.conf

En la Fig. 36 se muestra el bloque donde se especifica que los usuarios que posean el realm (dominio) unl.edu.ec y deseen conectarse desde alguna otra institución será redireccionados al Servidor Local Eduroam UNL.

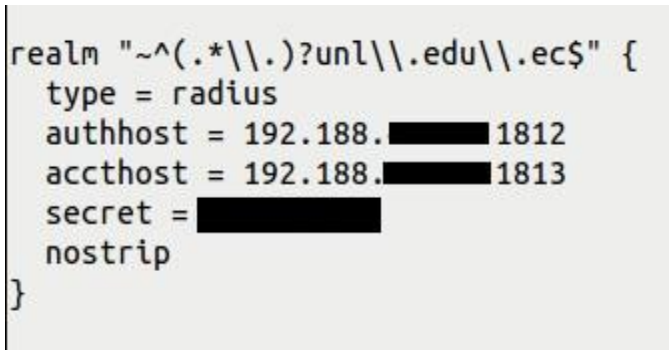


Figura 36. Bloque del Servidor Federado que redirecciona al Servidor Local

2.1.3.Pruebas a los servidores RADIUS

Las pruebas a los servidores RADIUS se realizaron mediante la utilidad **radtest,** comando con el que se consulta al servidor RADIUS. Los parámetros que conforman su sintaxis son:

- ✓ ***radtest usuario contraseña radius-server nas-port-number secret***

- **Usuario:** será el usuario que se desea comprobar la consulta al servidor RADIUS.
- **Contraseña:** será la contraseña del usuario.
- **Radius-server:** IP o nombre del servidor RADIUS
- **Nas-port-number:** será el número del puerto nas
- **Secret:** será la contraseña compartida con el servidor RADIUS para realizar las consultas

2.1.3.1. Pruebas al servidor RADIUS Local y al servidor RADIUS Federado

Para comprobar el funcionamiento de los servidores implementados se estableció varios escenarios de prueba con usuarios definidos.

- **Para evidenciar conexión con un usuario Local:** se ejecuta la línea de comando que se muestra a continuación y cuyo su resultado se puede apreciar en la Fig. 37.

  radtest jfcastillo@unl.edu.ec 1104742703 ftlr.cedia.org.ec 0 F3dera.UNL-EC

```
root@eduroam:~# radtest jfcastillo@unl.edu.ec 1104742703 ftlr.cedia.org.ec 0 F3dera.UNL-EC
Sending Access-Request of id 126 to 190.15.132.27 port 1812
        User-Name = "jfcastillo@unl.edu.ec"
        User-Password = "1104742703"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
rad_recv: Access-Accept packet from host 190.15.132.27 port 1812, id=126, length=43
```

Figura 37. Prueba con usuario local mediante radtest

- **Para evidenciar conexión con un usuario Nacional:** se ejecuta la línea de comando que se muestra a continuación y cuyo su resultado se puede apreciar en la Fig. 38.

  radtest test@ucuenca.edu.ec testecuador ftlr.cedia.org.ec 0 F3dera.UNL-EC

```
root@eduroam:~# radtest test@ucuenca.edu.ec testecuador ftlr.cedia.org.ec 0 F3dera.UNL-EC
Sending Access-Request of id 17 to 190.15.132.27 port 1812
        User-Name = "test@ucuenca.edu.ec"
        User-Password = "testecuador"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
rad_recv: Access-Reject packet from host 190.15.132.27 port 1812, id=17, length=20
```

Figura 38. Prueba con usuario nacional mediante radtest

- **Para evidenciar conexión con un usuario a nivel de Latinoamérica:** se ejecuta la línea de comando que se muestra a continuación y cuyo su resultado se puede apreciar en la Fig. 39.

  radtest raap@inictel-uni.edu.pe inictel ftlr.cedia.org.ec 0 F3dera.UNL-EC

```
root@eduroam:~# radtest raap@inictel-uni.edu.pe inictel ftlr.cedia.org.ec 0 F3dera.UNL-EC
Sending Access-Request of id 241 to 190.15.132.27 port 1812
        User-Name = "raap@inictel-uni.edu.pe"
        User-Password = "inictel"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
rad_recv: Access-Accept packet from host 190.15.132.27 port 1812, id=241, length=20
```

Figura 39. Prueba con usuario latinoamericano mediante radtest

- **Para evidenciar conexión con un usuario Europeo:** se ejecuta la línea de comando que se muestra a continuación y cuyo su resultado se puede apreciar en la Fig. 40.

  radtest testraap@test.rediris.es A7D0AB41 ftlr.cedia.org.ec 0 F3dera.UNL-EC

```
root@eduroam:~# radtest testraap@test.rediris.es A7D0AB41 ftlr.cedia.org.ec 0 F3dera.UNL-EC
Sending Access-Request of id 89 to 190.15.132.27 port 1812
        User-Name = "testraap@test.rediris.es"
        User-Password = "A7D0AB41"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
rad_recv: Access-Accept packet from host 190.15.132.27 port 1812, id=89, length=46
```

Figura 40. Prueba con usuario europeo mediante radtest

2.1.4. Ente encargado del servicio de movilidad a nivel nacional, CEDIA.

Una vez realizadas las configuraciones del servidor Radius Federado Ecuador de prueba en la Universidad Nacional de Loja se determina por disposición del responsable del servicio de movilidad EDUROAM en Latinoamericana, que el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA) sea el encargado de difundir el servicio a nivel nacional, montando el Servidor Radius Federado para Ecuador por lo cual la UNL procede a enlazarse con dicho servidor.

2.1.4.1. Certificados emitidos por CEDIA

Por considerarse a CEDIA el encargado de difundir Eduroam a nivel Nacional, toma el papel de Autoridad Certificadora, por tal razón es el único ente encargado de emitir los diferentes certificados a las instituciones que se adhieran al proyecto. En el caso particular y siguiendo el estándar, emite a la UNL los siguientes certificados: llave pública del CA, llave privada y llave pública del Radius Local Eduroam.

2.2. Servidor LDAP

2.2.1. Análisis de métodos de autenticación de conectividad móvil

Disponer de un método de autenticación fácil y ligero se consolida como una estrategia actual, de manera especial en las organizaciones que poseen varios servicios web y grandes cantidades de usuarios con el firme propósito de reducir costos y facilitar la administración. Además se debe cumplir los requerimientos de calidad del servicio al usuario, innovando soluciones que permitan cumplir con estas expectativas.

Los directorios LDAP viene desde entonces a ser parte importante de esta infraestructura proporcionando un punto único de almacenamiento de la información para la autenticación de los diferentes servicios de red, que por sus características principales provee un acceso rápido de lectura, exploración y búsqueda de la información contenida.

Se ha creído conveniente llevar a cabo la propuesta de implementar un nuevo método de autenticación como lo es un Directorio LDAP para los usuarios que hacen uso del servicio de internet inalámbrico.

A continuación se plasma 3 razones principales:

- Con la finalidad de utilizar las nuevas tecnologías que nos ofrece el mundo actual
- Visionar en un futuro no muy lejano para la Universidad Nacional de Loja en lograr que todos los servicios web que presta la institución posean una arquitectura de autenticación centralizada.
- La iniciativa Eduroam propone en sus manuales de instalación como una alternativa de autenticación de Usuarios (ver anexo 2).

2.2.1.1. Proceso de autenticación LDAP

El servicio de un directorio LDAP se basa en una arquitectura cliente-servidor, donde uno o más servidores de LDAP contienen los datos que forman el árbol de directorio o base de datos troncal. Se usa para guardar toda clase de información.

Para poder acceder al servicio LDAP, un cliente debe primero solicitar autenticarse con sus credenciales de usuario ante un servicio. Luego debe consultarle al servidor de LDAP quien posee la información requerida si esa persona puede acceder al servicio solicitado, en la Fig. 41 se ilustra de mejor manera.

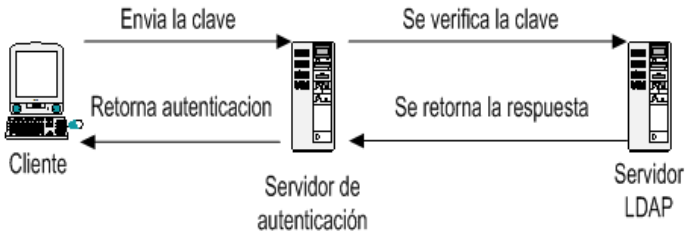


Figura 41. Proceso de autenticación LDAP

2.2.2.Comparativas de directorios LDAP

En la actualidad existen varias implementaciones de directorios LDAP, para lo cual se ha realizado una investigación previa.

- Se realizó una búsqueda en internet sobre directorios LDAP, para lo cual de concluye que las implementaciones más conocidas son: Novell Directory Service, Openldap, Iplanet Directory Service, Red Hat Directory Server, Apache Directory Server, Open DS y Microsoft Active Directory. En la tabla XXI se realiza una descripción de cada uno [1].

Tabla XXI. IMPLEMENTACIONES DE DIRECTORIOS LDAP

LDAP	DEFINICIÓN
Active Directory	Active Directory es el nombre utilizado por Microsoft (desde Windows 2000) como almacén centralizado de información de uno de sus dominios de administración. Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAP versión 3, lo cual permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc. Esta implementación viene distribuida por defecto con Windows Server 2008 R2
Novell Directory Services	También conocido como eDirectory es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Básicamente está compuesto por una base de datos jerárquica y orientada a objetos, que representa cada servidor, computadora, impresora, servicio, personas, etc. entre los cuales se crean permisos para el control de acceso, por medio de herencia. Esta implementación corre en diversas plataformas, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo.
IPlanet	Basado en la antigua implementación de Netscape, iPlanet se desarrolló cuando AOL adquirió Netscape Communications Corporation y luego conjuntamente con Sun Microsystems comercializaron software para servidores, entre ellos el iPlanet Directory Server, su implementación de LDAP. Actualmente se denomina Sun ONE Directory Server.

Red Hat Directory Server	Directory Server es un servidor basado en LDAP que centraliza configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas, así como información de control de acceso dentro de un sistema operativo independiente de la plataforma. Forma un repositorio central para la infraestructura de manejo de identidad, Red Hat Directory Server simplifica el manejo de usuarios, eliminando la redundancia de datos y automatizando su mantenimiento.
Apache Directory Server	Apache Directory Server (ApacheDS), es un servidor de directorio escrito completamente en Java por Alex Karasulu y disponible bajo la licencia de Apache Software, es compatible con LDAPv3 certificado por el Open Group, soporta otros protocolos de red tal como Kerberos y NTP, además provee procedimientos almacenados, triggers y vistas; características que están presente en las bases de datos relacionales pero que no estaban presentes en el mundo LDAP
Open DS	Basado en los estándares LDAPv3 y DSMLv2, OpenDS surgió como un proyecto interno de SUN, aunque posteriormente se puso a disposición de la comunidad. Está desarrollado en Java y precisa de un entorno de ejecución JRE (Java Runtime Environment) para funcionar. Es multiplataforma. La primera versión estable de Open DS fue liberada en julio de 2008
OpenLDAP	Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP. Tiene su propia licencia, la OpenLDAP Public License. Al ser un protocolo independiente de la plataforma, varias distribuciones GNU/Linux y BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS.

- En el link "http://bosque.udec.cl/~sram/manuals/informe.pdf ", publicado por Salvador Ramírez Flandes con la temática **Implementación de un Sistema de Directorios LDAP para la Universidad de Concepción**, realiza una comparativa comercial de los distintos software servidores LDAP que según su criterio son "**más conocidos y que por tanto tienen un mayor uso en la actualidad**" reflejada en la Tabla XXII:

Tabla XXII. COMPARACIÓN COMERCIAL DE SERVIDORES LDAP

SOFTWARE	COMERCIAL
OpenLDAP	No
Netscape Directory	Si
IBM eNetwork LDAP Directory	Si
Lotus Domino	Si
Novell Directory Services	Si
Microsoft Active Directory	Si

- En el sitio web informativo **El Pensamiento Blender**, " http://thoughtblender.info/2008/11/04/comparison-of-directory-ldap-servers/", expone de acuerdo a la experiencia el por qué utilizar solo dos implementaciones de una lista de contendientes, haciendo un análisis de acuerdo a ciertos requerimientos planteados.
    - ✓ OpenDS
    - ✓ OpenLDAP

2.2.2.1. Selección del directorio LDAP

Previo al estudio realizado en la sección anterior de las diferentes implementaciones de directorios LDAP, se determina que OpenLDAP es la mejor opción para el proceso de autenticación de usuarios por las siguientes razones:

- OpenLdap tiene mucha aceptación en el medio, de acuerdo a las publicaciones de los sitios web.
- Tiene bastante documentación en línea, además cuenta con su propia página de información y descarga (http://www.openldap.org/), debidamente respaldada por su comunidad.
- Posee una factibilidad adecuada, ya que cuenta con una herramienta de administración web para su manejo.
- Mediante Decreto Ejecutivo No. 1014 emitido el 10 de Abril de 2008, se dispone el uso de Software Libre en los sistemas y equipamientos informáticos de la Administración Pública de Ecuador. OpenLdap cumple con la disposición.
- Eduroam en su manual de instalación utiliza la implementación del directorio OpenLDAP.

2.2.3.Entorno de pruebas realizadas

Para realizar las pruebas de funcionalidad, la UTI (Unidad de Telecomunicaciones e Información) nos proporcionó un espacio en el BLADE HP PROLIANT BL460c G7 con tecnología KVM.

2.2.3.1. Hardware

En la Tabla XXIII se realiza una breve descripción del hardware utilizado en el entorno de pruebas para la instalación del servidor OpenLDAP.

Tabla XXIII. DESCRIPCIÓN HARDWARE

HARDWARE	DESCRIPCIÓN
Disco Duro	38GB
Memoria Ram	4GB
Tarjeta de Red	Ethernet 100 Mb/s

2.2.3.2. Software

En la tabla XXIV se realiza una breve descripción del software utilizado en el entorno de pruebas para la instalación del servidor OpenLDAP.

Tabla XXIV. DESCRIPCIÓN SOFTWARE

SOFTWARE	DESCRIPCIÓN
Sistema Operativo	Debian 6.0.6
Kernel	Linux 2.6.32-5-amd64
OpenLdap	Versión 3

2.2.3.3. Estructura del directorio UNL

En la Fig. 42 se muestra un esquema de la estructura del directorio UNL para su creación en el servidor LDAP. El diseño fue planteado en conjunto con el representante del departamento de Desarrollo de Software de la Unidad de Telecomunicaciones e Información**.**

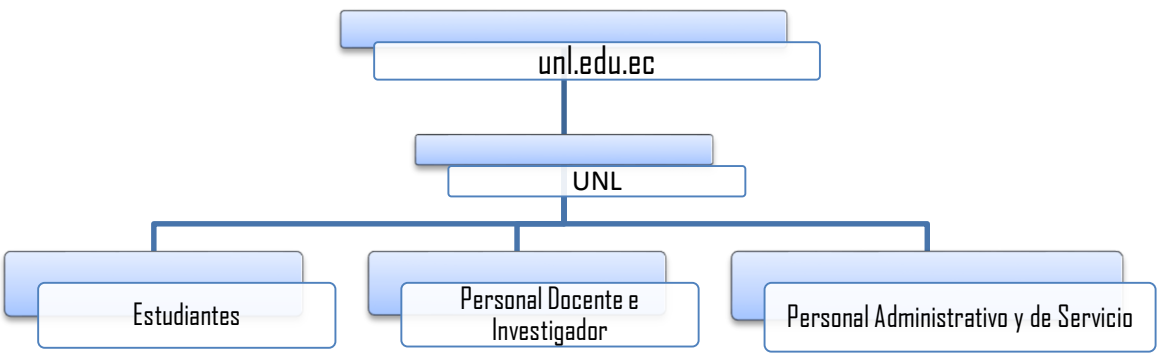


Figura 42. Esquema del directorio UNL

2.2.3.4. Creación del DN base del directorio UNL

El directorio raíz o DN base del directorio LDAP viene hacer el principal o punto de partida, del cual se subdividen grupos o subdirectorios. En el caso de la Universidad Nacional de Loja está dado por: unl.edu.ec (como se muestra en la Fig. 42). Este se lo crea al momento de realizar la configuración del servidor, como se muestra en la Fig. 43

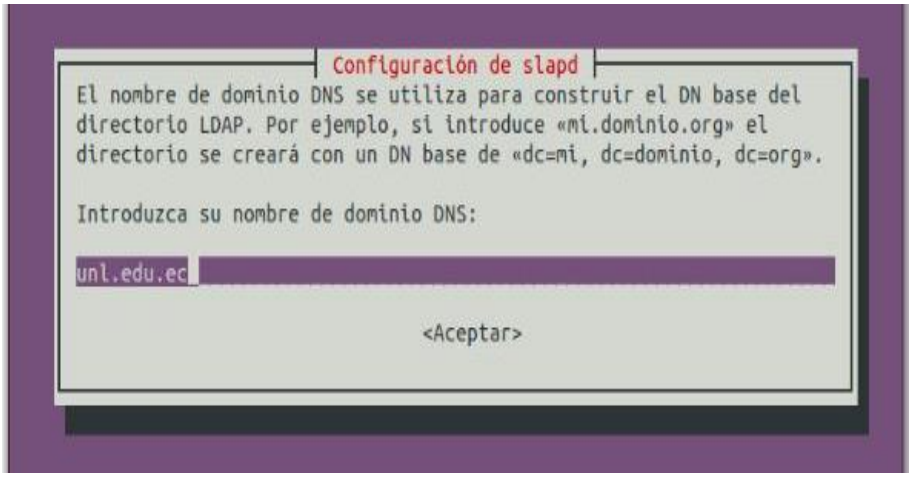


Figura 43. Creación del Directorio Raíz

2.2.3.5. Enlazar Servidor Radius con LDAP

Para que el servidor Radius Local Eduroam UNL consulte las credenciales de los usuarios admitidos para utilizar la red Eduroam en necesario permitir el acceso mediante la dirección IP del servidor LDAP, permisos de administrador y el nombre de dominio base del directorio, en la Fig. 44 se muestra la configuración. Estos cambios se los realiza en el servidor Radius Local Eduroam UNL, en el directorio /etc/freeradius/modules/ldap.

```
ldap {
        #
        #  Note that this needs to match the name in the LDAP
        #  server certificate, if you're using ldaps.
        server = 172.16.[redacted]
        identity = "cn=admin,dc=unl,dc=edu,dc=ec"
        password = [redacted]
        basedn = "ou=UNL,dc=unl,dc=edu,dc=ec"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        #base_filter = "(objectclass=radiusprofile)"
```

Figura 44. Enlace Radius con LDAP

2.2.3.6. Administración Web del LDAP

Una de las características principales del OpenLDAP, permite administrarlo de manera medianamente fácil a través de un navegador web. Para esto se ha instalado PHPLDAPAdmin que ayuda a simplificar el trabajo, en la Fig. 45 se visualiza la pantalla principal.

PHPLDAPAdmin es una aplicación que permite administrar el contenido de un servicio de directorios, específicamente de OpenLDAP. Está desarrollado en PHP.

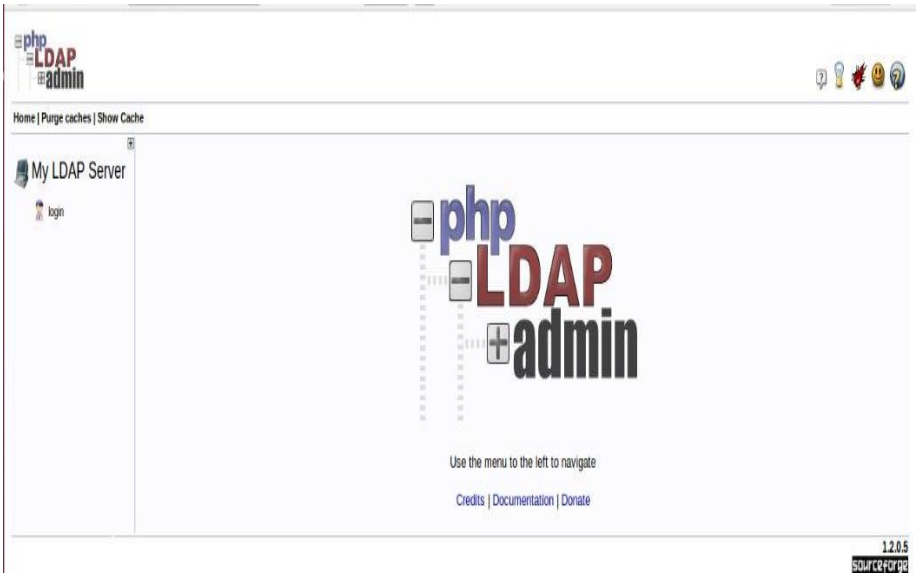


Figura 45. Interfaz Principal PHPLDAPAdmin

2.2.3.6.1. Conexión al Servidor LDAP

Para que PHPLDAPAdmin pueda establecer conexión con el servidor LDAP es importante configurar el archivo ***config.php*** del administrador web. Este proceso se lo realiza de una manera sencilla.

En la Fig. 46 se muestra la configuración del archivo, en cual se edita la línea 283 ingresando el DN Base del directorio LDAP (**'dc=unl, dc=edu, dc=ec'**), de esta manera se concede los permisos para visualizar, editar, modificar y evaluar el contenido del directorio.

- **root@ldap: # /etc/phpldapadmin/config.php**

Figura 46. Archivo config.php

2.2.3.7. Schema y/o Esquema Usuarios UNL

Los esquemas y/o *schemas* definen el tipo de objetos (*objectClass*) que podemos utilizar en nuestro directorio, además definen el tipo de atributos que podemos usar así como las reglas de sintaxis para cada uno de estos atributos.

Si fuera el caso que los esquemas que vienen instalados por defecto no cumplen con las exigencias del administrador, el LDAP posee la flexibilidad de implementar tus propios esquemas.

Cumpliendo con una petición por parte del responsable de Desarrollo de Software de incluir nuevos atributos al Servidor LDAP, se procedió a crear un nuevo esquema con los atributos sugeridos (ver anexo 3). El archivo debe estar guardado en formato schema (.schema).

2.2.3.8. Atributos del Usuario

Los atributos definidos por cada uno de los usuarios de Universidad Nacional de Loja se detallan en la Tabla XXV. Estos atributos son los más generales es decir que cualquier usuario de la institución puede o no cumplirlos.

Tabla XXV. ATRIBUTOS DE LOS USUARIOS UNL

DATOS A CARGAR	
DATOS OBLIGATORIOS	**DATOS NO OBLIGATORIOS**
• Usuario	• Dirección
• Contraseña	• Provincia
• Cédula/DNI	• Parroquia
• Nombres	• Carnet Conadis
• Apellidos	• Tipo de Discapacidad
• Sexo	• Correo Personal
• País	
• Ciudad	
• Fecha de Nacimiento	
• Correo Institucional	

Cabe mencionar que se ha divido los datos en 2 grupos:

- ✓ **Datos Obligatorios:** Al momento de cargar un usuario si estos campos no están llenos, el servidor LDAP no lo sube al directorio
- ✓ **Datos no Obligatorios:** Cuando se carga un usuario se puede agregar o no los datos.

2.2.3.9. Crear Usuarios

Para proceder a crear los usuarios primero se obtuvo dos archivos en formato .cvs con datos personales correspondiente a estudiantes que están legalmente matriculados y de docentes que poseen nombramiento o están contratados, la información fue proporcionada por el Responsable de la sección de Desarrollo de Software de la Unidad de Telecomunicaciones e Información.

Se desarrolló un algoritmo en el lenguaje de programación java, que permita de forma automática crear los usuarios en base a los nombres y apellidos. La lógica que se ejecuta en el algoritmo es el siguiente: obtener la inicial del primer y segundo nombre, el primer apellido y la inicial del segundo apellido, a raíz de esa información unirla para darle forma al usuario.

En el anexo 4 se muestra el código utilizado que vinculado con la Fig. 47 se visualiza los datos obligatorios en la que incluye el usuario una vez creado.

	A	B	C	D	E	F	G	H	I	J
1	USUARIO	CEDULA	NOMBRES	1ER APELLIDO	2DO APELLIDO	SEXO	PAIS	CIUDAD	F. NACIMIENTO	CORREO INSTITUCIONAL
2	aaabadp	1105054256	Alonso Antonio	Abad	Pena	masculino	Ecuador	Gonzanama	03/12/1990	aaabadp@unl.edu.ec
3	aaaguilam	1104649627	Alexander Anibal	Aguilar	Naranjo	masculino	Ecuador	Loja	02/04/1989	aaaguilam@unl.edu.ec
4	aaalulimac	1105033425	Adrian Arturo	Alulima	Cuenca	masculino	Ecuador	Loja	27/03/1993	aaalulimac@unl.edu.ec
5	aaalvarezj	1104106792	Armando Alexander	Alvarez	Jimenez	masculino	Ecuador	Gonzanama	01/04/1992	aaalvarezj@unl.edu.ec
6	aaamayg	1104111479	Andrea Alexandra	Amay	Guachizaca	femenino	Ecuador	Loja	21/05/1993	aaamayg@unl.edu.ec
7	aaarevalos	1150008918	Alexandra De Los Angeles	Arevalo	Soto	femenino	Ecuador	Loja	25/07/1994	aaarevalos@unl.edu.ec
8	aaariasj	1104865710	Andrea Alejandra	Arias	Jaramillo	femenino	Ecuador	Catamayo	02/02/1990	aaariasj@unl.edu.ec
9	aaarmijoa	1716743164	Ana Angelica	Armijo	Alvarado	femenino	Ecuador	QUITO	26/12/1993	aaarmijoa@unl.edu.ec
10	aaarmijosg	1900335165	Anibal Augusto	Armijos	Gonzalez	masculino	Ecuador	Yantzaza	30/09/2976	aaarmijosg@unl.edu.ec
11	aaarmijoss	1104533474	Andrea Anabel	Armijos	Sarango	femenino	Ecuador	loja	13/07/1991	aaarmijoss@unl.edu.ec
12	aaastudillov	1716565443	Andres Antonio	Astudillo	Villalta	masculino	Ecuador	QUITO	07/01/1980	aaastudillov@unl.edu.ec
13	aabenitezc	1900634617	Angel Arcenio	Benitez	Chamba	masculino	Ecuador	Loja	02/07/1988	aabenitezc@unl.edu.ec
14	aabenitezc02	1105044646	Andrea Alexandra	Benitez	Correa	femenino	Ecuador	Loja	18/12/1990	aabenitezc02@unl.edu.ec
15	aabustamantec	1105434003	Andrea Alexandra	Bustamante	Castillo	femenino	Ecuador	Loja	02/09/1993	aabustamantec@unl.edu.ec
16	aacalvaj	1105117319	Anabel De Los Angeles	Calva	Jimenez	femenino	Ecuador	Calvas	25/01/1991	aacalvaj@unl.edu.ec
17	aacarriona	1104403413	Angel Andres	Carrion	Aguilar	masculino	Ecuador	Loja	01/01/1992	aacarriona@unl.edu.ec
18	aacasierrac	1105015380	Angel Alberto	Casierra	Cardenaz	masculino	Ecuador	puyango	27/05/1992	aacasierrac@unl.edu.ec
19	aachambau	1106001157	Alexandra Abigail	Chamba	Uchuari	femenino	Ecuador	Loja	16/01/1994	aachambau@unl.edu.ec
20	aacondoloa	1105611196	Adrian Alejandro	Condolo	Aguirre	masculino	Ecuador	calvas	18/11/1991	aacondoloa@unl.edu.ec

Figura 47. Usuarios creados

2.2.3.10. Cargar usuarios

Al momento de cargar uno o varios usuarios al servidor LDAP, estos deben estar en un archivo formato LDIF (Data Interchange Format), ya que es el único formato que acepta para la importación y exportación de datos.

Hay que recordar que los usuarios creados están almacenados en un archivo .csv como se ve en la Fig. 47 para poder cargarlos al servidor, se ejecutó un script donde permite convertir un archivo en formato .csv a .ldif, en el anexo 5 se visualiza el código.

Por cada usuario que se pretende cargar, este siempre debe constar con la información del grupo o subdirectorio donde va hacer almacenado, datos en si del usuario y los objetos que son referenciados para hacer uso de sus atributos, en la Fig. 48 se muestra un ejemplo de usuario de prueba listo para cargarlo en el servidor.

Cabe indicar que se cargaron total de 9673 usuarios, de los cuales 9163 corresponden a estudiantes y 510 a docentes, estando en la facultad de acceder al servicio de internet mediante la red eduroam.

Figura 48. Esquema de un Usuario en formato LDIF

3. Fase 3: Pruebas de movilidad

3.1. Escenario real de pruebas

Para realizar las pruebas de movilidad, el servicio EDUROAM se pone en funcionamiento sobre la Red Mallada (Mesh), la cual esta implementada con equipos Access Point (AP's) Cisco Aironet 1552E, cuyas especificaciones señaladas anteriormente cumplen con los requerimientos del proyecto. Los AP's autenticarán a aquellos dispositivos móviles que intenten utilizar la red EDUROAM tales como portátiles, smartphones y tablets con sistemas operativos como Microsoft Windows, Linux, Android y Mac; los mismos que al solicitar el servicio deben ingresar sus credenciales determinadas por usuario y contraseña, las mismas serán consultadas al servidor LDAP para su validación.

3.1.1. Selección de la zona de prueba

Toda implementación informática supone una fase de pruebas que presente evidencia fidedigna de la operatividad, funcionalidad y eficiencia del sistema que va a someterse a dicha fase. Por tal motivo se determina que para el proyecto EDUROAM se toma como zona de prueba el A.E.I.R.N.N.R por ser el área que forma profesionales en carreras tecnológicas se considera que tenga mayor aceptación. En la Fig. 49 se observa el área cuyos profesionales en formación colaborarán con la fase de pruebas.

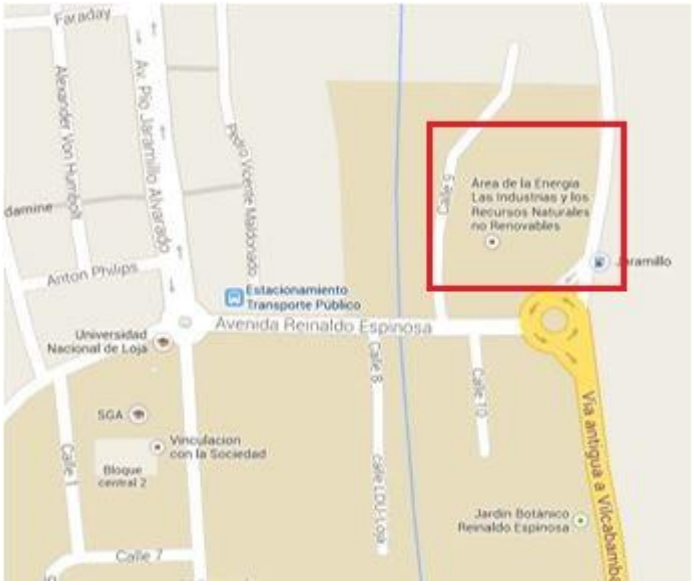


Figura 49. Área determinada para la fase de prueba

3.2. Topología de la red inalámbrica EDUROAM

En la Fig. 50 se presenta como está estructurada la red inalámbrica Eduroam, el cual a través de Access Point Aironet intercepta la solicitud que es enviada al Wireless Lan Controller, que a su vez reenvía al Servidor Radius quien es el encargado de aceptar o rechazar la solicitud.

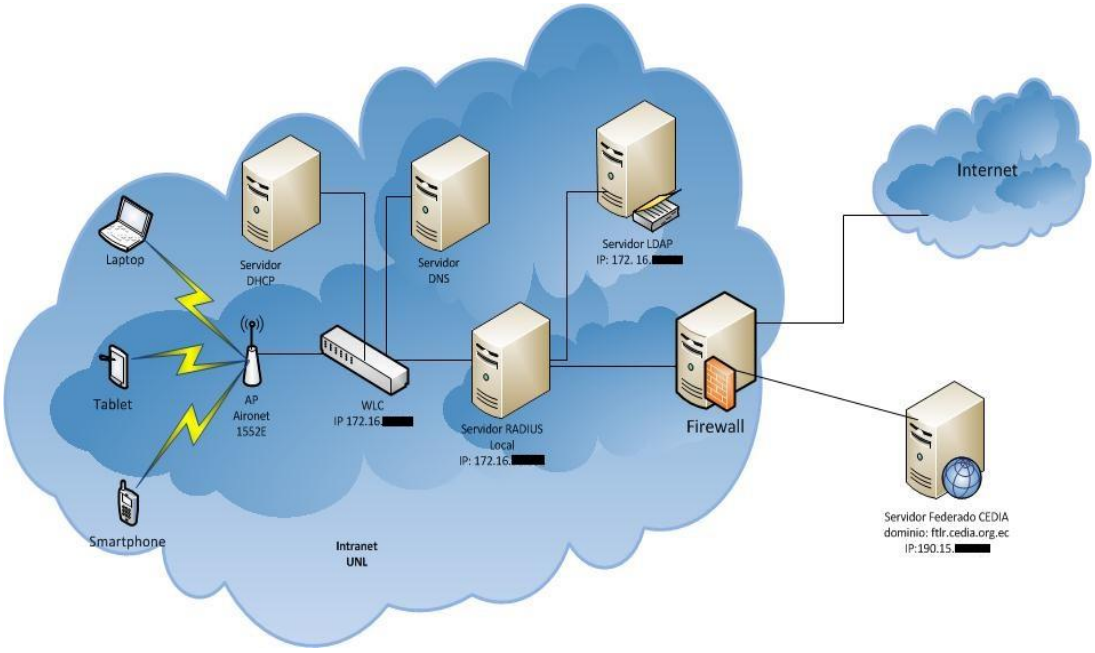


Figura 50. Topología de la red inalámbrica EDUROAM

3.3. Pruebas de conectividad

3.3.1. Pruebas de conexiones simultáneas al servidor Radius EDUROAM

Para las pruebas de conexiones simultáneas se hizo uso del software RADIUS TEST CLIENT, el cual es un simulador de solicitudes de acceso simultáneo, en la Fig. 51 se visualiza la configuración.

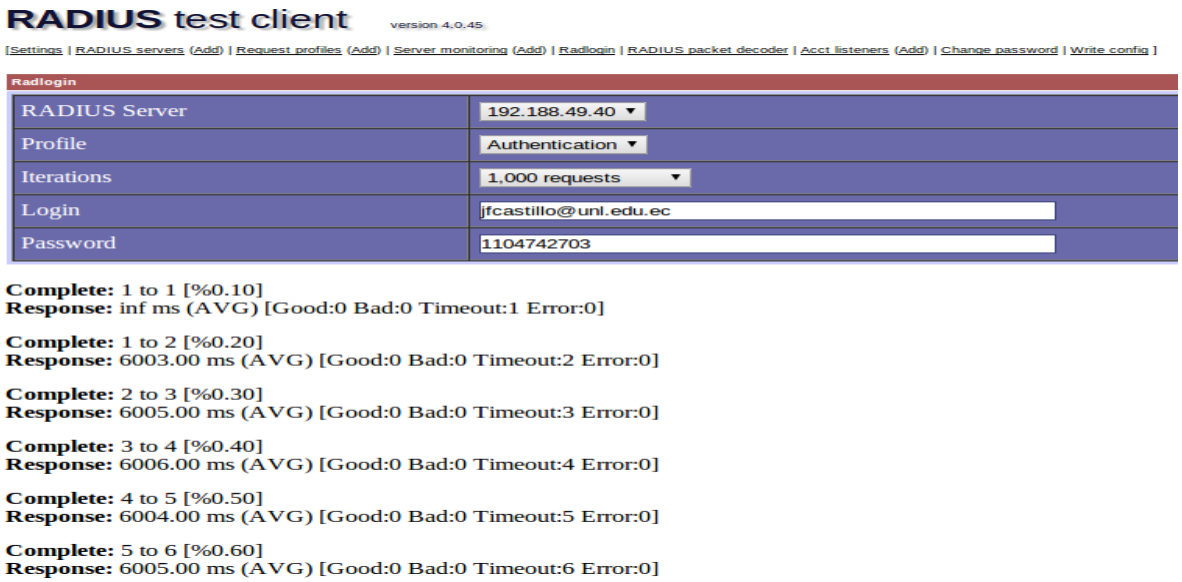


Figura 51. Configuración de RADIUS test client

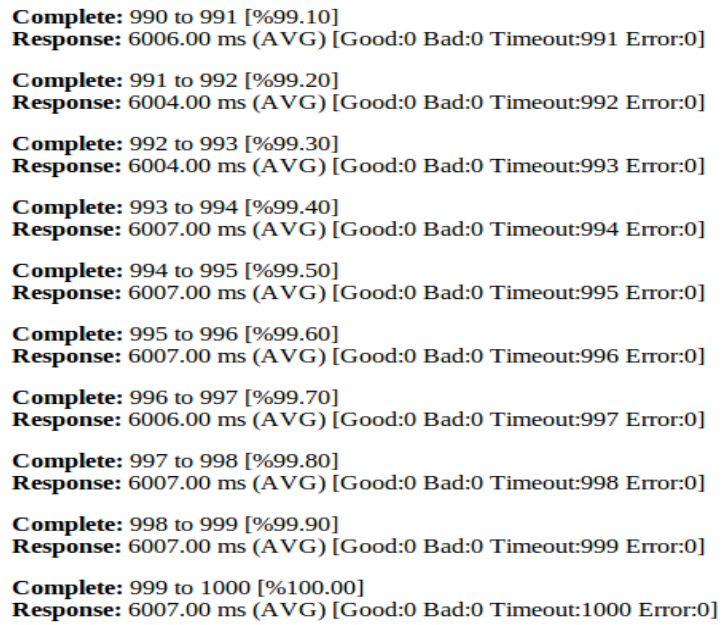


Figura 52. RADIUS test client en ejecución de 1000 solicitudes

Al enviar 1000 solicitudes simultáneas al Radius Local Eduroam las resuelve en un promedio de 6007.00ms, como se muestra en la Fig. 52.

3.3.2. Plataformas evaluadas con el servicio EDUROAM

Las plataformas a ser evaluadas con el servicio de movilidad son:

- Windows/Windows 7
- GNU Linux/Ubuntu
- Android
- Mac OS X/Marverick

Para evaluar el funcionamiento de Eduroam en las plataformas antes mencionadas, se determina realizar el proceso de autenticación con un usuario de prueba: **eduroam.ec@unl.edu.ec** el mismo que esta agregado en el servidor LDAP, dentro del grupo Personal Administrativo y de Servicios como se muestra en la Fig. 53.

Figura 53. Usuario de prueba agregado en el servidor LDAP

3.3.2.1. GNU Linux/Ubuntu

Para proceder a conectarse a la red eduroam en GNU Linux, es necesario tener la llave pública (certificado) del CA (Autoridad Certificadora), que se lo descarga del link http://www.eduroam.ec/certs/ca_eduroam_ec.pem. Para evidenciar el establecimiento de conexión, en la Fig. 54 podemos ver el SSID Eduroam, así como la dirección IP asignada, además con una captura del daloRADIUS se confirma el proceso de autenticación el cual registra la dirección IP, junto con el usuario que hizo petición del servicio como se ve en la Fig. 55.

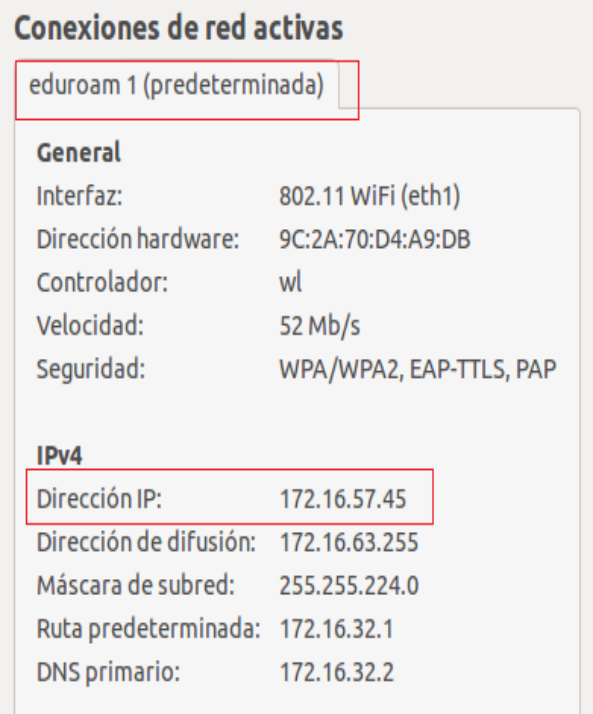


Figura 54. SSID utilizado y dirección asignada en la red eduroam en Ubuntu

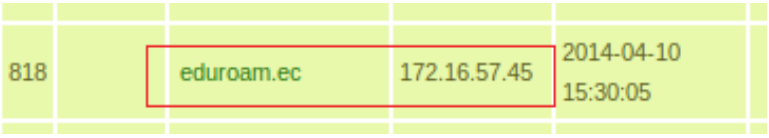


Figura 55. Registro del usuario en daloRADIUS

3.3.2.2. Windows/Windows 7

Para tener acceso a eduroam a través del S.O Windows, es necesario tener instalada la llave pública (certificado) del CA (Autoridad Certificadora), que se lo descarga del sitio oficial de eduroam https://cat.eduroam.org/ el cual es un archivo ejecutable. Para comprobar la conexión en Windows 7 en la Fig. 56 se muestra la dirección IP, parámetros de red asignados y el SSID eduroam, además para corroborar la autenticación en la Fig. 57 tomada del daloRADIUS se visualiza el usuario junto con la dirección IP asignada.

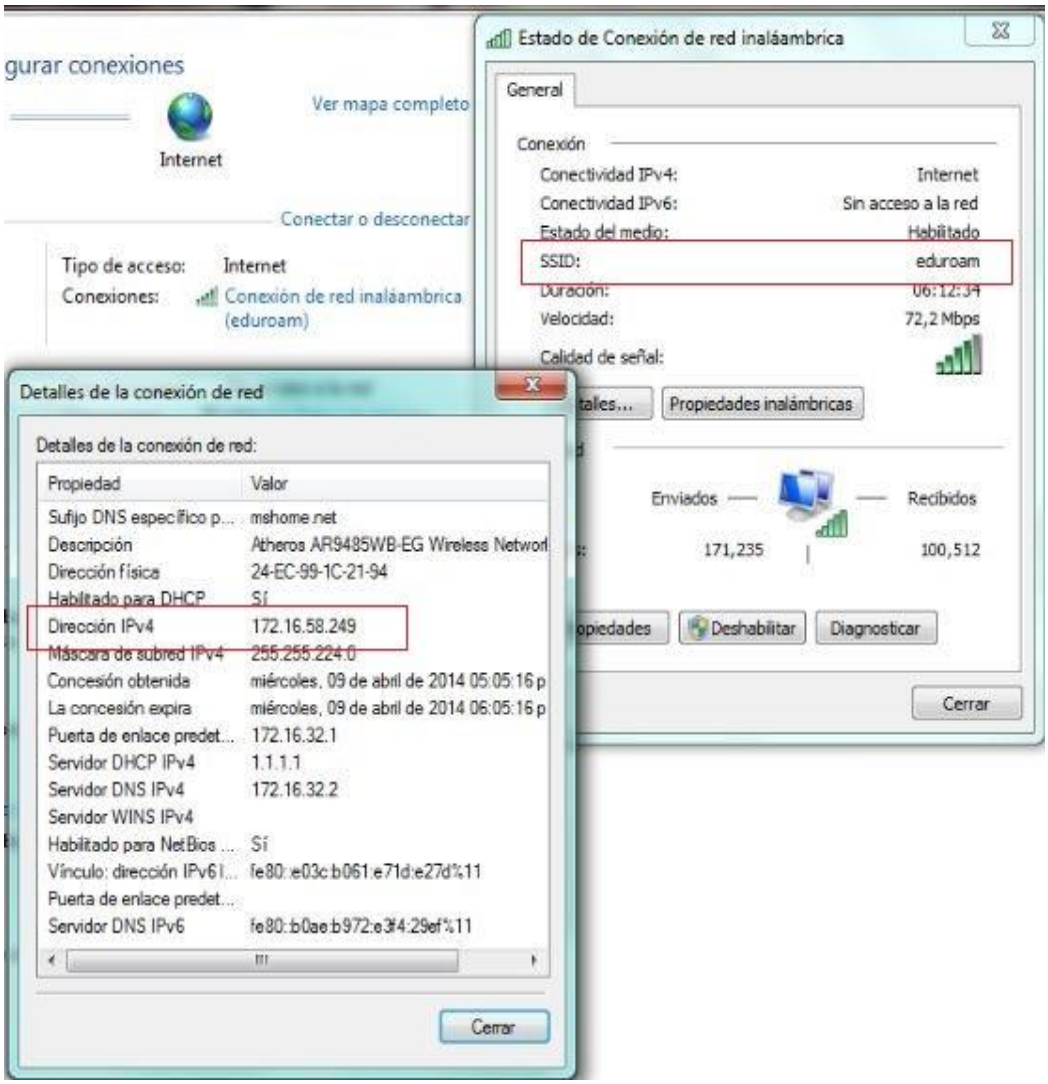


Figura 56. SSID utilizado y dirección asignada en la red eduroam en Windows

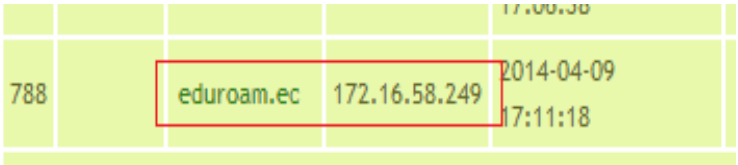


Figura 57. Registro del usuario en daloRADIUS

3.3.2.3. Android

Para establecer conexión desde dispositivos Android sean Smartphone o Tablet, el proceso de conectividad es más sencillo, donde se debe configurar algunos parámetros importantes y obligatorios, como son: método EAP, autenticación de fase 2, identidad y

contraseña. Se justifica la autenticación realizando una captura de los parámetros de red asignados en el dispositivo, donde se evidencia principalmente el SSID Eduroam y la dirección IP, como se muestra en la Fig. 59, además con la Fig. 60 obtenida del daloRADIUS se ratifica el proceso de validación.

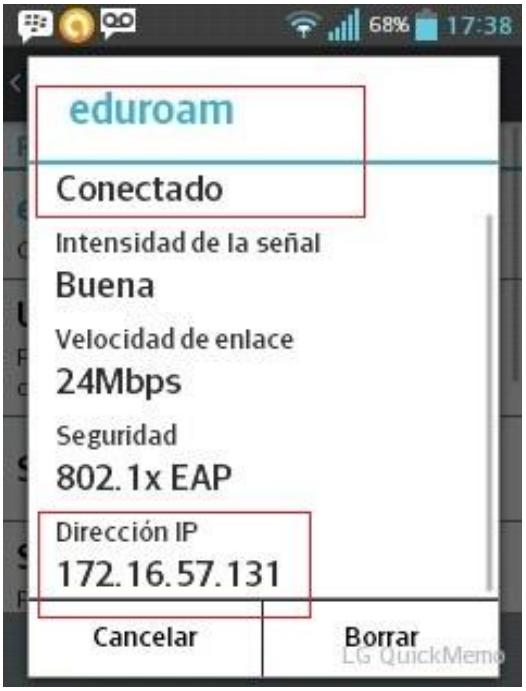


Figura 58. SSID utilizado y dirección asignada en la red eduroam en Android

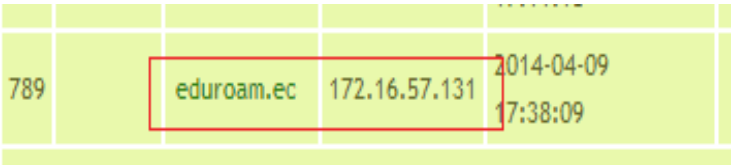


Figura 59. Registro del usuario en daloRADIUS

3.3.2.4. Mac OS X/Marverick

Como evidencia del proceso de autenticación en sistemas operativos Mac OS X, se hizo pruebas en la plataforma Marverick. En la Fig. 60 se muestra la dirección IP asignada y el SSID Eduroam, además se obtiene una captura del DaloRadius donde se comprueba su validación a través de dirección IP, como se visualiza en la Fig. 61.

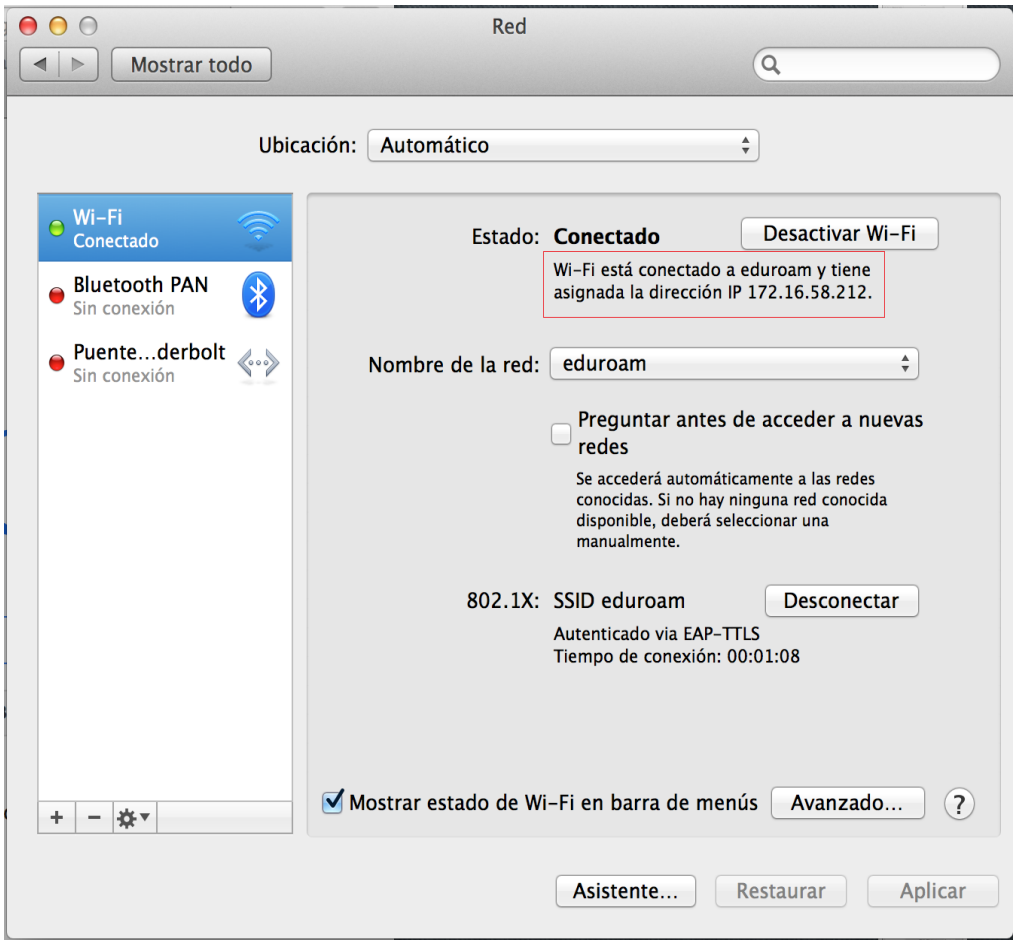


Figura 60. SSID utilizado y dirección asignada en la red eduroam en Mac OS X Mavericks

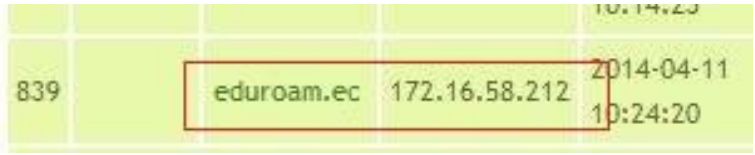


Figura 61. Registro del usuario en daloRADIUS

3.3.2.5. Apple iOS/ iPhone 5

Para evidenciar la autenticación a Eduroam con dispositivos móviles Apple iOS, se realizó pruebas de conexión con la ultimas versión hasta la fecha que corresponde a iPhone 5. En la Fig. 62 se visualiza que está conectado al SSID Eduroam con los parámetros de red asignados, haciendo hincapié en la IP, para ratificar el proceso en la Fig. 63 obtenida del DaloRadius se visualiza la IP asignada que hace correspondencia con el dispositivo.

Figura 62. SSID utilizado y dirección asignada en la red eduroam en iPhone

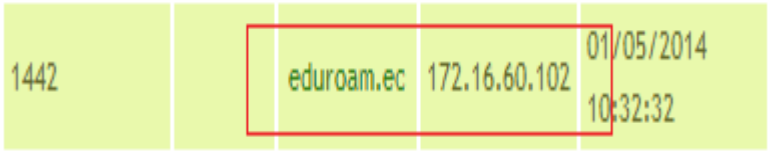


Figura 63. Registro del usuario en daloRADIUS

3.3.3. Manuales de configuración e instalación en las Plataforma Evaluadas

Para conocer más detallado el proceso de configuración en dispositivos móviles android y GNU Linux, así como el proceso de instalación en dispositivos Windows y Mac OS X, se encuentra disponible los manuales en la página oficial de Eduroam de la Universidad Nacional de Loja http://eduroam.unl.edu.ec/ ver anexo 6.

3.3.4.Información de usuarios conectados al SSID eduroam visualizada con DALOradius

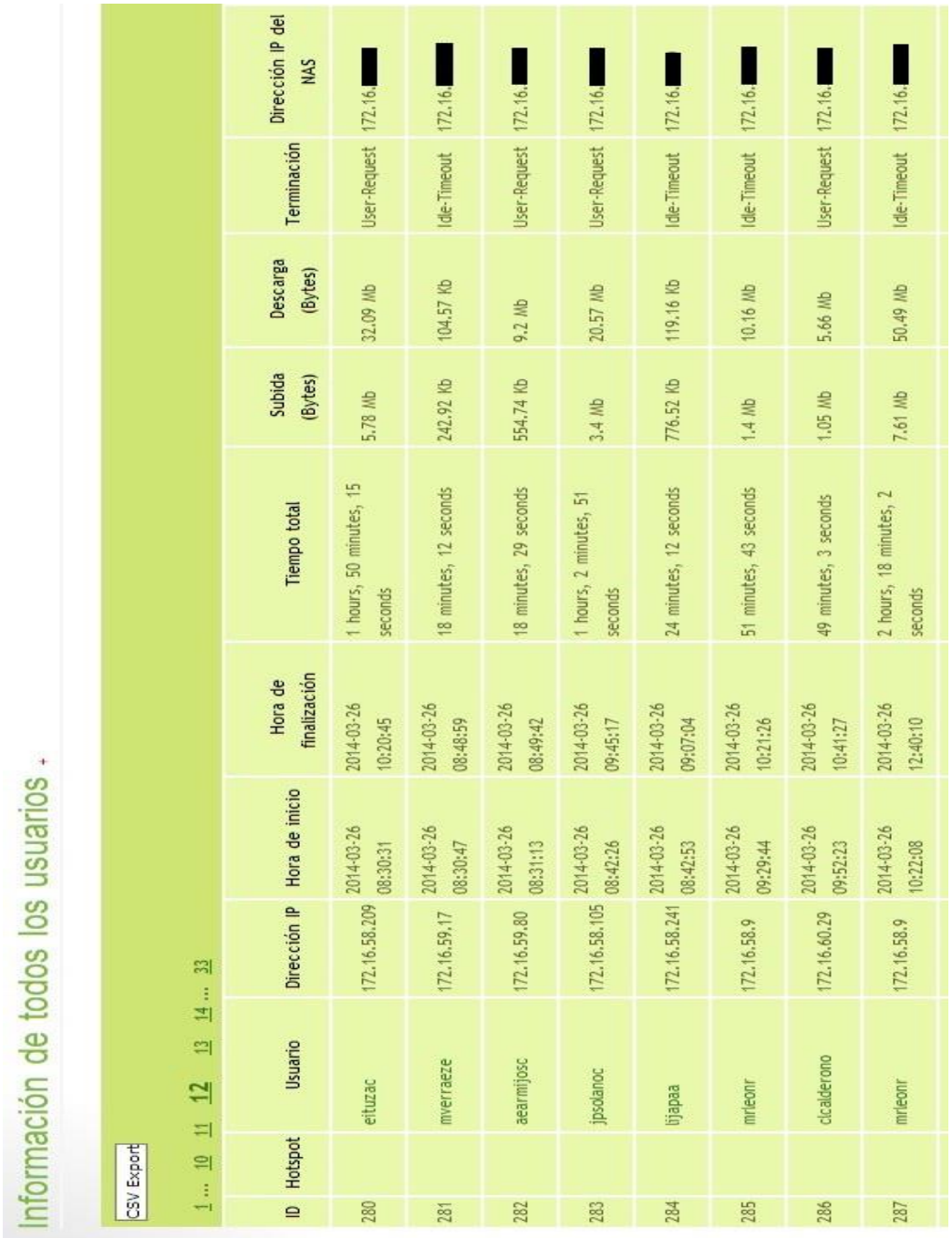
3.3.4.1. Usuarios en Línea

La herramienta web de administración DaloRadius muestra los usuarios en línea que están conectados en ese momento al Servidor RADIUS EDUROAM. La información que proporciona de cada usuario es: Usuario (dato obtenido del LDAP), Dirección IP, Dirección MAC, Hora de Inicio, Tiempo Total y Total de Mb de subida/bajada, como se muestra en la Fig. 64.

Figura 64. Usuarios en línea conectados en ese momento

3.3.4.2. Información de todos los usuarios

La información de todos los usuarios es el registro de todos los accesos realizados desde que estuvo disponible la red inalámbrica Eduroam. Los datos que se van almacenando por cada acceso es: usuario, dirección IP, hora de inicio, hora de finalización, tiempo total, subida (bytes) y descargas (bytes), como se muestra en la Fig. 65.



Información de todos los usuarios +

CSV Export

1 ... 10 11 12 13 14 ... 33

ID	Hotspot	Usuario	Dirección IP	Hora de inicio	Hora de finalización	Tiempo total	Subida (Bytes)	Descarga (Bytes)	Terminación	Dirección IP del NAS
280		eituzac	172.16.58.209	2014-03-26 08:30:31	2014-03-26 10:20:45	1 hours, 50 minutes, 15 seconds	5.78 Mb	32.09 Mb	User-Request	172.16.[redacted]
281		mverraeze	172.16.59.17	2014-03-26 08:30:47	2014-03-26 08:48:59	18 minutes, 12 seconds	242.92 Kb	104.57 Kb	Idle-Timeout	172.16.[redacted]
282		aearmijosc	172.16.59.80	2014-03-26 08:31:13	2014-03-26 08:49:42	18 minutes, 29 seconds	554.74 Kb	9.2 Mb	User-Request	172.16.[redacted]
283		jpsolanoc	172.16.58.105	2014-03-26 08:42:26	2014-03-26 09:45:17	1 hours, 2 minutes, 51 seconds	3.4 Mb	20.57 Mb	User-Request	172.16.[redacted]
284		tijapaa	172.16.58.241	2014-03-26 08:42:53	2014-03-26 09:07:04	24 minutes, 12 seconds	776.52 Kb	119.16 Kb	Idle-Timeout	172.16.[redacted]
285		mrleonr	172.16.58.9	2014-03-26 09:29:44	2014-03-26 10:21:26	51 minutes, 43 seconds	1.4 Mb	10.16 Mb	Idle-Timeout	172.16.[redacted]
286		cicalderono	172.16.60.29	2014-03-26 09:52:23	2014-03-26 10:41:27	49 minutes, 3 seconds	1.05 Mb	5.66 Mb	User-Request	172.16.[redacted]
287		mrleonr	172.16.58.9	2014-03-26 10:22:08	2014-03-26 12:40:10	2 hours, 18 minutes, 2 seconds	7.61 Mb	50.49 Mb	Idle-Timeout	172.16.[redacted]

Figura 65. Usuarios registrados desde la disponibilidad de Eduroam

3.3.4.3. Accesos Totales

Para evaluar el funcionamiento de la red inalámbrica eduroam, se procede a tabular los datos obtenidos durante los meses de febrero, marzo y abril, cada mes detallado por semanas.

En el mes de febrero se logró evidenciar un total de 140 accesos registrados, de los cuales 138 fueron acceso realizado por usuarios que forman parte de la Universidad Nacional de Loja y 2 accesos de usuarios itinerantes, es decir usuarios que no forman parte de la institución, ver Tabla XXVI. Cabe indicar que fue el primer mes donde se realizó un proceso de divulgación del servicio de red eduroam en el AEIRNNR para evaluar su funcionamiento.

Tabla XXVI NÚMERO DE ACCESO TOTAL EN EL MES DE FEBRERO

NRO. DE ACCESOS		
FEBRERO	**USUARIOS LOCALES**	**USUARIOS ITINERANTES**
Lunes 03 – Viernes 07	65	0
Lunes 10 – Viernes 14	45	0
Lunes 17 – Viernes 21	21	0
Lunes 24 – Viernes 28	7	2
TOTAL PARCIAL	138	2
TOTAL	**140**	

Para el mes de marzo se registra un total de 340 accesos a la red inalámbrica Eduroam, todos realizados por usuarios que pertenecen a la universidad, superando lo del mes anterior, se logra dando a conocer a los estudiantes del AEIRNNR la disponibilidad de Eduroam en la institución, ver Tabla XXVII.

Tabla XXVII NÚMERO DE ACCESO TOTAL EN EL MES DE MARZO

NRO DE ACCESOS		
MARZO	**USUARIOS LOCALES**	**USUARIOS ITINERANTES**
Lunes 03 – Viernes 07	0	0
Lunes 10 – Viernes 14	5	0
Lunes 17 – Viernes 21	68	0
Lunes 24 – Lunes 31	267	0
TOTAL PARCIAL	340	0
TOTAL	**340**	

Para las dos primeras semanas de abril se evidencia un total de 239 accesos, de los cuales 239 son de usuarios locales y 50 de usuarios itinerantes, ver Tabla XXVIII.

Tabla XXVIII NÚMERO DE ACCESO TOTAL EN EL MES DE ABRIL

NRO DE ACCESOS		
ABRIL	**USUARIOS LOCALES**	**USUARIOS ITINERANTES**
Martes 01 – Viernes 04	199	40
Lunes 07 – Martes 08	40	10
TOTAL PARCIAL	239	50
TOTAL	**289**	

Utilizando el menú Gráficos del DaloRadius se presenta mediante diagrama de barras, el total de accesos realizados durante el mes de febrero, marzo y abril del 2014, como se visualiza en la Fig. 66.

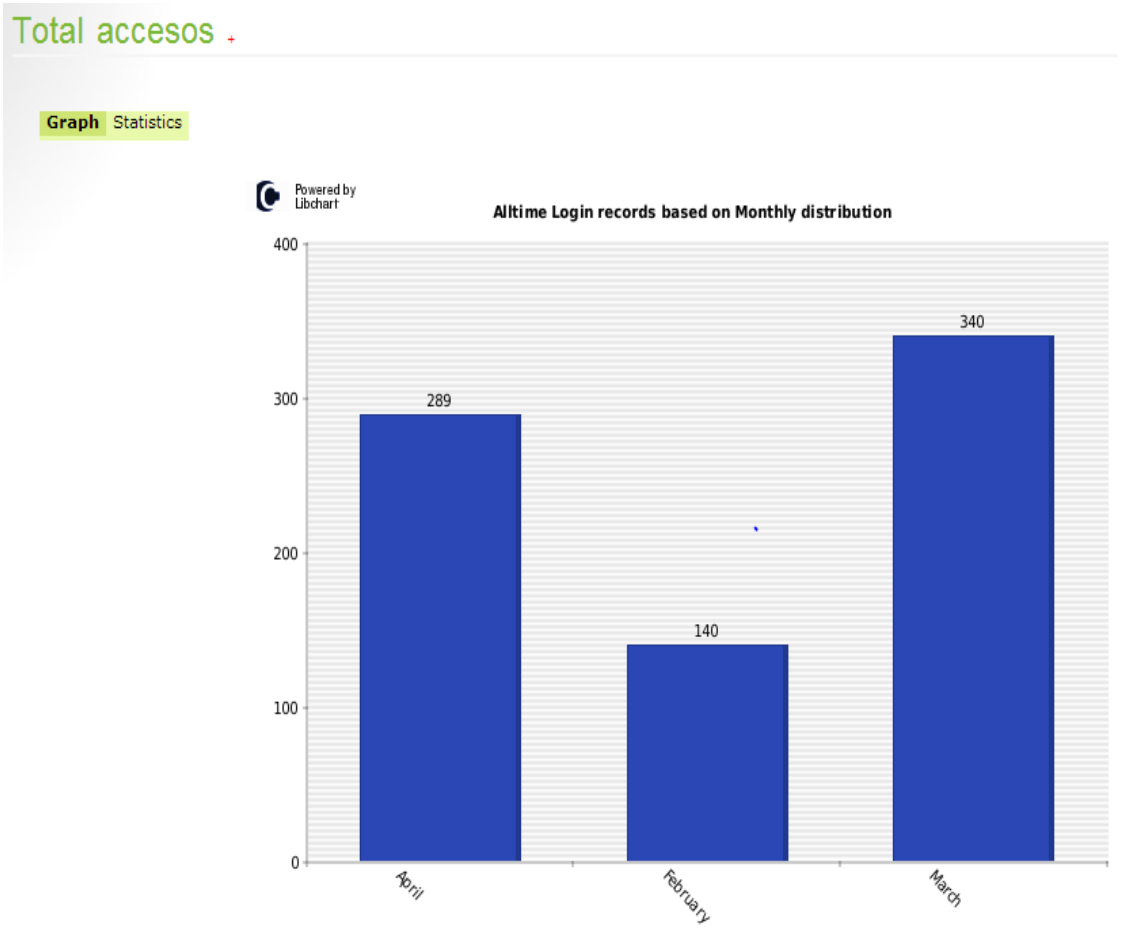


Figura 66. Diagrama de barras muestra el total de acceso en todos los meses evaluados

3.3.5. Prueba con Usuarios Itinerantes

Para evidenciar el proceso de movilidad en el campus universitario UNL con usuarios itinerantes, se obtuvo las credenciales de las siguientes instituciones:

- Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI).
- Instituto Nacional de Investigación y Capacitación de Telecomunicaciones-Universidad Nacional de Ingeniería (INICTEL-UNI).
- Red Española para **I**nterconexión de los Recursos Informáticos de las Universidades y Centros de Investigación (RedIRIS).

3.3.5.1. PUCESI

Para comprobar la itinerancia en la UNL con instituciones a nivel de Ecuador, se solicita la colaboración de la PUCESI, para lo cual muy amablemente proporciona credenciales de prueba para la evaluación respectiva. Las credenciales fueron emitidas a través de correo electrónico (ver anexo 7). En la Fig. 67 se evidencia el registro del usuario de la PUCESI.

654		usuarioldap	172.16.57.137	2014-04-03 15:30:09	2014-04-03 16:56:25	1 hours, 26 minutes, 16 seconds	58.06 Kb	159.42 Kb	User-Request	172.16.[redacted]

Figura 67. Registro en daloRADIUS del usuario de la PUCESI

3.3.5.2. INICTEL-UNI

Para comprobar la itinerancia en la UNL con instituciones a nivel de Latinoamérica, se dispone de las credenciales de INICTEL-UNI que se encuentra en Perú, la información del usuario de prueba fue proporcionada por correo, ver anexo 7. En la Fig. 68 se evidencia la autenticación.

653		raap@inictel-uni.edu.pe	172.16.57.74	2014-04-03 15:25:46	2014-04-03 17:28:23	2 hours, 2 minutes, 38 seconds	759.99 Kb	2.89 Mb	Idle-Timeout	172.16.[redacted]

Figura 68. Registro en daloRADIUS del usuario de inictel

3.3.5.3. RedIRIS

Para demostrar itinerancia en la UNL con redes a nivel de Europa, en la Fig. 69 se realiza la autenticación con credenciales de la RedIRIS que es parte de España, dichas credenciales se obtuvo mediante de correo electrónico, ver anexo 7.

638		testraap@test.rediris.es	172.16.60.17	2014-04-03 09:49:37	2014-04-03 11:39:34	1 hours, 49 minutes, 57 seconds	230.03 Kb	637.79 Kb	User-Request	172.16.[redacted]

Figura 69. Registro en daloRADIUS del usuario de RedIris

3.3.6. Movilidad: Usuario de prueba de la UNL en la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI)

Una valoración importante que permite evidenciar la movilidad de usuarios que forman parte de la Universidad Nacional de Loja en otras instituciones a nivel de Ecuador es mediante el proceso de autenticación, para esto se solicitó la colaboración de la PUCESI a través del encargado de la red Eduroam, al cual se le proporcionó las credenciales del usuario de prueba de la UNL (ver anexo 8) para que realice una prueba técnica, en la Fig. 70 se demuestra movilidad en la PUCESI mediante el mensaje de Access-Accept.

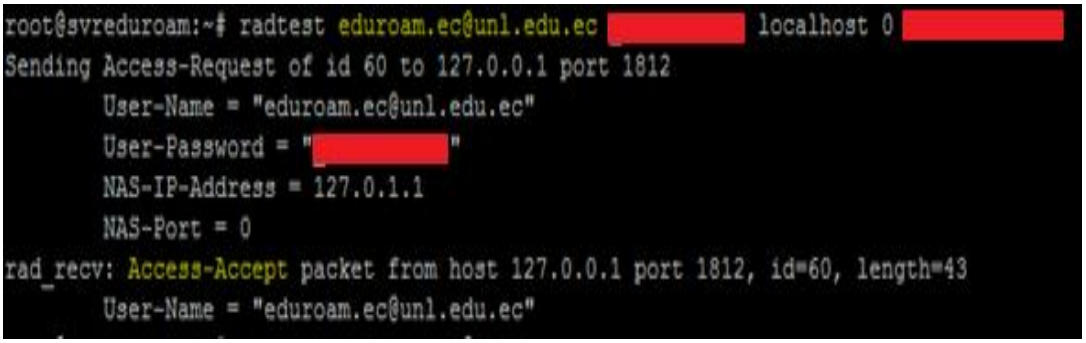


Figura 70. Registro del usuario de prueba de la unl en la PUCESI

3.4. Demostración del Proyecto Eduroam

3.4.1. Arquitectura Eduroam

En la Fig. 71 se muestra un ejemplo de arquitectura del proyecto Eduroam, donde se muestra una computadora portátil con credenciales de tipo itinerante (eduroam_test@pucesi.edu.ec) solicitando la autenticación en el RADIUS de la UNL, a través de un autenticador (Access Point). Por considerarse al usuario que forma parte de la PUCESI, la petición es reenviada al Servidor Federado de Ecuador ubicado en CEDIA, quien se encargará a su vez de reenviar al Servidor Radius de la PUCESI, quien es el único que conoce las credenciales del usuario y por ende se encarga de validarlas, de esa manera la solicitud es aceptada, permitiendo el acceso al servicio de internet de la UNL.

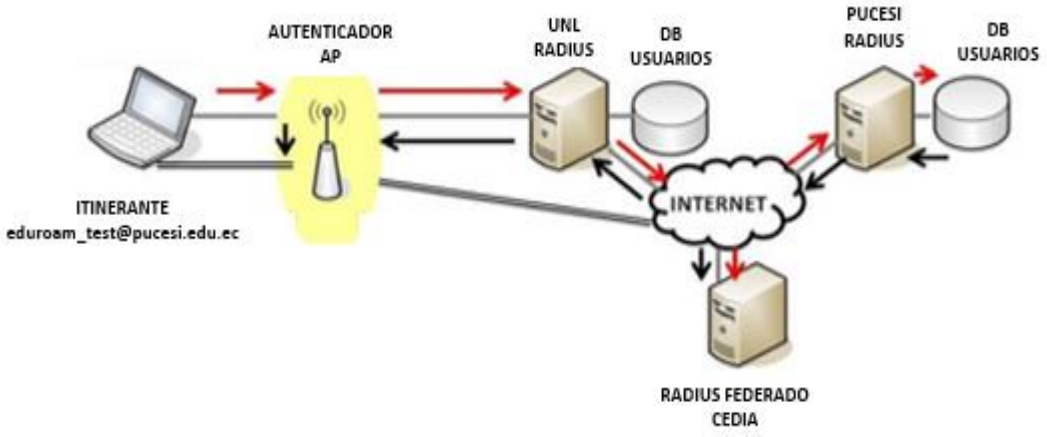


Figura 71. Ejemplo de Arquitectura Eduroam

3.4.2. Autenticación y Autorización en la red Eduroam

A continuación se detalla con un ejemplo la secuencia de pasos que en conjunto con la Fig. 72 se muestra el proceso que se lleva para la autenticación y autorización con un usuario itinerante en la arquitectura Eduroam:

1. El dispositivo móvil de pepe se une a SSID eduroam.
2. El cliente sobre el dispositivo móvil de eduroam_test envía una solicitud de conexión a la red eduroam de la UNL como eduroam_test@pucesi.edu.ec
3. El servidor local RADIUS de la UNL (que está conectado a la infraestructura inalámbrica de UNL) reconoce que el dominio de eduroam_test (@pucesi.edu.ec) no es local, por lo que reenvía la solicitud al servidor RADIUS nacional (RADIUS Ec).
4. El servidor RADIUS nacional (RADIUS Ec) envía la solicitud al destino apropiado, dominio pucesi.edu.ec
5. El servidor RADIUS de PUCESI, envía un certificado de desafío (*certificate challenge*) de regreso a eduroam_test. Este es el paso que permitirá a eduroam_test estar seguro que el SSID eduroam de UNIL es un miembro de confianza de la red de eduroam.
6. Si el certificado fue cargado previamente en el dispositivo de eduroam_test (un importante paso en el proceso de eduroam), el dispositivo aceptará el certificado y establece un túnel encriptado SSL/TLS entre el dispositivo de eduroam_test y el servidor RADIUS PUCESI (origen) de la institución de eduroam_test.

Si el dispositivo móvil de eduroam_test no reconoce el certificado, a eduroam_test se le pedirá que acepte o rechace el certificado. En todos los casos, el certificado mostrará el nombre común (por ejemplo: eduroam.radius.pucesi.edu.ec), eduroam_test no debería aceptar un Certificado con un nombre desconocido (por ejemplo: verdad.com).

7. Ahora que se ha establecido el túnel encriptado entre el dispositivo de eduroam_test y el servidor RADIUS de la PUCESI, las credenciales de eduroam_test son pasadas a través del túnel encriptado SSL/TLS entre el dispositivo de eduroam_test y el servidor RADIUS de PUCESI para la verificación. Este paso de autenticación permite al servidor RADIUS ser conectado al Servicio de Directorio de la institución.
8. Sobre la autenticación exitosa, el servidor RADIUS de la PUCESI envía un *Access-accept* y algún material clave a la infraestructura de UNL (fuera del túnel SSL) y algún material clave privado a eduroam_test (dentro del túnel).
9. La infraestructura inalámbrica eduroam de la UNL negocia con el dispositivo de eduroam_test el intercambio de la clave de encriptación para permitir el acceso a la red y habilitar la encriptación entre el dispositivo de eduroam_test y el punto de acceso inalámbrico de la UNL.
10. Ahora eduroam_test puede conectarse a SSID eduroam en la UNL y disfrutar de la conectividad autenticada y encriptada entre su dispositivo y la red inalámbrica de UNL.

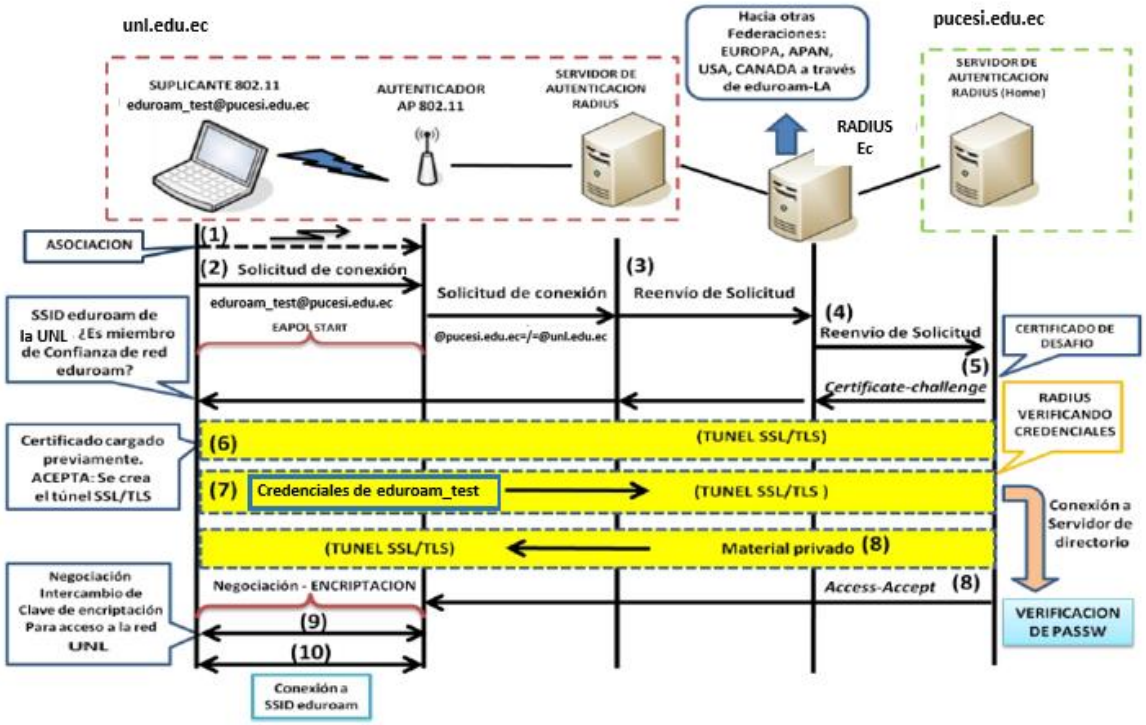


Figura 72. Ejemplo de Autenticación y Autorización en la red Eduroam

3.5. Despliegue de Eduroam en Ecuador

El servicio de movilidad Eduroam cada vez tiene mayor acogida en las universidades del Ecuador, por lo que su despliegue está avanzando con el transcurso del tiempo. En la actualidad según el mapa global de Eduroam localizado en el sitio web: http://monitor.eduroam.org/eduroam_map.php?type=all muestra 6 universidades entre ellas la UNL que ya tienen desplegado el servicio, a continuación se detalla:

- Pontificia Universidad Católica del Ecuador Sede Ibarra
- Universidad de Cuenca
- CEDIA
- Universidad Tecnológica Equinoccial
- Escuela Superior Politécnica del Litoral
- Universidad Nacional de Loja

En la Fig. 73 se muestra el mapa del Ecuador con el despliegue de Eduroam en las Universidades.

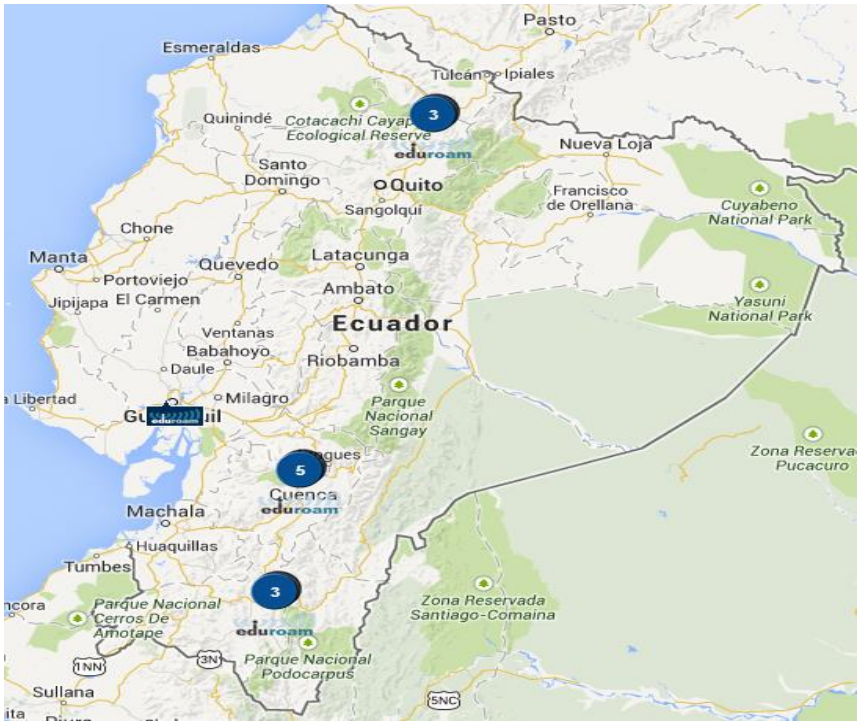


Figura 73. Despliegue de Eduroam en Ecuador

4. Fase 4: Difusión de los Resultados de la Investigación

Para el proceso de difusión de los resultados de la investigación del presente PFC se tomaron varias herramientas, con el ánimo de difundir y dar a conocer el trabajo realizado para aquellas personas que estén interesadas en este tipo de proyectos.

4.1. Artículo Técnico

Para presentar a la comunidad científica se redacta el artículo técnico titulado **"Implementation of Eduroam as Wirelless Infraestructure on the Campus of National University of Loja"** (ver anexo 9), que contiene principalmente temas como análisis, revisión de literatura, desarrollo y resultados obtenidos, el artículo será publicado de forma virtual en la revista universitaria de la UNL llamada Revista "Energía" en su Edición N°2 en Junio 2014. El artículo Técnico presentado sigue LAS NORMAS PARA LA PRESENTACIÓN DE ARTÍCULOS EN IEEE LATIN AMERICA TRANSACTIONS las cuales guían aspectos como: la presentación del documento, derechos del autor, disposiciones, reglas para el formato, etc. Para proceder con la publicación del artículo técnico es enviado al Comité Editorial de la Revista a través del correo electrónico revista.energia@unl.edu.ec. Cuya respuesta se muestra en la Fig. 74 , para luego ser sometido a un proceso de revisión, tomando aspectos importantes como: formato de revista, bibliografía y/o referencias adecuadas, redacción clara, tablas y figuras pertinentes; luego del cual se emite un Informe de Revisión que presenta los siguientes indicadores, mostrados en la Fig. 75

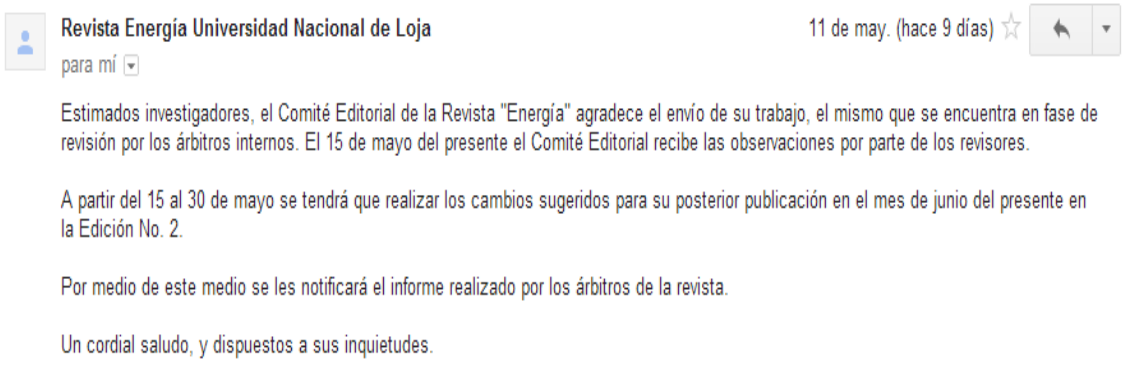


Figura 74. Notificación del Comité Editorial de la Revista "Energía"

Indicadores de contenido:

1. **Relación con otras investigaciones del mismo campo:** *Bien*

Comentarios, observaciones y sugerencias: los autores fundamentan el estado del arte adecuadamente, considerar la observación relacionada con la bibliografía.

2. **Pertinencia teórica-metodológica:** *Bien*

Comentarios, observaciones y sugerencias: los autores fundamentan adecuadamente la manera de lograr los objetivos propuestos, se sugiere, si es posible, agregar bibliografía documental.

3. **Aportación a estudios ya hechos:** *Bien*

Comentarios, observaciones y sugerencias: se detecta un adecuado aporte por otros trabajos de los autores relacionados con el campo de investigación.

4. **Análisis y síntesis:** *Bien*

Comentarios, observaciones y sugerencias: los autores presentan los resultados y las conclusiones adecuadamente.

Escala: Bien/Regular/Mal

Fecha de revisión: 14/05/2014

Firma del revisor responsable:.....

Figura 75. Informe de revisión del Comité Editorial de la Revista Energía

4.2. FLISOL 2014

Como parte del proceso de difusión del trabajo investigativo y aprovechando la celebración del FLISOL2014 Capítulo Loja, se colaboró con la participación del PFC demostrando el uso de herramientas libres aplicadas en su desarrollo. La participación de los investigadores en el evento, sin lugar a duda, aportó destreza en la exposición y confianza en el dominio de la temática, sin embargo como todo aporte también evidenció los puntos débiles que deben ser reforzados.

La conferencia fue tratada con el tema **"Servicio de Movilidad mundial Eduroam en la Universidad Nacional de Loja con FreeRADIUS, OpenSSL y OpenLDAP",** como se muestra en la Fig. 76.

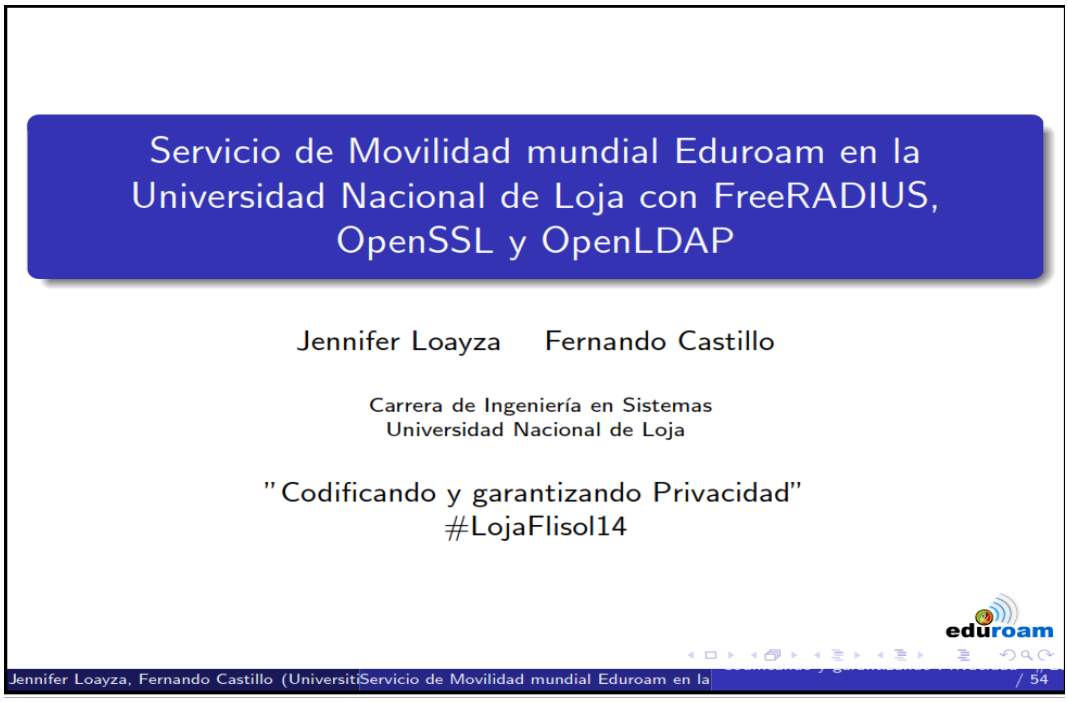


Figura 76. Presentación de conferencia en el evento FLISOL 2014

4.3. Página Web

Se crea un portal web propio de la UNL, para dar a conocer a todos y cada uno de los que forman parte de la Institución sobre el proyecto Eduroam, donde principalmente encuentran información introductoria del proyecto, los manuales de configuración en diferentes plataformas, los participantes de Eduroam a nivel nacional y los contactos de Eduroam en la UNL. En la Fig. 77 se visualiza la página principal, cuyo enlace es: http://eduroam.unl.edu.ec/.

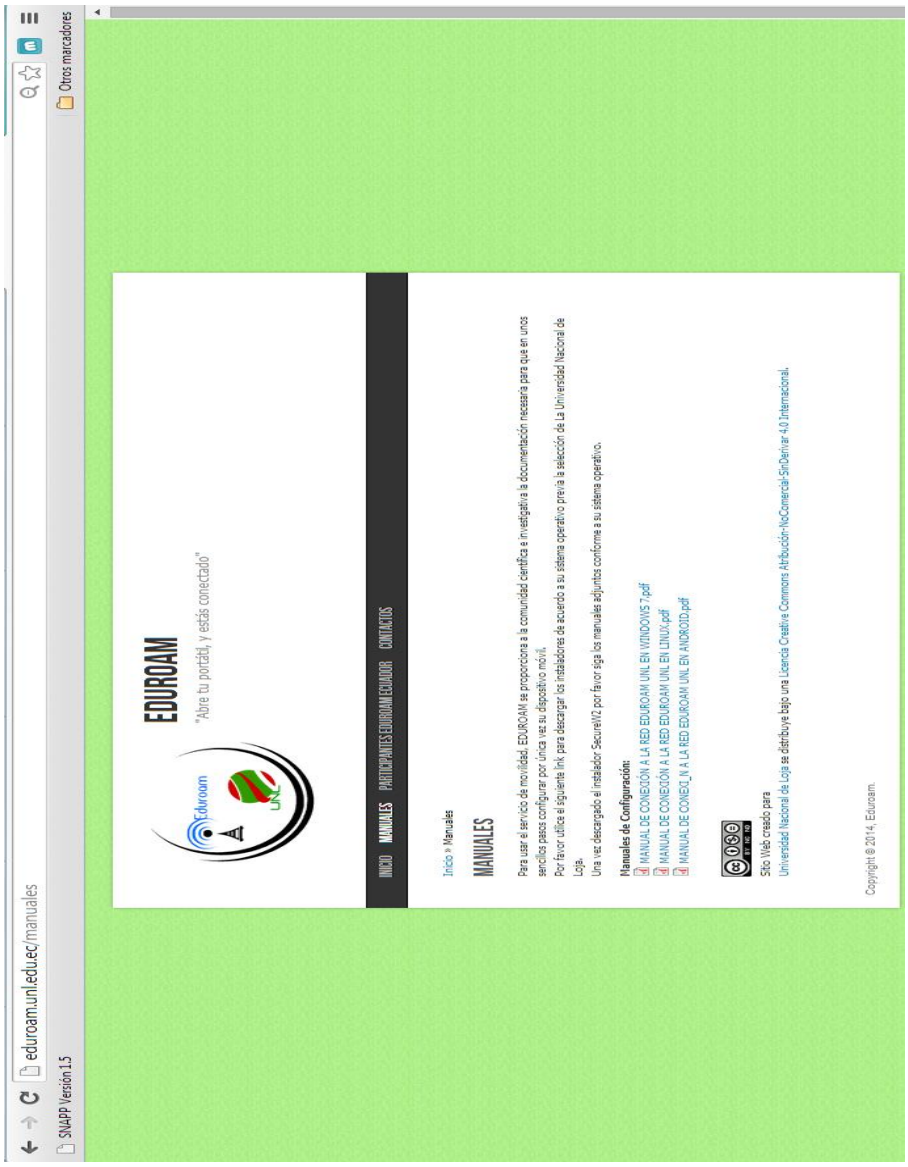


Figura 77. Página oficial de Eduroam de la UNL

F. DISCUSIÓN

1. DESARROLLO DE LA PROPUESTA ALTERNATIVA

El desarrollo de la propuesta alternativa se basa en la realización y cumplimiento de los objetivos planteados.

1. ***Analizar el estado actual de la red de datos inalámbrica de la Universidad Nacional de Loja para que cumpla con los lineamientos del proyecto EDUROAM.***

   Para llegar a cumplir el presente objetivo, se realizó una descripción de los equipos networking de la infraestructura de red inalámbrica que dispone la Universidad Nacional de Loja para ofrecer el servicio de internet inalámbrico a todos los que forman parte de la institución, de igual forma se describe la ubicación y direccionamiento IP de los diferentes Access Point. Así mismo se redacta como se llevaba el proceso de autenticación que deben realizar para acceder al servicio a través del SSID S.I. UNL.

   Como parte importante dentro de este objetivo se procede a realizar una comparativa de los lineamientos de EDUROAM frente a la Red S.I. UNL que comprende hardware, software y usuario final.

   Todo lo descrito anteriormente se encuentra detallado en la *Fase 1: Análisis de requerimientos de la sección Resultados.*

2. ***Establecer un método estándar de autenticación para el servicio de conectividad móvil en la Universidad Nacional de Loja.***

   Dentro de esta apartado se realiza un análisis del método de autenticación fácil, ligero y centralizado como es LDAP, el mismo que es llevado como propuesta para su utilización en el proyecto EDUROAM.

   Para seleccionar el mejor directorio de servicio LDAP se realiza una comparación entre los software más conocidos, tomando en cuenta aspectos como definición, valor comerciales y opiniones de implementación, todo esto con el fin de seleccionar la mejor alternativa.

   Se selecciona OpenLDAP como la mejor alternativa para la implementación, en base al análisis realizado. Se arma un entorno de pruebas del servicio donde se detalla

características de hardware, software, definición y creación de la estructura del directorio LDAP y por ende su instalación. Cabe indicar que dentro de esta apartado se definió un esquema personalizado en que implica agregar una Clase Objeto con atributos propios para cada usuario que forma parte Universidad Nacional de Loja.

Todo lo relacionado a este objetivo, se encuentra detallado en la sección *Resultados, Fase 2: Desarrollo, apartado Servidor LDAP.*

3. ***Desarrollar y validar las configuraciones de los servidores RADIUS Local y Federado para el servicio de movilidad.***

   Para el desarrollo y cumplimiento de este objetivo se realiza una descripción de la funcionalidad que desempeña cada uno de los servidores RADIUS Local y Federado dentro de la infraestructura de red EDUROAM, además mediante tablas se detalla las características tanto hardware, como de software requerido para su implementación.

   Para la instalación y configuración de los servidores se lo hizo con la ayuda de manuales de implementación proporcionado por la comunidad EDUROAM, en cual se creó una autoridad certificadora privada con la que se generaron certificados de consulta para el Servidor Radius Local.

   Dentro de los archivos configurados en el Servidor Radius Local está el users, eap.conf, proxy.conf, client.conf y para el Servidor Federado los archivos client.conf y proxy.conf.

   Para validar las configuraciones realizadas en los Servidores, se procede a utilizar el comando radtest que permite simular una solicitud de acceso al RADIUS, para lo cual se envió solicitudes de acceso con usuarios locales e itinerantes.

   Finalmente dentro de esta apartado se explica las razones del porque el Servidor Radius Federado, pasa a manos de CEDIA (Consorcio Ecuatoriano de Internet Avanzado).

   Todo lo relacionado al desarrollo de este objetivo, se encuentra detallado en la sección *Resultados, Fase 2: Desarrollo, apartado Servidores Radius,*

4. ***Ejecutar pruebas de movilidad a la red EDUROAM aplicadas a usuarios del campus universitario en diferentes escenarios.***

   Con la realización de este objetivo se demuestra la operatividad, funcionalidad y la ventaja de aplicación del proyecto Eduroam. Para el cumplimiento de las pruebas de movilidad se preseleccionó al A.E.I.R.N.N.R como escenario de prueba debido

principalmente a que su población, en concreto, a los usuarios de la Carrera de Ingeniería en Sistemas, hace mayor uso de las TIC's en comparación a las demás áreas que componen la institución. Un punto importante a probar es la capacidad del Servidor Proxy Radius Local para aceptar muchas peticiones, por lo que usar RADIUS test client resultó de mucha ayuda por su facilidad de uso frente a otras aplicaciones que no permiten enviar tantas solicitudes a la vez o resultan de difícil configuración para poner a prueba al servidor RADIUS.

Las plataformas de los S.O en que se evaluaron a la red Eduroam fueron determinadas por el uso o la estabilidad que éstas presentan; en el S.O Windows tuvo una excelente fase de pruebas debido a que la red Eduroam fue adaptada a su Versión 7 frente a su Versión 8 que por su reciente apogeo aún no se logra aplicar las configuraciones que necesita Eduroam. En la distribución Ubuntu del S.O Linux presenta facilidad en su configuración, y además es mayor su frecuencia de uso por parte del usuario final en contraste se puede evidenciar en el S.O Android con su reciente auge en smartphones o tablets. Los usuarios del S.O Mac no pueden tener restricción a este servicio por lo que existe la configuración respectiva tanto para laptop como para smartphones.

Frente a la gama de usuarios disponibles para realizar la fase de prueba se hace uso de un usuario creado propiamente para ese fin, el cual es previamente almacenado en el servidor LDAP y es de nuestro libre uso.

Realizar las pruebas de movilidad se centra principalmente en la demostración de conexión de un usuario itinerante en un campo diferente, por lo que gracias a su sentido de colaboración y cooperación para el despliegue de Eduroam por el país, se determinó mediante contacto previo que la institución que nos facilitaría en esta parte de la fase sería PUCESI a nivel nacional, y el INICTEL y RedIris a nivel internacional.

Todo lo descrito anteriormente se encuentra detallado en la *sección Resultados, Fase 3: Pruebas de movilidad.*

5. ***Establecer procesos de documentación de la implementación del proyecto y replicarlo a la comunidad científica.***

   Para lograr cumplir este objetivo, en esta fase del PFC se procedió a establecer algunas herramientas de difusión basadas en normas, reglas y disposiciones que rigen tanto a los documentos creados como a la conferencia ofrecida para

comunidades, investigadores o personas interesadas en este tipo de trabajos académicos-tecnológicos. Se participó en las conferencias de Software Libre denominado "FLISOL2014" capítulo Loja, con la temática orientada a las herramientas libres que se utilizaron para el desarrollo. De igual manera se implementó un sitio web, dando a conocer el proyecto Eduroam, donde se incluye manuales de configuración e instalación útil para el uso del servicio establecido, por último se redactó un Articulo Técnico donde se menciona en síntesis todo el proceso realizado para llegar a alcanzar resultados reales.

Todo lo relacionado a este objetivo, se encuentra más detallado en la sección *Resultados, Fase 4: Difusión de los Resultados de la Investigación.*

2. VALORACIÓN TÉCNICA ECONÓMICA AMBIENTAL

El presente PFC, titulado "Implementación del Sistema Federado Eduroam en la Universidad Nacional de Loja y configuración de la Infraestructura Tecnológica como iniciativa para el despliegue en las Universidades del Ecuador" se considera desde el punto de vista técnico como un trabajo factible y necesario dentro de la Universidad Nacional de Loja, puesto que permitirá tener acceso a internet a todos los que forman parte de la Institución, así como a personas de otras universidades cuando visiten el campus universitario, y viceversa. Además este proyecto de nivel mundial ahorra el trabajo de configurar Access Point de uso exclusivo para usuarios itinerantes, de igual manera se tiene un control de acceso a la red de todos aquellos que utilizan la infraestructura EDUROAM dentro del campus.

En el aspecto económico el proyecto se considera de igual manera factible por 2 situaciones relevantes:

- Los requerimientos de hardware son cubiertos por la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.
- Los requerimientos de software utilizados son de libre distribución y poseen licencia Open Source.

A continuación se detalla los recursos humanos, materiales, técnicos y tecnológicos utilizados:

Los recursos humanos hace hincapié del personal que formo parte del PFC, que principalmente fue llevado a cabo por sus investigadores, se tuvo la ayuda de un asesor de proyectos quien fue guía para esquematizar de mejor forma el anteproyecto. Sin duda durante el transcurso del desarrollo, se contó con las tutorías del director de tesis. De igual forma durante el proceso de implementación se obtuvo con la colaboración de entendidos en la materia de EDUROAM. En la Tabla XXIX se detalla los recursos humanos.

Tabla XXIX. RECURSOS HUMANOS

DESCRIPCIÓN	CANT.	COSTO/HORA	NRO. HORAS	TOTAL
Investigadores	2	$ 5.00	1280	$12800.00
Asesor de Anteproyecto	1	$ 10.00	10	$ 100.00
Director de Tesis	1	$ 10.00	70	$ 700.00
Asesor de Eduroam	2	$ 10.00	10	$ 200.00
SUBTOTAL				**$ 13800.00**

En la Tabla XXX se hace una descripción detallada de los recursos materiales que fueron necesarios para presentar los borradores y el informe final del PFC.

Tabla XXX. RECURSOS MATERIALES

DESCRIPCIÓN	CANT.	V. UNITARIO	TOTAL
Resmas de Papel A4	4	$5.00	$ 20.00
Cartuchos de Tinta	4	$25.00	$ 100.00
Empastado	4	$ 8.00	$ 32.00
Anillados	5	$2.00	$ 10.00
CD's	6	$0.50	$ 3.00
SUBTOTAL			$165.00

En la Tabla XXXI muestra en detalle los recursos de hardware que fueron que utilizaron para el desarrollo del PFC; que comprende dos portátiles personales que usados para montar temporalmente los servidores radius, el acceso remoto a los Servidores una vez implementados en Blade y la redacción de avances como del informe final.

Tabla XXXI. RECURSOS HARDWARE

DESCRIPCIÓN	COSTO	DEPRECIACIÓN (5 AÑOS)	T. UTILIZACIÓN (MESES)	TOTAL
Miniportátil DELL INSPIRON N4030	$ 805.00	$ 161	16	$214.67
Portátil TOSHIBA Satellite S845	$1070.00	$ 214	16	$285.33
Impresora	$80.00	$ 16	16	$21.33
Blade HP PROLIANT	$23911.00	------	-----	----------
SUBTOTAL				$521.33

En la Tabla XXXII muestra el software usado para la implementación del proyecto y su difusión en la UNL. Por tratarse de herramientas libres, no posee costo alguno.

Los servidores Ldap y Radius fueron montados en el Sistema Operativo GNU Linux distribución Debian. La implementación del protocolo radius se usó la herramienta freeradius para la autenticación y autorización de usuarios previamente registrados en el servidor Ldap, para lo cual se utilizó la herramienta OpenLdap y finalmente se usó Openssl que ayuda a la creación de la CA y emisión de certificados digitales. Para la difusión de Eduroam se creó una página web con ayuda del CMS Drupal.

Tabla XXXII. RECURSOS SOFTWARE

DESCRIPCIÓN	VALOR
GNU Linux/Debian	$00.00
freeRADIUS	$00.00
OpenLDAP	$00.00
OpenSSL	$00.00
PhpLdapAdmin	$00.00
DaloRADIUS	$00.00
Drupal	$00.00
SUBTOTAL	$00.00

En la Tabla XXXIII muestra el desglose del tiempo usado por los investigadores en lo que respecta al internet, medio principal para la obtener información importante y muy necesaria para el desarrollo del PFC, de igual forma las llamadas a celular fueron eje principal para estar comunicados entre los investigadores y director de tesis.

Tabla XXXIII. RECURSOS COMUNICACIONES

DESCRIPCIÓN	USUARIOS	PERIODO (16 MESES)			V. HORA	V.TOTAL
		FRECUENCIA		TOTAL		
		DIARIO	MES			
Internet	2	3 horas	60 horas	960 horas	$ 0.50	$ 480.00
Llamadas a Celular	2	-----	5 min	1 hora 20 min.	$0.10	$ 0.80
SUBTOTAL						**$ 480.80**

En la Tabla XXXIV. Se aprecia la suma parcial de los recursos técnicos y tecnológicos usados para su posterior inclusión en la suma total de recursos usados.

Tabla XXXIV. RECURSOS TÉCNICOS Y TECNOLÓGICOS

DESCRIPCIÓN	V.TOTAL
Recursos Hardware	$521.33
Recursos Software	$000.00
Recursos Comunicaciones	$800.00
SUBTOTAL	**$1321.33**

En la Tabla XXXV. Presenta la suma total de todos los recursos tanto humanos como materiales y técnicos y tecnológicos usados en el proyecto, que da una aproximación del costo real.

Tabla XXXV. APROXIMACIÓN DEL COSTO REAL DEL PROYECTO

DESCRIPCIÓN	V.TOTAL
Recursos Humanos	$ 9700.00
Recursos Materiales	$287.00
Recursos Técnicos y Tecnológicos	$1321.33
SUBTOTAL	**$11308.33**
IMPREVISTO 10%	**$1130.83**
	$12439.16

El PFC se considera factible en el aspecto ambiental puesto que los servidores implementados se encuentran en una zona adecuada, “cuarto frio”, dentro de la Unidad de Telecomunicaciones e Información. Además se puede tener acceso vía remota para su administración, sin necesidad de tener contacto físico.

G. CONCLUSIONES

Una vez culminado el presento PFC se puede concluir lo siguiente:

- Mediante el análisis de la infraestructura de red inalámbrica permitió conocer los equipos que se usan para ofrecer el servicio de internet inalámbrico, de igual manera se evidenció el proceso de autenticación y autorización que se llevaba, cuyo método implicaba ingresar las credenciales de usuario a través de un portal cautivo cada vez que se requería del servicio, con el pasar del tiempo se ha dejado a un lado. Actualmente con la red inalámbrica eduroam se ingresa las credenciales la primera vez y en posteriores conexiones se hará de forma automática cada vez que se identifique la red ya sea en el propio campus institucional o en otro que se esté visitando.

- Utilizando el Software de distribución Libre OpenLDAP, se implementó el servicio LDAP como método de consulta de credenciales (usuario/contraseña) para el acceso al servicio de internet inalámbrico mediante la infraestructura de red Eduroam, este proceso está enfocado a darle una nueva forma al usuario tradicional el cual estaba dado por el número de cédula para proceder a esquematizarlo en base a los nombres y apellidos quedando conformado por las iniciales de los nombres, el primer apellido y la inicial del segundo apellido.

- Se ha implementado un Servidor Radius Eduroam Institucional para ofrecer el servicio de movilidad, realizando las configuraciones requeridas en las que se incluye la implementación del protocolo SSL/TLS con la creación de certificados de consulta tanto público como privado para el Servidor Radius, garantizando de esta manera que la comunicación entre cliente-servidor se realice de forma segura y que la información viaje a través de un túnel de forma cifrada, casi imposible de descifrarla. Además con la iniciativa de disponer el servicio en Ecuador se implementó en la Universidad Nacional de Loja un Servidor Federado en fase de prueba para todas las instituciones del Ecuador, realizando las pruebas que garanticen la funcionalidad para luego pasar a formar parte del CEDIA.

- La implementación de un Servidor RADIUS desarrolló habilidad y destreza en los investigadores, adquiriendo conocimiento en cuanto al funcionamiento del protocolo de autenticación, autorización y registro, manipulación de certificados de confianza a través del protocolo SSL con algoritmos de encriptación RSA, además del TTLS como método de autenticación. En cuanto a la instalación y configuración de un Servidor LDAP destaca el conocer un nuevo proceso de autenticación de servicios que responde principalmente a consulta de perfiles de usuario.

- Se realizaron pruebas de autenticación para comprobar el funcionamiento del servicio de movilidad Eduroam con estudiantes de la Carrera de Ingeniería en Sistemas, de igual forma se hicieron las respectivas pruebas con credenciales de usuarios itinerantes comprobando movilidad a nivel de Ecuador, Latinoamérica y Europa, las pruebas también fueron orientadas hacia los Sistemas Operativos en las plataformas Ubuntu, Windows 7, Mac OS Marvericks, Android y iOS Apple.

- Al tratarse de un PFC, este se ha difundido por algunos medios, dentro de los cuales se participó en las Conferencias de Software Libre versión Loja denominado “FLISOL2014”, se creó un página web para conocimiento de Eduroam en la Universidad Nacional de Loja y por último se realizó un extracto de los más importante del proyecto en un Articulo Técnico para ser publicado en la Revista “Energía” edición nro. 2 de Junio del 2014.

- El uso de la aplicación web daloRADIUS permitió la visualización amigable de los accesos realizados en el Servidor Radius Local, presentando información estadística clasificada por accesos, usuarios y fechas, permitiendo determinar el inicio y fin de sesión, subida y descarga de archivos además de la dirección IP asignada al dispositivo y su respectiva MAC.

- La utilización del equipo networking Wireless Lan Controller (WLC), permitió la difusión del SSID eduroam en todo el campus universitario, ya que gestiona de forma conjunta todos los Access Point que componen la red inalámbrica de la UNL.

H. RECOMENDACIONES

Se propone las siguientes recomendaciones como parte del trabajo realizado:

- Realizar un estudio de sitio del campus universitario enfocado principalmente en cubrir oficinas, aulas, bibliotecas y campos abiertos que son de mayor concentración por quienes forman parte de la universidad, de esa manera se mejora las zonas de cobertura de la red inalámbrica y así ofrecer movilidad interna de calidad a usuarios locales e itinerantes.

- Desarrollar un módulo en el Web Services que permita la vinculación del SGA (Sistema de Gestión Académica) con el directorio LDAP, con el fin de gestionar de forma automática los usuarios y sus perfiles almacenados en el SGA, sincronizándose con el directorio LDAP.

- Efectuar una actualización periódica de los protocolos de seguridad, usados en el proyecto de movilidad, a su versión más reciente, estable y exhaustivamente probada con el fin de ofrecer confianza al usuario, garantizando confidencialidad y privacidad de la información.

- Establecer el SSID eduroam como principal y único medio de acceso al servicio de internet inalámbrico en el campus universitario, garantizando mediante el registro del usuario tener un control de todos los accesos realizados sean esporádicos o muy frecuentes, esto servirá para evaluar las fortalezas y debilidades que ayudarán a mejorar la red inalámbrica, además con esta infraestructura de red, la universidad estrecha lazos de colaboración y compartición del servicio de internet entre universidades encaminándose a formar parte de la gran comunidad Eduroam.

- Por tratarse de certificados emitidos cada 4 años por CEDIA y aprovechando la comunicación que existe entre los Servidores Radius Eduroam Locales/Institucionales y el Servidor Federado para Ecuador, realizar la renovación automática de los mismos, avalando de esta manera que no haya ningún descuido u olvido en la implementación e incluso eliminando la petición verbal de renovación de certificados.

- Darle seguimiento continuo a este PFC en futuros trabajos con el afán de ir mejorando acorde a las necesidades que se vayan presentando y que en conjunto con las nuevas tecnológicas, tales como el uso de IPSEC y RADSEC que ofrezca seguridad y confiabilidad en el uso de este medio.

- Realizar el subneteo (subredes) de la red de la UNL de tal manera que se creen dos grupos de usuarios (Locales e Itinerantes) y se asigne un rango de direcciones IP, para cada uno de estos, diferenciando el dominio del usuario en el Servidor Radius Local, garantizando de esta forma la utilización efectiva del servicio de movilidad eduroam.

I. BIBLIOGRAFÍA

SITIOS WEB:

[1] RedIRIS. 2006. ¿Qué es EDUROAM?. [Online]. Disponible en: http://www.EDUROAM.es/

[2] Arnol Alberto Hernández Serna, Andres Julián Grajales Marín. (2011). Revisión de los conceptos y tecnologías utilizadas en la implementación de un sistema federativo tipo EDUROAM. Disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/489/completo.pdf?sequence=1

[3] Andra FILIP, Esthefanía VASQUEZ TORRES. (2010). Seguridad en redes WIFI EDUROAM. Sevilla. Disponible en: http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20redes%20Wifi%20EDUROAM.pdf

[4] REUNA. Beneficios. [Online]. Disponible en: http://www.eduroam.cl/index.php/beneficios

[5] CRUZ GUZMÁN Norma Alicia. Modelo e Infraestructura de Seguridad basado en Identificación y Autentificación para Redes. Disponible en: http://www.biblio-sepi.esimez.ipn.mx/telecomunicaciones/2011/Modelo%20e%20infraestructura%20de%20seguridad%20basado%20en%20identificacion%20y%20autentificacion.pdf

[6] MOYA GALLARDO Edison Javier**.** Implementación de la Administración centralizada de la Red Inalámbrica de los Edificios Rocío I y II de EP Petroecuador mediante un Wireless Lan Controller. http://bibdigital.epn.edu.ec/bitstream/15000/6379/1/CD-4897.pdf

[7] CABRERA PROAÑO Claudio Armando. Análisis a la Seguridad de Redes Inalámbricas como extensión de una red Lan. http://repositorio.utn.edu.ec/bitstream/123456789/593/3/CAPITULO%20III.pdf

[8] ASADOVAY LEMA Gladis Sofía; CAIZA ORTZ Liliana Mercedes. Análisis comparativo de Servidores de Autentificación Radius y Ldap con el uso de Certificados Digitales para mejorar la Seguridad en el Control de Acceso a Redes Wifi. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/2422/1/98T00020.pdf

[9] MIRANDA RUIZ Helen Gabriela. Estudio e Implementación de mecanismos de Seguridad WP un sistema de distribución Inalámbrico para dar cobertura a tráfico de voz sobre IP. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/641/1/38T00258.pdf

[10] PLASENCIA BEDÓN Luis Carlos. Servidor AAA para validación y control de acceso de Usuarios hacia la Infraestructura de Networking de un ente del Ministerio de Defensa Nacional. Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/994/1/04%20RED%20009%20TESIS_SERVIDOR_AAA.pdf

[11] TAMAYO HIDALGO Lidia Marlene. Servidor remoto de autenticación de Usuarios (RADIUS) para la integración con el Sistema Administrativo Contable en el Proveedor de Servicio de Internet SPEEDYCOM CIA. LTDA. de la Ciudad de Ambato. Disponible en: http://repo.uta.edu.ec/bitstream/handle/123456789/6275/Tesis_t858si.pdf?sequence=1

[12] RAMIO Jorge. Seguridad Informática y Criptografía. http://dspace.ups.edu.ec/bitstream/123456789/216/2/Capitulo%201.pdf

[13] HARO MONTERO_Manuel Abelardo; GAVILANES SAGÑAY Fredy Marcelo. Análisis de funciones Criptográficas de Código Libre en los protocolos SSL y TLS aplicado al portal web de la Jefatura Provincial de Tránsito de Chimborazo. http://dspace.espoch.edu.ec/bitstream/123456789/55/1/18T00387.pdf

[14] LUCENA LOPEZ Manuel José. Criptografía y Seguridad en Computadores. http://iie.fing.edu.uy/ense/asign/seguro/Criptografia.pdf

[15] LEÓN SANGURIMA Jenny Maritza. Criptografía: Funciones Hash como alternativa de seguridad en Transacciones Online para Organizaciones o Empresas. http://186.42.96.211:8080/xmlui/bitstream/handle/123456789/501/tesis%20completa.pdf?sequence=1

[16] CANDO SALME Mirian del Rosario; LLUMITASIG GALARZA Mónica Elizabeth**.** Implementación de un Sistema de Autenticación para controlar la Seguridad de la Red Inalámbrica de la Brigada de Fuerzas Especiales No. 9 Patria, Ubicada en el Cantón Latacunga. http://repositorio.utc.edu.ec/bitstream/27000/438/1/T-UTC-1017.pdf

[17] Criado Sebastián, Puigpinos Julio. Lugro-Mesh: Tecnología Mesh Aplicada a Redes WiFi Comunitarias. http://www.lugro-mesh.org.ar/doc/LUGRo-Mesh%20-%20texto%20charla%208vas%20JRSL.pdf

[18] Cisco Aironet Dual-Band Antena Omnidireccional (AIR-ANT2547V-N). Cisco System. http://www.cisco.com/en/US/docs/wireless/antenna/installation/guide/ant2547vn.html#wp55078

[19] Cisco Aironet 1550 Series Outdoor Access Point Data Sheet. Cisco Systems. http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps11451/data_sheet_c78-641373.html

[20] FLORES, Fabricio y NEIRA, Lisset. Implantación de un sistema de seguridad para el acceso inalámbrico a la red de la Universidad Nacional de Loja utilizando Software Libre. Loja. Ecuador. 2012. Tesis previa a la obtención del título en ingeniero en sistemas.

[21] RUIZ CAÑAMERO María Ana. Autenticación y administración centralizada en sistemas VoIP con Asterisk y LDAP. http://e-archivo.uc3m.es/bitstream/handle/10016/11158/PFC_Maria_Ana_Ruiz_Canamero.pdf?sequence=1

J. ANEXOS

Anexo 1. Correo del Representante de Eduroam a nivel de Latinoamérica, que evidencia el inicio de la iniciativa EDUROAM en la UNL.

Jose Luis Quiroz_A <jlquiroza62@gmail.com> 25/08/12

para quiroz, mi

Hola Fernando

Como le dije a Jennifer, la comunicación con CEDIA es solo para que le hagan saber de su intención para iniciar eduroam en su universidad.
El material ya esta listo, les llegara la invitación para que pertenezcan a la comunidad de Movilidad de RedCLARA y desde alli utilizar las herramientas de comunicación que tiene.
La dedicación sera de 3 horas diarias durante 15 dias....
Ah!... no se olviden de tener para su federado una PC o servidor Core i3 (mínimo) con Debian, 4GB de RAM, 80 GB de HD. Puede estar virtualizado.....
Haciando una variación al curso anterior, sería bueno que iniciemos la configuración de al menos dos locales, donde uno de ellos cambiaría su estatus a Federado con una configuración adicional, asi tendrían su federado y local. Despues veríamos lo del Access point para su despliegue a los usuarios finales. En esta última parte si tendrán una lucha, la adm del servicio inalámbrico de su universidad debe estar convencido de incorporar eduroam.... :-)
Comunicate con Jennifer, le envie un mail...
Nos estamos comunicando.... Ah....me olvidaba, tienen ustedes cuentas oficiales de correo de sus universidades?.... es importante esto, si no lo tienen me avisan.
Saludos

Jose Luis Quiroz A.

Anexo 2. Guía de instalación de Servidor LDAP

8. Instalar y Configurar un servidor LDAP (Tiempo estimado < 2h)

8.1 Instalación de un servidor LDAP de pruebas.

Primero, instalamos los siguientes paquetes:

```
apache2 slapd ldap-utils phpldapadmin libapache2mod-php5
```

Como al instalar el servidor LDAP se generan parámetros por default, nos conviene reinstalarlo para su configuración manual.

Ejecutar:

dpkg-reconfigure slapd

```
¿Desea omitir la configuración del servidor OpenLDAP? No
Introduzca su nombre de dominio DNS: *******
Nombre de la organización: ******
Contraseña: ******
Motor de base de datos a utilizar: BDB
¿Desea que se borre la base de datos cuando se purgue el paquete slapd? No
¿Desea mover la base de datos antigua? SI
¿Desea permitir el protocolo LDAPv2?  No
```

Ejecutamos "**slapcat**" para ver los detalles de nuestra configuración inicial.

Guarde los cambios!

8.2 Configurar usuarios en LDAP

Primero, creamos un grupo LDAP llamado "usuarios", en el cuál se almacenarán los usuarios autorizados a eduroam, luego crearemos un perfil de usuario en LDAP. Editamos los siguientes archivos dentro del nuevo directorio /etc/ldap/ldif.

Anexo 3. Esquema UsuariosUNL

```
#UsuariosUnl.schema
#

# definición del atributo apellidoMaterno
attributetype ( 3.0.0.1 NAME ('ssn')
      DESC 'Segundo Apellido del Usuario UNL'
      SUP name )

# definición del atributo DNI
attributetype ( 3.0.0.2 NAME 'dni'
      DESC 'DNI delUsuario UNL'
      SUP name )

# definición del atributo Dirección
attributetype ( 3.0.0.3 NAME 'direccion'
      DESC 'Direccion del Usuario UNL'
      SUP name )

# definición del atributo Sexo
attributetype ( 3.0.0.4 NAME 'Sexo'
      DESC 'Sexo del Usuario UNL'
      SUP name )

# definición del atributo pais
attributetype ( 3.0.0.5 NAME 'pais'
      DESC 'Nacionalidad del Usuario UNL'
      SUP name )

# definición del atributo Provincia
attributetype ( 3.0.0.6 NAME 'provincia'
      DESC 'Provincia del Usuario UNL'
      SUP name )

# definición del atributo Cantón
attributetype ( 3.0.0.7 NAME 'canton'
      DESC 'Canton del Usuario UNL'
      SUP name )

# definición del atributo Parroquia
attributetype ( 3.0.0.8 NAME 'parroquia'
      DESC 'Parroquia del Usuario UNL'
      SUP name )
```

 # definición del atributo Ciudad
attributetype (3.0.0.9 NAME 'ciudad'
DESC 'Ciudad del Usuario UNL'
SUP name)

 # definición del atributo F. Nacimiento
attributetype (3.0.0.10 NAME 'fechaDeNacimiento'
DESC 'Fecha de Nacimiento del Usuario UNL'
SUP name)

 # definición del atributo Carnet Conadis
attributetype (3.0.0.11 NAME 'carnetConadis'
DESC 'Carnet Conadis del Usuario UNL'
SUP name)

 # definición del atributo Tipo de Discapacidad
attributetype (3.0.0.12 NAME 'tipoDeDiscapacidad'
DESC 'Tipo de Discapacidad del Usuario UNL'
SUP name)

 # definición del atributo Email Personal
attributetype (3.0.0.13 NAME 'emailPersonal'
DESC 'Email Personal del Usuario UNL'
SUP name)

 # definición del atributo Email Institucional
attributetype (3.0.0.14 NAME 'emailInstitucional'
DESC 'Email Institucional del Usuario UNL'
SUP name)

 # definición del objectclassUsuariosUnl
 # extiende de person (definido en core.scheme de LDAP)
 # son forzosos los atributos ssn, dni, sexo, ...
 # puede contener los atributos direccion, provincia, canton, ...
objectclass (3.5.0.1 NAME 'UsuariosUnl'
DESC 'Representa un UsuarioUnl'
SUP top
MUST (ssn $ dni $ sexo $ pais $ ciudad $ fechaDeNacimiento $ emailPersonal)
MAY (direccion $ provincia $ canton $ parroquia $ carnetConadis&tipoDeDiscapacidad $ emailInstitucional))

Anexo 4. Código para crear usuarios en base a los Nombres y Apellidos

```
public class Docente {
   private String cedula;
   private String nombres;
   private String apellidos;

   public String getCedula() {
      return cedula;
   }
   public void setCedula(String cedula) {
      this.cedula = cedula;
   }
   public String getNombres() {
      return nombres;
   }
   public void setNombres(String nombres) {
      this.nombres = nombres;
   }
   public String getApellidos() {
      return apellidos;
   }
   public void setApellidos(String apellidos) {
      this.apellidos = apellidos;
   }
}
```

****

```
public class Algoritmo {

   public String getInicialPrimerNombre(String primerNombre){
      //nombres.split(" ")[0]
      return primerNombre.split(" ")[0].charAt(0)+"";
   }

   public String getInicialSegundoNombre(String segundoNombre){
      if(segundoNombre.split(" ").length==1)
         return "";
      else
         return segundoNombre.split(" ")[segundoNombre.split(" ").length-1].charAt(0)+"";
   }

   public String getApellidoPaterno(String apellidoPaterno){
      return apellidoPaterno.split(" ")[0];
   }
```

```
    public String getApellidoMaterno(String apellidoMaterno){
        if(apellidoMaterno.split(" ").length==1)
            return "";
        else
            return apellidoMaterno.split(" ")[apellidoMaterno.split(" ").length-1].charAt(0)+"";
    }

    public List<String> guardar(String usuario, List<String> lista,List<String>listaCompleta){
        if(!lista.contains(usuario)){
            listaCompleta.add(usuario);
        }
        else{
            int contador = getNumeroUsuario(usuario, lista);
            if((contador-1)>0)
                listaCompleta.add(usuario+(contador-1));
            else
                listaCompleta.add(usuario);
        }
        return listaCompleta;
    }

    public int getNumeroUsuario(String usuario, List<String> lista){
        int cont=0;
        for (String u : lista) {
            if(u.equals(usuario))
                cont++;
        }
        return cont;
    }
}
```

****

```
public class Archivo {

    Algoritmo algoritmo;
    List<String> lista;
    List<String> listaCompleta;

    public Archivo(){
        algoritmo = new Algoritmo();
        lista = new ArrayList<String>();
        listaCompleta = new ArrayList<String>();
    }

    public void leer(String url) throws FileNotFoundException, IOException{
        DataInputStream entrada=new DataInputStream(new FileInputStream(url));
        try {
            String linea;
            while ((linea=entrada.readLine())!=null) {
                //System.out.println(linea.split("\t")[0]+" "+linea.split("\t")[1]+linea.split("\t")[2]);
```

```
            String cedula = linea.split("\t")[0];
            String nombres = linea.split("\t")[1];
            String apellidos = linea.split("\t")[2];
            String usuario =
algoritmo.getInicialPrimerNombre(nombres)+algoritmo.getInicialSegundoNombre(nombres)+algo
ritmo.getApellidoPaterno(apellidos)+algoritmo.getApellidoMaterno(apellidos);
            lista.add(usuario);
            //usuarioEduroam = usuarioEduroam+""+
"\n"+cedula+";"+nombres+";"+apellidos+";"+usuario;
            listaCompleta = algoritmo.guardar(usuario, lista,listaCompleta);
            //System.out.println(cedula+";"+nombres+";"+apellidos+";"+usuario);
         }
      }catch (EOFException e) {}
      entrada.close();
   }

   public void escribir(String url) throws FileNotFoundException, IOException{
      DataOutputStream salida=new DataOutputStream(new FileOutputStream(url));
      try {
         salida.writeChars(usuarioEduroam);
      }catch (EOFException e) {}
      salida.close();
   }

   public void imprimir(){
      for (String string : listaCompleta) {
         System.out.println(string);
      }
   }

   public static void main(String[] args) throws FileNotFoundException, IOException {
      Archivo a = new Archivo();
      a.leer("/home/rene/Desktop/docentes.csv");
      a.imprimir();
      a.escribir("/home/rene/Desktop/listado.csv");
   }
}
```

****

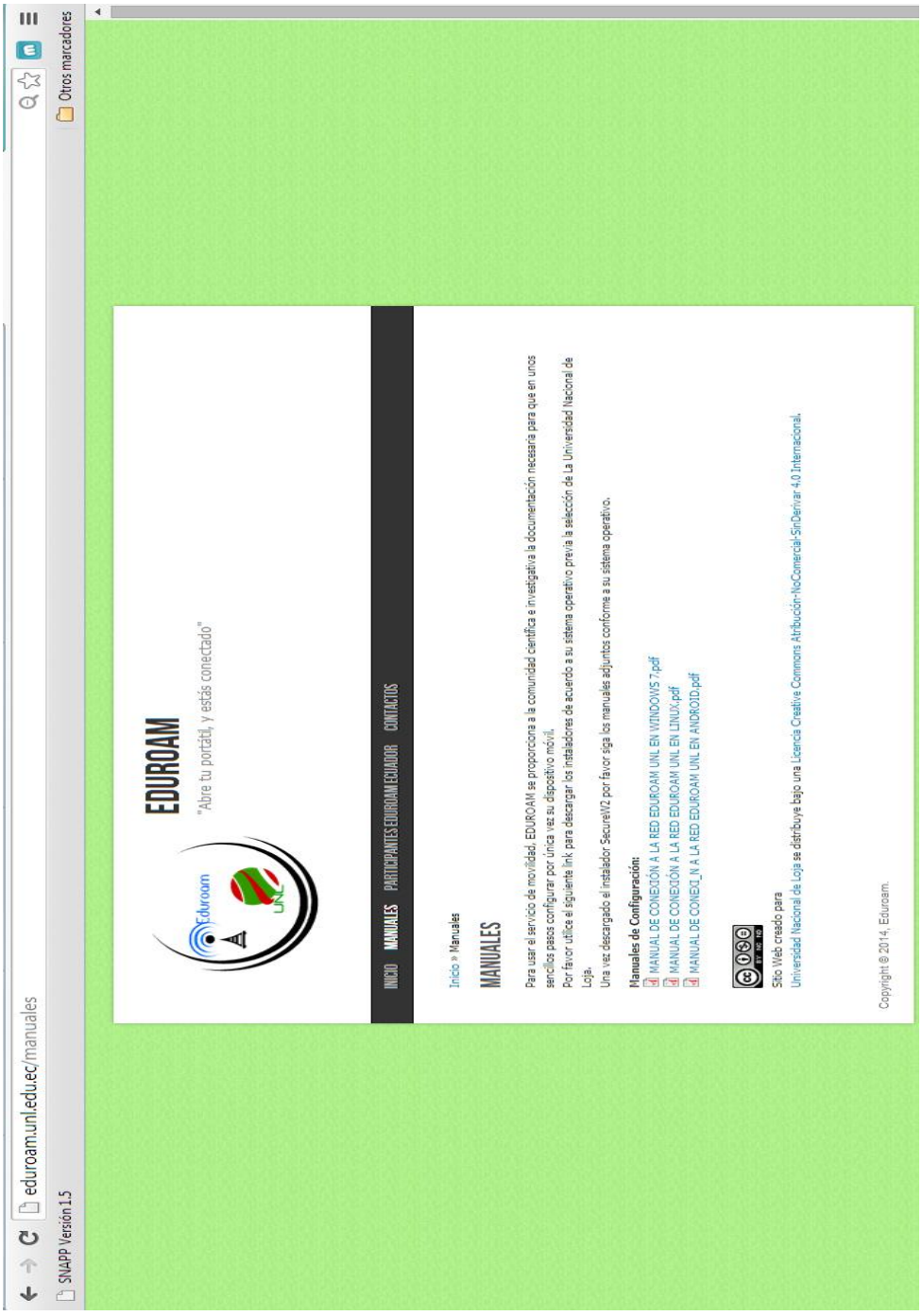
```
public class ScriptJennifer {

   public static void main(String[] args) throws FileNotFoundException, IOException {
      Archivo a = new Archivo();
      a.leer("/home/rene/Desktop/docentes.csv");
   }
}
```

Anexo 5. Convertir archivos CSV a LDIF

```
# Script para convertir archivos CSV a LDIF
clear
echo
echo
echo " ###################### Programa de conversión CSV a LDIF ################### "
echo
echo "Nombre del archivo a ser convertido:"
read arquivo1

echo "Delimitador a ser utilizado:"
read delimitador
sed '1,$s/"//g' $arquivo1 > /tmp/arquivo2
cont=1

while [ $cont -le 510 ]
do

f1=$(head -n$cont /tmp/arquivo2 | cut -f1 -d$delimitador | tail -n1)
f2=$(head -n$cont /tmp/arquivo2 | cut -f2 -d$delimitador | tail -n1)
f3=$(head -n$cont /tmp/arquivo2 | cut -f3 -d$delimitador | tail -n1)
f4=$(head -n$cont /tmp/arquivo2 | cut -f4 -d$delimitador | tail -n1)
f5=$(head -n$cont /tmp/arquivo2 | cut -f5 -d$delimitador | tail -n1)
f6=$(head -n$cont /tmp/arquivo2 | cut -f6 -d$delimitador | tail -n1)
f7=$(head -n$cont /tmp/arquivo2 | cut -f7 -d$delimitador | tail -n1)
f8=$(head -n$cont /tmp/arquivo2 | cut -f8 -d$delimitador | tail -n1)
f9=$(head -n$cont /tmp/arquivo2 | cut -f9 -d$delimitador | tail -n1)
f10=$(head -n$cont /tmp/arquivo2 | cut -f10 -d$delimitador | tail -n1)
f11=$(head -n$cont /tmp/arquivo2 | cut -f11 -d$delimitador | tail -n1)
f12=$(head -n$cont /tmp/arquivo2 | cut -f12 -d$delimitador | tail -n1)
f13=$(head -n$cont /tmp/arquivo2 | cut -f13 -d$delimitador | tail -n1)
f14=$(head -n$cont /tmp/arquivo2 | cut -f14 -d$delimitador | tail -n1)
f15=$(head -n$cont /tmp/arquivo2 | cut -f15 -d$delimitador | tail -n1)

echo dn:uid=$f1,ou=$f11,ou=$f12,dc=$f13,dc=$f14,dc=$f15 >> docentesUnl.ldif
echo uid:$f1 >> docentesUnl.ldif
echo userPassword: $f2 >> docentesUnl.ldif
echo dni:$f2 >> docentesUnl.ldif
echo cn:$f3 >> docentesUnl.ldif
echo sn:$f4 >> docentesUnl.ldif
echo ssn:$f5 >> docentesUnl.ldif
echo sexo:$f7 >> docentesUnl.ldif
echo pais:$f8 >> docentesUnl.ldif
echo ciudad:$f9 >> docentesUnl.ldif
echo fechaDeNacimiento:$f10 >> docentesUnl.ldif
echo emailInstitucional:$f6 >> docentesUnl.ldif
echo objectClass:top >> docentesUnl.ldif
echo objectClass:person >> docentesUnl.ldif
echo objectClass:inetOrgPerson >> docentesUnl.ldif
echo objectClass:UsuariosUnl >> docentesUnl.ldif
```

```
echo "" >> docentesUnl.ldif

cont=`expr $cont + 1`
done

rm /tmp/arquivo2

echo "Archivos convertidos con éxito"

cat docentesUnl.ldif
```

Anexo 6. Sitio Oficial de Eduroam de la Universidad Nacional de Loja



Anexo 7. Usuarios Itinerantes obtenidos por correo

Franklin Sanchez E. <fsanchez@pucesi.edu.ec> 31 de mar. (hace

para mí, Gustavo

Estimado Fernando, mucho gusto.

Por el presente le envío las credenciales para realizar las pruebas respectivas, cualquier novedad favor comunicarnos.

Credenciales:
Nombre de usuario: usuarioldap@pucesi.edu.ec
Clave: [redacted]

Saludos cordiales,

Franklin
PUCESI

Claudio Chacon <claudio.chacon@cedia.org.ec> 3(

para mí, Luis, Jennifer

EStimados

El dia de hoy me encontre con Milton, quien dio luz verde para continuar.

Ya se encuentra en el federado nacional acceso al radius,

nombre del federado: ftlr.cedia.org.ec (por favor colocar el nombre envez de ip, por cuestiones de redundancia futura)
clave: [redacted]

usuarios de pruebas:

test@ucuenca.edu.ec clave: [redacted]

testraap@test.rediris.es [redacted]
raap@inictel-uni.edu.pe [redacted]

saludos

Claudio Chacon A.
Coordinador Técnico de CEDIA
PGP KEY: 8FFA0931
claudio.chacon@cedia.org.ec
CEDIA
Av. 12 de Abril s/n, Universidad de Cuenca · Edif. Laboratorios Tecnológicos, 3er. Piso
(593) 7 405 1000 ext. 4220
www.cedia.org.ec

Anexo 8. Solicitud de prueba a la PUCESI

Fernando Castillo <jfcastillo@unl.edu.ec>
para Franklin

Saludos Cordiales

Ing. Franklin le agradezco por habernos proporcionado las credenciales, por comentarle que hemos hecho las pruebas respectivas en android y ubuntu, logrando conectarnos sin ningún problema.

Por otro lado quería preguntarles si se han conectado a EDUROAM a través de windows 8 usando el instalador, pregunto esto ya que nosotros no hemos logrado establecer conexión en esta plataforma y queríamos saber si solo nos pasa a nosotros o también sucede en otras universidades.

Anteriormente les había comentado que la implantación de EDUROAM en la UNL es parte de un Proyecto de Fin de Carrera, por lo que quería solicitarles su ayuda para comprobar que se pueda autenticar con credenciales de la Universidad Nacional de Loja en la Pontificia Universidad Católica del Ecuador Sede Ibarra,

Credenciales
USUARIO: eduroam.ec@unl.edu.ec
CLAVE:_eduroamunl

Esperando me puedan enviar capturas técnicas de registro en el RADIUS, de antemano les agradezco.

Anexo 9. Articulo Técnico

Implementation of Eduroam as Wirelless Infraestructure on the Campus of National University of Loja

Implementación de Eduroam como Infraestructura Inalámbrica en el Campus de la Universidad

J. J. Loayza, J. F. Castillo and L. A. Chamba.

***Abstract*– The paper presents proposes the integration to the global mobility in response to the complex administrative process needed to use the wireless network each time to play the visitor role in an educational institution and / or research. Today, the mobile connectivity takes the name of Eduroam (Educational Roaming), a project to worldwide level created by scientific / academic community that allows students and researchers from the participating institutions have an Internet connection through a secure and stable authentication. In the same form, disclosed a solution to the problem of computing security has the National University of Loja (UNL) in connection to the wireless network. This security problem is located in the free access to the network by the general public, the overhead in addressing institutional resources, in free exposure of confidential information to unknown users. The implementation consisted mainly in the protocol authentication, authorization and recording of user activity, well known for computing network management, RADIUS (Remote Authentication Dial-In User Server). To give a tone of innovation and break with the traditional way of storing, was performed the relevant settings for installing an LDAP (Lightweight Directory Access Protocol) server to manage users whose credentials are protected by the SSL (Secure Socket Layer) and TLS (Transport Layer Security) cryptographic protocols managed by the OpenSSL tool. And finally, as in any authentication system is important need to manage user records, proceed to configure a general-purpose software that manages access points as DaloRADIUS.**

***Resumen*– El presente artículo propone la integración a la movilidad global como respuesta al complejo trámite administrativo necesario para usar la red inalámbrica cada vez que se desempeñe el rol de visitante en una institución educativa y/o investigativa. Hoy por hoy, la conectividad móvil toma el nombre de Eduroam, un proyecto a nivel mundial creado por la comunidad científica/académica que permite que los estudiantes e investigadores de las instituciones participantes tengan conexión a Internet mediante una autenticación segura y estable. En la misma medida, se da a conocer una de las soluciones al problema de seguridad informática que presenta la Universidad Nacional de Loja (UNL) en su conexión a la red inalámbrica. Dicho problema de seguridad radica en el libre acceso a la red por parte de la ciudadanía en general, en la sobrecarga en los recursos de direccionamiento institucionales, en la libre exposición de información confidencial a usuarios desconocidos. La implementación consistió principalmente en el protocolo de autenticación, autorización y registro de la actividad de los usuarios, muy bien conocido para la gestión de redes informáticas, RADIUS. Para dar un tono de innovación y romper con la tradicional forma de almacenamiento, se realizó las configuraciones pertinentes para la instalación de un servidor LDAP que administre a los usuarios cuyas credenciales son protegidas mediante los protocolos criptográficos SSL y TLS gestionados por la herramienta OpenSSL. Y finalmente, como en todo sistema de autenticación resulta imperiosa la necesidad de gestionar los registros de los usuarios, se procede a configurar un software de propósito general que gestione los puntos de acceso como DaloRADIUS.**

***Keywords*– Movility, eduroam, scientific/academic, RADIUS, trust, OpenSSL.**

Palabras Clave- Movilidad, eduroam, científica/académica, RADIUS, confianza, OpenSSL.

J. J. Loayza, Universidad Nacional de Loja, Loja, Ecuador, jloayza@unl.edu.ec
J. F. Castillo, Universidad Nacional de Loja, Loja, Ecuador, jfcastillo@unl.edu.ec
L. A. Chamba, Universidad Nacional de Loja, Loja, Ecuador, lachamba@unl.edu.ec

I. INTRODUCCIÓN

La movilidad de usuarios en redes académicas y/o de investigación se caracteriza principalmente por la oportunidad de compartir recursos a través de una serie de redes interconectadas, promoviendo de esta manera el desarrollo constante de las sociedades de la información, acortando las distancias entre ciudades, países y continentes; y sobre todo dando cabida a la rápida difusión del conocimiento y los avances tecnológicos que se genera en el día tras día.

En el transcurso del tiempo han ido apareciendo todo tipo de dispositivos de comunicación que permiten al usuario estar conectado a Internet en cualquier lugar (roaming) gracias a las tecnologías inalámbricas. No solamente PC's portátiles sino también teléfonos móviles, tablets y muchos más que son difíciles de visionar en el presente pero que seguro serán realidad en un futuro muy cercano.

El modelo de conectividad a Internet está evolucionando rápidamente hacia un enfoque basado en la movilidad de los usuarios gracias a la aparición de nuevos dispositivos cada vez más inteligentes que a su vez van de la mano con las masivas áreas de cobertura de las redes de acceso. Lo que se quiere lograr gracias al constante avance de las redes es que los usuarios puedan siempre estar conectados de manera transparente, independiente de la red inalámbrica en la que se encuentren.

Un proyecto esencialmente actual y cuyo principal objetivo reside en la movilidad es, Eduroam, creado por y para la comunidad científica/académica para el uso de estudiantes e investigadores basado fundamentalmente en la autenticación segura [1]. Eduroam nació en España para luego extenderse por Europa, Asia, Estados Unidos y Canadá facilitando la conectividad móvil entre las instituciones participantes, en la actualidad se está abriendo camino por territorio latinoamericano tales como Argentina, Brasil, Chile, Perú, Nicaragua y Ecuador. Pero, ¿cómo funciona Eduroam? Es preciso empezar mencionando que la red Eduroam, es la interconexión de varios servidores los cuales están organizados en un orden jerárquico, que en términos del proyecto se puede distinguir, por un lado a los servidores locales, destinados a gestionar usuarios de la propia institución y a redireccionar a aquellos que pertenecen a otras instituciones, y por otro lado a los servidores federados, que se encargan de recibir aquellas peticiones de usuarios enviadas por los servidores locales para ser re direccionadas al servidor correcto [2]; este proceso se canaliza mediante el análisis del dominio, el cual permite identificar la institución del usuario solicitante que luego de un proceso de intercambio de certificados provee la conexión a la red inalámbrica Eduroam.

El dominio compone una parte del usuario, el usuario en definitiva es una dirección de correo institucional que junto con su respectiva contraseña constituye la credencial, ahora bien, en el caso particular de la UNL todas las credenciales de los estudiantes y docentes investigadores se encuentran almacenadas en un servidor de directorio al cual el servidor local realiza la consulta respectiva con cada petición de conexión que reciba.

II. ESTADO DEL ARTE

A. *Eduroam*

Eduroam [3] [4] es una iniciativa a nivel internacional que tiene el objetivo de crear un espacio único de movilidad entre las instituciones adscritas al proyecto.

Este espacio único de movilidad consiste en un amplio grupo de organizaciones académicas de ámbito nacional e internacional, que en base a una política de uso y una serie de requerimientos tecnológicos y funcionales, permiten que sus usuarios puedan desplazarse entre ellas, disponiendo en todo momento de servicios móviles que pudieran necesitar.

El objetivo último sería que un usuario al llegar a otra institución dispusiera, de la manera más transparente posible, de un entorno de trabajo virtual con conexión a Internet, acceso a servicios y recursos de su universidad origen, así como de acceso a servicios y recursos de la institución que en ese momento le acoge. Es responsabilidad del usuario móvil respetar las políticas de uso tanto de la institución visitada, como la de su organización origen.

Eduroam es una infraestructura basada en RADIUS que utiliza como tecnología de seguridad 802.1X para permitir la movilidad entre las distintas instituciones que la forman [5]. En la Fig. 1, podemos visualizar la infraestructura que implementa Eduroam.

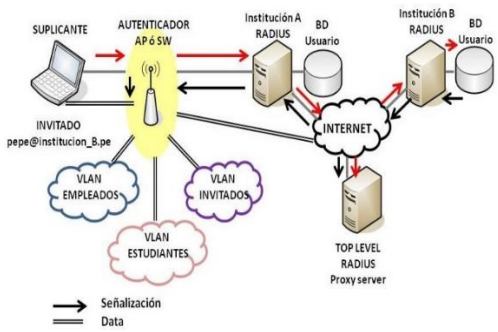


Figura 1. Infraestructura de Red Eduroam

B. Tecnología Radius AAA (authentication, authorization, and accounting)

RADIUS es un protocolo que nos permite gestionar la "autenticación, autorización y registro" de usuarios remotos sobre un determinado recurso [6].

- Autenticación *(authentication)* hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.
- Autorización (*authorization*) se refiere a conceder servicios específicos (entre los que se incluye la "negación de servicio") a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema.
- Registro *(accounting)* a menudo traducido también como contabilidad se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio.

C. Estándar 802.1X

El estándar 802.1X es normado por la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) el cual define al 802.1X como el acceso seguro a la red por medio de puertos, los mismos que son de acceso público, el estándar trabaja cuando existe una conexión punto a punto donde existe un cliente o usuario que es el que realiza la petición a un servidor el cual restringe el acceso cerrando el puerto cuando la autenticación es inválida o abriendo el puerto si la autenticación se da de forma correcta [7].

Este protocolo funciona de manera conjunta con otros, que suelen ser EAP (Extensible Authentication Protocol) y RADIUS. La relación entre ellos se describe brevemente a continuación [8]:

- EAP define una serie de mensajes que soportan el protocolo de alto nivel que verdaderamente lleva a cabo la autenticación. En un sistema como éste, los mensajes que el solicitante envía al autenticador deberán ser reenviados hacia el servidor de autenticación, que será otro sistema remoto.
- RADIUS se usa en la interfaz Autenticador - Servidor de Autenticación. Como el sistema de autenticación está en una localización remota, estos mensajes EAP requieren de un protocolo que les permita alcanzar su destino. El protocolo RADIUS permite que estos mensajes lleguen a su destino.

D. Protocolo EAP-TTLS

Los principales rasgos de TTLS que se tienen en cuenta son [9]:

- Soporta protocolos de autenticación basados en login y password (no es necesario disponer de certificado en la parte del usuario).
- La información basada en el password y la identidad del usuario no son observables en el canal de comunicación entre el nodo cliente y el proveedor de servicio lo que le protege contra ataques de diccionario y suplantaciones.
- El proceso de autenticación finaliza en la distribución de la información de clave compartida entre el cliente y el punto de acceso.
- El mecanismo de autenticación soporta traspasos entre pequeños dominios en los que el usuario no tiene relación previa (roaming), gracias a su definición en 802.11. Sin embargo 802.1X estipula que mientras se esté re-autenticando al cliente éste no tendrá acceso a la red.

III. SITUACIÓN ACTUAL DE LA MOVILIDAD EN LA UNL

A. *Análisis actual de la red inalámbrica*

Actualmente la UNL cuenta con una red inalámbrica implementada en el campus universitario denominado con el SSID (Service Set IDentifier): "S.I. UNL" que en sus inicios de implantación proveía del servicio únicamente a usuarios registrados o que forman parte de la universidad, por medio de un inicio de sesión o portal cautivo ingresaban sus credenciales (usuario y contraseña) que a su vez son consultadas al Servicio Web del Sistema de Gestión Académica de la UNL.

En la actualidad el inicio de sesión o portal cautivo del servicio inalámbrico no se encuentra funcionando.

B. *Wireless Lan Controller 5500 Cisco (WLC)*

La red inalámbrica cuenta con un equipo WLC cuya arquitectura permite configurar y controlar los 17 puntos de acceso distribuidos en el campus universitario de forma centralizada a través de una interfaz Web, como se muestra en la Fig. 2.

Number of APs	17	
AP Name	**AP Model**	**AP MAC**
AP_Economia_UNL	AIR-CAP1552E-A-K9	54:78:1a:0d:95:80
AP_Adm_Central	AIR-CAP1552E-A-K9	1c:e6:c7:2a:8d:e0
AP_Obelisco_Juridica	AIR-CAP1552E-A-K9	1c:e6:c7:2a:91:e0
AP_TrabajoSocial_JuB2	AIR-CAP1552E-A-K9	20:3a:07:98:49:60
AP_Postgrado_Salud	AIR-CAP1552E-A-K9	54:78:1a:0c:55:20
AP_Torre_Salud	AIR-CAP1552E-A-K9	54:78:1a:0c:71:00
AP_Artes_Educativa	AIR-CAP1552E-A-K9	34:a8:4e:51:d5:60
AP_Idiomas_Educativa	AIR-CAP1552E-A-K9	1c:e6:c7:2a:97:60
AP_Med_Unl	AIR-CAP1552E-A-K9	54:78:1a:0c:7a:c0
AP_Nivelacion	AIR-CAP1552E-A-K9	34:a8:4e:51:ed:00
AP_Salud	AIR-CAP1552E-A-K9	1c:e6:c7:2a:c9:00
AP_Biblioteca_Agropecuaria	AIR-CAP1552E-A-K9	1c:e6:c7:2a:09:c0
AP_ComunicacionSocial_Educati	AIR-CAP1552E-A-K9	20:3a:07:98:2c:60
AP_Sistemas_Energia	AIR-CAP1552E-A-K9	54:78:1a:0c:72:60
AP_Post_Educativa	AIR-CAP1552E-A-K9	1c:e6:c7:2a:97:40
AP_Colegio_Educativa	AIR-CAP1552E-A-K9	54:78:1a:0c:75:60
AP_Forestal_Agropecuaria	AIR-CAP1552E-A-K9	54:78:1a:0d:b8:20

Figura 2. Nombre de los Access Point en el WLC.

El controlador gestiona la configuración y operaciones de control como autenticaciones 802.1x. El tráfico de datos inalámbricos viaja por la vía de comunicación entre Access Point y el controlador.

C. *AP (Access Point) Aironet 1552E*

El diseño de la red inalámbrica en la UNL implementa varios puntos de acceso con dispositivos networking Aironet 1552E que poseen antenas omnidireccionales distribuidos en las diferentes infraestructuras físicas del campus universitario.

IV. CASO DE ESTUDIO

Para implementar Eduroam en la UNL se tuvo el asesoramiento técnico del GT- Movilidad de RedCLARA, esto facilitó la instalación y configuración de dos servidores RADIUS.

Los servidores se montaron en un equipo BLADE HP PROLIANT BL460c G7 con tecnología KVM, bajo el Sistema Operativo GNU/Linux con distribución Debian 6.0 Squeeze.

A. *Servidor Radius Eduroam UNL*

Para las configuraciones del servidor RADIUS Eduroam se procede a instalar algunos paquetes y librerías necesarias: *apt-get install freeradius freeradius-ldap freeradiusmysql make pkg-config vim nmap mysql-server mysql-client libssl-dev libgnutls-dev libsnmp-dev libmysqlclient-dev libldap-dev libtool libpcap0.8-dev gnutls-bin*

Mediante la siguiente línea de comando *openssl req -new -x509 -extensions v3_ca - keyout private/ca.key -out ca.crt* se crean la llave pública y privada de la Autoridad Certificadora, haciendo una petición en formato X509 al paquete openssl. La llave privada se guarda en el archivo ca.key (Fig. 3) y su llave pública en el archivo ca.crt (Fig. 4).

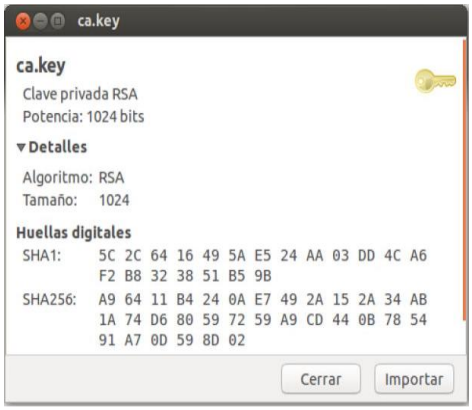


Figura 3. Llave privada en el servidor RADIUS

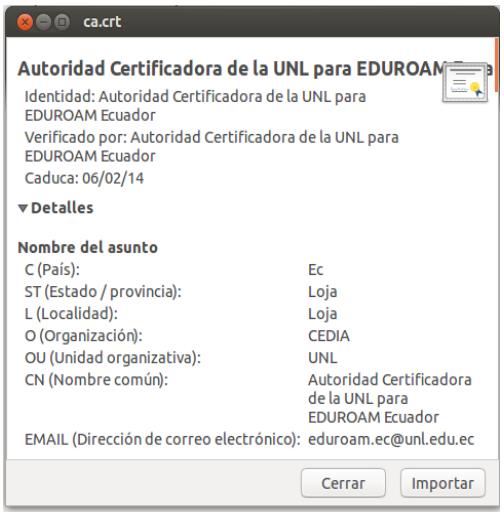


Figura 4. Llave pública en el servidor RADIUS.

Luego se procede a crear el certificado de consulta para el servidor RADIUS Eduroam UNL. El certificado de consulta se crea con la siguiente línea de comando *openssl req -new -keyout radius.key -out radius.unl.edu.ec.csr -days 3650*. El archivo radius.key (Fig. 5) contiene la llave privada del servidor RADIUS.

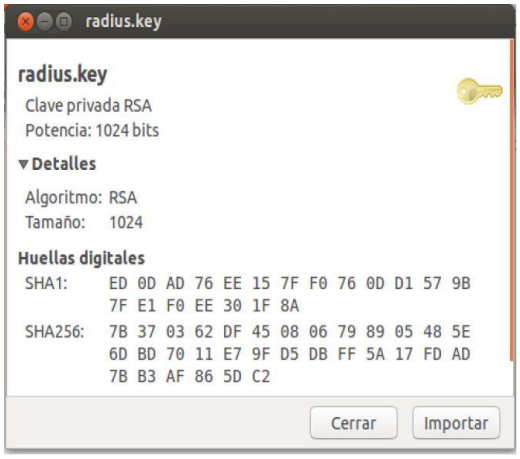


Figura 5. Certificado privado del servidor RADIUS.

Lo siguiente es firmar el certificado de consulta para el servidor RADIUS, se lo realiza con la línea de *comandos openssl ca -policy policy_anything -out radius.unl.edu.ec.crt -extensions xpserver_ext -extfile xpextensions -infiles radius.unl.edu.ec.csr*. La llave pública del servidor RADIUS está contenida en el archivo radius.unl.edu.ec.crt (Fig. 6).

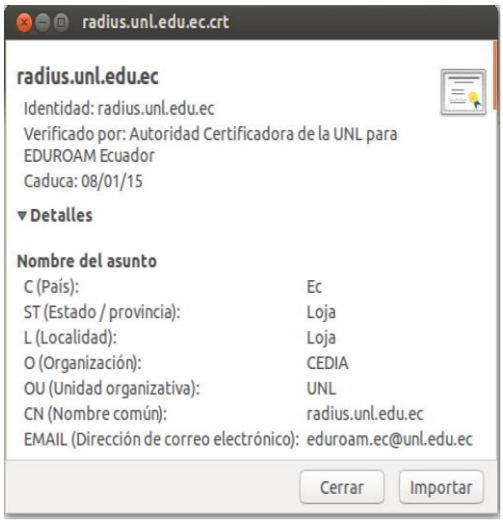


Figura 6. Certificado público del Servidor RADIUS

En el archivo *clients.conf* se registra los clientes del servidor RADIUS local Eduroam UNL, tal es el caso del servidor RADIUS federado Ecuador como se muestra en la Fig. 7 y el WLC visualizado en la Fig. 8.

```
client cedia_federado_ftlr {
        #  Allowed values are:
        #       dotted quad (1.2.3.4)
        #       hostname    (radius.example.com)
        #ipaddr = 172.16.63.61
        #ipaddr = 192.188.49.39
        ipaddr = ftlr.cedia.org.ec
        secret = [redacted]
        #  OR, you can use an IPv6 address, but not both
        #  at the same time.
#       ipv6addr = ::   # any.  ::1 == localhost
```

Figura 7. Cliente Servidor RADIUS Federado

```
client WLC {
  ipaddr =[redacted]
  secret= [redacted]
  shortname= AP-UNL
  nastype=other
}
```

Figura 8. Cliente WLC

En el archivo *eap.conf* se determina el tipo de protocolo de autenticación EAP-TTLS que es utilizado en la comunidad del servicio de movilidad Eduroam, como se muestra en la Fig. 9

```
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 9. Configuración del protocolo de autenticación

Se determina que el tipo de repositorio donde se va a consultar los usuarios, que en este caso es el servidor de directorio LDAP (Fig. 10); el cual contiene los diferentes usuarios de la UNL.

```
DEFAULT
        User-Name=  `%{User-Name}`,
        Fall-Through = yes
user Cleartext-Password := "pass"
DEFAULT Auth-Type = LDAP
    Fall-Through = 1
#DEFAULT Auth-Type = SQL
#     Fall-Through = 1
```

Figura 10. Configuración de consulta al LDAP

En el archivo *proxy.conf*, se crea un bloque donde se especifica que los usuarios que posean el *realm (@unl.edu.ec)* se autenticarán en el servidor local como se muestra en la Fig. 11 y segundo bloque donde se especifica que los usuarios que posean un *realm* distinto al de la institución, la solicitud se reenvía al servidor RADIUS federado, como se muestra en la Fig. 12.

```
realm unl.edu.ec {
        type=radius
        authhost=LOCAL
        accthost=LOCAL
}
```

Figura 11. Configuración *realm* para el dominio *unl.edu.ec*

```
home_server ftlr {
    type = auth+acct
    ipaddr = ftlr.cedia.org.ec
    port = 1812, 1813
    secret = [redacted]
    response_windows = 20
    zombie_period = 40
    revive_interval = 60
    status_check = status-server
    check_interval = 30
    num_answers_to_alive = 3
 }
home_server_pool EDUROAM-FTLR {
        type=fail-over
        home_server=ftlr
}
```

Figura 12. Configuración *realm* para el RADIUS federado

El servidor RADIUS Eduroam UNL tiene como función principal:

- Resolver las solicitudes de su propio dominio *(@unl.edu.ec):* es decir si un usuario local identifica el SSID eduroam dentro del campus universitario.
- Reenviar al servidor RADIUS federado del Ecuador las solicitudes de otros dominios distintos al *(@unl.edu.ec):* se trata de un usuario visitante o itinerante, el cual es identificado por su dominio que no pertenece a la UNL, para lo cual se reenvía la solicitud al servidor RADIUS federado Ecuador.
- Aceptar solicitudes del servidor RADIUS federado Ecuador: si un usuario con dominio *@unl.edu.ec* se encuentra en otra institución y esta forma parte de la iniciativa Eduroam, se remite la solicitud a través del servidor RADIUS federado Ecuador.

B. Servidor RADIUS FEDERADO de prueba para Ecuador

Para las configuraciones del servidor RADIUS federado de prueba para Eduroam se procede a instalar los paquetes y librerías: *apt-get install freeradius, freeradius-utils.*

Seguidamente en el archivo *clients.conf* se registra los diferentes clientes del servidor RADIUS federado de prueba para Ecuador, que pueden ser servidores RADIUS locales a nivel nacional que forman parte de Eduroam. En la Fig. 13 se muestra como ejemplo el ingreso del servidor RADIUS local UNL a la constelación roaming.

```
client UNL {
        #  Allowed values are:
        #       dotted quad (1.2.3.4)
        #       hostname    (radius.exampl
        ipaddr = [redacted]
        secret = [redacted]
        require_message_authenticator = no
        netmask = 32
        shortname       = org-UNL
        #  OR, you can use an IPv6 address
```

Figura 13. Clientes del servidor RADIUS federado de prueba para Ecuador.

Luego en el archivo *proxy.conf* se configura los diferentes *realm* o dominios a nivel de Ecuador que

permitirá reenviar las solicitudes a los distintos servidores RADIUS institucionales en la Fig. 14 se muestra el ingreso del *realm* de la UNL.

```
realm "~^(.*\\.)?unl\\.edu\\.ec$" {
  type = radius
  authhost = [redacted]:1812
  accthost = [redacted]:1813
   secret = 1234
   nostrip
}
```

Figura 14. Ingreso del *realm* de la UNL.

Una vez realizadas las configuraciones del servidor RADIUS federado de prueba para Ecuador, por disposición del responsable del servicio de movilidad Eduroam en Latinoamericana, se determinó al Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA) será el encargado de difundir el servicio a nivel nacional por lo que se implementó el servidor RADIUS federado para Ecuador el mismo que es administrado por el CEDIA, para utilizar el servicio Eduroam, la UNL procede a enlazarse con dicho servidor federado.

El servidor RADIUS federado para Ecuador tiene la siguiente funcionalidad:

- Aceptar y reenviar solicitudes de servidores RADIUS de las instituciones a nivel de Ecuador que formen parte de Eduroam.
- Aceptar solicitudes que provengan de servidores RADIUS de mayor nivel, a la vez reenviarlas al servidor RADIUS correspondiente de acuerdo al dominio

V. EXPERIMENTACIÓN CON EDUROAM

Dentro del mapa global de instituciones que disponen de Eduroam, la UNL ya es parte de la misma, tal como se muestra en la Fig. 15 o también se lo puede visualizar a través del link http://monitor.eduroam.org/eduroam map.php?type=all

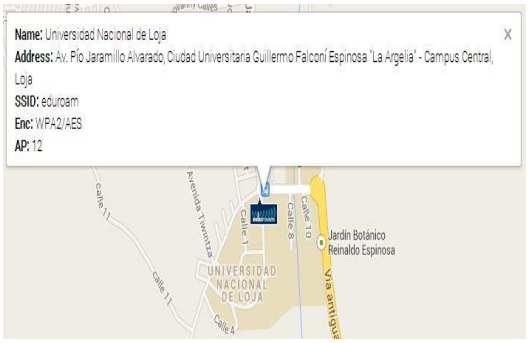


Figura 15. Mapa global de instituciones con Eduroam a nivel mundial

Así mismo se encuentra disponibles los instaladores para los usuarios de la UNL en el sitio oficial https://cat.eduroam.org/ como se muestra en la Fig. 16.

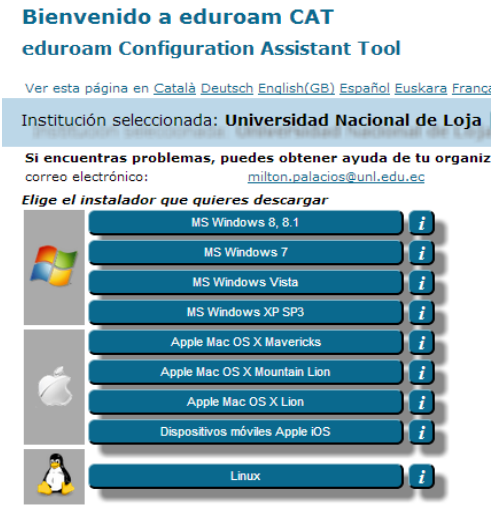


Figura 16. Instaladores en las diversas plataformas para el dominio unl.edu.ec

Las pruebas de conexión a Eduroam se realizaron en cuatro sistemas operativos:

- GNU Linux/Ubuntu
- Windows/Windows 7
- Android
- Mac OS X/Marverick

Para evaluar el funcionamiento de Eduroam en las plataformas antes mencionadas, se determina realizar el proceso de autenticación/validación con un usuario de prueba: eduroam.ec@unl.edu.ec el mismo que está agregado en el servidor LDAP, dentro del

grupo Personal Administrativo y de Servicios como se muestra en la Fig. 17. Además con la ayuda de la herramienta web de administración DaloRadius, nos permite monitorear al usuario de prueba en el Servidor RADIUS EDUROAM.

Figura 17. Usuario de prueba agregado en el LDAP

- **GNU Linux/Ubuntu:** Para proceder a conectarse a la red eduroam en GNU Linux, es necesario tener la llave pública (certificado) del CA (Autoridad Certificadora), que se lo descarga del link http://www.eduroam.ec/certs/ca_eduroam_ec.pem. Para evidenciar el establecimiento de conexión, en la Fig. 18 podemos ver el SSID Eduroam, así como la dirección IP asignada, además con una captura del DaloRadius se confirma el proceso de autenticación el cual registra la dirección IP, junto con el usuario que hizo petición del servicio como se ve en la figura 19.

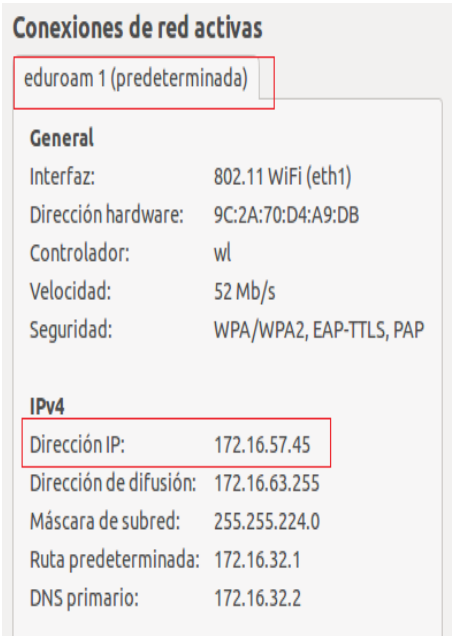


Figura 18. Parámetros de red asignados en Ubuntu

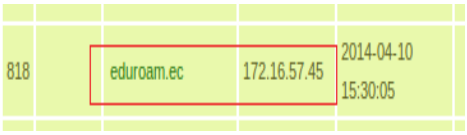


Figura 19. Autenticación/Validación en el DaloRadius-Ubuntu

- **Windows/Windows 7:** Para tener acceso a eduroam a través del Sistema Operativos Windows, es necesario tener instalada la llave pública (certificado) del CA (Autoridad Certificadora), que se lo descarga del sitio oficial de eduroam https://cat.eduroam.org/ el cual es un archivo ejecutable. Para comprobar la conexión en Windows 7 en la Fig. 20 se muestra la dirección IP, parámetros de red asignados y el SSID eduroam, además para corroborar la autenticación en la Fig. 21 tomada del DaloRadius se visualiza el usuario junto con la dirección IP asignada.

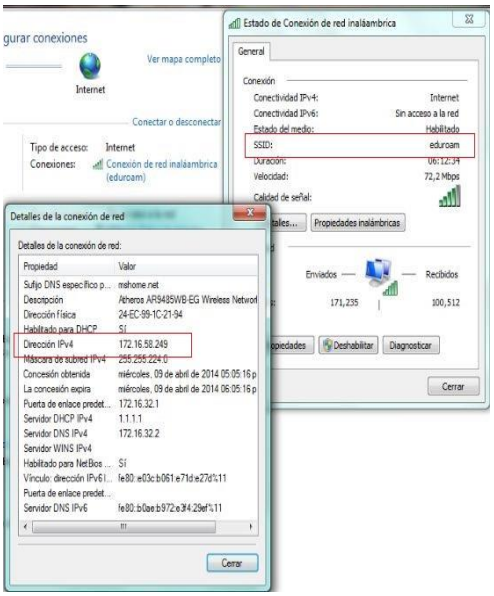


Figura 20. Parámetros de red asignados en Windows 7

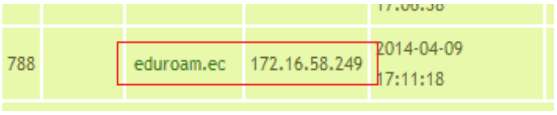


Figura 21. Autenticación/Validación en el DaloRadius-Windows 7

- **Android:** Para establecer conexión desde dispositivos Android sean Smartphone o Tablet, el proceso de conectividad es más sencillo, donde se debe configurar algunos parámetros importantes y obligatorios, como son: método EAP, autenticación de fase 2, identidad y contraseña. Se justifica la autenticación realizando una captura de los parámetros de red asignados en el dispositivo, donde se evidencia principalmente el SSID Eduroam y la dirección IP, como se muestra en la Fig. 22, además con la Fig. 23 obtenida del DaloRadius se ratifica el proceso de validación.

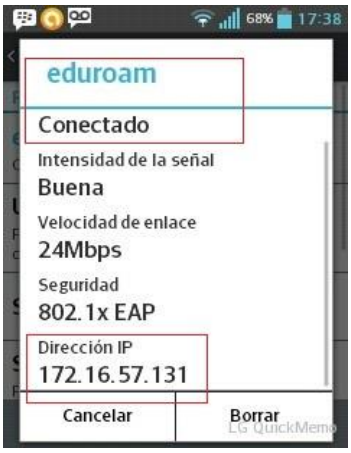


Figura 22. Parámetros de red asignados en Android

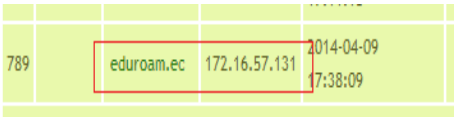


Figura 23. Autenticación/Validación en el DaloRadius-Android

- **Mac OS X/Marverick:** Como evidencia del proceso de autenticación en sistemas operativos Mac OS X, se hizo pruebas en la plataforma Marverick. En la Fig. 24 se muestra la dirección IP asignada y el SSID Eduroam, además se obtiene una captura del DaloRadius donde se comprueba su validación a través de dirección IP, como se visualiza en la Fig. 25.

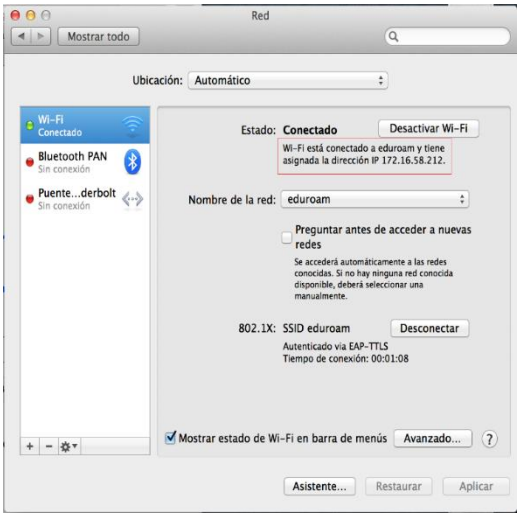


Figura 24. Parámetros de red asignados en Marverick

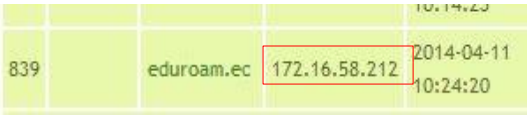


Figura 25. Autenticación/Validación en el DaloRadius-Mac OS X/Marverick

Para conocer más detallado el proceso de configuración en dispositivos móviles android y GNU Linux, así como el proceso de instalación en dispositivos Windows y Mac OS X, se encuentra disponible los manuales en la página oficial de Eduroam para la Universidad Nacional de Loja http://eduroam.unl.edu.ec/

Los datos que se van registrando por cada acceso realizado a la red inalámbrica Eduroam son: usuario, dirección IP, hora de inicio, hora de finalización, tiempo total, subida (bytes) y descargas (bytes), como se muestra en la Fig. 26

Figura 26. Datos registrados por cada acceso **en el DaloRadius**

Para evaluar el funcionamiento de la red inalámbrica Eduroam, se procede a tabular los datos obtenidos en los meses de febrero, marzo y abril del 2014, cada mes detallado por semanas.

En el mes de febrero se logró evidenciar un total de 140 accesos registrados, de los cuales 138 fueron accesos realizados por usuarios que forman parte de la Universidad Nacional de Loja y 2 accesos de usuarios itinerantes, es decir usuarios que no forman parte de la institución, ver tabla 1. Cabe indicar que fue el primer mes donde se pidió la ayuda a ciertos usuarios del AEIRNNR para evaluar el funcionamiento.

Tabla 1. Total de Accesos registrados en EDUROAM en el mes de Febrero

Nro. de Accesos		
Febrero	**Usuarios Locales**	**Usuarios Itinerantes**
Lunes 03 – Viernes 07	65	0
Lunes 10 – Viernes 14	45	0
Lunes 17 – Viernes 21	21	0
Lunes 24 – Viernes 28	7	2
Total Parcial	138	2
Total	140	

Para el mes de marzo se registra un total de 340 accesos a la red inalámbrica Eduroam, todos realizados por usuarios que pertenecen a la universidad, superando lo del mes anterior, se logra dando a conocer a los estudiantes del AEIRNNR la disponibilidad de Eduroam en la institución, ver tabla 2.

Tabla 2. Total de accesos registrados en EDUROAM en el mes de Marzo

Nro. de Accesos		
Marzo	**Usuarios Locales**	**Usuarios Itinerantes**
Lunes 03 – Viernes 07	0	0
Lunes 10 – Viernes 14	5	0
Lunes 17 – Viernes 21	68	0
Lunes 24 – Lunes 31	267	0
Total Parcial	340	0
Total	340	

Para las dos primeras semanas del mes de abril se evidencia un total de 239 accesos, de los cuales 239 son de usuarios locales y 50 de usuarios itinerantes, ver tabla 3.

Tabla 3. Total de accesos registrados en EDUROAM en el mes de Abril

Nro. de Accesos		
Abril	**Usuarios Locales**	**Usuarios Itinerantes**
Martes 01 – Viernes 04	199	40
Lunes 07 – Martes 08	40	10
TOTAL PARCIAL	239	50
TOTAL	289	

Utilizando el menú Gráficos del DaloRadius, en la Fig. 27 se presenta mediante diagrama de barras, el total de accesos realizados durante el mes de febrero, marzo y abril detallados en las tablas 1,2 y 3.

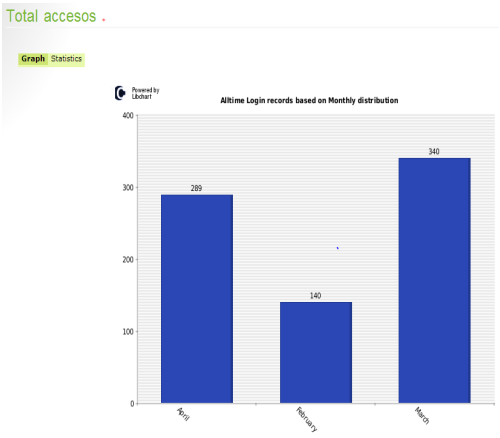


Figura 27. Total de accesos registrado al servicio de movilidad EDUROAM

Para evidenciar el proceso de movilidad en el campus universitario con usuarios itinerantes, se obtuvo las credenciales de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI), Instituto Nacional de Investigación y Capacitación de Telecomunicaciones-Universidad Nacional de Ingeniería (INICTEL-UNI) que se encuentra en Perú y la Red Española para **I**nterconexión de los Recursos Informáticos de las Universidades y Centros de Investigación (RedIRIS).

Se obtuvo capturas de autenticación/validación disponible en el DaloRadius de los usuarios usuarioldap@pucesi.edu.ec de PUCESI, raap@inictel-uni.edu.pe de INICTEL-UNI y testraap@test.rediris.es de la RedIRIS, ver Fig. 28, 29 y 30 respectivamente

654		usuarioldap	172.16.57.137	2014-04-03 15:30:09	2014-04-03 16:56:25	1 hours, 26 minutes, 16 seconds	5 K

Figura 28. Usuario registrado de la PUCESI

653		raap@inictel-uni.edu.pe	172.16.57.74	2014-04-03 15:25:46	2014-04-03 17:28:23	2 hours, 2 minutes, 38 seconds	

Figura 29. Usuario registrado de INICTEL-UNI

638		testraap@test.rediris.es	172.16.60.17	2014-04-03 09:49:37	2014-04-03 11:39:34	1 hours, 49 minutes, 57 seconds	2 K

Figura 30. Usuario registrado de RedIRIS

Finalmente una valoración importante que permite evidenciar la movilidad de usuarios que forman parte de la Universidad Nacional de Loja en otras instituciones a nivel de Ecuador es mediante el proceso de autenticación, para esto se solicitó la colaboración de la PUCESI a través del encargado de la red Eduroam, al cual se le proporcionó las credenciales del usuario de prueba de la UNL, para que realice un ensayo técnico, donde se demuestre la movilidad hacia otras universidades. La Fig. 31 se visualiza el resultado a través de un **Access-Accept** que indica que la solicitud de acceso solicitado por eduroam.ec@unl.edu.ec a la red Eduroam en PUCESI ha sido aceptada.

Figura 31. Usuario de prueba de la UNL en PUCESI

VI. DISCUSIÓN DE LA EXPERIMENTACIÓN

Los resultados son los esperados durante la implantación de la infraestructura Eduroam en la Universidad Nacional de Loja en reemplazo al modelo actual de movilidad, debido a que se realizaron pruebas con usuarios locales e itinerantes, logrando disponer del servicio de Internet/Intranet sin ningún problema. Cabe mencionar que dichas pruebas se las realizaron con estudiantes y docentes de la Carrera de Ingeniería en Sistemas (CIS), pasantes y administrativos de la Unidad de Telecomunicaciones e Información (UTI) estableciendo conexión en dos Access Point ubicado en el Área de la Energía, las Industrias y los Recursos Naturales no Renovables (A.E.I.R.N.N.R) y Administración Central, presentando en el primero problemas de estabilidad por lo que no provee de una

buena cobertura, se considera que es debido a la mala ubicación y configuración. Los equipos que se utilizan para proporcionar el servicio de internet inalámbrico son Cisco Aironet 1552E Access Point [10], por lo que sugiere realizar un Site Survey[11] (Evaluación de Sitio), para una reubicación debido a que el campus universitario tiene infraestructura física continua, unos más altos que otros, de esa manera tratar en lo posible de cubrir edificios y espacios abiertos de mayor afluencia por los usuarios y así facilitar la utilización de la red inalámbrica en sus desplazamientos.

En la práctica, la implementación de Eduroam como infraestructura inalámbrica en el campus de la UNL, es que si se utiliza como medio de conexión a Internet una vez que se haya mejorado su área de cobertura y a su vez se configure en un dispositivo final, sea este un teléfono, tablet o portátil, automáticamente poseerá el servicio, beneficiando a los estudiantes, docentes e investigadores que se movilizan alrededor del campus, la ciudad o viajan a otros países sin necesidad de hacer configuraciones adicionales.

VII. CONCLUSIONES Y TRABAJOS FUTUROS

La movilidad es un hecho real y cotidiano en la actualidad para las comunidades académicas y de investigación a nivel mundial, por lo que el concepto de movilidad toma relevancia en la medida en que las herramientas tecnológicas prestan la facilidad de conexión independiente de la ubicación geográfica.

El proyecto Eduroam implementada a nivel internacional y ahora en Ecuador, permitirá gestionar una conexión desde cualquier institución que posea el servicio utilizando una infraestructura de movilidad innovadora y segura, con el fin de tener control sobre la itinerancia de sus usuarios y no adicionar carga en la administración a la red que se visita.

Una buena configuración y ubicación de los puntos de acceso en cada uno de los campus universitarios es la clave del éxito para que la movilidad por medio de Eduroam se cumpla a satisfacción en los diferentes equipos móviles.

Como trabajos futuros se plantea realizar la replicación en todas las universidades ecuatorianas afiliadas al CEDIA la iniciativa Eduroam en sus campus, por medio de estudios de casos para implementar la solución de acuerdo a la realidad de cada universidad.

Se debe realizar investigación en las universidades de tal manera que permitan encontrar soluciones de movilidad para otro tipo de infraestructura de redes inalámbricas con dispositivos reciclables o de bajo costo.

AGRADECIMIENTOS

El presente artículo científico forma parte del Proyecto de Fin de Carrera, previa la obtención del Título de Grado de Ingeniería en Sistemas, cuyo tema versa: "*Implementación del Sistema Federado EDUROAM en la UNL y configuración de la Infraestructura Tecnológica como iniciativa para el despliegue en las Universidades del Ecuador'*. Los autores expresan su agradecimiento a las autoridades de la UNL y del Área de Energía, las Industrias y los Recursos Naturales No Renovables, de igual forma se agradece al personal técnico y administrativo de la Unidad de Telecomunicaciones e Información y a la planta docente de la Carrera de Ingeniería en Sistemas. Además, se agradece el soporte técnico y humano brindado por el GT-Movilidad de RedCLARA

REFERENCIAS

[1] Revista de DeClara. Recuperado de: http://www.redclara.net/doc/DeCLARA/DeCLARA es 33.pdf

[2] Seguridad en redes WiFi Eduroam. Recuperado de: http://traiano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20red es%20Wifi%20Eduroam.pdf

[3] What is Eduroam?. https://www.eduroam.org/

[4] ¿Qué es eduroam?. http://www.eduroam.es/

[5] Seguridad en redes WiFi Eduroam. Recuperado de: http://traiano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20red es%20Wifi%20Eduroam.pdf

[6] Instalación y configuración de un Servidor Radius. Recuperado de: http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

[7] Implementación de un plan piloto de seguridad bajo el protocolo IEEE 802.1X para el Departamento de Gestión Tecnológica del Ministerio de Telecomunicaciones y Sociedad de la Información. Recuperado de: http://repositorio.espe.edu.ec/handle/21000/7286

[8] Seguridad en redes WiFi Eduroam. Recuperado de: http://traiano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20red es%20Wifi%20Eduroam.pdf

[9] Especificación técnica Wi-Fi. Recuperado de: https://siwiki.upct.es/mediawiki/index.php/Especificaci%C3%B3nt%C3%A9cnica WIFI.pdf

[10] Cisco Aironet 1550 Series. Recuperado de: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1550- series/data sheet c78-719520.html

[11] Site Survey. Recuperado de: http://actech.com.mx/servicios/downloads/ACTECH SiteSurvey newlogo.pdf

Fernando Castillo Graduate career in systems engineering from the National University of Loja, Ecuador in 2012. His current research interest is computer networks, information security IT and roaming.

Jennifer Loayza Graduate career in systems engineering from the National University of Loja, Loja, Ecuador 2012. Her current research: computer networks, interested in the field of web development, computer networks and digital edition

Anexo 10. Declaración de Confidencialidad

Jennifer Jomaira Loayza Castro, con CI: **0705210946** y **José Fernando Castillo Alba,** con CI: **1104742703** (en adelante los declarantes); residentes a la fecha **junio del 2014** en la ciudad de **Loja.**

DECLARAN lo siguiente:

PRIMERO: Antecedentes

Los declarantes han desarrollado el proyecto de fin de carrera titulado: **"IMPLEMENTACIÓN DEL SISTEMA FEDERADO EDUROAM EN LA UNIVERSIDAD NACIONAL DE LOJA Y CONFIGURACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA COMO INICIATIVA PARA EL DESPLIEGUE EN LAS UNIVERSIDADES DEL ECUADOR"** en la Unidad de Telecomunicaciones e Información (UTI), teniendo como Director de Tesis al Docente investigador: **Ing. Luis Antonio Chamba Eras**

SEGUNDO: Información Confidencial

La información referida en pruebas, configuraciones y experimentaciones debe ser utilizada con fines académicos y no con otros propósitos; por lo tanto se considerará siempre como Información Confidencial y/o Sensible en el caso de un uso ilegal.

TERCERO: Excepciones

No será considerada como Información Confidencial:

- La información que era de dominio público o pase a serlo, con posterioridad, por haberse publicado sin intervención ni negligencia del declarante.
- La información que sea accesible por pasantes u otros tesistas en la UTI donde se desarrolló el PFC.
- La información revelada por una tercera persona con derecho a divulgarla.

CUARTO: Secretos de la Información Confidencial

Los declarantes se comprometen a:

- Mantener de forma confidencial y a no revelar a personas ajenas al Director de la UTI y al encargado de la Sección de Redes sin autorización previa, toda la información y material de carácter sensible a la que se acceda en el desarrollo del proyecto de fin de carrera, tanto teórico como práctico, salvo con las excepciones antes mencionadas.
- Utilizar el material e información sensible, suministrados por el personal de la UTI, única y exclusivamente para la realización del proyecto de fin de carrera.
- Mantener en absoluta reserva la información o documentos de carácter sensible, a los que tenga acceso como consecuencia de su formación profesional.

QUINTO: Duración

La obligación de los declarantes respecto al compromiso de mantener en secreto la Información Confidencial, tendrá una duración indefinida a partir de la fecha de entrega de éste documento.

En Loja, 24 de Junio del 2014.

……..
José Fernando Castillo Alba
CI: 1104742703

……..
Jennifer Jomaira Loayza Castro
CI: 0705210946

Anexo 11. Certificado de Traducción del Resumen

Lic. Karina Gabriela Calva Vicente
DOCENTE DEL ÁREA DE INGLÉS DEL CENTRO EDUCATIVO "SAGRADO CORAZÓN"

C E R T I F I C A:

Que el Sr. **JOSÉ FERNANDO CASTILLO ALBA** con Nro. de cédula 1104742703 y la Srta. **JENNIFER JOMAIRA LOAYZA CASTRO** con Nro. de cédula 0705210946, autores del Proyecto de Fin de Carrera, cuyo tema versa **"IMPLEMENTACIÓN DEL SISTEMA FEDERADO EDUROAM EN LA UNIVERSIDAD NACIONAL DE LOJA Y CONFIGURACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA COMO INICIATIVA PARA EL DESPLIEGUE EN LAS UNIVERSIDADES DEL ECUADOR"**, han cumplido con la traducción al idioma ingles del resumen empleando las reglas gramaticales y así dar cumplimiento con la sección Summary.

Es cuanto puedo certificar en honor a la verdad, pudiendo los interesados hacer uso del presente en lo que estime conveniente.

Loja, mayo del 2014.

CENTRO EDUCATIVO "SAGRADO CORAZÓN" EDUCACIÓN EN VALORES DIRECCIÓN LOJA - ECUADOR

Lic. Karina Calva.
DOCENTE

Anexo 12. Licencia Creative Commons

Tipo de Licencia:

Creative Commons

Título de la Obra:

Implementación del Sistema Federado Eduroam en la Universidad Nacional de Loja y Configuración de la Infraestructura Tecnológica como Iniciativa para el despliegue en las Universidades del Ecuador.

Código de la licencia:

 Implementación del Sistema Federado Eduroam en la Universidad Nacional de Loja y Configuración de la Infraestructura Tecnológica como Iniciativa para el despliegue en las Universidades del Ecuador by Jennifer Loayza, Fernando Castillo is licensed under a Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional License.

Términos de la Licencia:

Reconocimiento-NoComercial-CompartirIgual
CC BY-NC-SA

Esta licencia permite a otros distribuir, remezclar, retocar, y crear a partir de tu obra de modo no comercial, siempre y cuando te den crédito y licencien sus nuevas creaciones bajo las mismas condiciones.