UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

TITULO:

"IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL ACCESO INALÁMBRICO A LA RED DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE"

"TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO EN INGENIERO EN SISTEMAS"

AUTORES:

Fabricio Alejandro Flores Gallardo

Lisset Alexandra Neyra Romero

DIRECTOR:

Ing. Juan Manuel Galindo Vera

Loja-Ecuador

2012

CERTIFICACIÓN

Ing. Juan Manuel Galindo Vera

DOCENTE DEL ÁREA DE ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES Y DIRECTOR DE TESIS.

CERTIFICA:

Que los egresados Fabricio Alejandro Flores Gallardo y Lisset Alexandra Neyra Romero realizaron el presente proyecto fin de carrera titulado **"IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL ACCESO INALÁMBRICO A LA RED DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE"** bajo mi dirección y asesoramiento.

Loja, 28 de Septiembre del 2012

……

Ing. Juan Manuel Galindo Vera

DIRECTOR DE TESIS

AUTORÍA

Todos los conceptos, opiniones, descripciones, conclusiones y recomendaciones vertidas en el desarrollo del presente proyecto fin de carrera son de absoluta responsabilidad de los autores, exceptuando aquellas que se encuentran citadas para lo cual firmamos su constancia.

Fabricio Alejandro Flores Gallardo **Lisset Alexandra Neyra Romero**

AGRADECIMIENTO

Al haber culminado el presente proyecto fin de carrera queremos dejar constancia de nuestros más sinceros agradecimientos a todos aquellos que participaron en el proceso de desarrollo del mismo:

A la Universidad Nacional de Loja, a la Unidad de Telecomunicaciones e Información, que nos brindaron todo el apoyo y la información necesaria para la implementación del presente proyecto fin de carrera, al Ing. Juan Manuel Galindo Vera, director del proyecto fin de carrera quien con su experiencia y conocimiento fue nuestra guía.

LOS AUTORES

DEDICATORIA

En Primer lugar dedico el presente proyecto fin de carrera a Dios, porque día a día reconozco que sin su ayuda no hubiese llegado hasta este punto de mi vida académica, así mismo a mis padres Moisés Neyra y Beli Romero, que con su sabia guía forjaron en mi lo que soy ahora, a mis hermanos Stefanny, Debbie y David por su apoyo incondicional y cariño, finalmente a mis familiares y amigos que siempre me han apoyado desinteresadamente.

Primeramente, quiero dedicar este triunfo a Dios, pues sin Él no estaría donde estoy. Por supuesto también a mis padres Franz e Ivanova por todo el apoyo y esfuerzo que han realizado para que pueda lograr este triunfo. A mis hermanos, primos, tíos, abuelitos y amigos que me han apoyado y ayudado en todo lo que he necesitado. A todos... Gracias...

Fabricio Alejandro Flores Gallardo

CESIÓN DE DERECHOS

Fabricio Alejandro Flores Gallardo y Lisset Alexandra Neyra Romero, autores intelectuales del presente proyecto fin de carrera, autorizan 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 hacer uso del mismo en lo que estime sea conveniente.

A. TÍTULO

"IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL ACCESO INALÁMBRICO A LA RED DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE"

B. RESUMEN

En la Universidad Nacional de Loja, la implantación de un sistema de seguridad para el acceso inalámbrico a la red de datos utilizando software libre es muy importante, porque actualmente no existe un sistema de seguridad que controle el acceso al uso del servicio de internet.

El presente proyecto fin de carrera (PFC) describe la implantación de un servidor RADIUS, que en conjunto con un portal cautivo proveerá de las seguridades necesarias para el acceso a la red de la Universidad Nacional de Loja a través de los puntos de acceso inalámbricos, permitiendo así que únicamente el personal autorizado (usuario y contraseña) puedan tener acceso al servicio de Internet. La implantación del servidor, además de mejorar la seguridad en la red, ayudará a que el servidor proxy wireless no se sobrecargue de solicitudes mejorando así la calidad de servicio y mejoras en tiempos de conexión por parte de los usuarios finales.

El sistema operativo sobre el cual se ha implementado la solución es GNU/Linux, distribución Ubuntu Server 12.04, debido a que ofrece estabilidad y compatibilidad con las soluciones de software planteadas y se requiere mantener un estándar respecto a los servidores que se utilizan en la Unidad de Telecomunicaciones e Información. Para el servidor RADIUS se usó el software **FreeRADIUS** versión 2.1.10 **(***ver sección resultados apartado 1.1.13. Determinación de las herramientas adecuadas para la solución del problema*). Para el portal cautivo se escogió **Coovachilli** versión 1.2.6, ya que está lanzado bajo una licencia libre GPL (*ver anexo 8*). Además, Coovachilli funciona perfectamente con un servidor RADIUS, y cuenta con una comunidad que colabora en cuanto al desarrollo de la aplicación (*ver sección resultados apartado 1.2.12. Selección del portal cautivo adecuado*).

Para el proceso de autenticación, se hizo uso del Web Services del Sistema de Gestión Académica de la Universidad Nacional de Loja (*ver sección resultados apartado 1.2.5. Autenticación de FreeRADIUS con el Web Services del Sistema de Gestión Académico*) y se procedió a realizar las pruebas respectivas del sistema de seguridad en el área de la Energía las Industrias y los Recursos Naturales no Renovables (*ver sección resultados apartado 1.4.3.2. Pruebas en el Área de la Energía las Industrias y los Recursos Naturales no Renovables*).

SUMMARY

At the Universidad Nacional de Loja, the implementation of a security system for the wireless access to data network using free software is very important, because there is currently no security system that controls access to the use of the internet service.

This final career project (PFC) describes the implementation of a RADIUS server, which with a captive portal will provide the necessary assurances for access to the network of the Universidad Nacional de Loja through wireless access points, allowing only authorized personal (username and password) can access the Internet service. The implementation of the server, in addition to improving network security, helps the wireless proxy server is not overloaded with request, improving the quality of service and improved connection times by users.

The operating system on which the solution has been implemented is GNU / Linux, Ubuntu Server 12.04, because it offers stability and support software solutions raised and is required to maintain a standard for the servers used in Unidad de Telecomunicaciones e Información. For the RADIUS server software was used FreeRADIUS version 2.1.10 (see Resultados section 1.1.13. Determinación de las herramientas adecuadas para la solución del problema). For captive portal Coovachilli version 1.2.6 was chosen as it is released under a free license GPL (see Anexo 8). Furthermore, Coovachilli works perfectly with a RADIUS server, and has a community that collaborates in the development of the application (see Resultados section 1.2.12. Selección del portal cautivo adecuado).

For the authentication process, we use the Web Services of the Sistema de Gestión Académica of Universidad Nacional de Loja, (see Resultados section 1.2.5 Autenticación de FreeRADIUS con el Web Services del Sistema de Gestión Académico) and proceeded to respective testing the security system in the Área de la Energía, las Industrias y los Recursos Naturales no Renovables (see Resultados section 1.4.3.2 Results section. Pruebas en el Área de la Energía las Industrias y los Recursos Naturales no Renovables).

INDICE

Índice de Tablas

Índice de Figuras

C. INTRODUCCIÓN

En la actualidad se conoce, la importancia y facilidad del uso de las redes inalámbricas, estas nos permiten de una manera muy fácil tener conectividad, pero existe una serie de inconvenientes debido a no prestar atención a los aspectos básicos de seguridad.

Para asegurar la interconexión de una red inalámbrica se puede a más de utilizar los mecanismos a nivel de dispositivos, autenticar la interconexión a nivel de usuario, para lo cual es necesario establecer mayores mecanismos de seguridad en la interconexión de dispositivos de una red inalámbrica LAN (WLAN).

Para la autenticación de redes inalámbricas LAN a nivel de usuarios se requiere la instalación de un servidor que permita la interconexión con los dispositivos inalámbricos, para permitir el acceso de acuerdo a una lista de usuarios los mismos que estén acorde a políticas de acceso y seguridad para brindarles los servicios de conexión a la red inalámbrica, y también a otras redes como el Internet de la forma más cómoda y fácil para el usuario.

El objetivo de este proyecto fin de carrera se enfoca en la seguridad en los puntos de acceso inalámbricos ya que es una necesidad dentro de la administración de la red de la Universidad Nacional de Loja. Al implantar un sistema de seguridad, se garantiza que únicamente las personas autorizadas puedan acceder a la red de la Universidad Nacional de Loja.

Se analizará la situación actual de la red de datos de la Universidad Nacional de Loja y los problemas de seguridad informática que se encontraron, seguidamente se realizará el proceso de implantación y configuración del servidor RADIUS y el análisis para la selección del portal cautivo y la herramienta web para la administración correspondiente del servidor RADIUS.

El sistema de seguridad para el acceso inalámbrico, tendrá la capacidad de realizar un control de acceso al servicio Internet a través del empleo de una página de autenticación y será administrada a través de una herramienta web para llevar el control de forma más eficiente y fácil. Además se presentará un escenario real donde se realizaron las pruebas correspondientes de los elementos que conforman el sistema.

A lo largo del presente PFC, se estudiará detalladamente los estándares, mecanismos de autenticación y RADIUS que es un protocolo de autenticación y autorización para aplicaciones de acceso a la Red.

Es importante mencionar que la información recolectada sobre la infraestructura de la red de datos, direccionamiento IP, ubicación de los equipos de networking etc. Está bajo una declaración de confidencialidad (*ver anexo 11*) donde se detalla los aspectos necesarios para la protección correcta contra el uso inadecuado de esta información.

La investigación desarrollada se encuentra estructurada de acuerdo a los lineamientos establecidos por la Universidad Nacional de Loja y el Área de la Energía la Industria y los Recursos Naturales No Renovables de la siguiente manera, RESUMEN que describe una síntesis general del contenido del proyecto fin de carrera, INTRODUCCION, donde se describen de forma general los objetivos que va a cubrir el PFC, METODOLOGÍA, donde se detalla cada uno de los métodos de investigación tanto científicos, experimentales y ciertas técnicas investigativas, también la descripción de las fases que se realizaron para el desarrollo del proyecto fin de carrera, REVISION DE LA LITERATURA, comprende las diferentes temáticas que han contribuido para la mejor comprensión y desarrollo del trabajo, RESULTADOS, tiene como fin evaluar cada uno de los objetivos planteados así como su cumplimiento, además hacer una evaluación técnica, económica, ambiental sobre el trabajo realizado, DISCUSIÓN, describe el cumplimiento de los objetivos planteados y la opinión personal de los tesistas, para terminar con las CONCLUSIONES, RECOMENDACIONES, y la respectiva BIBLIOGRAFIA y ANEXOS.

D. REVISIÓN LITERARIA O MARCO TEÓRICO

CAPÍTULO I: Seguridad en las Redes Inalámbricas

1. SEGURIDAD EN LAS REDES INALÁMBRICAS

1.1. Seguridad

"El término seguridad proviene de la palabra *securitas* del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo." [1]

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 (Figura 1) [1].

Figura 1. Triada de la seguridad [1]

1.1.1. 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 a, o 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 [1].

[1] Seguridad Diccionario de la Real Academia: http://lema.raer/ ?val=seguridad

1.1.2. 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 [1].

1.1.3. 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[2] [1].

1.2. Estándar IEEE 802.11

La familia de protocolos 802.11, definidos como estándar industrial por el IEEE (Institute of Electrical and Electronics Enginneers), son los más utilizados en los sistemas de comunicaciones inalámbricos para redes de datos [2].

En la actualidad existen sistemas operativos que soportan nativamente el estándar 802.11b (conocido como Wi-Fi) que usa la banda de radiofrecuencia de 2,4GHz., alcanzando velocidades de transmisión de hasta 11Mbps con radios de acción de hasta 400 metros en condiciones óptimas. Esta es la variante más utilizada en la actualidad de la familia de protocolos 802.11, aunque poco a poco va ganando mercado el estándar 802.11g con una velocidad de transmisión de 54Mbps [2].

Los elementos fundamentales dentro de una red inalámbrica Wi-Fi son el punto de acceso (AP, Access Point), que centraliza el servicio de acceso a la red inalámbrica, semejante a un Hub o Switch en una red cableada, y los nodos inalámbricos, que son los distintos dispositivos que se conectan a la red inalámbrica utilizando algún tipo de adaptador de red sin cables [2].

Dentro de las redes inalámbricas existen dos modos de operación diferentes dependiendo del tipo de conectividad existente entre los distintos nodos que forman la red [2]:

[2] **DoS:** Denial of Service (Denegación de Servicio).

- **Modo "ad hoc" o IBSS(Independent Basic Service Set)**

Esta topología, tal y como se encuentra en la figura 2, se caracteriza por no tener un punto de acceso (AP) encargado de centralizar y coordinar las comunicaciones, sino que los nodos se comunican directamente entre sí (peer-to-peer) [2].

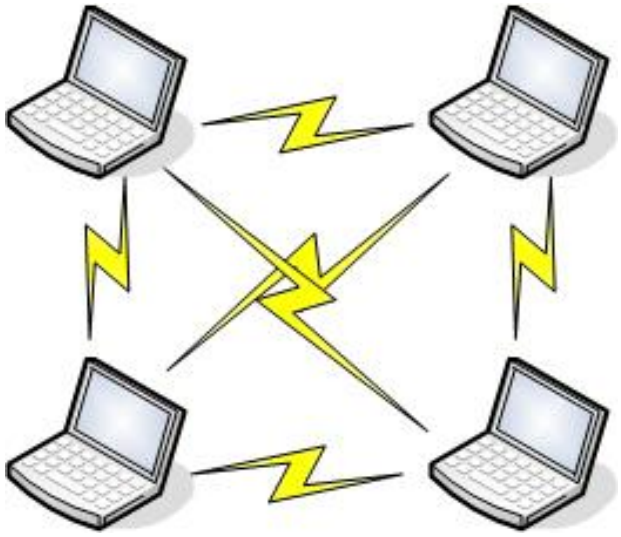

Figura 2. Conexión en modo "ad hoc" [2].

Es equivalente al modo entre iguales de las redes locales cableadas. El área de cobertura está limitada al alcance de cada estación individual [2].

- **Modo infraestructura o BSS(Basic Service Set)**

En esta topología hay como mínimo un Punto de Acceso encargado de centralizar las comunicaciones, las estaciones inalámbricas no se pueden comunicar entre si, y todo el tráfico debe de pasar de forma obligatoria por el AP [2].

La mayoría de redes inalámbricas en las empresas utilizan el modo infraestructura con uno o más puntos de acceso, actuando estos como un HUB en una LAN, redistribuyen los datos hacia todas las estaciones inalámbricas. Si existe más de un punto de acceso en la red, cada uno puede actúa como repetidor o puente entre redes inalámbricas, y al conjunto se le denomina ESS (Extended Service Set) [2].

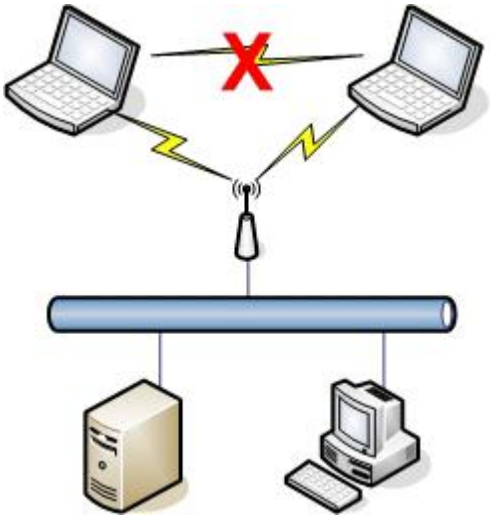

Figura 3. Conexión en modo infraestructura [2].

En la figura 3 se observa que el punto de acceso actúa de puente entre la red inalámbrica y otras redes cableadas, permitiendo el acceso transparente a éstas de los nodos inalámbricos.

Los dos temas más importantes a controlar en la seguridad de las redes inalámbricas de área local (WLAN) son la autenticación de usuario y el cifrado de datos [2].

El protocolo 802.11b provee un mecanismo para cifrar los datos conocido como WEP (Wired Equivalent Privacy), pero como se detallará mas adelante, posee multitud de problemas convirtiéndolo en un sistema poco seguro [2].

1.2.1. WEP

WEP o Wired Equivalent Privacy corresponde al método original para autenticación y cifrado propuesto por el estándar IEEE 802.11. La principal ventaja de WEP es su alta compatibilidad, los equipos que utilizan el estándar inalámbrico utilizarán al menos WEP como sistema de autenticación y cifrado. Sin embargo sus deficiencias en la generación del vector de inicialización, el largo de la contraseña y el hecho que la misma sea necesariamente compartida, entre otros, lo hace un sistema muy inseguro [3].

Cuando una estación se intenta asociar a un punto de acceso, la estación debe autenticarse frente al punto de acceso. En el proceso de asociación, la estación y el punto de acceso negocian el tipo de autenticación que utilizarán, que puede ser “abierta” o “compartida” [2]:

- **Autenticación abierta:** como su propio nombre lo indica, la entrada a la red es totalmente expedita a cualquiera que conozca el SSID[3] (Service Set Identifier) del punto de acceso [2].
- **Autenticación compartida:** es un mecanismo parecido a la clásica autenticación desafío/respuesta en la que el AP envía un desafío a la estación cliente, la cual devuelve cifrado con clave WEP para comprobar que comparten la misma clave [2].

Algunos de los ataques realizables sobre WEP son [3]:

- Ataques pasivos basados en el análisis de paquetes para intentar descifrar el tráfico.
- Ataques activos basados en la introducción de paquetes.
- Ataques activos basados en el ataque y engaño al punto de acceso.
- Ataques de diccionario.

1.2.1.1. Problemas del WEP

Desafortunadamente, la especificación WEP incluida en el estándar 802.11 no proporciona una seguridad equivalente a una red cableada. Son varios los problemas que tiene para considerarlo un protocolo seguro [2].

1.2.1.1.1. Manejo de claves

El estándar WEP ignora completamente el uso de manejadores de claves. Esto causa problemas cuando el número de usuarios de la red inalámbrica crece. El uso de claves compartidas por todos los usuarios implica que cualquier usuario puede descifrar las comunicaciones de los demás, es decir, debe existir una confianza plena entre todos los usuarios de la red. Esto es una situación idílica, sobre todo cuando crece el número de usuarios [2].

Existe la posibilidad de realizar rotaciones entre un conjunto de claves prestablecidas. Este sistema no mejora en exceso la seguridad, ya que todos los usuarios son conocedores del conjunto de claves [2].

[3] **SSID:** Service Set Identifier (Identificador del conjunto de servicio)

1.2.1.1.2. Cifrado

El IEEE seleccionó un sistema de cifrado de 40 bits porque es el nivel más alto de encriptación que permiten las leyes internas de algunos países, como Estados Unidos, para poder exportar dispositivos de cifrado a otros países. Desafortunadamente, por un fallo de algoritmo generador de claves, las longitudes efectivas de las claves sólo alcanzan un nivel de 22 bits. Con niveles de cifrado tan bajos es fácil romper la clave [2].

Actualmente existen en el mercado herramientas software gratuitas que permiten encontrar las claves de cifrado [2].

Es importante resaltar que cuando se realiza una "autenticación compartida", el mensaje enviado por el punto de acceso viaja en texto plano, y la respuesta del nodo lo hace cifrado, la posesión de los dos mensajes facilita mucho el proceso de ruptura de la clave WEP [2].

1.2.1.1.3. Integridad

El estándar WEP no verifica la integridad de los paquetes que se envían y reciben, basta que un atacante use una herramienta de análisis de tráfico para poder manipular un simple bit cualquiera en los paquetes en circulación por la red para causar problemas en las comunicaciones, e incluso llegar a impedirlas, sería lo que se conoce como un ataque de denegación de servicio (DoS) [2].

El IEEE está trabajando en el protocolo 802.11i que implementa integridad de mensajes para evitar este problema [2].

1.2.2. WPA

WPA o Wireless Protected Access se inicio a raíz de los problemas detectados en WEP. El proceso de encriptación es similar al utilizado por WEP, sin embargo el largo tanto del vector de inicialización como el largo de las claves es mayor, lo cual hace al protocolo más resistente a ataques [3].

La versión WPA2, estándar IEEE 802.11i, es la versión considerada actualmente segura para redes inalámbricas, la cual posee diferentes modos de operación, destacándose el modo Personal (utilizando una clave compartida) y el modo Enterprise (utilizando un servidor de autenticación) [3].

1.3. Sistemas de seguridad adicional

Una vez visto los problemas de seguridad que conlleva el protocolo WEP, es necesario implementar nuevos sistemas de seguridad adicionales que permitan conseguir un auténtico nivel de seguridad en las redes WLAN, proporcionando integridad, autenticación y confidencialidad [2].

1.3.1. 802.1x

El estándar IEEE 802.1x no fue diseñado inicialmente para redes inalámbricas, realmente se diseñó para redes cableadas y proporcionaba un nivel añadido de seguridad a las redes, evitando el acceso a los equipos de la red sin una autenticación previa; además, proporciona los mecanismos necesarios para la gestión y reparto de las claves de cifrado. En la figura 4 se muestra la arquitectura del estándar IEEE 802.1x [2].

El puerto de comunicaciones de los dispositivos que implementan el estándar 802.1x se encuentra por defecto cerrado, permitiendo exclusivamente el paso de tramas de autenticación, en el momento que el cliente se ha autenticado, el puerto de comunicaciones se abre permitiendo el paso de cualquier tipo de trama [2].

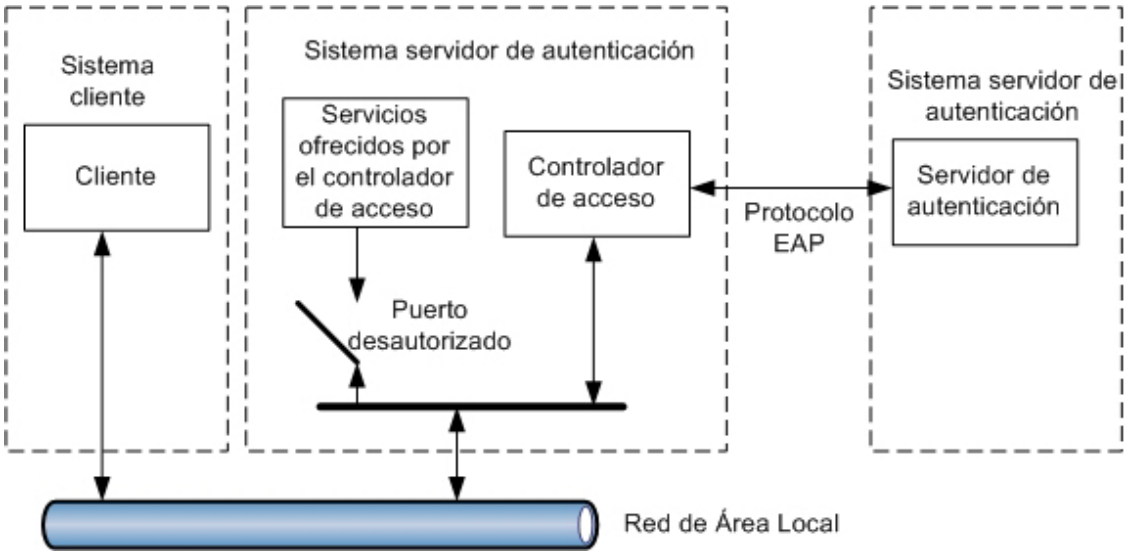

Figura 4. Arquitectura IEEE 802.1x [2].

El estándar 802.1x se basa en el protocolo EAP(Extensible Authentication Protocol) que le permite integrarse en sistemas externos de autenticación y autorización. El uso

de este protocolo de seguridad conlleva la existencia de un servidor de autenticación de usuarios, normalmente un servidor RADIUS [2].

1.3.2. EAP

El protocolo EAP (Extensible Authentication Protocol) se creó como una extensión al protocolo PPP (Point-to-Point Protocol) que permitiese el uso de cualquier tipo de sistema de autenticación para el acceso a redes [2].

Al contrario que en PPP, con EAP el mecanismo de autenticación no se escoge durante la fase de establecimiento de la conexión punto a punto, sino que se negocia el sistema a emplear entre los nodos que se comunican. Este sistema permite el uso de cualquier tipo de método de autenticación (conocidos como tipos EAP), basta con instalar tanto en los clientes como en los servidores los controladores adecuados [2].

Esta enorme flexibilidad permite dotar de diversos sistemas de autenticación a las conexiones (desafío-respuesta, certificados digitales, tarjetas inteligentes…), convirtiéndose en una tecnología fundamental para la seguridad de las conexiones [2].

EAP está soportado explícitamente en la capa de conexión de la especificación 802 del IEEE y por lo tanto está soportado por los dispositivos inalámbricos adheridos al estándar IEEE 802.11x [2].

El protocolo 802.1x define como se debe usar EAP para autenticar a este tipo de dispositivos y de hecho es el único protocolo de autenticación que soporta [2].

Los tres tipos de autenticación EAP más utilizados son:

- **EAP-MD5 CHAP:**

Utiliza el mismo protocolo de desafío que PPP, pero empleando mensajes EAP. Se utiliza para validar credenciales a partir de nombres de usuario y contraseñas. Sin embargo, no es adecuado para las redes inalámbricas por varios motivos, pero fundamentalmente por que requiere que las contraseñas se almacenen de forma que se puedan descifrar [2].

- **EAP-TLS:**

Esta variante utiliza TLS(Transport Level Security) para habilitar la autenticación en entornos de seguridad basados en certificados digitales. Es obligatorio su uso en el

caso de requerir tarjetas inteligentes, por ejemplo. El intercambio de mensajes EAP-TLS proporciona autenticación mutua (evita ataques de "hombre en el medio") así como intercambio seguro de claves entre el servidor y los clientes [2].

En la actualidad es tal vez el método de autenticación más seguro que existe. Es la elección más adecuada para redes inalámbricas por muchos motivos pero fundamentalmente porque usa certificados digitales, no depende de ninguna contraseña que el usuario deba conocer, no requiere intervención por parte del usuario, y utiliza infraestructura de clave pública de alta seguridad [2].

- **EAP-TTLS:**

El EAP-TTLS (Extensive Authentication Protocol-Tunneles Transport Layer Security) es una extensión de EAP-TLS, solo requiere certificados en el servidor, lo que subsana una desventaja importante respecto a EAP-TLS, cuya gestión de certificados es mucho más tediosa y pesada [2].

Con EAP-TTLS se elimina la necesidad de configurar certificados para cada cliente de la red inalámbrica. Además, EAP-TTLS autentica al cliente en el sistema con las credenciales ya existentes basadas en password, y encripta credenciales y password para garantizar la protección de la comunicación inalámbrica [2].

1.3.3. Autenticación mediante 802.1x

El estándar inicial no incorporaba un mecanismo robusto de autenticación. En las siguientes mejoras se incluyó la posibilidad de hacer servir el estándar 802.1x el cual proporciona varios métodos que podemos considerar seguros para redes inalámbricas [1].

El estándar 802.1x no está relacionado directamente con el desarrollo del estándar 802.11, sino que es un conjunto de especificaciones totalmente independientes al estándar inalámbrico [1].

Este estándar nació de la necesidad de disponer de un método de autenticación seguro, flexible y optimizado para redes IP tanto LAN como WAN, el cual funcionara sobre la capa LLC. El estándar 802.1x utiliza el protocolo EAP para la comunicación y el concepto de puertos de autenticación [1].

Los dispositivos que quieren conectar a una red basada en este estándar realizan una primera conexión con el dispositivo que actúa como puente entre el cliente y el servidor de autenticación (en nuestro caso este puente es el AP) [1].

Los puertos de conexión entre la red y el cliente pueden estar autorizados o desautorizados, dependiendo de la validación del servidor de autenticación [1].

En la figura 5 podemos observar la arquitectura de un sistema 802.1x y la nomenclatura usada en este sistema, donde [1]:

- **Suplicante:** cliente que quiere ser autenticado [1].
- **Autenticador:** es el que provee al cliente del acceso a la red. Este acceso primero será sólo mediante el puerto de autenticación el cual sólo permitirá mensajes de autenticación. Si la autenticación es válida, se le asignará un puerto abierto exclusivo [1].
- **Servidor de autenticación:** la decisión de la concesión de acceso a un usuario la realiza este servidor, el cual indica al autenticador si debe asignar un puerto válido o debe denegar la petición. Este servidor puede estar en cualquier red y contendrá la información necesaria para dar validez al usuario según el tipo de EAP utilizado [1].

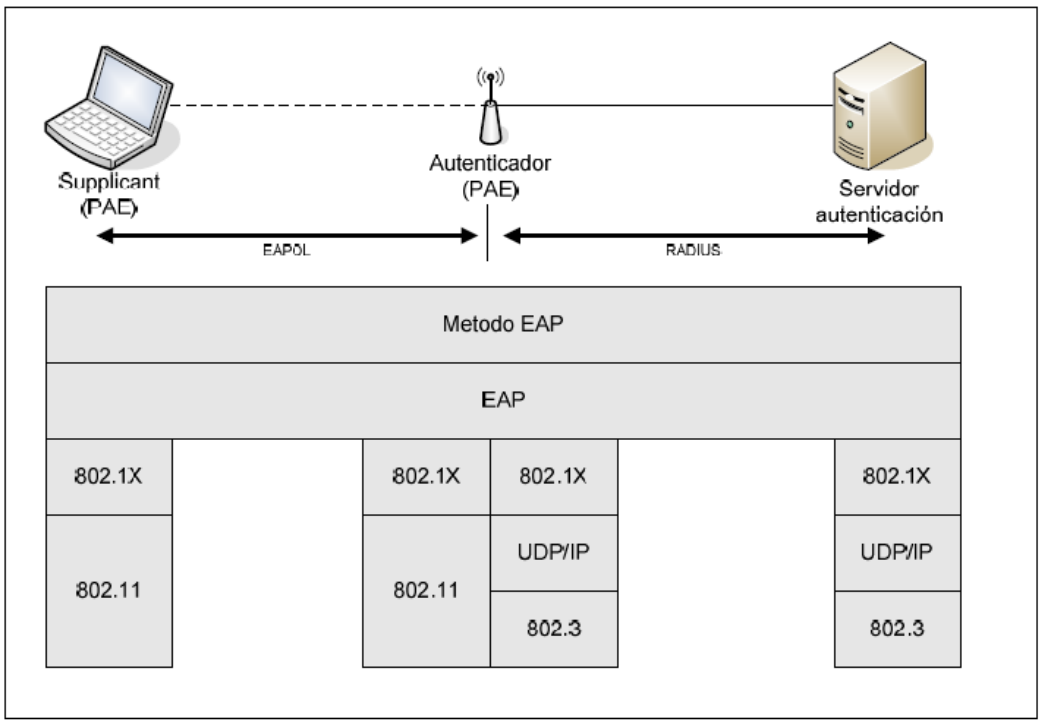

Figura 5. Comunicación EAP y pila de protocolos usados [1]

El suplicante y el autenticador son los elementos que funcionan mediante el método de puertos, por eso son llamados elementos PAE (Puerto de Entidades de autenticación, Port Authentication Entities). Estas entidades se pueden comunicar mediante mensajes EAPOL (EAP sobre LAN) aun cuando el cliente no tenga ni dirección IP ni tenga un puerto autorizado (sólo se permitirán los mensajes de inicio de autenticación). El autenticador y el servidor de autenticación se comunican mediante mensajes RADIUS, ya que RADIUS proporciona una gran variedad de métodos de autenticación, flexibilidad y compatibilidad con muchas de las bases de datos de usuarios [1].

En definitiva, este sistema de autenticación se incorporó al estándar 802.11 el cual intenta eliminar una de las dos debilidades más importantes de WEP en este campo. El punto fuerte del 802.1x es que evita el paso de cualquier tipo de tráfico hacia la red si el usuario no ha sido previamente autorizado. El usuario no autenticado sólo puede conseguir enviar paquetes del tipo EAPOL al puente para que éste los envíe al servidor de autenticación [1].

CAPÍTULO II: RADIUS

2. RADIUS

RADIUS son las siglas de Remote Authentication Dial-Up Server, que significa Servidor de Autenticación de Autorización Remota para sistemas de Marcado Telefónico a Redes. Este nombre proviene de sus comienzos, donde su único uso era el acceso a redes a través de MÓDEM, pero actualmente su funcionalidad es mucho más amplia [1].

El motivo por el cual RADIUS es el protocolo AAA hegemónico en la actualidad no es solamente porque haya sido el primero, ni porque haya sido muy comercializado para alcanzar su globalización, sino porque ha ido creciendo y mejorando desde sus comienzos hasta el día de hoy. A pesar de algunas de sus limitaciones, ha ido adoptando una serie de mejoras que le han llegado a permitir gestionar desde pequeñas redes seguras y medianas empresas hasta redes de alto nivel [1].

2.1. Protocolo AAA

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Arqueo (contabilización) (Authentication, Authorization and Accounting en inglés). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados. AAA se combina a veces con auditoria, convirtiéndose entonces en AAAA [1].

2.1.1. Autenticación:

La Autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc.) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, o los números de teléfono en la identificación de llamadas [1].

Viene al caso mencionar que los protocolos de autenticación digital modernos permiten demostrar la posesión de las credenciales requeridas sin necesidad de transmitirlas por la red (véanse por ejemplo los protocolos de desafío-respuesta) [1].

2.1.2. Autorización:

Autorización se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema [1].

Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son, pero sin estar limitados a: filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda y Cifrado [1].

2.1.3. Arqueo:

Se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación u otros propósitos. El arqueo en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes (en inglés "batch accounting") consiste en la grabación de los datos de consumo para su entrega en algún momento posterior. La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó [1].

2.2. 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 [1].

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 [1].

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 [1].

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 [1].

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 [1].

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 [1].

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 [1].

Es un protocolo extensible, por lo que permite la introducción mediante su sistema de atributos o variables definibles (AVP) de cualquier adaptación a cualquier nuevo equipo de cualquier fabricante. Este sistema de funcionamiento mediante atributos es

uno de los principales pilares de este protocolo, ya que toda la estructura modular se basa en ellos [1].

2.3. Especificaciones del RADIUS

Todas estas características, dependiendo del tipo de implementación que necesitemos, son las que definen a RADIUS o a cualquier servidor AAA.

- Cumplir la función para la cual se va a adquirir.
- Incluir todas las tecnologías necesarias para que pueda cubrir las necesidades del usuario final de la autenticación, a través de cualquier sistema operativo y/o plataforma segura.
- Soportar y ser soportado por todas las plataformas de hardware que utilicemos en la infraestructura interna de red, como equipos de electrónica de Red, NAS, Plataformas de PPP, ADSL, GSM, Wi-Fi, Wi-Max, enrutadores, etc.
- Soportar el sistema o sistema de base de datos o servicio de directorios que hayamos elegido para gestión de usuarios y de arqueo de cuentas.
- Disponer de la arquitectura adecuada para la instalación en la plataforma servidora elegida.
- Disponer de las librerías de programación y personalización adecuadas para la personalización de sistemas como PHP, Java, Perl, Python, etc.
- Ser fácilmente configurable y administrable.
- Fidelidad a los estándares y RFC, que los regulan.
- Ser transportable y migrable a otros entornos [1].

2.4. Autenticación contra la base de datos

Se realiza la autenticación con una base de datos, normalmente del tipo SQL, como Oracle, Microsoft SQL Server, MySQL, etc. Los datos de credenciales de usuarios se almacenan en estas bases de datos, así como los atributos de autorización y la información de arqueo de cuentas. De esta manera es muy sencilla la administración de estos datos, así como la consulta, edición o eliminación de las mismas. El rendimiento que ofrecen los sistemas SQL y las posibilidades de redundancia y balanceo de carga son espectaculares para implementaciones de gran tamaño [1].

La mayor parte de los servidores de RADIUS incluyen soporte para bases de datos, lo que simplifica la tarea de administración de las bases de datos necesarias. Todos los

servidores importantes incorporan plantillas SQL para la creación de las instancias y tablas necesarias [1].

Para la gestión de autenticación de un elevado número de usuarios la base de datos es la solución más apropiada, pudiéndose crear scripts automáticos en lenguaje SQL para su administración. Además siempre podemos usar funciones como MD5, SHA 1 u otras personalizables para el almacenamiento cifrado de las contraseñas o información importante. Podemos modificar o crear cualquier secuencia o script SQL a ejecutar durante el proceso de Autenticación, Autorización o Arqueo, con lo que la potencia de este sistema es ilimitada. La autenticación de usuarios por base de datos va unida al uso de un método de autenticación y/o de transporte de la autenticación como CHAP, PAP, EAP-TLS, EAP-PEAP, etc [1].

2.5. Proceso de RADIUS

Un cliente RADIUS envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje RADIUS al servidor. Éste autentica y autoriza la solicitud del cliente y envía de regreso un mensaje de respuesta. Los clientes RADIUS también envían mensajes de cuentas a servidores RADIUS [4].

Los mensajes RADIUS son enviados como mensajes UDP (User Datagram Protocol). El puerto UDP 1812 es usado para mensaje de autenticación RADIUS y, el puerto UDP 1813, es usado para mensajes de cuentas RADIUS. Algunos servidores usan el puerto UDP 1645 para mensajes de autenticación y, el puerto 1646, para mensajes de cuentas. Esto último debido a que son los puertos que se usaron inicialmente para este tipo de servicio [4].

2.6. Formato de paquetes enviados por RADIUS

Los datos entre el cliente y el servidor son intercambiados en paquetes RADIUS. Cada paquete contiene la siguiente información como se muestra en la figura 6 [4]:

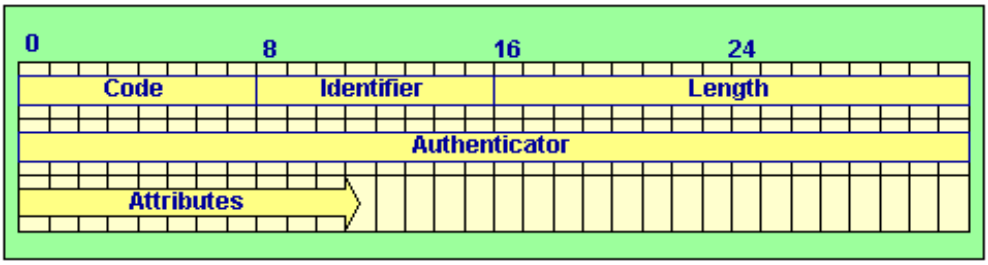

Figura 6. Formato de paquetes RADIUS [4].

Los campos en un paquete RADIUS son [4]:

- **Code (Código):** Un octeto que contiene el tipo de paquete [4]. En la tabla I se detalla el valor de cada code.

TABLA I

Descripción de los valores del campo Code [4]

Valor	Descripción
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo.	

- **Identifier (Identificador):** Un octeto que permite al cliente RADIUS relacionar una respuesta RADIUS con la solicitud adecuada [4].
- **Length (Longitud):** Longitud del paquete (2 octetos) [4].
- **Authenticator (Verificador):** Valor usado para autenticar la respuesta del servidor RADIUS. Es usado en el algoritmo de encubrimiento de contraseña [4].
- **Attributes (Atributos):** Aquí son almacenados un número arbitrario de atributos. Los únicos atributos obligatorios son el User-Name (usuario) y el User-Password (contraseña) [4].

2.7. Tipos de mensajes RADIUS

A continuación en la tabla II se describen los tipos de mensajes RADIUS que están definidos por los RFC 2865 y 2866 [4].

TABLA II

Descripción de tipos de mensaje RADIUS RFC 2865 y 2866 [4].

Tipo	Descripción
Access-Request	Enviado por un cliente RADIUS para solicitar autenticación y autorización para conectarse a la red. Debe contener el usuario y contraseña (ya sea de usuario o CHAP); además del puerto NAS, si es necesario.
Access-Accept	Enviado por un servidor RADIUS en respuesta a un mensaje de Access-Request. Informa que la conexión está autenticada y autorizada y le envía la información de configuración para comenzar a usar el servicio.
Access-Reject	Enviado por un servidor RADIUS en respuesta a un mensaje de Access-Request. Este mensaje informa al cliente RADIUS que el intento de conexión ha sido rechazado. Un servidor RADIUS envía este mensaje ya sea porque las credenciales no son auténticas o por que el intento de conexión no está autorizado.
Acces-Callenge	Envío de un servidor RADIUS en respuesta a un mensaje de Access-Request. Este mensaje es un desafío para el cliente RADIUS. Si este tipo de paquete es soportado, el servidor pide al cliente que vuelva a enviar un paquete Access-Request para hacer la autenticación. En caso de que no sea soportado, se toma como un Access-Reject.
Accounting-Request	Enviado por un cliente RADIUS para especificar información de cuenta para una conexión que fue aceptada.
Accounting-Response	Enviado por un servidor RADIUS en respuesta a un mensaje de Accounting-Request. Este mensaje reconoce el procesamiento y recepción exitosa de un mensaje de Accouting-Response.
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo	

2.8. Diagrama de secuencia

En la figura 7 se muestra la secuencia seguida cuando un cliente accede a la red y se desconecta de la misma [4].

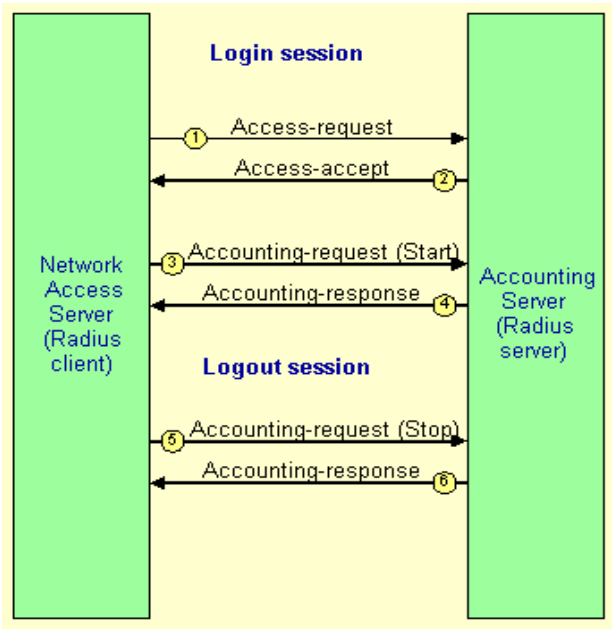

Figura 7. Diagrama de secuencia de RADIUS [4]

1. El cliente envía su usuario/contraseña, esta información es encriptada con una llave secreta y enviada en un Access-Request al servidor RADIUS (Fase de Autenticación) [4].

2. Cuando la relación usuario/contraseña es correcta, entonces el servidor envía un mensaje de aceptación, Access-Accept, con información extra (Por ejemplo: dirección IP, máscara de red, tiempo de sesión permitido, etc.) (Fase de Autorización) [4].

3. El cliente ahora envía un mensaje de Accounting-Request (Start) con la información correspondiente a su cuenta y para indicar que el usuario está reconocido dentro de la red (Fase de *Accounting*) [4].

4. El servidor RADIUS responde con un mensaje Accounting-Response, cuando la información de la cuenta es almacenada [4].

5. Cuando el usuario ha sido identificado, éste puede acceder a los servicios proporcionados. Finalmente, cuando desee desconectarse, enviará un mensaje de Accounting-Request (Stop) con la siguiente información [4]:

- **Delay Time:** Tiempo que el cliente lleva tratando de enviar el mensaje.
- **Input Octets:** Número de octetos recibido por el usuario.
- **Output Octets:** Número de octetos enviados por el usuario.
- **Session Time:** Número de segundos que el usuario ha estado conectado.
- **Input Packets:** Cantidad de paquetes recibidos por el usuario.
- **Output Packets:** Cantidad de paquetes enviados por el usuario.
- **Reason:** Razón por la que el usuario se desconecta de la red.

6. El servidor RADIUS responde con un mensaje de Accounting-Response cuando la información de cuenta es almacenada [4].

2.9. FreeRADIUS

Proyecto iniciado en 1999 por Alan DeKok y Miquel van Smoorenburg (quien colaboró anteriormente en el desarrollo de Cistron RADIUS), es una alternativa libre hacia otros servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que le componen. Puede operar tanto en sistemas con recursos limitados así como sistemas atendiendo millones de usuarios [5].

FreeRADIUS inició como un proyecto de servidor RADIUS que permitiera una mayor colaboración de la comunidad y que pudiera cubrir las necesidades que otros servidores RADIUS no podían. Actualmente incluye soporte para todos los protocolos comunes de autenticación y bases de datos [5].

FreeRadius es el primer OpenSource Radius Server, entre sus principales características esta la factibilidad de usar software de Base de Datos como OpenLDAP, MySQL, PostgreSQL, Oracle y soporta varios protocolos de autenticación como EAP, con EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, MSCHAPv2 y subtipos de Cisco LEAP. Todos estos protocolos son usados en la mayoría de los equipos wireless de equipos portátiles y Access point del mercado, por lo que es un

servidor bastante completo. Permite usar los estándares de encriptación WEP, WPA, WPA2, etc [6].

En la figura 8 se muestra el funcionamiento de un servidor RADIUS en este caso FreeRADIUS.

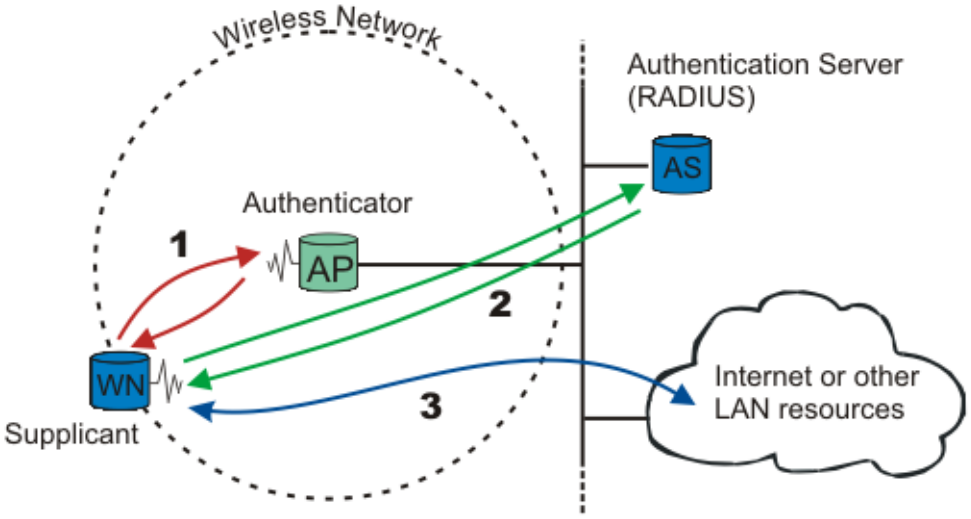

Figura 8. Funcionamiento de FreeRADIUS [6].

CAPÍTULO III: Portal Cautivo

3. PORTAL CAUTIVO

Un portal cautivo es un servicio web para el acceso a Internet. Con él se recoge todo el tráfico http y se redireccionan estas peticiones a un conjunto de páginas especiales, previamente definidas, como paso previo para permitir al usuario la navegación normal [7].

Es decir, antes de que el usuario pueda salir a Internet, está obligado a pasar por determinadas páginas en donde, normalmente, deberá autenticarse y se le muestra información importante de diversa índole, como puede ser instrucciones de uso, recomendaciones o acuerdos de utilización del servicio de acceso a Internet. Una vez que el usuario cumple con los requisitos exigidos en estas páginas iníciales, se permite su navegación a Internet con toda normalidad, siempre y cuando los sitios que quiera visitar estén permitidos [7].

A primera vista este servicio se asemeja bastante al trabajo que realiza un cortafuego, y a las que realiza un proxy, pero en la práctica un portal cautivo no sustituye a ninguno de ellos. Pensado para gestionar el acceso a Internet, su ámbito de actuación está limitado al tráfico http, peticiones que atiende en función de la autenticación válida del usuario que las solicita y de reglas que permiten o prohíben alcanzar los sitios solicitados, todo ello en un entorno dirigido a través de páginas web predefinidas. Los portales cautivos operan detrás del firewall, cuando estos están presentes y pueden combinarse con el trabajo de proxy [7].

3.1. Características generales de los portales cautivos

A continuación se mencionan las características más relevantes de un Portal Cautivo [8]:

- Independiente de la plataforma (Windows, Linux).
- Soporte para clientes con acceso alámbrico o inalámbrico.
- Filtrado de paquetes, ya sea por dirección MAC4, IP o por URLs. Se puede especificar reglas de bloqueo para una IP o puertos para tráfico saliente. La opción puede ser usada para limitar específicamente ciertos servicios, como limitar el uso de FTP5 o correo electrónico bloqueando esos puertos.

- No se necesita una configuración del lado del cliente, no requiere instalarse ningún programa en el PC del cliente, el Portal Cautivo asegura el enrutamiento de todos los clientes a la pantalla de inicio de sesión.
- Cualquier sistema operativo o navegador puede ser usado en el PC del cliente (Internet Explorer, Firefox, Opera, Safari, Konqueror).
- Control de información de los usuarios (Datos Personales).
- Las cuentas tienen límite de tiempo, cuando la sesión termina, el cliente puede continuar usando Internet después de comprar tiempo adicional.
- Existen portales cautivos por hardware y por software [8].

3.2. Tipos de portales cautivos

Hay dos grandes tipos de portales cautivos y un subtipo. El que hace falta un nombre de usuario y contraseña (una cuenta) y en el que simplemente se debe aceptar las condiciones de ingreso. El subtipo que puede ser de las dos es la variante “walled garden”. Esta última es la que limita a un grupo de sitios web pero no permite el acceso a internet en general (o a ciertos puertos.) [7].

3.3. Funcionamiento de portales cautivos

Una herramienta común de autenticación utilizada en las redes inalámbricas es el portal cautivo. Este utiliza un navegador web estándar para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso Aceptable) a los usuarios antes de permitir el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC) [7].

Para comenzar, el usuario abre su computadora portátil y selecciona la red. Su computadora solicita una dirección mediante DHCP y le es otorgada. Luego usa su navegador web para ir a cualquier sitio en Internet como se muestra en la figura 9 [7].

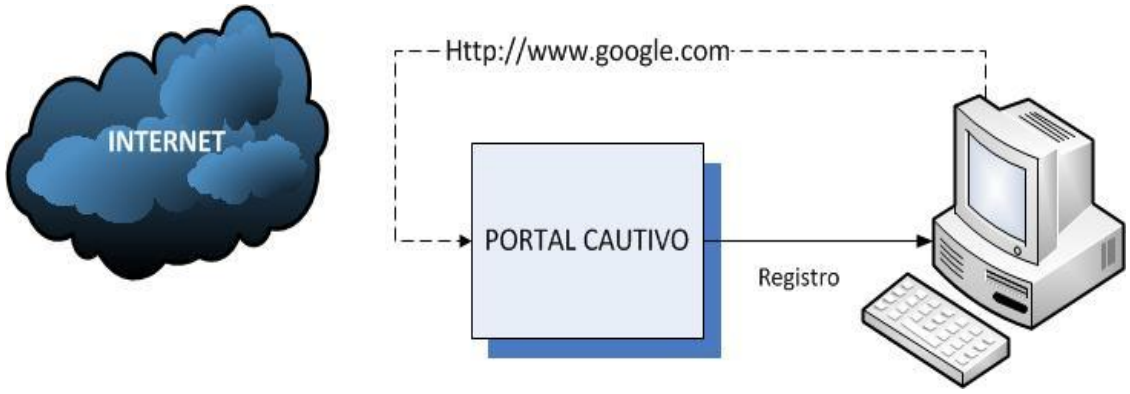

Figura 9. El usuario solicita una página web y es redireccionado [7].

En lugar de recibir la página solicitada, al usuario se le presenta una pantalla de registro. Esta página puede solicitarle al usuario que ingrese su nombre de usuario y una contraseña y al oprimir el boton de “registro” (login) el punto de acceso u otro servidor en la red verifica los datos. Cualquier otro tipo de acceso a la red se bloquea hasta que se verifiquen las credenciales como se puede observar en la figura 10 [7].

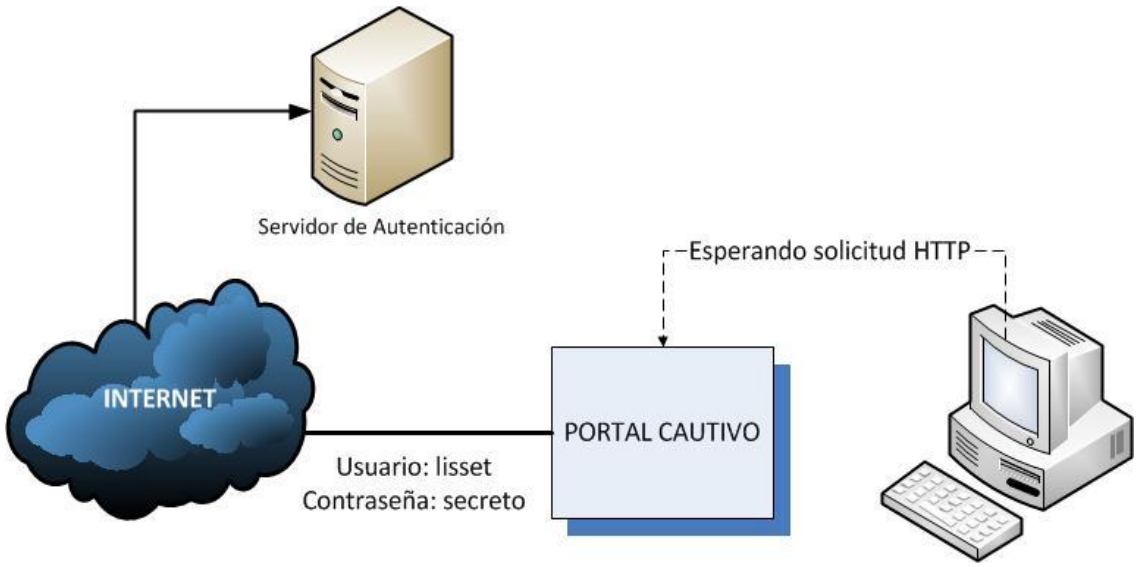

Figura 10. Verificación de credenciales [7].

Una vez que el usuario ha sido autenticado, se le permite el acceso a los recursos de la red, y en general es re direccionado al sitio web que solicitó originalmente como se ve en la figura 11 [7].

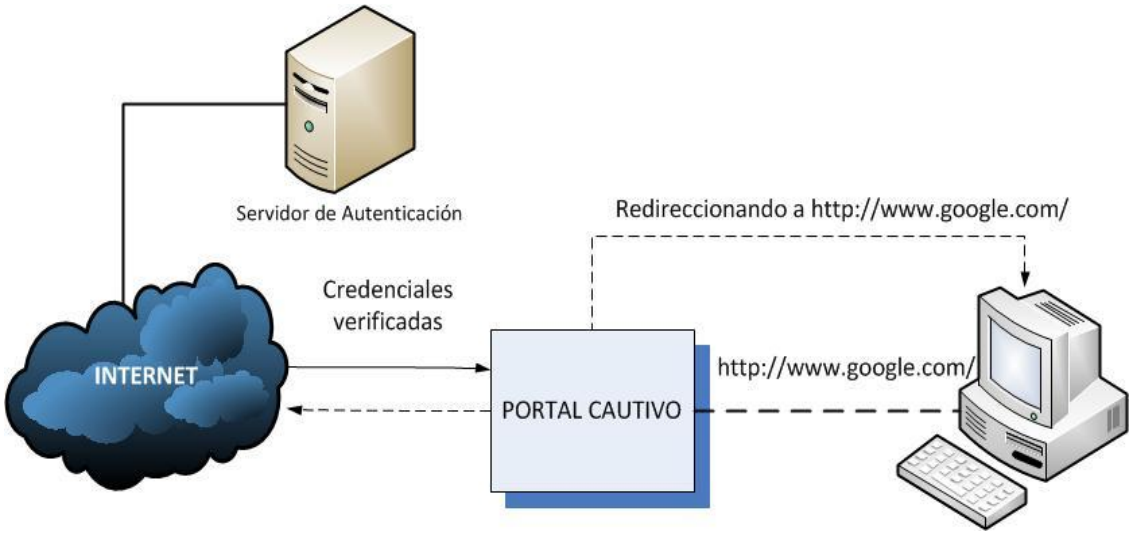

Figura 11. Se permite acceso al resto de la red [7].

Los portales cautivos no proveen encriptación para los usuarios de redes inalámbricas, en su lugar confían en las direcciones MAC e IP del cliente como identificadores únicas. Si bien esto no es necesariamente muy seguro, muchas implementaciones van a solicitar que el usuario se re-autentique periódicamente. Esto puede hacerse automáticamente, minimizando una ventana emergente (pop-up) del navegador, cuando el usuario se registra por primera vez [7].

3.4. CoovaChilli

CoovaChilli es un software libre de control de acceso, basado en el proyecto ChilliSpot que actualmente esta en desuso, y es mantenido activamente por un contribuyente ChilliSpot original. CoovaChilli está publicado bajo la licencia GNU General Public License (GPL). CoovaChilli provee un ambiente de portal cautivo y utiliza RADIUS para la autenticación y contabilidad [9].

En la figura 12 se puede observar a grandes rasgos como funciona la aplicación. Un cliente solicita acceso a los recursos de la red, el software CoovaChilli captura las solicitudes y se direcciona el usuario al portal cautivo para que realice el proceso de autenticación. Una vez el usuario haya entregado las credenciales correctas se le concede el acceso a los recursos, en el ejemplo a la WAN (Internet) [9].

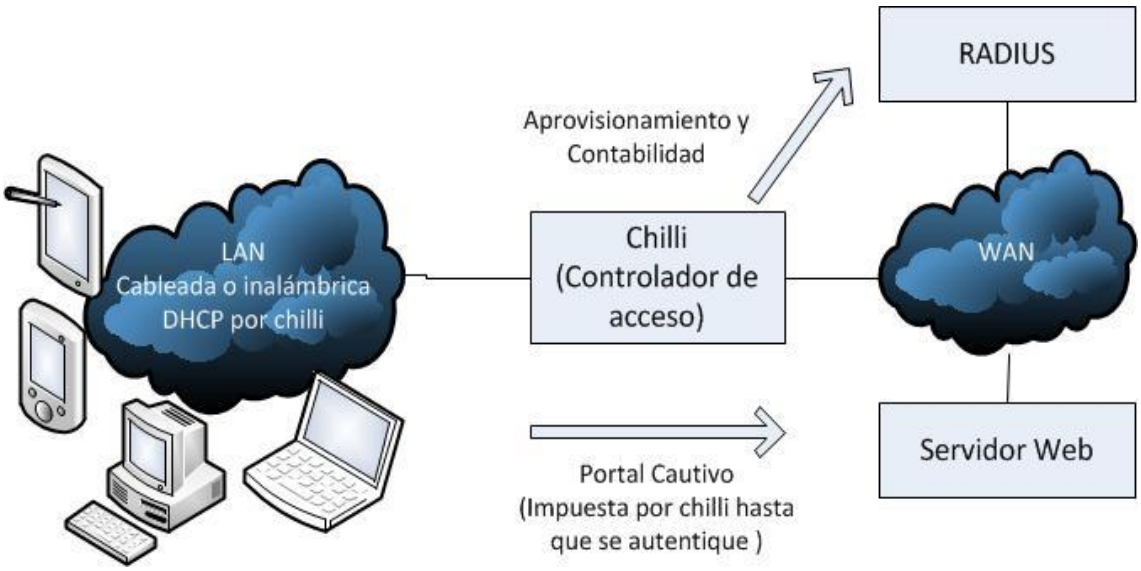

Figura 12. Diagrama del funcionamiento de CoovaChilli [9].

E. METODOLOGÍA

Durante el proceso de desarrollo del proyecto fin de carrera se hizo uso de distintas técnicas, métodos, herramientas y procedimientos que la investigación científica pone a disposición, para describir, analizar y valorar críticamente el desarrollo del proyecto.

MÉTODOS CIENTÍFICOS

El desarrollo del proyecto fin de carrera requirió seguir los lineamientos de ciertos métodos, así como de técnicas e instrumentos que permitieron la recopilación y análisis de la información necesaria para la presentación del presente PFC, tales como:

- **Método Inductivo.-** Este método permitió analizar las particularidades de la realidad actual sobre la forma en que se lleva el control de los usuarios en la conexión a los puntos de accesos inalámbricos, y con ello realizar el diagnóstico de la problemática identificada para extraer sus causas y características. Asimismo gracias a la generalización de los datos recogidos en la fase de análisis se pudo dar paso a la construcción de la propuesta alternativa y a la elaboración de conclusiones y recomendaciones.

- **Método Deductivo.-** Este método permitió conocer los problemas más relevantes y generales de la falta de seguridad en los puntos de acceso inalámbricos, a partir de los cuales se pudo determinar la problemática que se presenta al momento de conectarse a los puntos de accesos inalámbricos. Así mismo ayudó a obtener, clasificar y deducir, por medio del razonamiento lógico, la información y documentación necesarias para lograr un conocimiento que fortalezca el desarrollo del proyecto.

- **Método Analítico.-** permitió realizar un análisis del objeto en estudio, y así conocer el estado actual de los problemas de seguridad en la conexión a los puntos de acceso inalámbrico, la cantidad de usuarios que acceden a los mismos, los mecanismos de autenticación, lo que ayudó a la delimitación del problema, recolección, organización, comparación e interpretación de datos.

- **Metodología para el desarrollo del proyecto.-** Para la implantación del presente PFC no existen metodologías de desarrollo apropiadas es por esto que se ha propuesto dividir al PFC en las siguientes fases:

- ***Fase 1: Diagnóstico de la situación actual***

En esta fase se obtuvo toda la información necesaria para determinar la situación real de la red de la UNL y sus vulnerabilidades apoyada por técnicas como lo son la entrevista, encuesta y observación directa.

- ***Fase 2: Implantación de la Solución Planteada***

Durante esta fase se desarrolló la implantación del servidor RADIUS en la Unidad de Telecomunicaciones e Información y la selección de la mejor alternativa para la implantación del portal cautivo acorde con los requerimientos ya adquiridos.

- ***Fase 3: Implementación de la aplicación web para la administración del servidor RADIUS.***

Durante esta fase se buscó una herramienta web para la administración del servidor RADIUS que sea sencilla de manejar y configurar, acorde con las necesidades y se la implementó.

- ***Fase 4: Pruebas y Validación***

En esta fase se realizaron las pruebas pertinentes para validar la correcta configuración y funcionamiento del sistema de seguridad.

TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Las técnicas que se utilizaron para la recopilación de la información en el PFC son las siguientes:

- **Lectura comprensiva:** Permitió obtener un conocimiento ordenado y sistemático de los hechos e ideas relacionadas con el tema objeto de estudio, además sirvió para comprender correctamente como efectuar la implementación del PFC específicamente: las especificaciones técnicas y requisitos para la implementación del servidor RADIUS, configuración de FreeRADIUS, configuración de CoovaChilli, configuración de daloRADIUS, instalación de certificados de seguridad entre otros.

- **La Entrevista:** Esta técnica es una de las más importantes porque permitió obtener todos los requerimientos necesarios de manera directa de las personas responsables en la Unidad de Telecomunicaciones e Información (ver anexo 2, 3 y 4), como es la necesidad de tener el control de los usuarios que se conectan a los puntos de acceso inalámbricos.

- **La Observación directa:** Esta técnica permitió conocer la situación actual de la red de datos de la Universidad Nacional de Loja y así poder determinar los problemas existentes en la falta de seguridad en la conexión a los puntos de accesos inalámbricos (*ver sección resultados apartado 1.1.12. Problemas de seguridad informática en la red de datos*), también fue un gran apoyo para la vinculación con el problema de investigación, y con sus fuentes de información.

F. RESULTADOS

Esta sección se divide en dos partes importantes como es desarrollo de la propuesta alternativa y valoración técnica económica ambiental.

El desarrollo de la propuesta alternativa contiene la descripción de cada una de las fases del PFC, mientras que la valoración técnica económica ambiental comprende la justificación si el PFC es viable o no desde el punto de vista técnico, económico y ambiental.

1. DESARROLLO DE LA PROPUESTA ALTERNATIVA

1.1. FASE 1: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

1.1.1. Análisis de la infraestructura en la red de datos de la Universidad Nacional de Loja.

Durante los últimos años la Universidad Nacional de Loja ha ido incrementando de manera sorprendente, donde nace la necesidad de mejorar su infraestructura, tanto física como tecnológica y al mismo tiempo estar en continua actualización con los diferentes avances dentro del ámbito informático.

En la actualidad la Universidad dentro de su estructura funcional cuenta con la Unidad de Telecomunicaciones e Información, la cual esta dividida en cuatro secciones importantes las cuales son: sección de desarrollo de software, sección de mantenimiento y equipos electrónicos, sección de telecomunicaciones y la sección de redes y equipos informáticos.

La sección de redes y equipos informáticos es el responsable que está autorizado para la administración y gestión de la Red de la Universidad Nacional de Loja.

Es allí donde se realiza un monitoreo constante a los dispositivos y medios de networking e incluso a los servicios de internet (dhcp, dns, firewall, mail, etc). De acuerdo a ciertos criterios se toma la mejor solución si se ven falencias tanto en el servicio del Internet como en el estado de los dispositivos, así mismo se dan directrices para mejorar la conectividad entre los diferentes dispositivos de networking y equipos finales; sabiendo que es función primordial velar por la seguridad de la red de datos.

1.1.2. Simbología de los elementos que conforman la red de datos de la Universidad Nacional de Loja.

En la tabla III se especifica los símbolos que se utilizan para describir la topología de la red de datos de la Universidad Nacional de Loja.

TABLA III

Simbología de los elementos de la red

SÍMBOLO	DESCRIPCIÓN
	**Conexión Inalámbrica**
	**Router**
	**Switch de Acceso**
	**Servidor**
	**Pc Personal**
	**Torre**
	**Punto de Acceso inalámbrico**
	**Antena**
	Fibra óptica
	Cable UTP

Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo

1.1.3. Backbone de la Universidad Nacional de Loja

En la figura 13 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.

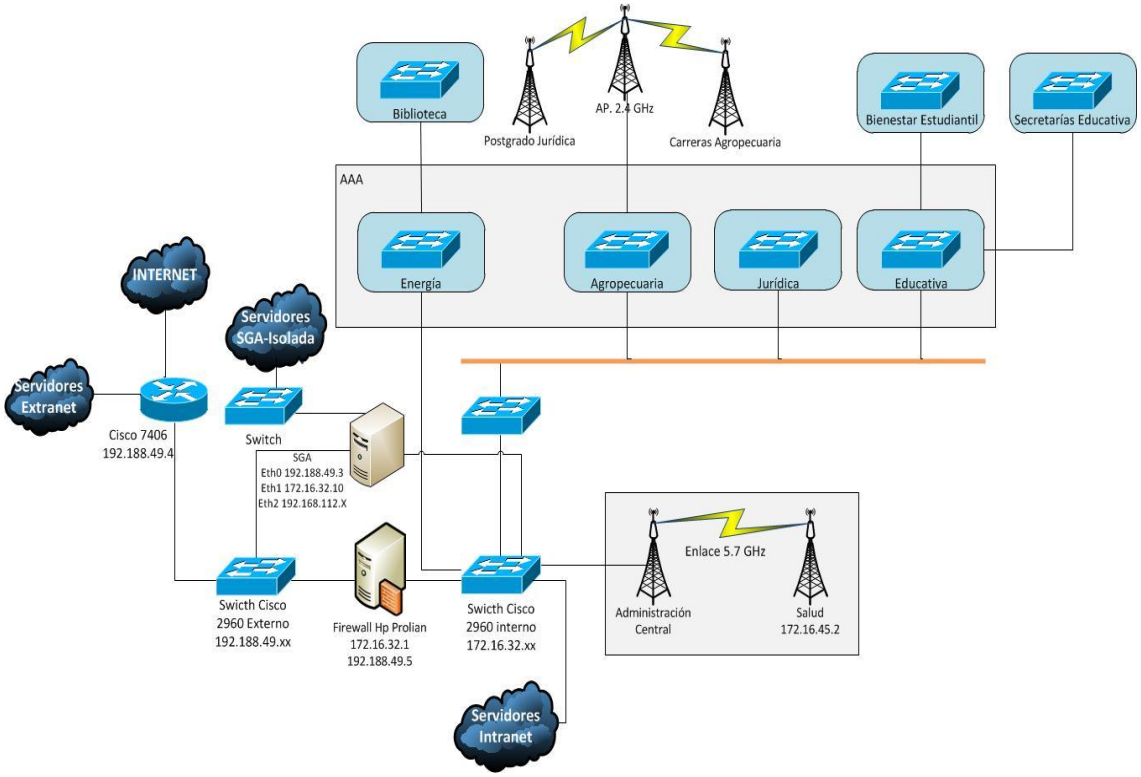

Figura 13. Backbone de la Universidad Nacional de Loja

El backbone de la Universidad esta compuesta de un gran número de switches interconectados los cuales llevan los datos a través de las distintas dependencias, utilizando como medio de transmisión fibra óptica, cable UTP cat. 5e, ondas electromagnéticas etc.

El proveedor de servicios de Internet (ISP) es la empresa Telconect S.A. garantizando la conexión con la red de redes tanto para el uso de internet, como para que la Universidad Nacional de Loja este en la capacidad de brindar sus servicios de forma eficaz y eficiente, vale enfatizar que en la actualidad la universidad cuenta con un ancho de banda de 80 Mbps.

La tecnología con que trabaja la red actualmente permite velocidades de 10 Mbps y 100 Mbps, la cual no necesita repetidores o amplificadores intermedios, debido a que trabaja con las distancias necesarias para el campus universitario.

La red de datos se compone de la interconexión de los bloques de Administración Central (Bloque 1 y Bloque 2) con las Áreas Académico Administrativas (AAA.)

En los bloques de Administración Central la rede de datos se compone de un backbone que usa como medio de transmisión fibra óptica multimodo del tipo 62.5/125 micrones (µm) con y seis hilos de fibra con una cubierta buferizada en su mayoría ocupando dos hilos para la interconexión la que comunica las AAA: Jurídica, Educativa, Agropecuaria y Energía y los dispositivos de networking activos para las comunicaciones.

Las distancias de transmisión de este tipo de fibra esta alrededor de los 1,604 km y se utilizan a diferentes velocidades: 10 Mbps, 100 Mbps. Cada terminación de fibra de cada edificio, distribuido en el campus universitario, que llega a su respectiva bandeja de fibra se encuentra empalmada con conectores del tipo ST, y estos a los Switch que poseen puertos de fibra.

Este cableado troncal es el que soporta todo el tráfico de información entre las áreas, permitiendo de esta manera hacer uso de los diferentes servicios de red que brinda la Universidad en todo el campus universitario como son: Internet, Acceso Inalámbrico, Correo Electrónico, Videoconferencias, Sistema de Gestión Académico etc.

1.1.4. Dispositivos de Networking del Cuarto de Telecomunicaciones

Los dispositivos de networking con los que cuenta la institución actualmente como: routers, switch, tranceiver, etc. Son los que permiten y garantizan la comunicación con los equipos finales (pc, pda, Tablet, Impresoras, etc.).

Cabe mencionar que la mayoría de los servidores (dns, dhcp, email, proxy, etc.) no cumplen con los requerimientos necesarios de hardware de un servidor, lo que ocasiona eventualmente problemas dentro de la red de datos, produciendo limitaciones y obstáculos para el correcto desempeño de las herramientas y aplicaciones que funcionan en cada servidor y así mismo en el servicio que brinda a cada uno de los usuarios tanto administrativos como estudiantes.

1.1.5. Diagrama de topología de la intranet

En el diagrama de topología se describen todos los enlaces principales, servidores y dispositivos de networking que sirven para la comunicación en la red de datos de todo el campus universitario durante agosto del 2011.

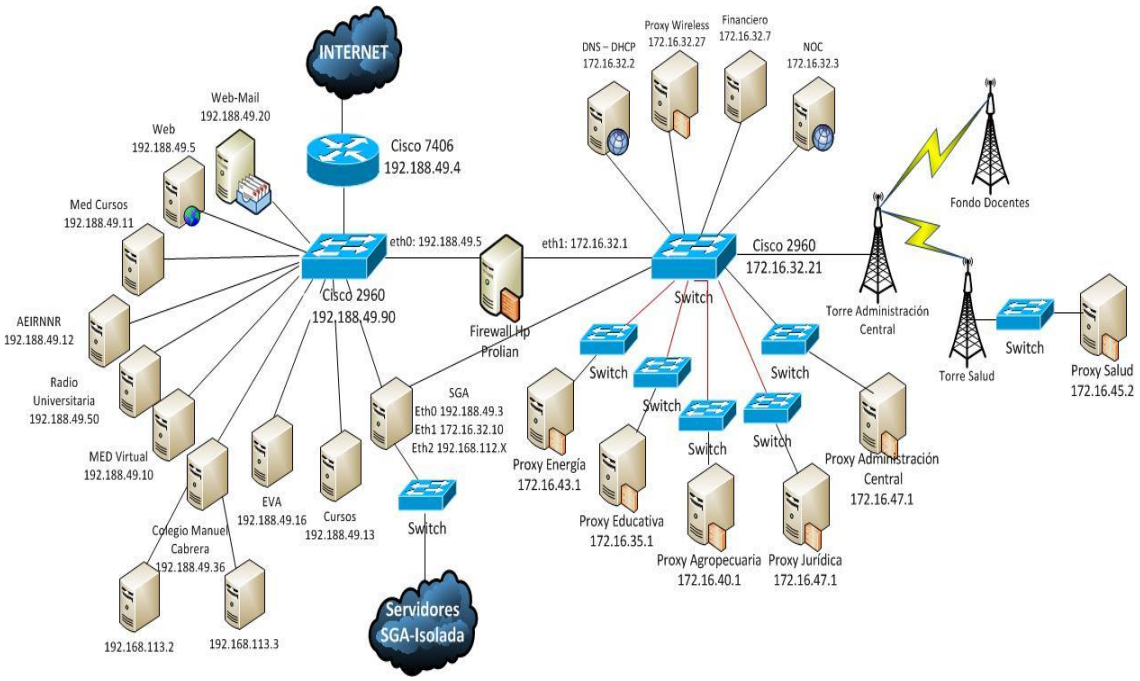

Figura 14. Topología de la intranet de la Universidad Nacional de Loja

En la figura 14 se puede observar detalladamente los dispositivos de networking activos principales como son: Router cisco 7604, switch cisco 1960 externo, switch cisco 2960 interno, firewall HP ProLiant, los cuales se describen más adelante. También se visualiza los servidores públicos y privados, los cuales brindan servicios muy importantes en el campus universitario dentro de ellos están DNS, DHCP, Cursos, Web Mail, Proxys etc.

1.1.6. Descripción de los dispositivos de networking principales

A continuación se detalla los principales dispositivos de networking activos de la red de la Universidad Nacional de Loja con su respectiva descripción y funcionamiento.

- **Router Cisco 7604:** Dispone de una dirección IP pública 192.188.49.4/24, este ruteador facilita la interconexión de las redes con las que cuenta la institución determinando cual es la mejor ruta que deben tomar los paquetes para llegar a su destino.

También Permite acceder a Internet comercial e Internet2 que brinda el CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado). El ISP Telconet S.A emplea un enlace de fibra óptica multimodo lo que se conecta al router que esta ubicado en el cuarto de telecomunicaciones dentro de la Unidad de Telecomunicaciones e Información.

- **Switch Cisco 2960 externo:** tiene la dirección IPv4 pública 192.188.49.15/24 lo que permite su administración. Este dispositivo opera en la capa 2 del modelo OSI el cual facilita la interconexión de dos o más segmentos de red.

Una de las interfaces Fast Ethernet 1000 Mbps se encuentra conectado al router cisco 7604 y los puertos 10/100 Mbps se conectan con los servidores públicos (firewall, web, cursos, MED, SGA, etc).

- **Switch Cisco 2960 interno:** esta configurado con la dirección IP privada 172.16.32.21/19 para realizar la administración, este dispositivo funciona en la capa 2 del modelo OSI y opera con direcciones MAC para el envío de tramas en la red.

Una interfaz Fast Ethernet 10/100 Mbps establece la conexión directa con el firewall HP Proliant para facilitar el acceso a los servidores públicos e internet.

Los puertos 10/100 Mbps permite la conexión con los diferentes servicios de Internet que brinda la institución como lo son: DNS, DHCP, email, proxy, SGA, etc. Y facilita también la comunicación con las diferentes áreas académico administrativas.

- **Firewall HP Proliant:** es un dispositivo (router-firewall) posee dos direcciones de red, una pública 192.188.49.5/24 y otra privada 172.16.32.1/19 en la cual cada una de las interfaces Fast Ethernet 10/100 Mbps se encuentra conectado a los switch cisco 2960 interno y externo respectivamente.

En el firewall se maneja la configuración de NAT la cual permite que los equipos con direcciones privadas IP compartan una dirección IP enrutable (IP Pública). También se manejan políticas de seguridad como son las iptables, enrutamiento hacia el exterior de la red y VPN (Red Privada Virtual).

En conjunto dichos equipos de networking componen el núcleo principal de la infraestructura de la red de datos de la Universidad Nacional de Loja. En la tabla IV se presenta las especificaciones de hardware de los dispositivos de networking existentes en el cuarto de telecomunicaciones.

TABLA IV

Dispositivos de networking administración central

Dispositivo	Marca / Modelo	Puertos
Router de Borde	Cisco 7604 ws-sup32-ge-3b	• 8 port Gigabit / Ethernet • 1 port 100 / 1000 Mbps
Switch Público	Catalyst 2960 Series ws-c2960-24TT-LV02	• 24 port 100 Mbps • 2 port 1000 Mbps
Switch Privado	Catalyst 2960 Series ws-c2960-24TT-LV02	• 24 port 100 Mbps • 2 port 1000 Mbps
Switch Interno	3com 3300 -3c16980A	• 24 port 100 Mbps
Switch Interno	Dlink DES-3624	• 20 port 10/100 Mbps
Switch Interno	Dlink DES-3624	• 22 port 10/100 Mbps
Switch Interno	Dlink DSS/-4	• 24 port 10/100 Mbps
Router SDSL	Cisco 673	• 3 port ENET, MGMT y WALL
Transceiver	Dlink 300 SC	• 10/100 Base-Tx / 100 Base-Fx
Transceiver	Dlink DFE 855	• 100 Base-Tx to 100 Base-Fx
Transceiver	Dlink DMC 700SC	• 1000 Base-T / 1000 Base-SX
Transceiver	Dlink 300 SC	• 10/100 Base-Tx / 100 Base-Fx
Transceiver	Dlink DFE 855	• 100 Base-Tx to 100 Base-Fx

Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo

Fuente: Unidad de Telecomunicaciones e Información

1.1.7. Descripción de servidores públicos

Como se muestra en la figura 14 el Switch cisco 2960 están conectados los servidores públicos. Estos servidores son necesarios ser accedidos tanto desde afuera (red de redes) como desde la intranet de la universidad. A continuación se detallan los servidores que se encuentran implementados y en producción en la Unidad de Telecomunicaciones e Información.

- **Correo Electrónico:** La institución brinda servicio de correo electrónico a un número limitado de funcionarios que laboran en las distintas dependencias y áreas

académico administrativas (AAA). Este servicio de red permite enviar y recibir mensajes electrónicos, adjuntar documentos digitales y así tener comunicación fiable.

- **Servidor Web:** la función de este servidor es brindar al mundo entero la vida digital de la Universidad a través de aplicaciones web dinámicas como son: blogs, cursos, etc. Donde se encuentra información de cada una de las dependencias y áreas académico administrativas lo que permite la interacción de los usuarios con las páginas.

- **Sistema Académico:** en el cuarto de telecomunicaciones existe todo un cluster de servidores que cumplen la función de brindar un Sistema de Gestión Académico (SGA) de alto rendimiento y disponibilidad. Lo que permite la automatización de procesos académicos que se realizaban de forma manual. Este servicio esta disponible tanto para estudiantes como docentes.

- **Modalidad a Distancia:** los servidores con los que cuenta la Modalidad de Estudios a Distancia (MED) permiten brindar una educación a distancia virtualizada a través de plataformas de e-learning (moodle) las cuales incorporan aplicación como: foros de discusión, blog personales, mensajería instantánea etc.

En la tabla V se detalla el hardware de los equipos donde están funcionando los diferentes servicios de internet en la red de datos pública de la Universidad Nacional de Loja durante el periodo de abril del 2011.

TABLA V

Descripción del hardware de los servidores públicos

Servidor	Marca / Modelo	Características
Web Universidad	HP Proliant ML150	• Procesador: Intel Xeon 3.2 Ghz • Memoria: 1GB • Disco Duro: 100 GB
Cursos Elearning	HP Proliant ML150	• Procesador: Intel Xeon 3.2 Ghz • Memoria: 1GB • Disco Duro: 100 GB
MED 1 (Módulos)	HP Compaq	• Procesador: Core 2Duo Inside • Memoria: 5GB

		• Disco Duro: 500 GB
MED 2 (Evaluación)	HP Compaq	• Procesador: Core 2Duo Inside • Memoria: 4GB • Disco Duro: 250 GB
MED 3 (Cursos)	HP Proliant ML115	• Procesador: AMD Attlon • Memoria: 5GB • Disco Duro: 250 GB
Sistema Académico 1	Aopen	• Procesador: Pentium 4, 2.0 Ghz • Memoria: 512 MB • Disco Duro: 60 GB
Sistema Académico 2	Compaq Presario	• Procesador: Intel Pentium 4, 3.6 GHZ • Memoria: 512 MB • Disco Duro: 160 GB
Correo Electrónico	HP Compaq 6000 Pro MT PC	• Procesador: Intel Core 2Duo, 2.9 Ghz • Memoria: 2GB • Disco Duro: 300 GB
Radio Universitaria	HP Compaq 6000 Pro MT PC	• Memoria: 1957 MB • Disco Duro: 295 GB
Firewall	HP Proliant ML370G5	• Procesador: Intel Xeon 1.8 Ghz • Memoria: 2GB • Disco Duro: 66 GB
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo ***Fuente: Unidad de Telecomunicaciones e Información***		

1.1.8. Descripción de servidores privados

Como se muestra en la figura 14 los servidores de la intranet están interconectados con el Switch cisco 2960 y existe un segmento conectado para wireless Lan (WLan). Todos estos servidores se consideran privados por lo que solo pueden ser accedidos desde la intranet, es decir no se pueden visualizar los servicios de Internet desde afuera (red de redes).

A continuación se detallan los servidores que se encuentran implementados y en producción en el cuarto de telecomunicaciones como son: Sistema de nombres (DNS), Asignación de direcciones IP (dhcp), proxy administración, proxy wireless, Sistema Académico (SGA). Etc.

- **Sistema de Nombres:** permite la resolución directa o inversa de las direcciones de Internet, se encuentra configurado como DNS primario haciendo uso del domino unl.edu.ec, facilitando de esta forma la resolución de nombres a los equipos finales en el campus universitario.

- **Asignación de direcciones IP:** este servidor asigna a los clientes (pc, impresoras, entre otros) automáticamente por medio de direcciones MAC los parámetros de configuración de la red como son: IP, máscara de subred, puerta de enlace, DNS y dominio.

- **Proxy Administración:** es un equipo intermedio que facilita el acceso a los servicios de la intranet, servicios públicos e Internet a todos los equipos finales de la institución que no cuentan con una conexión directa a internet.

En los servidores de este tipo (proxy) se manejan ciertas políticas de seguridad como es el control de contenido pornográfico, acceso a sitios infectados de virus, etc. Existen un proxy por cada Área académico administrativa (AAA), administración central, modalidad de estudios a distancia y red inalámbrica (proxy transparente).

- **Proxy Wireless:** es un equipo intermediario que intercepta las peticiones de navegación de los usuarios que utilizan cualquier dispositivo que se conecta de forma inalámbrica a la red de la Universidad y permite el acceso a los servicios de la intranet, servicios públicos e Internet.

Es importante recalcar que este proxy es un proxy transparente la mayor diferencia es que con un proxy transparente, no hay que hacer configuraciones de red en los usuarios para que el tráfico http sea capturado. Al estar construido como parte de la arquitectura de red, todo el tráfico del puerto 80 tiene que pasar por este proxy transparente.

- **Sistema de Gestión Académico:** el Sistema de Gestión Académico que se accede por medio de la intranet universitaria facilita a los estudiantes, docentes y funcionarios cumplir sus actividades académicas de forma eficaz y eficiente.

En la tabla VI se detalla el hardware de los equipos en donde están funcionando los diferentes servicios de internet en la red de datos de la intranet de la Universidad Nacional de Loja durante el periodo de abril del 2011.

TABLA VI

Descripción del hardware de los servidores privados

Servidor	Marca / Modelo	Características
DNS- DHCP	HP Proliant ML150	• Procesador: Intel Xeon 3.2 Ghz • Memoria: 1GB • Disco Duro: 100 GB
Proxy Administración	HP Compaq	• Procesador: Pentium D 3.4 Ghz • Memoria: 1GB • Disco Duro: 145 GB
Proxy Wireless (transparente)	HP Compaq	• Procesador: Pentium D 3.4 Ghz • Memoria: 2 GB • Disco Duro: 145 GB
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo		
Fuente: Unidad de Telecomunicaciones e Información		

1.1.9. Direccionamiento IPv4 público de la Universidad Nacional de Loja

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 mundo entero, como lo son cursos, correo electrónico, sistema de gestión académico, radio universitaria, etc.

En la tabla VII se detalla el direccionamiento IPv4 público de clase C.

TABLA VII

Direccionamiento IPv4 público

Descripción	Especificación
Red de clase C	192.188.49.0/24
Dominio	unl.edu.ec
Máscara de Subred	255.255.255.0
Dirección de Broadcast	192.188.49.255

Puerta de enlace	192.188.49.4
Sistema de Nombres de Dominio (DNS) primario	200.93.221.17
Sistema de Nombres de Dominio (DNS) secundario	200.93.192.188
Número de hosts disponibles	254
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo	
Fuente: Unidad de Telecomunicaciones e Información	

En la tabla VIII se detalla el direccionamiento IPv4 de los servidores públicos de la universidad ubicados en la Unidad de telecomunicaciones e Información.

TABLA VIII

Direccionamiento IPv4 servidores públicos

Nombre	Interfaz	Dirección IPv4	Gateway	DNS- Primario
Servidor Web	eth0	192.188.49.2/24	192.188.49.4	200.93.222.17
Admisiones SGA	eth1	192.188.49.3/24	192.188.49.4	200.93.222.17
Router Cedia Telconet	eth0	192.188.49.4/24	192.188.49.4	200.93.222.17
Firewall	eth0	192.188.49.5/24	192.188.49.4	200.93.222.17
Sistema Académico (SGA)	eth1	192.188.49.6/24	192.188.49.4	200.93.222.17
Web vinculación	eth0:0	192.188.49.9/24	192.188.49.4	200.93.222.17
Web Virtual (MED)	eth0	192.188.49.10/24	192.188.49.4	200.93.222.17
Web Cursos (MED)	eth0	192.188.49.11/24	192.188.49.4	200.93.222.17
Web Área Energía	eth0	192.188.49.12/24	192.188.49.4	200.93.222.17
Web Cursos Universidad	eth0	192.188.49.13/24	192.188.49.4	200.93.222.17
Web Virtual (MED)	eth0	192.188.49.16/24	192.188.49.4	200.93.222.17
Correo Electrónico	eth0	192.188.49.20/24	192.188.49.4	200.93.222.17
Radio Universitaria	eth0	192.188.49.50/24	192.188.49.4	200.93.222.17
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo				
Fuente: Unidad de Telecomunicaciones e Información				

1.1.10. Direccionamiento IPv4 de intranet de la Universidad Nacional de Loja

La Universidad 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 IX se detalla el direccionamiento IPv4 de la UNL.

TABLA IX

Direccionamiento IPv4 de la Intranet

Descripción	Especificación
Red de clase B	172.16.0.0/16
Dominio	unl.edu.ec
Subred de la Universidad	172.16.32.0/19
Máscara 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
Número de hosts disponibles	8190
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo ***Fuente: Unidad de Telecomunicaciones e Información***	

En la tabla X se detalla el direccionamiento IPv4 de los servidores privados de la universidad ubicados en la Unidad de telecomunicaciones e Información.

TABLA X

Direccionamiento IPv4 servidores públicos

Nombre	Interfaz	Dirección IPv4	Gateway	DNS Primario
Firewall	eth1	172.16.32.1/19	172.16.32.1	172.16.32.2
Sistemas de Nombres (DNS)	eth0	172.16.32.2/19	172.16.32.1	172.16.32.2
Asigancion IPv4 (DHCP)	eth0	172.16.32.4/19	172.16.32.1	172.16.32.2
Sistema Académico (SGA)	eth0	172.16.32.10/19	172.16.32.1	172.16.32.2
Proxy Administración	eth1	172.16.32.13/19	172.16.32.1	172.16.32.2

Sistema de monitoreo (nagios)	eth0:0	172.16.32.20/19	172.16.32.1	172.16.32.2
Proxy Wireless	eth0	172.16.32.27/19	172.16.32.1	172.16.32.2
Proxy MED	eth0	172.16.32.28/19	172.16.32.1	172.16.32.2
Proxy Educativa	eth0	172.16.35.1/19	172.16.32.1	172.16.32.2
Proxy Jurídica		172.16.37.1/19	172.16.32.1	172.16.32.2
Proxy Agropecuaria	eth0	172.16.40.1/19	172.16.32.1	172.16.32.2
Proxy Energía	eth0	172.16.43.1/19	172.16.32.1	172.16.32.2
Proxy Salud	eth0	172.16.45.2/19	172.16.32.1	172.16.32.2
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo ***Fuente: Unidad de Telecomunicaciones e Información***				

1.1.11. Distribución de los puntos de acceso inalámbricos

En la actualidad la Universidad Nacional de Loja no posee una red Wireless debido a la falta de equipos para la implementación de la misma, lo que ha llevado a que se coloquen puntos de accesos inalámbricos distribuidos en las diferentes áreas de la institución de acuerdo a las necesidades de los requerimientos de cada lugar. Durante estos últimos años ha ido creciendo notablemente la cantidad de usuarios que se conectan inalámbricamente debido al incremento y fácil acceso a dispositivos con conexión inalámbrica.

El estudio de la red de datos de la UNL llevó a determinar la ubicación física de los puntos de acceso en administración central y en cada una de las áreas que conforman el campo universitario asimismo la cantidad de direcciones IP, el rango de direcciones IP, marca de los equipos etc. La recolección de estos datos se obtuvo durante el mes de Septiembre del 2012.

1.1.11.1. Administración Central

El edificio de administración central se encuentra ubicado en el lado Norte de la UNL dividido en dos bloques. En este edificio se encuentran localizados la mayoría de los departamentos administrativos de la Universidad en el bloque uno encontramos departamentos como son, el Rectorado, Vicerrectorado, Secretaria General, Jefatura

de Bibliotecas Auditoria Interna, Procuraduría General, Tesorería, Documentación y Archivo, Venta de Derechos Especiales y Construcciones.

En el bloque dos se encuentra los departamentos de Recursos Humanos, Bienestar Estudiantil, Compras Públicas, Sucursal del Banco de Loja , Contabilidad General, Dirección Financiera, Nóminas, Sistema de Gestión Académico, Centro de Investigaciones y Apoyo al Desarrollo Universitario y la Unidad de Redes Telecomunicaciones e Información.

En administración central existen un total de 10 puntos de acceso inalámbricos los que se detallan en la tabla XI.

TABLA XI

Descripción de puntos de acceso administración central

IP RADIO	SSID	MARCA	INICIO	FIN	#IP	UBICACIÓN
ADMINISTRACIÓN CENTRAL						
172.16.57.4 - 11	**Libres**					
172.16.57.13 - 23	**Libres**					
172.16.57.12	SISoftware	D-Link 2100 AP	172.16.63.175	172.16.63.179	5	UTI-SGA
172.16.57.24	SICisaq02	D-Link 2100 AP	172.16.57.25	172.16.57.34	10	CISAQ
172.16.57.35	SIAdminCentral01	D-Link 2100 AP	172.16.57.36	172.16.57.45	10	Bloque 1. Adm. Central, 4 Piso
172.16.57.46	SICisaq03	D-Link 2100 AP	172.16.57.47	172.16.57.56	10	CISAQ
172.16.57.57	SIHardware	D-Link 2100 AP	172.16.57.58	172.16.57.62	5	UTI-SGA
172.16.57.63	SICisaq04	D-Link 2100 AP	172.16.57.64	172.16.57.73	10	CISAQ
172.16.57.74	SIBienestar01	D-Link DAP 1360	172.16.57.75	172.16.57.79	5	Ex - FEUE, personas con discapacidad
172.16.57.80	SIBienestar02	D-Link DAP 1360	172.16.57.81	172.16.57.85	5	Ex - FEUE, becas
172.16.57.86	SITae	D-Link	172.16.57.87	172.16.57.96	10	Bloque 1.

		2100 AP				Adm. Central, 3 piso
172.16.57.97	SIRedes02	Router Linksys	192.168.1.100	192.168.1.120	20	UTI-Redes
172.16.57.98 - 101	**Libres**					
172.16.57.102	MeshMed	WRT-Linksys				MED
172.16.57.103 -139	**Libres**					
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo ***Fuente: Unidad de Telecomunicaciones e Información***						

1.1.11.2. Área de la Educación Arte y Comunicación

Se encuentra ubicada al Noroccidente de la ciudadela Universitaria es una de las más grandes con que cuenta la Universidad, su estructura física en su mayoría construida de edificios de dos pisos, a diferencia del edificio de la Carrera de Comunicación Social, la cual actualmente está ubicada en una construcción antigua, es parte de esta área el colegio Universitario Manuel Cabrera Lozano, en este bloque se encuentra la biblioteca del área, donde esta ubicado un servidor proxy, el cual da acceso a la red a dicha área, cuenta con switchs de acceso para la red cableada, así como también para la inalámbrica, se encuentran distribuidos en esta área alrededor de 9 puntos de acceso inalámbricos lo que se detalla en la tabla XII.

Forman parte de esta área, las carreras de Comunicación social, Informática Educativa, Ingles, Químico Biológicas, Físico Matemáticas, Artes Plásticas, Música, Educación Física, Psicología, y Posgrado de Educativa.

TABLA XII

Descripción de puntos de acceso Área de la Educación, Arte y Comunicación

IP RADIO	SSID	MARCA	INICIO	FIN	#IP	UBICACIÓN
ÁREA DE LA EDUCACIÓN ARTE Y COMUNICACIÓN						
172.16.57.140 - 150	**Libres**					
172.16.57.151	SIBiblioEducativa	D-Link 2100 AP	172.16.57.152	172.16.57.171	20	1 Piso Bloque 1, Biblioteca
172.16.57.172	SIInfEducativa	D-Link 2100 AP	172.16.57.173	172.16.57.182	10	2 Piso Bloque 2,

						Centro de computo # 2
172.16.57.183	SIEducativa01	D-Link 2100 AP	172.16.57.184	172.16.57.193	10	
172.16.57.194 -226	**Libres**					
172.16.57.227	SIInvestEduc	D-Link 2100 AP	172.16.57.228	172.16.57.237	10	A Piso Bloque 3, Coord Investigaciones
172.16.57.238 - 248	**Libres**					
172.16.57.249	SIComunicacio Social	D-Link 2100 AP	172.16.57.250	172.16.57.255	6	Ex - Cater
172.16.58.1 - 6	Libres					
172.16.58.7	SIEducativa03	D-Link 2100 AP	172.16.58.8	172.16.58.15	7	2 Piso Bloque 3
172.16.58.16	SICoordInfEdu	D-Link 2100 AP	172.16.58.16	172.16.58.26	11	2 Piso bloque 7, Direccion del area
172.16.58.27	Col_MCL	Wap				
172.16.58.28	SIMusica	Router Linksys	192.168.1.100	192.168.1.124	25	Bloques de Artes
172.16.58.29 - 50	**Libres**					
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo						
Fuente: Unidad de Telecomunicaciones e Información						

1.1.11.3. Área de la Salud Humana

Esta área se encuentra ubicada al Norte de la ciudadela Universitaria, junto al hospital Isidro Ayora, la conexión con la red de datos se la hace de manera inalámbrica desde la torre central, contando también con un servidor proxy para el acceso a la red, cuenta con 6 puntos de acceso los cuales les permiten la comunicación inalámbrica a los usuarios de la red de datos lo que se detalla en la tabla XIII.

Forman parte de esta área las carreras de: Laboratorio clínico, Odontología, Medicina, Psicología Clínica, Enfermería y su nivel de posgrado con especialidades Médicas y Maestría.

TABLA XIII

Descripción de puntos de acceso Área de la Salud Humana

IP RADIO	SSID	MARCA	INICIO	FIN	#IP	UBICACIÓN
ÁREA DE LA SALUD HUMANA						
172.16.58.51	SIBiblioAS	D-Link 2100 AP	172.16.58.52	172.16.58.71	20	Biblioteca ASH
172.16.58.72	SISalud01	D-Link 2100 AP	172.16.58.73	172.16.58.82	10	
172.16.58.83- 93	**Libres**					
172.16.58.94	SISalud05	D-Link 2100 AP	172.16.58.95	172.16.58.104	10	
172.16.58.105-116	**Libres**					
172.16.58.117	SIInvestigaciones	D-Link 2100 AP	172.16.58.118	172.16.58.137	20	Investigaciones ASH
172.16.58.138	Tics-ash	Router Linksys	192.168.91.1	192.168.91.77	21	
172.16.58.139	SIEnfermeria	Router Linksys	172.16.58.140	172.16.58.144	5	
172.16.58.145-200	**Libres**					
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo						
Fuente: Unidad de Telecomunicaciones e Información						

1.1.11.4. Área de la Energía las Industrias y los Recursos Naturales no Renovables.

El Área de la Energía como se la denomina usualmente se encuentra ubicada al Nororiente del Campus Universitario, forman parte de esta área los edificios de la Modalidad de Estudios a Distancia (MED) así como también los edificios pertenecientes a la FEUE, en su mayoría está compuesta por edificios nuevos a diferencia del edificio donde funcionan las coordinaciones de carrera, que es un edificio antiguo, donde además se concentran la mayor parte de equipos informáticos, ya sea por encontrarse aquí cuatro laboratorios virtuales, cuenta con ocho edificios que conforman esta área, uno de los edificios más nuevos es la biblioteca donde se concentra la mayoría de los usuarios de la red de datos, al igual que con el resto de áreas también dispone de un servidor proxy para dar acceso a la red a los usuarios así como también switchs de acceso, tanto para la red cableada como para la inalámbrica,

cuenta con 9 puntos de acceso que se encuentran distribuidos en los diferentes bloques lo que se detalla en la tabla XIV.

Forman parte de esta área las carreras de: Ingeniería en Sistemas. Ingeniería Electromecánica, Ingeniería en Geología, Ingeniería en Electrónica, y la Maestría en Electromecánica.

TABLA XIV

Descripción de puntos de acceso Área de la Energía, las Industrias y los Recursos Naturales no Renovables

IP RADIO	SSID	MARCA	INICIO	FIN	#IP	UBICACIÓN
ÁREA DE LA ENERGÍA LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES						
172.16.58.201	SIBiblioteca	D-link 3200 AP	172.16.58.202	172.16.58.221	20	1 Piso Bloque 5, Biblioteca Área
172.16.58.222	SIDocentesSistemas	Router	192.168.0.100	192.168.0.120	20	Bloque 1
172.16.58.223 - 242	**Libres**					
172.16.57.1	SIEnergia02	Router Linksys	192.168.1.100	192.168.1.119	20	Bloque 1
172.16.57.2	SIEnergia03	Router Linksys	192.168.1.100	192.168.1.119	20	Bloque 1
172.16.57.3	SIEnergia04	Router Linksys	192.168.1.100	192.168.1.119	20	Bloque 1
172.16.58.243	SIGeologia01	D-Link 2100 AP	172.16.58.244	172.16.58.255	12	Bloque 2
172.16.59.28	SI_Geologia Docentes	Router	192.168.100.1			Bloque 2
172.16.59.29-58	**Libres**					
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo ***Fuente: Unidad de Telecomunicaciones e Información***						

1.1.11.4.1. Cobertura Inalámbrica

Tomando en cuenta la configuración de los equipos (Data Rate) y potencia de la antena de los access point distribuidos en el Área de la Energía, las Industrias y los Recursos Naturales no Renovables, se ha determinado el espectro que llegan a cubrir dichos equipos.

La tabla XVI describe el rango de cobertura de los puntos de acceso dentro del área.

TABLA XV

Cobertura de puntos de acceso AEIRNNR

N°	SSID	Modelo	Ubicación	Rango de Cobertura*
1	SIDocentesSistemas	Router DLink DIR 300	Bloque 1	14,4 m
2	SIEnergia02	Router Linksys E1200	Bloque 1	15 m
3	SIEnergia03	Router Linksys E1200	Bloque 1	15 m
4	SIEnergia04	Router Linksys E1200	Bloque 1	15 m
5	SIGeologia01	Router Linksys E1200	Bloque 2	15 m
6	SI_GeologiaDocentes	DLink 1200AP	Bloque 2	15 m
7	SIBiblioteca	DLink 3200AP	Primer Piso Bloque 5, Biblioteca AEIRNNR	14,4 m

Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo

Fuente: Unidad de Telecomunicaciones e Información

* Obtenidos de acuerdo a las especificaciones del producto y al data rate configurado (12 Mbps).

En la figura 15 se muestra la distribución de los puntos de acceso y la cobertura correspondiente.

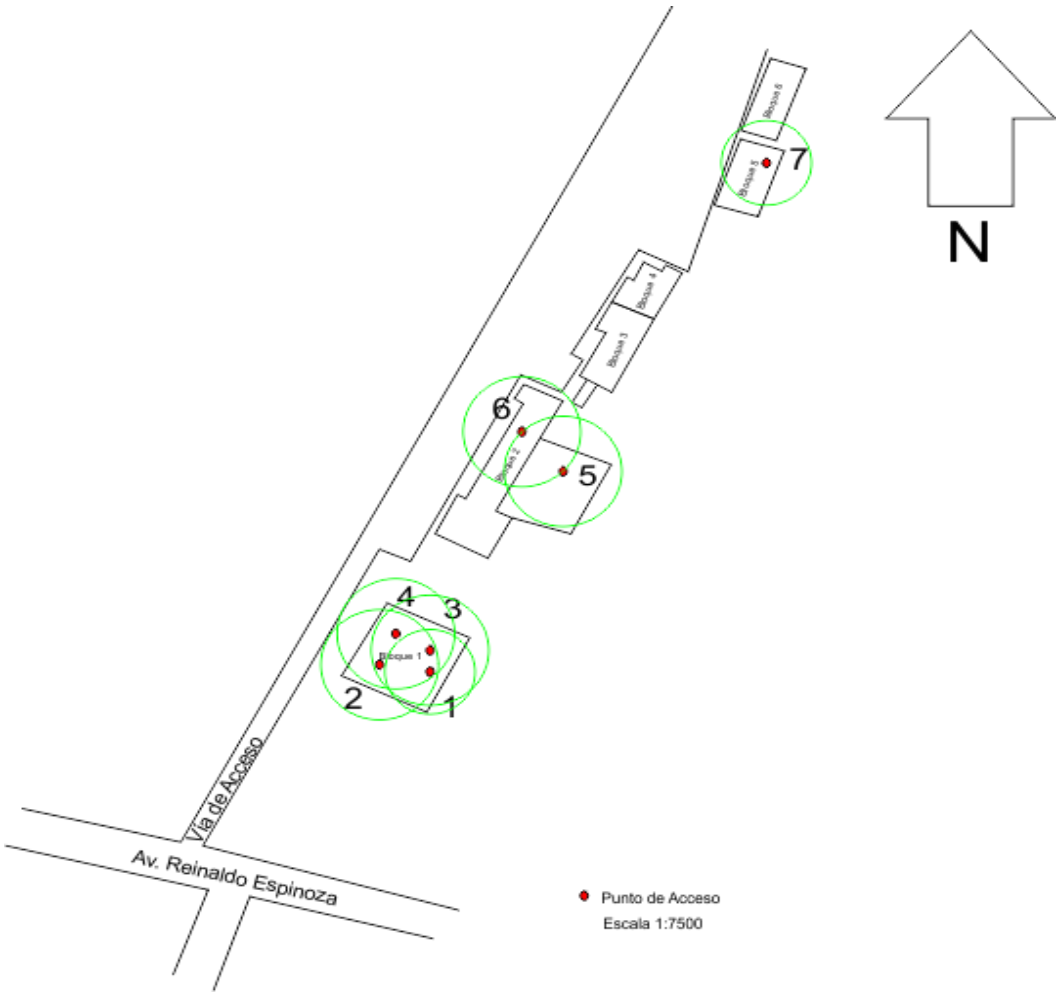

Figura 15 Cobertura de puntos de acceso AEIRNNR

El espacio físico ocupado por el Área de la Energía, las Industrias y los Recursos Naturales no Renovables es de aproximadamente 3680 metros cuadrados. El espacio cubierto por los Access Point ubicados cubre aproximadamente 1235 metros cuadrados, lo que representaría el 33.55 % del área cubierta por acceso inalámbrico.

1.1.11.5. Área Agropecuaria y de Recursos Naturales Renovables.

Ubicada al Sur del campus Universitario, compuesta por edificios en su mayoría actuales, cuenta con aproximadamente con dieciséis edificios, tiene la biblioteca perteneciente al área que es el lugar donde se encuentra un servidor proxy para dar acceso a la red, switchs de acceso así como también se ha podido determinar que aquí existen 23 puntos de acceso inalámbrico, distribuidos en los diferentes edificios lo que se detalla en la tabla XVI.

Forman parte de esta área las carreras de: Ingeniería Agrícola , Ingeniería Agronómica, Ingeniería en Manejo y Conservación del Medio Ambiente, Ingeniería en Producción, Ingeniería Forestal, Medicina Veterinaria y los Programas de Posgrado.

TABLA XVI

Descripción de puntos de acceso Área Agropecuaria y de Recursos Naturales Renovables.

IP RADIO	SSID	MARCA	INICIO	FIN	#IP	UBICACIÓN
ÁREA AGROPECUARIA Y DE RECURSOS NATURALES RENOVABLES						
172.16.59.59 - 60	**Libres**					
172.16.59.61	SILabCinfa	D-Link 2100 AP	172.16.59.62	172.16.59.81	20	Laboratorio del Cinfa, exinglés
172.16.59.82	SIMaderas	D-Link 2100 AP	172.16.59.83	172.16.59.86	4	Laboratorio de Maderas
172.16.59.87	SIHerbario	D-Link 2100 AP	172.16.59.88	172.16.59.92	5	Herbario
172.16.59.93	SISanidadVegetal	D-Link 2100 AP	172.16.59.94	172.16.59.100	7	
172.16.59.101	SIAsoProf	D-Link 2100 AP	172.16.59.102	172.16.59.109	8	Asociación de Profesores
172.16.59.110	SIAgricola	D-Link 2100 AP	172.16.59.111	172.16.59.118	8	Agrícola
172.16.59.119	SIBiotecnologia01	D-Link 2100 AP	No tiene DHCP	Biotecnología		
172.16.59.120	SIMiccambio	D-Link 2100 AP	172.16.59.121	172.16.59.128	8	2° piso, biodiversidad, bloque CINFA
172.16.59.129	SIAgropecuaria04	D-Link 2100 AP	172.16.59.130	172.16.59.137	8	Salón de sesiones del área
172.16.59.138	SIAgropecuaria01	D-Link 2100 AP	172.16.59.139	172.16.59.146	8	2° piso, investigaciones, bloque CINFA
172.16.59.147	SIAmbiente01	D-Link 2100 AP	172.16.59.148	172.16.59.155	8	Medio Ambiente
172.16.59.156	MAmbiente02	D-Link 2100 AP	172.16.59.157	172.16.59.164	8	Medio Ambiente
172.16.59.165	MAmbiente03	D-Link 2100 AP	172.16.59.166	172.16.59.173	8	Medio Ambiente
172.16.59.174	MAmbiente04	D-Link 2100 AP	172.16.59.175	172.16.59.182	8	
172.16.59.183	SIPostAgrop01	D-Link 2100 AP	172.16.59.184	172.16.59.188	5	Postgrado Agropecuaria
172.16.59.189	SIPostAgrop02	D-Link 2100 AP	172.16.59.190	172.16.59.194	5	
172.16.59.195	SIPostAgrop	D-Link	172.16.59.196	172.16.59.200	5	Postgrado

	03	2100 AP				Agropecuaria
172.16.59.201	SIPostAgrop 04	D-Link 2100 AP	172.16.59.202	172.16.59.206	5	Postgrado Agropecuaria
172.16.59.207	SICater	D-Link 2100 AP	172.16.59.208	172.16.59.217	10	
172.16.59.218	SIForestal01	D-Link 2100 AP	172.16.59.219	172.16.59.226	8	Forestal
172.16.59.227	SIForestal02	D-Link 2100 AP	172.16.59.228	172.16.59.235	8	Forestal
172.16.59.236	SICinfa	D-Link 2100 AP	172.16.59.237	172.16.59.246	10	1° piso bloque CINFA
172.16.59.247	Laboratorio-LOUNAZ	D-Link 2100 AP	172.16.59.248	172.16.59.255	8	Medio Ambiente, 1° piso
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo						
Fuente: Unidad de Telecomunicaciones e Información						

1.1.11.6. Área Jurídica Social y Administrativa

Es el área más grande dentro de la Universidad, ubicada al Noroccidente de la misma contigua al Área Educativa, dispone de edificios en su mayoría de dos pisos, es la que cuenta con el mayor número de estudiantes, tiene aproximadamente diez de bloques en los que se distribuyen las diferentes carreras, al igual que todas las áreas dispone de una biblioteca que es el lugar donde se encuentra ubicado el servidor proxy que permite el acceso a la red, switchs de acceso así como también APs inalámbricos ubicados en los diferentes bloques que pertenecen al área, aquí se encuentran 23 puntos de acceso inalámbrico lo que se detalla en la tabla XVII.

Forman parte del área Jurídica las carreras de: Derecho, Banca y Finanzas, Administración Publica, Turismo Posgrado de Derecho, Administración de Empresas, Economía, Trabajo Social, Contabilidad y Auditoría.

TABLA XVII

Descripción de puntos de acceso Área Jurídica, Social y Administrativa

IP RADIO	SSID	MARCA	INICIO	FIN	#IP	UBICACIÓN
ÁREA JÚRIDICA SOCIAL Y ADMINITRATIVA						
172.16.60.1	SIBibliotecaJuridica	D-Link 2100 AP	172.16.60.2	172.16.60.21	20	Bloque 1, Biblioteca
172.16.60.22	SITurismo01	D-Link 2100 AP	172.16.60.23	172.16.60.27	5	Turismo
172.16.60.28	SITurismo02	D-Link 2100 AP	172.16.60.29	172.16.60.33	5	Turismo
172.16.60.34	SITurismo03	D-Link	172.16.60.35	172.16.60.39	5	Turismo

		2100 AP				
172.16.60.40	SITurismo04	D-Link 2100 AP	172.16.60.41	172.16.60.45	5	Turismo
172.16.60.46	SITurismo05	D-Link 2100 AP	172.16.60.47	172.16.60.51	5	Turismo
172.16.60.54-57	**Libre**					
172.16.60.58	SIPostJur01	D-Link 2100 AP	172.16.60.59	172.16.60.73	15	Postgrado Jurídica
172.16.60.74	SIPostJur02	D-Link 2100 AP	172.16.60.75	172.16.60.89	15	Postgrado Jurídica
172.16.60.90	SIPostJur04	D-Link 2100 AP	172.16.60.91	172.16.60.105	15	Postgrado Jurídica
172.16.60.106	SIPostJur05	D-Link 2100 AP	172.16.60.107	172.16.60.121	15	Postgrado Jurídica
172.16.60.122	SIPostJur06	D-Link 2100 AP	172.16.60.123	172.16.60.137	15	Postgrado Jurídica
172.16.60.138	SIJuridica01	D-Link 2100 AP	172.16.60.139	172.16.60.146	8	
172.16.60.147	SIJuridica02	D-Link 2100 AP	172.16.60.148	172.16.60.155	8	2° piso bloque 1
172.16.60.156	SIJuridica03	D-Link 2100 AP	172.16.60.157	172.16.60.164	8	
172.16.60.165	SIJuridica08	D-Link 2100 AP	172.16.60.166	172.16.60.173	8	2° piso bloque 8, Banca y Finanzas
172.16.60.174	SIJuridica09	D-Link 2100 AP	172.16.60.175	172.16.60.182	8	
172.16.60.183	SIAdmPublica01	D-Link 2100 AP	172.16.60.184	172.16.60.191	8	1° piso bloque 5, Admin. Pública
172.16.60.192	SIAdmPublica02	D-Link 2100 AP	172.16.60.193	172.16.60.200	8	2° piso bloque 5, Admin. Pública
172.16.60.201	SICC40Juridica	D-Link 2100 AP	172.16.60.202	172.16.60.211	10	CC. "Luis German Ojeda" Bloque 3
172.16.60.212	SIEconomia02	D-Link 2100 AP	172.16.60.213	172.16.60.227	15	2o piso bloque 10, IDISE
172.16.60.228	SIEconomia01	D-Link 2100 AP	172.16.60.229	172.16.60.243	15	2o piso bloque 10, IDISE
172.16.60.244	SITrabSocial	D-Link 2100 AP	172.16.60.245	172.16.60.255	11	2o piso bloque 6, Trabajo Social
172.16.60.212	SIEconomia02	D-Link 2100 AP	172.16.60.213	172.16.60.227	15	2o piso bloque 10, IDISE

Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo
Fuente: Unidad de Telecomunicaciones e Información

1.1.11.7. Resumen de la Distribución de los puntos de acceso

Como ya se ha detallado la descripción de la distribución de los puntos de acceso por cada área del campus universitario a continuación en la tabla XVIII se muestra el resumen del total de puntos de acceso y la cantidad de IP disponibles.

TABLA XVIII

Resumen de la distribución de puntos de acceso.

Nombre	Número de Puntos de Acceso	Números de IP
Administración Central	10	90
Área de la Educación, el Arte y la Comunicación	9	89
Área Jurídica, Social y Administrativa	23	242
Área de la Energía y los Recursos Naturales No Renovables	7	112
Área Agropecuaria y de Recursos Naturales Renovables.	23	172
Área de la Salud Humana	6	86
TOTAL	78	791
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo ***Fuente: Unidad de Telecomunicaciones e Información***		

1.1.12. Problemas de Seguridad Informática en la red de datos

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática se resume, por lo general, en los siguientes objetivos principales:

- **Integridad**: garantizar que los datos sean los que se supone que son.
- **Confidencialidad**: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.

- **Disponibilidad**: garantizar el correcto funcionamiento de los sistemas de información.

Durante la fase 1 del presente PFC al realizar un análisis sobre la situación actual de la red de datos de la Universidad Nacional de Loja se logró obtener información a través de las técnicas de Observación, entrevistas (ver anexo 2, 3 y 4) y así detectar los principales problemas de seguridad informática en la red de datos de la institución.

A continuación se enfoca los problemas de seguridad informática enmarcado dentro de los objetivos ya mencionados como son: Integridad, Confidencialidad, Disponibilidad.

1.1.12.1. Integridad

- **Falta de verificación de la integridad de paquetes:** al usar el estándar WEP en las configuraciones de la mayoría de los puntos de acceso no verifica la integridad de los paquetes que se envían y reciben, basta que un atacante use una herramienta de análisis de tráfico para poder manipular un simple bit cualquiera en los paquetes en circulación por la red.

1.1.12.2. Confidencialidad

- **Métodos de autenticación débiles:** la mayoría de los dispositivos inalámbricos (Puntos de acceso, router) que se encuentran distribuidos en el campus universitario están configurados con métodos de autenticación WEP la cual es el método de autenticación más inseguro ver apartado (problemas del WEP). Lo que permite la intromisión de cualquier usuario al acceso de los servicios de red que brinda la institución.

- **Facilidad de capturas de paquetes:** al no poseer métodos de encriptación seguro es posible que la información transmitida a través de los puntos de acceso pueda ser escuchada y capturada. Existen en la actualidad mucho software especializado para este tipo de ataques.

1.1.12.3. Disponibilidad

- **Diseño inadecuado de la infraestructura de la red de datos:** La universidad posee un solo dominio de broadcast, lo que hace que se altere el rendimiento de

la red de datos debido a que el paquete debe ser procesado por todos los dispositivos que integren el dominio de broadcast.

Existe dos firewalls, uno que divide la red pública de la red privada y otro que divide la red pública de la red isolada del Sistema de Gestión Académica, lo que hace que los servidores públicos estén desprotegidos contra posibles ataques. Cabe recalcar que estos firewall son administrados por dos departamentos diferentes el Departamento de Redes y Equipos Informáticos, y por el Departamento de Desarrollo de Software.

Las áreas carecen de switchs administrables que controlen y monitoreen el tráfico al interior de las áreas.

- **Hardware inadecuado:** una de las necesidades para filtrar el contenido es el uso de proxies en la universidad debido a que no existe una segmentación de ancho de banda. Por las características de hardware de algunos de estos equipos y la cantidad de solicitudes que reciben hace que el acceso a los servicios de la red sean lentos, un claro ejemplo es el servidor proxy wireless.

- **Interrupción de componentes físicos de red:** uno de los problemas que afecta comúnmente a la red de datos es que algunos dispositivos de red (switch, puntos de red, router) se encuentran ubicados al alcance de cualquier usuario y están propensos a la manipulación incorrecta de los mismos. Lo que ocasiona graves inconvenientes dentro de toda la intranet de la universidad, mayormente se producen los denominados bucles de red ocasionando así la denegación de servicios de red a determinadas áreas.

- **Obstrucción de medios de comunicación:** este problema se ve enfocado a la duplicación de IP lo que ocasiona que a la persona que le pertenece la dirección IP duplicada no pueda comunicarse adecuadamente ni tenga los servicios de Internet que brinda la universidad. La duplicación de IP se evidencia de forma común debido a la falta de control de los usuarios al acceso de los recursos de la red.

1.1.13. Determinación de las herramientas adecuadas para la solución al problema.

Para determinar las herramientas adecuadas para la solución al problema se realizó un análisis de herramientas existentes y ya utilizadas en escenarios similares.

En cuanto a la solución del problema de seguridad que se tiene al momento de acceso a la red por parte de personal no autorizado se decidió la utilización de un servidor que utilice el concepto de AAA (Autenticación, Autorización y Contabilidad o Accounting). La razón y ventaja principal de contar con un servidor AAA es que se centraliza el manejo de cuentas de usuario para el acceso.

Los dos protocolos más utilizados en AAA son dos: Cisco TACACS+ y RADIUS. TACACS+, Sistema de control de acceso mediante control del acceso desde terminales es un protocolo de autenticación remota, propietario de Cisco. RADIUS, Remote Authentication Dial-In User Server es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

RADIUS ofrece disponibilidad en varios clientes mientras TACACS+ es lo mejor en una infraestructura basada en equipos Cisco. Al no poseer la Universidad Nacional de Loja toda una infraestructura Cisco, la opción a implementar sería RADIUS.

Para la implementación del servidor RADIUS en la Unidad de Telecomunicaciones e Información se ha tomado en consideración usar como software FreeRADIUS, el cual es un servidor RADIUS open source y que es la base para múltiples productos comerciales. FreeRADIUS también se utiliza ampliamente en la comunidad académica, incluyendo el proyecto EDUROAM. El servidor es rápido, multifuncional, modular y escalable. Además cuenta con una licencia BSD.

Respecto al proceso de autenticación, se trató de encontrar una solución en la que el usuario final tengo la menor interacción con el sistema. Es así que un portal cautivo soluciona el problema de que el usuario final tenga que saber el tipo de autenticación que está usando, aceptando únicamente un certificado en el navegar.

Debido a que existen varios portales cautivos por software en el medio, se hace necesario un análisis para elegir la mejor opción en cuanto al software. El primer requisito que debe tomarse en cuenta es que debe funcionar sobre un Sistema Operativo Linux, y que además cuente con un tipo de licencia libre.

Además deben tomarse en cuenta requisitos tales como facilidad de instalación, configuración, la forma en que afecta el uso del procesador, tiempo de respuesta de los usuarios y seguridad de los portales cautivos.

De acuerdo a un estudio realizado sobre portales cautivos [7] en el cual se llega a la conclusión que la mejor alternativa para una universidad sería la implementación de Coovachilli. Coovachilli es un portal cautivo por software, basado en el proyecto Chillispot, y es mantenido activamente por uno de los contribuyentes originales de Chillispot. Además, Coovachilli está lanzado bajo una licencia GPL, lo cual justifica su uso para la implementación en la Universidad Nacional de Loja. Coovachilli funciona perfectamente con un servidor RADIUS, y cuenta con una comunidad que colabora en cuanto al desarrollo de la aplicación.

Como se menciona anteriormente, todos estos servicios deben funcionar sobre Sistemas Operativos Linux, puesto que en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja se utilizan servidores Linux y para mantener una concordancia en cuanto a Sistemas Operativos se decidió utilizar Linux Ubuntu Server versión 12.04.

1.2. FASE 2: IMPLANTACIÓN DE LA SOLUCIÓN PLANTEADA

1.2.1. Análisis de las características del Servidor a adquirir

Para determinar los requerimientos de hardware del servidor RADIUS se han considerado las características de hardware para la instalación del S.O Linux Ubuntu Server 12.04. Adicionalmente se ha considerado las aplicaciones que se van a ejecutar en el equipo para determinar características adicionales y la carga que pueda llegar a tener el equipo.

En cuanto al Sistema Operativo, los requerimientos mínimos de funcionamiento son los siguientes:

- Procesador x86 a 1 GHz.
- Memoria RAM de 1 GB.
- Disco Duro de 15 GB (swap incluida).
- Tarjeta gráfica y monitor capaz de soportar una resolución de 800x600.

Considerando que el Sistema Operativo va a funcionar bajo modo consola, se podrían considerar aceptables los requerimientos anteriormente expuestos. Además se debe tomar en cuenta que el servidor debe contar con dos tarjetas de red para el correcto funcionamiento del portal cautivo.

Respecto al software que va a ejecutar el servidor, tanto FreeRADIUS como Coovachilli son paquetes pequeños y que no requieren demasiado espacio en el disco ni procesamiento. El paquete FreeRADIUS ocupa en el disco duro 4.05 MB y en memoria RAM 1 MB. El paquete Coovachilli ocupa en disco 849 KB y en memoria RAM 200 KB.

Para realizar las pruebas de carga del servidor se tomó como referencia estadísticas obtenidas en la tesis “Análisis Para El Diseño De Una Red Mesh En La Universidad Nacional De Loja Y Su Implementación En Administración Central” , el cual nos entrega como dato que el número máximo de conexiones concurrentes es actualmente de 269 [10].

Para determinar el tamaño de la muestra se utilizó la siguiente fórmula estadística:

$$n = \frac{Z^2 pqN}{NE^2 + Z^2 pq}$$

Donde:

- n = tamaño de la muestra
- Z = nivel de confianza
- p = variabilidad positiva
- q = variabilidad negativa
- N = tamaño de la población
- E = precisión del error

$$n = \frac{(0.95)^2(0.5)(0.5)(269)}{(269)(0.05)^2 + (0.95)^2(0.5)(0.5)}$$

$$n = \frac{60.69}{0.6725 + 0.226}$$

$$n = \frac{60.69}{0.67 + 0.23}$$

$$n = \frac{60.69}{0.9}$$

$$n = 67.43$$

El tamaño de la muestra es de 68. Para simular las 68 conexiones concurrentes se utilizó el software radLogin. RadLogin es un software el cual permite simular solicitudes RADIUS hacia un servidor. Se obtuvo un tiempo de respuesta promedio de 0.6 ms y un uso en RAM de FreeRADIUS de 2 MB y en procesamiento un 6 % del total del procesamiento del servidor de pruebas.

1.2.2. Análisis de la mejor propuesta para la adquisición del Servidor

Tomando en cuenta las pruebas anteriores, se determinó que el servidor en donde se realizaron las pruebas de carga es el adecuado, el cual tiene las siguientes características:

- Procesador: Intel Core2Duo CPU E7500 @ 2.93 GHz x 2
- 2 GB de Memoria RAM
- 320 GB de Disco Duro

Tomando en cuenta el crecimiento que va a tener tanto el uso del servicio como los usuarios se consideró que es viable utilizar el equipo como servidor.

1.2.3. Selección del servidor RADIUS

Para la implementación del servidor RADIUS en la Unidad de Telecomunicaciones e Información se ha tomado en consideración usar como software **FreeRADIUS**, el cual es el servidor RADIUS más utilizado en el mundo.

Es un servidor open source que es la base para múltiples productos comerciales. También se utiliza ampliamente en la comunidad académica, incluyendo eduroam. El servidor es rápido, rico en funciones, modular y escalable. Además cuenta con una licencia BSD, que es una licencia de software libre.

1.2.4. Base de Datos de FreeRADIUS.

FreeRADIUS posee métodos de autorización soportados habitualmente por un servidor de RADIUS incluyen bases de datos LDAP, bases de datos SQL (como Oracle, MySQL y PostgreSQL), o incluso el uso de ficheros de configuración locales al servidor.

Cabe resaltar que primeramente los usuarios se los va a obtener mediante el web services del Sistema de Gestión Académica de la Universidad Nacional de Loja, pero se van a almacenar en una base de datos local en MYSQL, para asegurar conectividad así el web services no esté disponible.

1.2.4.1. Tablas de FreeRADIUS

El servidor RADIUS maneja algunas tablas en la base de datos creada llamada radius donde registra datos de los usuarios, parámetros de conexión etc. las cuales se muestra a continuación en la figura 16.

```
+-------------------------+
| Tables_in_radius        |
+-------------------------+
| batch_history           |
| billing_history         |
| billing_merchant        |
| billing_paypal          |
| billing_plans           |
| billing_plans_profiles  |
| billing_rates           |
| cui                     |
| dictionary              |
| hotspots                |
| invoice                 |
| invoice_items           |
| invoice_status          |
| invoice_type            |
| nas                     |
| node                    |
| operators               |
| operators_acl           |
| operators_acl_files     |
| payment                 |
| payment_type            |
| proxys                  |
| radacct                 |
| radcheck                |
| radgroupcheck           |
| radgroupreply           |
| radhuntgroup            |
| radippool               |
| radpostauth             |
| radreply                |
| radusergroup            |
| realms                  |
| userbillinfo            |
| userinfo                |
| wimax                   |
+-------------------------+
```

Figura 16. Tablas de FreeRADIUS

1.2.4.1.1. Tablas de gestión de usuarios

Las tablas que usa RADIUS para la gestión de usuarios son las siguientes:

Tabla radcheck: En esta tabla se inserta cada usuario cuando se autentica y se almacena su contraseña como se observa en la figura 17.

```
mysql> desc radcheck;
+-----------+------------------+------+-----+---------+----------------+
| Field     | Type             | Null | Key | Default | Extra          |
+-----------+------------------+------+-----+---------+----------------+
| id        | int(11) unsigned | NO   | PRI | NULL    | auto_increment |
| username  | varchar(64)      | NO   | MUL |         |                |
| attribute | varchar(64)      | NO   |     |         |                |
| op        | char(2)          | NO   |     | ==      |                |
| value     | varchar(253)     | NO   |     |         |                |
+-----------+------------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

Figura 17. Estructura de la tabla radcheck

Campos

- **Id:** Identificador de registro.
- **UserName.** Nombre de Usuario que puede ser la Cédula de Identidad o usuario creado por los administradores.
- **Attribute:** Tipo de contraseña. En este caso, 'User-Password'.
- **Op:** Es el operador que se usará para la comprobación. En este caso '==='.
- **Value:** La contraseña.

Tabla radusergroup: Aquí se define a qué grupo pertenece cada usuario, en la figura 18 se muestra la estructura de esta tabla.

```
mysql> desc radusergroup;
+-----------+-------------+------+-----+---------+-------+
| Field     | Type        | Null | Key | Default | Extra |
+-----------+-------------+------+-----+---------+-------+
| username  | varchar(64) | NO   | MUL |         |       |
| groupname | varchar(64) | NO   |     |         |       |
| priority  | int(11)     | NO   |     | 1       |       |
+-----------+-------------+------+-----+---------+-------+
3 rows in set (0.00 sec)
```

Figura 18. Estructura de la tabla radusergroup

Campos:

- **UserName:** Nombre de Usuario que puede ser la Cédula de Identidad o usuario creado por los administradores.
- **GroupName.** Grupo al que pertenece el usuarios
- **Priority:** Prioridad de el grupo.

Tabla radacct: Aquí se agregan los datos de los usuarios que se conectan al servidor RADIUS, en la figura 19 se puede ver la estructura de esta tabla.

```
mysql> desc radacct;
+----------------------+-------------+------+-----+---------+----------------+
| Field                | Type        | Null | Key | Default | Extra          |
+----------------------+-------------+------+-----+---------+----------------+
| radacctid            | bigint(21)  | NO   | PRI | NULL    | auto_increment |
| acctsessionid        | varchar(64) | NO   | MUL |         |                |
| acctuniqueid         | varchar(32) | NO   | MUL |         |                |
| username             | varchar(64) | NO   | MUL |         |                |
| groupname            | varchar(64) | NO   |     |         |                |
| realm                | varchar(64) | YES  |     |         |                |
| nasipaddress         | varchar(15) | NO   | MUL |         |                |
| nasportid            | varchar(15) | YES  |     | NULL    |                |
| nasporttype          | varchar(32) | YES  |     | NULL    |                |
| acctstarttime        | datetime    | YES  | MUL | NULL    |                |
| acctstoptime         | datetime    | YES  | MUL | NULL    |                |
| acctsessiontime      | int(12)     | YES  | MUL | NULL    |                |
| acctauthentic        | varchar(32) | YES  |     | NULL    |                |
| connectinfo_start    | varchar(50) | YES  |     | NULL    |                |
| connectinfo_stop     | varchar(50) | YES  |     | NULL    |                |
| acctinputoctets      | bigint(20)  | YES  |     | NULL    |                |
| acctoutputoctets     | bigint(20)  | YES  |     | NULL    |                |
| calledstationid      | varchar(50) | NO   |     |         |                |
| callingstationid     | varchar(50) | NO   |     |         |                |
| acctterminatecause   | varchar(32) | NO   |     |         |                |
| servicetype          | varchar(32) | YES  |     | NULL    |                |
| framedprotocol       | varchar(32) | YES  |     | NULL    |                |
| framedipaddress      | varchar(15) | NO   | MUL |         |                |
| acctstartdelay       | int(12)     | YES  |     | NULL    |                |
| acctstopdelay        | int(12)     | YES  |     | NULL    |                |
| xascendsessionsvrkey | varchar(10) | YES  |     | NULL    |                |
+----------------------+-------------+------+-----+---------+----------------+
26 rows in set (0.01 sec)
```

Figura 19. Estructura de la tabla radacct

Campos:

- **Radacctid:** identificador de registro.
- **Username:** Nombre de Usuario que puede ser la Cédula de Identidad o usuario creado por los administradores.
- **Groupname:** Nombre del Grupo al que pertenece.
- **Realm:** Reino al que pertenezca.
- **Nasipaddress:** Dirección IP que le asigna el NAS en este caso una IP dentro de la red 10.1.0.0/24.
- **Nasportid:** puerto del nas
- **Nasporttype:** modelo del nas
- **Acctstarttime:** fecha y hora de inicio de sesión.
- **Acctstoptime:** fecha y hora de sesión terminada.
- **CallingStationId:** Dirección MAC del usuario.

Tabla radreply: En esta tabla se definen los atributos sobre la conexión y sesión de los usuarios; por ejemplo, IP asignada y tiempo de espera máximo. En este caso, se permite que se asignen los de DEFAULT contenidos en el archivo 'users'; por lo tanto, no se inserta nada en la tabla. En la figura 20 se puede observar la estructura de esta tabla.

```
mysql> desc radreply;
+-----------+------------------+------+-----+---------+----------------+
| Field     | Type             | Null | Key | Default | Extra          |
+-----------+------------------+------+-----+---------+----------------+
| id        | int(11) unsigned | NO   | PRI | NULL    | auto_increment |
| username  | varchar(64)      | NO   | MUL |         |                |
| attribute | varchar(64)      | NO   |     |         |                |
| op        | char(2)          | NO   |     | =       |                |
| value     | varchar(253)     | NO   |     |         |                |
+-----------+------------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

Figura 20. Estructura de la tabla radreply

radgroupreply: Similar a la tabla radcheck pero permite establecer atributos a un grupo de usuarios completo. En la figura 21 se muestra la estructura de esta tabla.

```
mysql> desc radgroupreply;
+-----------+------------------+------+-----+---------+----------------+
| Field     | Type             | Null | Key | Default | Extra          |
+-----------+------------------+------+-----+---------+----------------+
| id        | int(11) unsigned | NO   | PRI | NULL    | auto_increment |
| groupname | varchar(64)      | NO   | MUL |         |                |
| attribute | varchar(64)      | NO   |     |         |                |
| op        | char(2)          | NO   |     | =       |                |
| value     | varchar(253)     | NO   |     |         |                |
+-----------+------------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

Figura 21. Estructura de la tabla radreply

Campos:

- **id.** Identificador de registro.
- **GroupName.** Nombre de grupo.
- **Attribute.** Nombre del atributo que se quiere agregar.

1.2.5. Autenticación de FreeRADIUS con el Web Services del Sistema de Gestión Académico.

Figura 22. Logo de Web Service del SGA

Web Services es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. El Web Services del Sistema de Gestión Académico de la Universidad Nacional de Loja, proporciona una biblioteca de métodos que facilitan la obtención de datos personales, académicos y estadísticos que se han generado durante la vigencia del sistema principal de la institución, con la finalidad de que se pueda hacer uso de la información contenida en el Sistema de Gestión Académico.

Para usar el SGAWebservices de la Universidad Nacional de Loja, lo primero que tiene que asegurarse es que el lenguaje de programación que utiliza para construir su aplicación cliente está preparado para enviar y recibir mensajes según el estándar SOAP.

Incluso en el caso de que no tenga una librería específica, es imprescindible la posibilidad de enviar y recibir mensajes XML vía HTTP. Independientemente de cómo se haga la solicitud, las respuestas son en XML formateado con JSON.

SOAP es un protocolo elaborado para facilitar la llamada remota de funciones a través de Internet, permitiendo que dos programas se comuniquen de una manera muy similar técnicamente a la invocación de páginas Web.

Al contener el Web Services los métodos necesarios para realizar la autenticación mediante un script en el cual se deben enviar como parámetros el usuario y la contraseña obtenidos de la solicitud (request) y agregarlos a la base de datos local.

Se decidió realizar la conexión de esta manera ya que FreeRADIUS soporta realizar el proceso de autorización (comprobar credenciales) desde varias fuentes de datos: bases de datos, archivos de texto, usuarios UNIX, scripts, entre otros.

Respecto a los lenguajes de programación que soporta FreeRADIUS, se encontró la limitante que en la versión estable de FreeRADIUS soporta únicamente el lenguaje de programación Perl. Así que se decidió realizar el script en el lenguaje de programación Perl, teniendo compatibilidad tanto con el Web Services del Sistema de Gestión Académico como con FreeRADIUS, y lograr así obtener los datos necesarios para realizar el proceso de autorización dentro de FreeRADIUS.

1.2.5.1. Conexión de FreeRADIUS con el Web Services del Sistema de Gestión Académico de la Universidad Nacional de Loja

FreeRADIUS al poseer gran cantidad de módulos en su configuración permite la integración de herramientas externas para su funcionamiento.

Es así que se hará uso del módulo Perl de FreeRADIUS para la conexión con el Web Services. Por parte de FreeRADIUS el módulo Perl soporta programar scripts para autenticación, autorización, contabilidad, pre proxy, post proxy y sesión. Mientras que por parte del Web Services soporta varios lenguajes de programación, entre ellos Perl, razones por las cuales Perl se convierte en el lenguaje de programación que mejor se acopla para la conexión de FreeRADIUS con el Web Services.

Para el código del script Perl se tomó como base el archivo que se encuentra en la documentación oficial de FreeRADIUS [referencia a la pg web del rlm_perl http://wiki.freeradius.org/modules/Rlm_perl]

El código es el siguiente:

```
#!/usr/bin/perl -w
#declaracion de librerias necesarias
use strict;
use DBI;
use strict;
use LWP::UserAgent;
use HTTP::Request::Common;
```

```
use XML::Simple;
use vars qw(%RAD_REQUEST %RAD_REPLY %RAD_CHECK);
use Data::Dumper;
#declarar variables constantes q usa freeradius
   use constant    RLM_MODULE_REJECT=>    0;#  /* immediately reject the request */
   use constant    RLM_MODULE_FAIL=>      1;#  /* module failed, don't reply */
   use constant    RLM_MODULE_OK=>        2;#  /* the module is OK, continue */
   use constant    RLM_MODULE_HANDLED=>   3;#  /* the module handled the request, so
stop. */
   use constant    RLM_MODULE_INVALID=>   4;#  /* the module considers the request invalid.
*/
   use constant    RLM_MODULE_USERLOCK=>  5;#  /* reject the request (user is locked out) */
   use constant    RLM_MODULE_NOTFOUND=>  6;#  /* user not found */
   use constant    RLM_MODULE_NOOP=>      7;#  /* module succeeded without doing anything
*/
   use constant    RLM_MODULE_UPDATED=>   8;#  /* OK (pairs modified) */
   use constant    RLM_MODULE_NUMCODES=>  9;#  /* How many return codes there are */
# declarar todas las variables que va a usar script con autorizacion contra web services
my $usuario = '';
my $clave = '';
my $userAgent = '';
my $message = '';
my $response = '';
my $bool = '';
my $sub = '';
my $db= '';
my $host='';
my $port='';
my $userid='';
my $passwd='';
my $connectionInfo='';
my $dbh = '';
my $query='';
```

```
my $sth ='';
my $rv ='';
#funcion de autorizacion
sub authorize {
#declara un user agent en este caso perl
$userAgent = LWP::UserAgent->new(agent => 'perl post');
#guardo en variables lo q obtengo de la solicitud de radius (usuario y clave)
$usuario = $RAD_REQUEST{'User-Name'};
$clave = $RAD_REQUEST{'User-Password'};
#envio la consulta embebida en un xml
$message = '<?xml version="1.0" encoding="UTF-8"?><soap:Envelope
xmlns:types="http://ws.unl.edu.ec/sgaws/wsvalidacion/soap/types"
soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://ws.unl.edu.ec/sgaws/wsvalidacion/soap/"><cedula
xsi:type="xsd:string">'.$usuario.'</cedula><clave
xsi:type="xsd:string">'.$clave.'</clave></soap:Envelope>';
#almaceno en $response la respuesta a la solicitud que lo voy a enviar al url del metodo validar
estudiante del web service
$response = $userAgent->request(POST
'http://usuariows:clavews@ws.unl.edu.ec/sgaws/wsvalidacion/sgaws_validar_estudiante',
Content_Type => 'text/xml
',
Content => $message);
#obtengo solo el resultado
for( @{$response->{result}} ) {
   print "$_->{result}";
}
#almaceno la respuesta
```

```
$bool = $response->{_content};
#obtengo la subcadena T o F (true or false) de acuerdo a lo q respondio el web service
$sub = substr($bool,8,1);
#declaro variables para almacenar en base de datos MySQL
$db="nombrebd";
$host="localhost";
$port="3306";
$userid="usuariobd";
$passwd="clavebd";
#establezco conexión con MySQL
$connectionInfo="DBI:mysql:database=$db;$host:$port";
$dbh = DBI->connect($connectionInfo,$userid,$passwd);
#consulta si el usuario ya está en la bd
$query="select * from radcheck where username='".$usuario."'";
# Primero hay que "preparar" el query
$sth = $dbh->prepare($query);
#si la respuesta fue verdadera o falsa
if( $sub eq 'T' or $sub eq 'F'){
   #si la respuesta fue verdadera
   if($sub eq 'T'){
      $query="select * from radcheck where username='".$usuario."'";
      # Primero hay que "preparar" el query
      $sth = $dbh->prepare($query);
      # Ejecutamos el query
      $sth->execute();
      $rv  = $sth->rows;
      if ($rv>0){
         #registro ya existe... actualizamos password
         $query="update radcheck set value = '".$clave."'where username='".$usuario."' and
attribute ='User-Password'";
         $sth = $dbh->prepare($query);
         $sth->execute();
         print "registro actualizado\n";
```

```
    }else{
        #no existe lo agregamos
        $query="INSERT INTO radcheck (id ,username ,attribute ,op ,value ) VALUES (NULL ,
'".$usuario."', 'User-Password', ':=', '".$clave."')";
        $sth = $dbh->prepare($query);
        $sth->execute();
        print "registro agregado\n";
        #inserta dentro del grupo
        $query="INSERT INTO radusergroup VALUES ('".$usuario."','general',0);";
        $sth=$dbh->prepare($query);
        $sth->execute();
        print "agregado al grupo";
    }
  }else{
    #cuando estan mal los datos en el SGA estudiantes va a buscar en docentes, el
procedimiento es el mismo
    $userAgent = LWP::UserAgent->new(agent => 'perl post');
    $usuario = $RAD_REQUEST{'User-Name'};
    $clave = $RAD_REQUEST{'User-Password'};
    $message = '<?xml version="1.0" encoding="UTF-8"?><soap:Envelope
xmlns:types="http://ws.unl.edu.ec/sgaws/wsvalidacion/soap/types"
soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://ws.unl.edu.ec/sgaws/wsvalidacion/soap/"><cedula
xsi:type="xsd:string">'.$usuario.'</cedula><clave
xsi:type="xsd:string">'.$clave.'</clave></soap:Envelope>
';
    $response = $userAgent->request(POST
'http://wifi:w8728k@ws.unl.edu.ec/sgaws/wsvalidacion/sgaws_validar_docente',
```

```
Content_Type => 'text/xml',
Content => $message);
      for( @{$response->{result}} ) {
         print "$_->{result}";
      }
      $bool = $response->{_content};
      $sub = substr($bool,8,1);
      $db="nombrebd";
      $host="localhost";
      $port="3306";
      $userid="usuariobd";
      $passwd="clavebd";
      $connectionInfo="DBI:mysql:database=$db;$host:$port";
      $dbh = DBI->connect($connectionInfo,$userid,$passwd);
      $query="select * from radcheck where username='".$usuario."'";
      # Primero hay que "preparar" el query
      $sth = $dbh->prepare($query);

      if( $sub eq 'T'){
         $query="select * from radcheck where username='".$usuario."'";
         # Primero hay que "preparar" el query
         $sth = $dbh->prepare($query);
         # Ejecutamos el query
         $sth->execute();
         $rv  = $sth->rows;
          if ($rv>0){
            #registro ya existe... actualizamos password
            $query="update radcheck set value = '".$clave."'where username='".$usuario."' and
attribute ='User-Password'";
            $sth = $dbh->prepare($query);
            $sth->execute();
            print "registro actualizado\n";
         }else{
```

```
        #no existe lo agregamos
        $query="INSERT INTO radcheck (id ,username ,attribute ,op ,value ) VALUES (NULL ,
'".$usuario."', 'User-Password', ':=', '".$clave."')";
        $sth = $dbh->prepare($query);
        $sth->execute();
        print "registro agregado\n";
        #lo agregamos al grupo
        $query="INSERT INTO radusergroup VALUES ('".$usuario."','general',0)";
         $sth=$dbh->prepare($query);
                $sth->execute();
                print "agregado al grupo";
        }
      }else{
        #no es ni usuario ni alumno, procede a buscar en la base de datos MySQL
        print "no valido contra sga\n";
      }
   }
}else{
   #no devolvio ni T ni F (web service caido). Procede a buscar en MySQL
   print "sistema abajo";
}
   #retornar siempre para que proceda con el resto de proceso de AAA
   return RLM_MODULE_OK;
}
```

La subrutina que va a permitir realizar la autenticación con el Web Services del Sistema de Gestión Académica es la de Autenticación. Aquí se programó que si el usuario y contraseña coinciden con las que se encuentran en el Sistema de Gestión Académica se acepte el acceso, caso contrario se lo niegue. Además si el usuario es correcto se ingresará en una Base de Datos MySQL local, para asegurar la autenticación de usuarios incluso en el caso que el Web Services no se encuentre disponible.

1.2.6. Autorización y Contabilidad en FreeRADIUS

Para que FreeRADIUS autorice y haga la contabilidad usando mysql se debe agregar una variable sql en el archivo **/etc/freeradius/sites-available/default** específicamente en las secciones authorize y accounting.

Es importante agregar la variable "perl" antes de "sql" en authorize. Esto permitirá que primero se realice la conexión con el web services del S.G.A. y luego realizar la autorización y la contabilidad desde MySQL.

1.2.7. Configuración del archivo clients.conf

Para mayor seguridad, se requiere que se coloque una contraseña para el cliente **localhost** puesto que ese cliente va a ser el portal cautivo que va a estar en el mismo servidor. Para ello modificamos el archivo **clients.conf**

```
root@radius:~ # vim /etc/freeradius/clients.conf
```

Y editamos la contraseña que se encuentra en el parámetro **secret** dentro del cliente **localhost**.

```
client localhost {
     ipaddr = 127.0.0.1
     secret = clavesegura2
```

1.2.8. Arrancando el servicio de FreeRADIUS

Es importante tener en cuenta que se debe primero parar el servicio que se estaba ejecutando cuando se instaló FreeRADIUS, se lo realiza con el siguiente comando.

```
root@radius:~ # /etc/init.d/freeradius stop
```

La razón por la que se para el servicio y no se lo reinicia es porque para arrancar correctamente es necesario que antes del comando de iniciar el servicio se coloque un comando, el cual hace que las librerías que utiliza el script perl se carguen antes de la ejecución de FreeRADIUS y se pueda levantar el servicio y ejecutar el script.

Para ver que versión de perl se esta usando se ejecuta el siguiente comando.

```
root@radius:~ # perl -V | grep libperl
```

Cuando se ha comprobado que versión de perl se encuentra en el equipo que en este caso es libperl.so.5.14.2 se procede a ejecutar el comando para iniciar, reiniciar o detener FreeRADIUS.

```
root@radius:~ # LD_PRELOAD=/usr/lib/libperl.so.5.14.2
/etc/init.d/freeradius restart
```

1.2.9. Uso de radtest

Para comprobar la conexión y funcionalidad tanto del script perl como la configuración de FreeRADIUS existe el comando **radtest** el cual permite simular una solicitud de acceso RADIUS y comprueba tanto conectividad como parámetros de envío.

Se ejecuta el siguiente comando enviando los parámetros que se detallan a continuación:

```
root@radius:~# radtest usuarioSGA claveSGA 127.0.0.1 1812
clavesegura2
```

Donde:

- **radtest:** nombre del comando
- **usuarioSGA:** usuario almacenado en el Sistema de Gestión Académico
- **claveSGA:** clave del usuario almacenado en el Sistema de Gestión Académico
- **127.0.0.1:** cliente de FreeRADIUS
- **1812:** Puerto por donde escucha la solicitud FreeRADIUS
- **clavesegura2:** clave del cliente de FreeRADIUS

Una vez enviada la solicitud de acceso, FreeRADIUS se encarga de receptar esta solicitud y dar una respuesta.

```
Sending Access-Request of id 42 to 127.0.0.1 port 1812
        User-Name = "usuarioSGA"
        User-Password = "claveSGA"
        NAS-IP-Address = 172.16.32.20
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=42, length=20
```

Figura 23. Respuesta de radtest

En este caso, al ser correctas las credenciales la solicitud de acceso receptada se acepta al usuario como se puede observar en la figura 23.

1.2.10. Análisis del portal cautivo a elegir

Un portal cautivo (o captivo) es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.

El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica. Una vez que el usuario se autentifica se permite la navegación con total normalidad. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo, logrando así, que únicamente personal autorizado o con credenciales pueda hacer uso del servicio.

El portal cautivo funciona sobre un navegador cualquiera, para darle la oportunidad al usuario de ingresar sus credenciales. Los portales cautivos funcionan sobre cualquier navegador en cualquier dispositivo y sistema operativo.

Para comenzar, el usuario abre su computador portátil o dispositivo móvil y se conecta a la red disponible. El portal cautivo se encarga de entregar una dirección IP mediante el servidor DHCP. Luego, intenta acceder a cualquier página. En lugar de mostrar la página solicitada, se mostrará una pantalla de registro, en la que el usuario necesita ingresar su usuario y contraseña para poder acceder al servicio solicitado (Internet). Mientras el usuario no cumpla con este requisito no podrá hacer uso de Internet, logrando así, que únicamente personas autorizadas (con usuario y contraseña) puedan hacer uso del servicio de Internet.

1.2.11. Tipo de Portal Cautivo a Utilizar

Se decidió implementar una solución mediante una aplicación, puesto que es mucho más sencillo configurar un solo equipo que todos los puntos de acceso. Además la administración se realizará únicamente a un solo dispositivo y no a varios equipos.

Adicionalmente, debe operar sobre un Sistema Operativo Linux para que tenga una similar administración que el resto de servidores con los que se trabaja en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

Para la implantación de un portal cautivo es necesario un equipo con dos tarjetas de red y que cumpla con los requisitos en cuanto a procesamiento y almacenamiento necesarios.

1.2.12. Selección del portal cautivo adecuado

Debido a que existen varios portales cautivos por software en el medio, se hace necesario un análisis para elegir la mejor opción en cuanto al software. El primer requisito que debe tomarse en cuenta es que debe funcionar sobre un Sistema Operativo Linux, y que además cuente con un tipo de licencia libre.

Además deben tomarse en cuenta requisitos tales como facilidad de instalación, configuración, la forma en que afecta el uso del procesador, tiempo de respuesta de los usuarios y seguridad de los portales cautivos.

Referenciándonos en un estudio realizado sobre portales cautivos en el cual se llega a la conclusión que la mejor alternativa para una universidad sería la implementación de Coovachilli [7].

Coovachilli es un portal cautivo por software, basado en el proyecto Chillispot, y es mantenido activamente por uno de los contribuyentes originales de Chillispot. Además, Coovachilli está lanzado bajo una licencia GPL, lo cual justifica su uso para la implementación en la Universidad Nacional de Loja. Coovachilli funciona perfectamente con un servidor RADIUS, y cuenta con una comunidad que colabora en cuanto al desarrollo de la aplicación.

1.2.13. Interfaces de Red

Como se dijo anteriormente, el equipo necesita dos tarjetas de red. Una tarjeta de red (eth0) tiene que estar conectada a la red y configurada para internet.

La otra tarjeta de red tiene que dejarse sin configuración. Esto significa, no IP estática y no DHCP. Esto se logra previniendo que el Administrador de Red, manipule la tarjeta.

En este caso, la tarjeta de red en la que funcionara con el portal cautivo (hacia la red inalámbrica) es eth1, y con la configuración estática de la interfaz de red eth0 para que se conecte a internet.

1.2.14. Uso de ip_forward

El mecanismo de IP forwarding se encarga de la retransmisión de los paquetes que se reciben por una interfaz física y de retransmitirlos por otra interfaz. El IP forwarding

debe ser habilitado, pues una vez que el usuario se autentique a través del portal cautivo se redireccionará su tráfico hacia la interfaz de red eth0, permitiendo así que el usuario pueda navegar.

1.2.15. Activación del modo tun

Es importante habilitar el módulo tun, ya que este permitirá a Coovachilli hacer un "túnel" entre las interfaces eth0 y la red virtual que crea en eth1.

Con esta orden se carga el módulo tun en el kernel del sistema directamente sin tener que reiniciar. Además se tiene que agregar la palabra "tun" al final del archivo /etc/modules como se observa en la figura 24.

```
root@radius:~# sudo vim /etc/modules
```

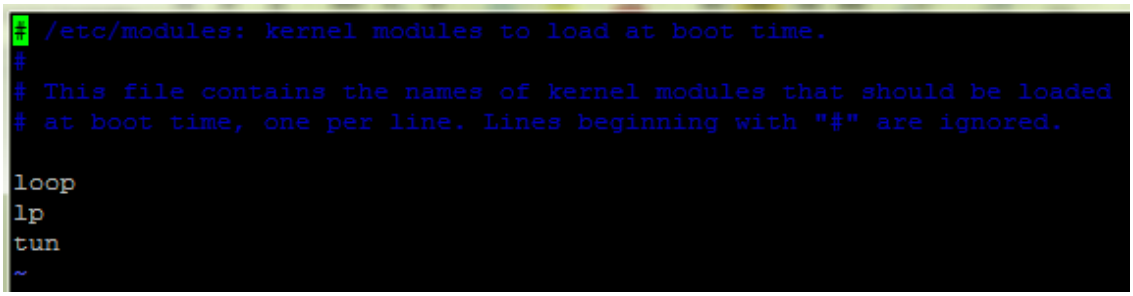

Figura 24. Configuración del kernel a modo tun

1.2.16. Archivos de CoovaChilli

El demonio coovachilli tiene un script de inicio especial. Cada vez que este script se ejecuta, crea un nuevo archivo de configuración para el demonio coovachilli. En La tabla XIX se describe una lista de los archivos de configuración y el papel que desempeñan.

TABLA XIX

Descripción de los archivos de CoovaChilli

Archivo	Funcionamiento	Ubicación
chilli.conf	Este es el archivo que se ejecuta al correr el demonio de chillli y aquí están tres archivos que se generan automáticamente con las configuraciones de chilli los cuales son: main.conf, hs.conf y local.conf. También aquí se levantan las iptables.	/etc/chilli.conf

main.conf	Este archivo se genera automáticamente, por lo que no debería hacer cambios en él, ya que se sobrescribirá.	/etc/chilli/main.conf
hs.conf	Este archivo está vacío - es creado por el script de arranque.	/etc/chilli/hs.conf
local.conf	Este archivo está vacío - es creado por el script de arranque	/etc/chilli/local.conf
config	Este archivo contiene las configuraciones principales de CoovaChilli es decir los valores predeterminados que se utilizarán para generar el archivo main.conf.	/etc/chilli/config
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo		

1.2.16.1. Descripción del archivo principal de CoovaChilli

El archivo principal de configuración del CoovaChilli esta ubicado en el directorio /etc/chilli/ y el nombre del archivo es config es aquí donde se encuentran todas las directivas, las cuales se modifican de acuerdo a las necesidades. Es importante saber cuales son los parámetros que se configurarán los cuales se detallan a continuación en la tabla XX:

TABLA XX

Descripción de parámetros generales de CoovaChilli

Parámetro	Descripción	Valor
HS_WANIF	Interfaz de red donde se conecta a internet en este caso es la eth0.	eth0
HS_LANIF	Interfaz de red donde se va a escuchar las peticiones DHCP y donde se conecta los puntos de acceso en este caso es la eth1.	eth1
HS_NETWORK	Dirección de red del portal cautivo	10.1.0.0
HS_NETMASK	Dirección de mascara de red	255.255.255.0
HS_DNS1	Dirección IP del DNS (Sistema de Nombres de Dominio).	172.16.32.2
HS_DNS2	Dirección IP del DNS	10.1.0.1
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo		

1.2.17. Configuración de CoovaChilli con FreeRADIUS

Para que CoovaChilli funcione con FreeRADIUS se debe configurar ciertos parámetros en el mismo archivo donde se configuró anteriormente el cual se encuentra en el directorio /etc/chilli.

A continuación en la tabla XXI se describen los aspectos básicos de configuración que se debe tomar en cuenta para que el servidor RADIUS se comunique con el portal cautivo.

TABLA XXI

Descripción de parámetros entre CoovaChilli y FreeRADIUS

Parámetro	Descripción	Valor
HS_NASID	Nombre del NAS (Servidor de Acceso a la Red)	nas01
HS_RADIUS	Aquí se define la dirección IP del servidor RADIUS como en nuestro caso el servidor en el mismo equipo que el portal cautivo se define la IP del localhost.	127.0.0.1
HS_RADIUS2	Dirección de IP del servidor RADIUS	127.0.0.1
HS_RADSECRET	Clave secreta del cliente que configuramos en FreeRADIUS en localhost.	xxxxxxx
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo		

1.2.18. Parámetros de configuración UAM (Método Universal de Acceso)

Los parámetros UAM se configuran en el archivo principal de CoovaChilli. Aquí se definen algunos aspectos importantes los que se detallan a continuación en la tabla XXII.

TABLA XXII

Descripción de parámetros UAM de CoovaChilli

Parámetro	Descripción	Valor
HS_UAMLISTEN	Dirección IP del portal cautivo.	10.1.0.1
HS_UAMPORT	Puerto donde escucha CoovaChilli.	3990

HS_UAMSECRET	Clave segura del portal cautivo	xxxxxxx
HS_UAMALLOW	Dirección de red, url o dirección IP que se permite la navegación sin la necesidad de logearse.	10.1.0.1/24
HS_UAMFORMAT	Aquí se define la ruta donde va a estar el archivo que se va a mostrar al usuario al momento de conectarse al servidor RADIUS que en este caso se llama hotspotlogin.php el cual se lo describe más adelante	https://\$HS_UAMLISTEN/cgi-bin/hotspotlogin.php
HS_DEFSESSIONTIMEOUT	Tiempo que va a durar las sesiones de los usuarios logeados definido en segundos.	7200
HS_DEFIDLETIMEOUT	Tiempo que controla de inactividad para desconectar a un usuario, también esta definido en segundos.	1800
Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo		

1.2.19. Archivo hotspotlogin.php

Para la parte visible al usuario donde ingresara los credenciales (Cédula de Identidad y clave del SGA) se procedió a modificar un archivo proporcionado por chillispot.org que originalmente esta hecho en perl el cual se lo convirtió a un archivo php. Este archivo se encuentra ubicado en el directorio del servidor web apache2 en /var/www/hotspot/cgi-bin/. También se adecuó de acuerdo a las sugerencias de los administradores del departamento de redes de la Unidad de Redes y Telecomunicaciones.

En este archivo existen variables importantes como **$uamsecret** debido a que aquí se pone la clave que se configura en el archivo principal de CoovaChilli en

HS_UAMSECRET, también se fijó en la variable **$redirurl** la url de la Universidad Nacional de Loja ya que esto permitirá que después de logearse el portal cautivo lo redireccione a la página de la universidad.

1.2.20. Iptables

Es un sistema de firewall que viene integrado con el kernel en las versiones de Linux con kernel superior al 2.4, es parte del sistema operativo.

El firewall viene ha ser un punto en el cual se controla el tráfico que se intercambia entre dos redes y en función de las políticas de seguridad definidas para cada una de las redes, se podrá establecer o no conexiones hacia los servicios de red entre las redes involucradas. La Unidad de Telecomunicaciones maneja políticas de seguridad generales las cuales se las aplicó para mantener el estándar.

1.2.20.1. Archivo ipup.sh

En el paquete CoovaChilli, existen archivos con reglas tipo iptables ya creadas. Se usaron estas mismas reglas y se añadió más reglas acordes con las políticas de seguridad de la Unidad de Telecomunicaciones e Información.

Existen dos scripts de shell que contienen las reglas de iptables que maneja CoovaChilli los que son up.sh y down.sh, estos scripts se ejecutan al instante en que se levanta el proceso de CoovaChilli.

Para agregar más reglas de iptables se creó el scripts de Shell llamado ipup.sh donde se establecieron los siguientes aspectos:

- **Conexión ssh**

Para permitir administrar remotamente el servidor mediante SSH desde la interfaz eth0, ya que por defecto está inhabilitado se procedió a abrir el puerto que se usa dentro de la unidad de telecomunicaciones.

- **Resolución de Nombres (DNS)**

Se procedió a abrir el puerto 53 udp, el cual es el puerto por defecto del DNS. Aquí se especifico la dirección IP del DNS de la universidad.

- **Peticiones http**

Para que se permita la navegación se procedió a abrir el puerto 80 tcp.

- **Conexión segura**

Para que el servidor web escuche por el puerto de conexión segura se procedió a abrir el puerto 443 tcp.

- **Puerto por el que escucha CoovaChilli**

Para que CoovaChilli escuche las peticiones de los usuarios se procedió a abrir el puerto 3990 tcp.

- **NAT (Traducciones de direcciones de red)**

El NAT permite la traducciones de direcciones ip en este caso se da con la Red 10.1.0.0/24, de modo que todo el trafico generado en esta red pueda salir por la IP 172.16.32.20/19, ya que esta ip esta configurada en la interfaz eth0 que es el medio por el cual se da acceso a internet.

1.2.21. Certificados SSL apache2

Para que la conexión al servidor RADIUS sea de una forma segura a través del portal cautivo se procedió a crear un certificado ssl el cual los usuarios tendrán que añadir a su navegador de forma manual.

Es importante que se haya instalado previamente la tarea LAMP Server si no está instalada mediante el comando tasksel se lo puede instalar.

El certificado SSL se lo utilizó dentro del host virtual en el que se especifica una serie de parámetros (Localidad, Provincia, etc.), siendo el más importante el nombre del host. En el que se configuró la dirección IP "10.1.0.1". De esta forma se consigue que el nombre del host y el del certificado coincidan, ya que los navegadores dan avisos de posibilidad de intrusión en caso de que no coincidan.

1.2.22. Host virtual

Virtual Host (ingles) es la expresión con la que comúnmente se le conoce al Hosting Virtual (español), consiste en hacer funcionar más de un sitio web en una misma máquina física y con nombres diferentes. Para conseguir esto se procedió a crear un

archivo llamado hotspot donde se configuró el host virtual dentro del directorio /etc/apache2/sites-available. Para la configuración correcta del virtual host se debe tener en cuenta los siguientes aspectos que se detallan en la tablaXXIII.

TABLA XXIII

Descripción de parámetros de virtual host

Parámetro	Descripción	Valor
NameVirtualHost	se indica la dirección IP de la tarjeta de red y el puerto	10.1.0.1:443
DocumentRoot	Directorio principal que contiene la estructura de directorios visible desde la Web Esta directiva especifica el directorio desde el cuál apache2 servirá los ficheros	/var/www/hotspot
ServerName	La directiva ServerName especifica el nombre de host y el puerto que usa el servidor para identificarse.	radius.unl.edu.ec
Directory index	Engloba a un grupo de directivas que se aplicarán solamente al directorio del sistema de ficheros especificado y a sus subdirectorios. Aquí es donde se indica el nombre de la página principal del sitio.	/var/www/hotspot /cgi-bin/
ServerAdmin	Dirección de email que el servidor incluye en los mensajes de error que se envían al cliente	webmaster@localhost
ErrorLog	Ubicación del fichero en el que se almacenan los mensajes de error	${APACHE_LOG_DIR}/error.log
CustomLog	Ubicación de donde esta el archivo en el cual se registran los accesos al sitio	${APACHE_LOG_DIR}/ssl.acces.log
SSLCertificateFile	Aquí se ubica la ruta donde se creó los certificados ssl.	/etc/apache2/ssl/apache.pem

Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo

En la figura 25 se muestra la configuración realizada para el virtual host para el portal cautivo.

```
<IfModule mod_ssl.c>
<VirtualHost 10.1.0.1:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/hotspot
        ServerName radius.unl.edu.ec
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/hotspot/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>
        Alias "/dialupadmin/" "/usr/share/freeradius-dialupadmin/htdocs/"
        <Directory "/usr/share/freeradius-dialupadmin/htdocs/">
                Options Indexes FollowSymLinks  MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /var/www/hotspot/cgi-bin/
        <Directory "/var/www/hotspot/cgi-bin/">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
```

Figura 25. Configuración de virtual host

1.2.23. Diseño y Funcionamiento de la Red

La figura 26 describe como se encuentra actualmente el sistema de seguridad que está implementado en la unidad de telecomunicaciones e información específicamente en la sección de redes.

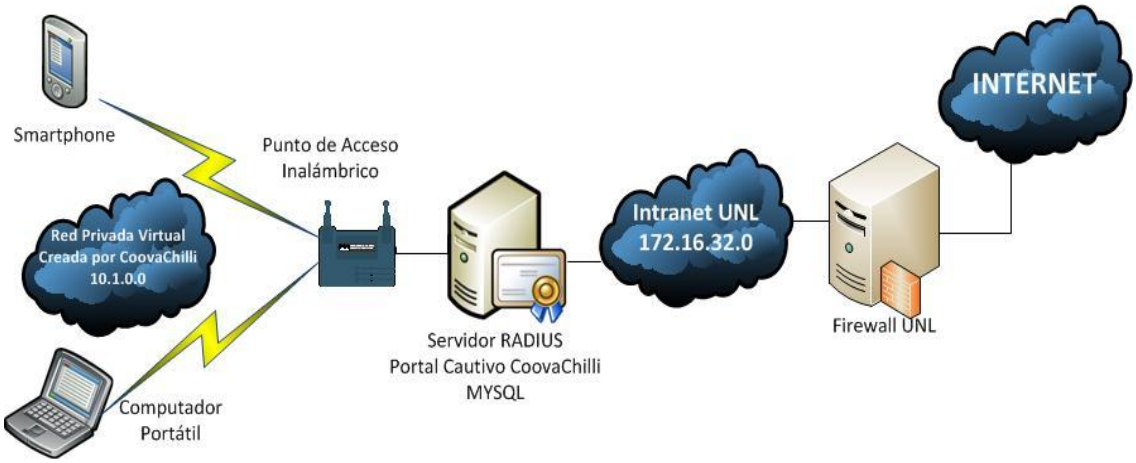

Figura 26. Topología del diseño del sistema de seguridad

Como se observa en la figura el servidor RADIUS que contiene instalado freeRADIUS, el portal cautivo CoovaChilli, MYSQL está ubicado en el cuarto de servidores (Data Center) conectado la interfaz eth0 a la red de la Universidad Nacional de Loja y la eth1 a un punto de acceso inalámbrico.

1.2.23.1. Funcionamiento Lógico del sistema

Para entender mejor el sistema, se va a describir el procedimiento que ocurre desde que un usuario detecta la red hasta que se autentica, sólo se detallan los pasos lógicos que se llevan a cabo hasta conseguir la autenticación del usuario.

1. Un cliente detecta la red con el SSID "SIRadius" y se conecta como se muestra en la figura 27.

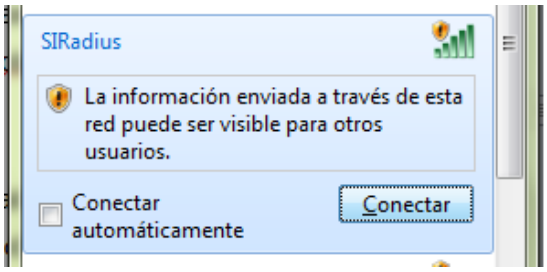

Figura 27. Ventana de conexión de red inalámbrica

2. El servidor DHCP (propio del CoovaChilli) le proporciona una dirección IP del rango de la red privada virtual creada por el portal cautivo CoovaChilli configurado en el servidor. En este caso la red privada virtual es la 10.1.0.0/24.

3. El cliente abre el navegador y accede a una página web. Se crea por tanto una petición TCP que es capturada por el servidor. Éste le responde redireccionándolo a la

página inicial de inicio de sesión, cuando el usuario ingresa por primera vez en el navegador debe de aceptar la excepción donde se agrega el certificado de seguridad para conexión ssl como se muestra en la figura 28.

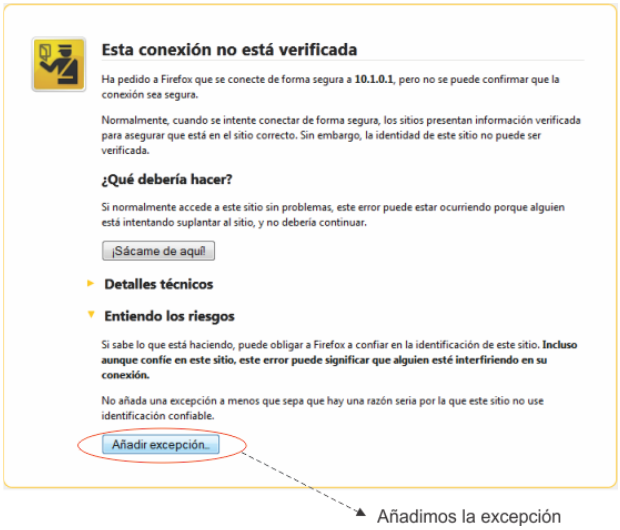

Figura 28. Ventana de añadir excepción.

Se debe de agregar el certificado de seguridad como se ve en la figura 29.

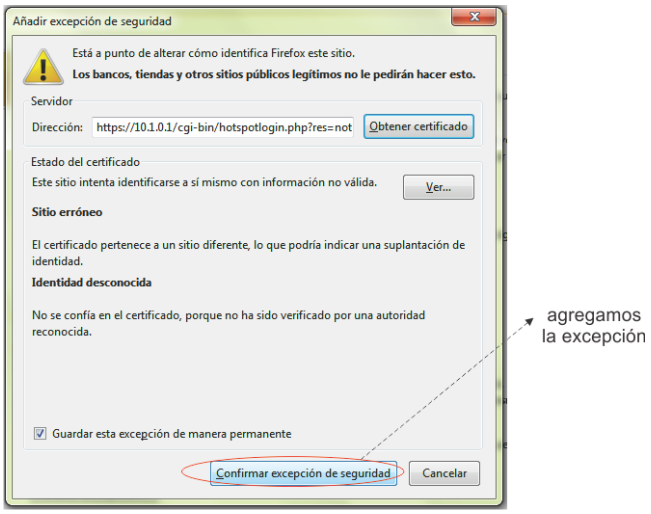

Figura 29. Ventana de confirmación de excepción de seguridad.

4. Al haber aceptado el certificado de seguridad nos presenta la página de inicio de sesión donde se requerirá el nombre de usuario (Cédula de Identidad) y contraseña, los cuales son los datos con los que se accede al SGA (Sistema de Gestión Académica) de la UNL .El usuario debe introducir los datos y pulsar en el botón login como se muestra en la figura 30.

Figura 30. Ventana principal de inicio de sesión de usuarios

5. Una vez introducido los datos, el portal cautivo CoovaChilli envía al servidor RADIUS (configurado en el mismo servidor) una petición de autenticación con las credenciales del usuario, si es la primera vez que el usuario ingresa las credenciales se ejecuta el script de perl, el cual consulta al webservice del SGA si los datos son correctos y si lo son se guardan en la base de datos llamada "radius" de MySQL, específicamente en la tabla radcheck.

El servidor RADIUS comprueba en su base de datos los datos ingresados y devuelve al portal cautivo un mensaje donde le indica si se le concede el acceso o no.

Si el servidor RADIUS concede el acceso le envía a CoovaChilli los siguientes atributos:

- **Tiempo de conexión**. Se le indica el tiempo restante de la sesión activa, la cual se ha configurado que sea de 7200 segundos (2 horas).

- **Sesiones simultáneas**. Los usuarios no podrán tener más de 1 sesión activa al mismo tiempo.

6. El navegador abre una nueva instancia donde se le indica el tiempo restante. Aparece además la opción Cerrar Sesión que deberá ser pulsado cuando se finalice el acceso. Esta ventana deberá ser minimizada.

7. El servidor redirecciona al cliente a la página principal de la Universidad Nacional de Loja como se ve en la figura 31. A partir de ese instante y hasta que decida finalizar

el servicio o se le agote el tiempo de conexión diario, el usuario dispondrá de acceso a la red y conexión a Internet.

Figura 31. Página principal de la Universidad Nacional de Loja.

Todas estas acciones se hacen de forma transparente al usuario, es decir, en su equipo no se tiene que instalar ningún software ni certificado digital. Esto es así debido al uso de protocolos soportados por prácticamente todos los navegadores web.

1.2.24. Diseño de la red mesh inalámbrica.

La propuesta de diseño de la red inalámbrica para la Universidad Nacional de Loja está relacionada con la consolidación de los recursos de control, administración, seguridad y monitoreo de los dispositivos que interactúan en la red Inalámbrica de una forma centralizada. Se pretende implementar una solución unificada que brinda Cisco, y que permite un mejor desarrollo, funcionamiento y despliegue [10].

1.2.24.1. Selección de equipos para la red inalámbrica

Para la implementación del diseño de la Red Inalámbrica, se describen equipos basados en el estándar 802.11n, los mismos que permitan una estructura y una configuración mallada. Y así permitir una mayor cobertura del sistema cuando se desee brindar los servicios de Internet a usuarios internos al campus universitario [10].

1.2.24.1.1. Comparación de alternativas de puntos de acceso mesh

En la tabla XXIV se detallan las características de los equipos Access point exteriores para redes malla.

TABLA XXIV

Equipos Access Point exteriores para redes malla

Especificación	Cisco	Motorola	3Com
Modelo	Aironet 1552e	Motorola 7181	3Com 9550
Estándares	IEEE 802.11 a/b/g/h	IEEE 802.11 b/g/h	IEEE 802.11 a/b/g/h
Tipo de Dispositivo	Punto de acceso inalámbrico externo.	Punto de acceso inalámbrico externo.	Punto de acceso inalámbrico.
Velocidades	**802.11a** 6, 9, 12, 18, 24, 36, 48, 54 Mbps **802.11b** 1, 2, 5.5, y 11 Mbps **802.11g** 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54 Mbps **802.11n** 300 Mbps (velocidades teóricas)	**802.11b** 1, 2, 5.5, y 11 Mbps **802.11g** **802.11n** 300Mbps (velocidades teóricas)	**802.11a** 6, 9, 12, 18, 24, 36, 48, 54 Mbps **802.11b** 1, 2, 5.5, y 11 Mbps **802.11g** 6, 9, 12, 18, 24, 36, 48, 54 Mbps **802.11n** MCS 0-15 de HT20MHz, 6,5 hasta 130 Mbps MCS 0-15 de HT40MHz, 13,5 hasta 270 Mbps
Potencia de Transmisión	**2,4 GHz** • 802.11b (CCK) • 28 dBm con 2 antenas	**2,4 GHz** 36 dBm **5 GHz**	**802.11a** 6 to 36 Mbps: 21 dBm

	• 802.11g (no el modo HT duplicado) • 28 dBm con 2 antenas • 802.11n (HT20) • 28 dBm con 2 antenas **5 GHz** • 802.11a • 28 dBm con 2 antenas • 802.11n no HT duplicado (802.11a duplicado) el modo de • 28 dBm con 2 antenas • 802.11n (HT20) • 27 dBm con 2 antenas • 802.11n (HT40) • 27 dBm con 2 antenas	32 dBm	48 Mbps: 19 dBm 54 Mbps: 17dBm • 802.11b 23 dBm • 802.11g 6 a 24 Mbps: 23dBm 36 Mbps: 22 dBm 48 Mbps: 20 dBm 54 Mbps: 19 dBm **2,4GHz n** 28 dBm **5 GHz n** 26dBm
Sensibilidad	• 802.11b -101 DBm a 1 Mb / s -98 DBm a 2 Mb / s -92 DBm@5.5 Mb / s -89 DBm a 11 Mb / s • 802.11g -94 DBm @ 6 Mb / s …… -79 DBm a 48 Mb / s -78 DBm a 54 Mb / s **802.11a** -92 DBm @ 6 Mb / s …… -77 DBm a 48 Mb / s -76 DBm a 54 Mb / s **802.11n 2,4 GHz** -93 DBm @ MCS0 -91dBm @ MCS1 -89dBm @ MCS2	• **802.11g** 2.4 GHz: -78 dBm @ 54 Mbps a -89 dBm @ 6 Mbps • **802.11n** 2.4 GHz: -70 dBm @ MCS 15 a -80 dBm @ MCS0 • **802.11a** 5.x GHz: -72 dBm @ 54 Mbps a -89 dBm @ 6 Mbps • **802.11n** 5.x GHz: -63 dBm @ MCS15 a -88 dBm @	• 802.11a 6 Mbps: -91 dBm 12 Mbps: -88 dBm 18 Mbps: -87 dBm 24 Mbps: -82 dBm 36 Mbps: -79 dBm 48 Mbps: -74 dBm 54 Mbps: -71 dBm •802.11b 1 Mbps: -94 dBm 2 Mbps: -92 dBm 5.5 Mbps: -90 dBm

	…… 5-GHz 802.11n (HT20) -92 DBm @ MCS0 -89 DBm @ MCS1 -87 DBm @ MCS2 …… 5HHz 802.11n (HT40) -89 DBm @ MCS0 -86 DBm @ MCS1 -84 DBm @ MCS2	MCS0	11 Mbps: -85 dBm •802.11g 6 Mbps: -90 dBm 12 Mbps: -88 dBm 18 Mbps: -86 dBm 24 Mbps: -83 dBm 36 Mbps: -79 dBm 54 Mbps: -72 dBm
Soporte de antena externa	SI	NO	SI
Modo de operación	Bridge y Access Point	Access Point	Bridge y Access Point
Banda de Frecuencia	**•802.11 b/g/n** 2,401 a 2,4835 GHz **• 802.11 a/n** 5,470 a 5,725 GHz 5745 a 5825 MHz	**•802.11 b/g/n** 2.4 -2.462 GHz **•802.11 a/n** 5.470 -5.865 GHz	**•802.11ª** 5,15 a 5,85 GHz **•802.11b / g** 2,4 a 2,484 GHz **•802.11n** 2.4 a 2,484 GHz, y 5.15-5.85 GHz
Algoritmo de Cifrado	AES , LEAP , PEAP , TKIP , TLS , TTLS , WPA , WPA2	WEP, AES-CCM,TKIP	WEP cifrado 64-/128-bit
Modulación	Multiplexación por División Ortogonal de Frecuencia (OFDM) y DSSS	Multiplexación por División Ortogonal de Frecuencia (OFDM) • (BPSK, QPSK, 16-QAM, 64-	802.11b: DSSS (Direct Spread Spectrum) 802.11a/g/n: OFDM y DSSS

		QAM) • 802.11b –DSS (BPSK, QPSK, CCK)	
Método Autentificación	Aautenticación 802.1X, incluido el Protocolo de autenticación extensible protegido y EAP (EAP-PEAP), EAP transporte Lauer Seguridad (EAP-TLS), EAP-TLS túnel LEAP (EAP-TTLS), y Cisco	MAC y 802.1x	EEE 802.1X EAP tipos: EAP-TLS, EAP-TTLS, PEAP
Filtrado MAC	SI	SI	SI
Protocolo de Gestión Remota	SNMP 1, SNMP 2, Telnet, HTTP	SNMTP v1, v2c, Http, Telnet	SNMTP v1, v2c, Http, Telnet
Precio	$4100	$6500	$2750
Elaborado por: Diego Mendoza			

1.2.24.1.2. Elección Punto de Acceso

Como hemos visto en la tabla anterior podemos dar una apreciación acerca de los diferentes dispositivos, de modo que los Puntos de Acceso 3-Com brinda buenas características que permiten configurar una red mallada y además posee un sistema de control de puntos de acceso y administración de la red inalámbrica, a diferencia del Punto de Acceso Motorola, que no posee sistemas de control de puntos de acceso, y no pueden trabajar en modo puente caso que los cisco y 3con si , el modo puente de una u otra forma son requeridos en la implementación de una red inalámbrica, también no posee antenas externas que en caso de querer hacer una implementación con este requerimiento no seria posible. Los puntos de acceso Motorola y 3Com no disponen

de las características que se requieren para la implementación por tal razón no se puede considerar para este caso [10].

De modo que se propone trabajar con equipos Cisco Aironet 1552e, dado que permiten desarrollar un esquema mesh y posee dos radios que trabajan a frecuencias de 5 GHZ y 2.4 GHz, disponen de batería de dos horas de duración, mas económico que el Punto de Acceso promocionado por Motorola, mejores características de funcionalidad que los Puntos de acceso 3com, el precio del AP de Cisco se encuentra en un termino medio, el AP. Aironet trabajará en conjunto con el Wireless LAN Controller y el Wireless Control System, para poder de igual manera estructurar un esquema unificado y centralizado; proporcionando escalabilidad a la red [10].

1.2.24.1.3. Comparación de alternativas de los equipos de gestión de red

En la tabla XXV se detallan las características de los equipos de gestión de red.

TABLA XXV

Características de equipos de gestión de red

Especificación	Cisco	3Com
Modelo	AIR-WLC4402-25-K9	3CRWX220095A-M
Tipo	Gestión de Red	Gestión de Red
Wiffi	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n	IEEE 802.11a, 802.11g/b, 802.11n
Encriptación	WEP and TKIP, SSL and TLS, AES: CCM, CCMP, IPSec	AES, WEP de 128 bits, SSL, TKIP
Autenticación	RADIUS 802.1X	RADIUS 802.1X
Protocolo de Transporte	Gigabit Ethernet	Gigabit Ethernet
Frecuencias	2.4 GHz y 5 GHz	2.4 GHz y 5 GHz
Protocolo de Gestión Remota	SNMP v1, v2c, v3, Telnet, SNM, TFTP, SNTP, HTTP	SNMP, Telnet, HTTPS
Precio	$12300	$13120
Elaborado por: Diego Mendoza		

1.2.24.1.4. Elección del equipo de gestión de red

El WLC de 3-Com permite un control de los puntos de acceso centralizadamente y de una forma segura, pero no trabaja muy eficientemente de una manera mallada WLAN, además no permite informes de dispositivos dentro de la red que posean fallas en tiempo real, ni detección de redes ad-hoc cercanas a los puntos de acceso. Además carece especificación que permita trabajar con el protocolo IPv6 [10].

El WLC de Cisco permite una comunicación más segura con cada uno de los puntos de acceso que forman la Red Mallada mediante el Protocolo Ligero de Puntos de Acceso (LWAPP), que crea túneles de comunicación. El WLC de Cisco ofrece una configuración unificada de todos sus equipos, y permite una administración en tiempo real de todos sus dispositivos ubicados en cualquier punto de la red. Permite trabajar con el protocolo IPv6 mediante la implementación de túneles que son manejados por el WLC, en cuanto a precios no tenemos marcada diferencia ya que se encuentran casi iguales de modo que tratándose que sea compatible la arquitectura en cuanto a hardware, el Wireless Lan Controller de Cisco lo tenemos como primera opción en esta propuesta [10].

La plataforma de Cisco será la que se usará para el diseño de la Red Inalámbrica Mallada, por todas las razones expuestas y que además tiene muchas garantías de funcionamiento [10].

1.2.24.2. Antenas a utilizar

Las antenas a utilizar en la configuración de la Red Wireless podrán ofrecer con ayuda de los Access Point la cobertura deseada en cada una de las áreas ubicadas y distribuidas, las áreas fueron establecidas y seleccionadas con la ayuda del personal de DOS [10].

Estas antenas poseen características compatibles con cada punto de acceso y trabajan muy bien, es así que a continuación se describe el tipo de antena, utilizada para el diseño de la red inalámbrica [10].

Todos los equipos cisco Aironet de las Serie 1552e trabajarán con estas antenas las cuales son diseñadas espacialmente para estos modelos de radios [10].

1.2.24.3. Cobertura de la red inalámbrica

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 [10].

Las figuras 32 y 33 muestran las áreas de cobertura de los Puntos de Acceso, distribuidos de forma que pueda ser utilizado por el mayor número de usuarios [10].

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 [10].

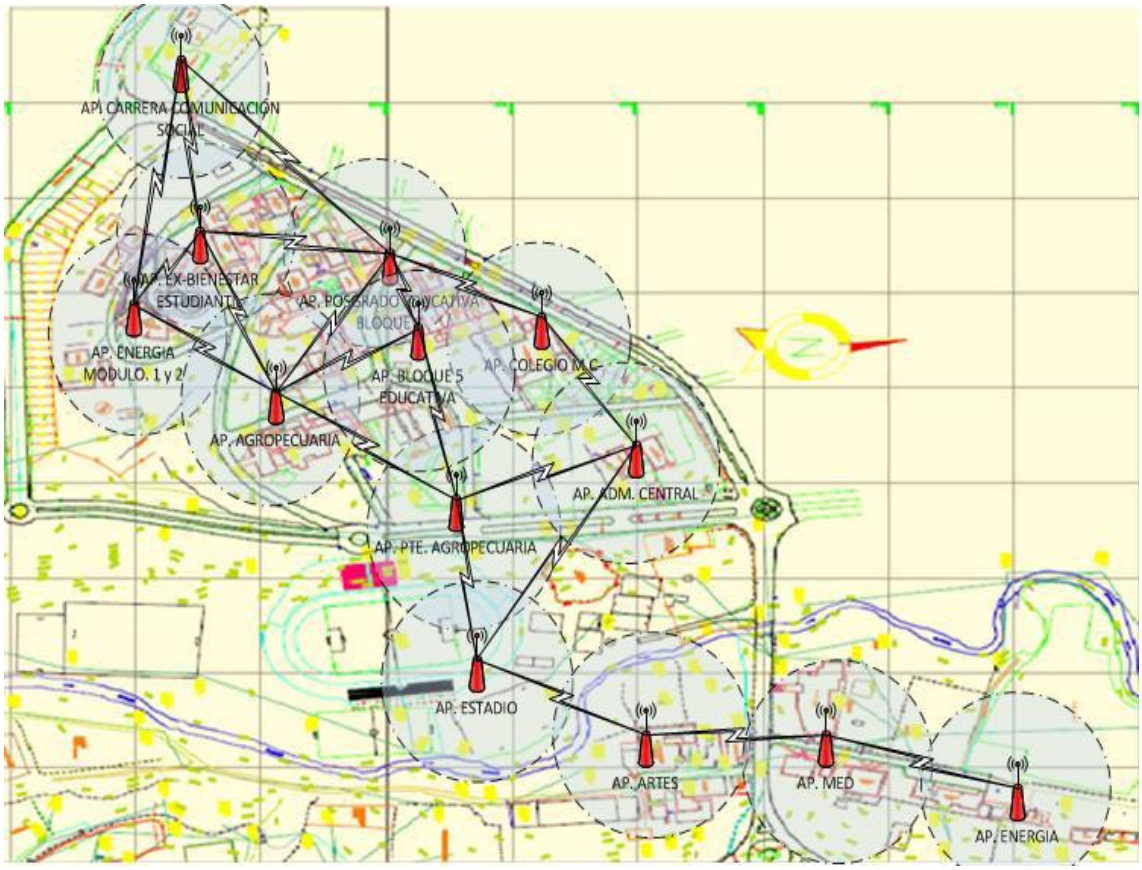

Figura 32. Cobertura de los AP en el campus universitario sector la argelia

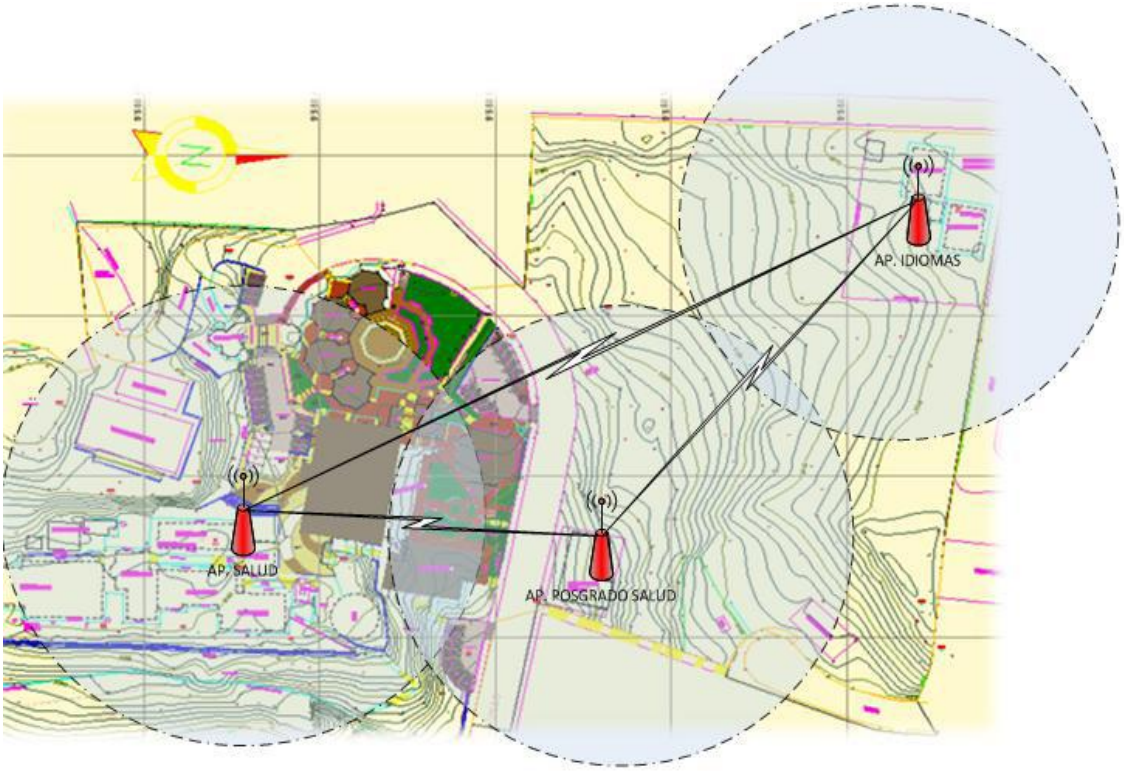

Figura 33. Cobertura de los AP en el Área de la Salud e Instituto de Idiomas

1.2.24.4. COSTOS DE EQUIPAMIENTO

Los estudios previos de diseño dan una referencia de los costos para la infraestructura de la red *mesh* en la Universidad Nacional de Loja. De acuerdo al diagrama de red existen 16 puntos de acceso (se han pedido 17 pero uno es de respaldo), un Wireless Lan Controller, y el software Wireless Control System, para lo se necesita una estimación de costos del proyecto dividiéndolos en varios grupos de la siguiente forma [10].

- ✓ Costos de Equipos.
- ✓ Costos de Instalación.
- ✓ Costos de Mantenimiento.

1.2.24.4.1. Costo de equipos

La propuesta de Red Mallada cuenta con los siguientes equipos como se observa en la tabla XXVI [10].

TABLA XXVI

Costos de los equipos para la implementación de la red inalámbrica.

Equipo	Cantidad	Precio Unitario ($)	Subtotal
AP Aironet 1552e (A)	17	**4.096.87**	**69.686.42**
Antena Omni Dual Band, N Conector	57	**272.52**	**13.898.37**
Wireless Lan Controller 4400 Series	1	**13.120.01**	**13.120.01**
Total Precio			**96.704.80**
I.V.A 12%			**11.604.576**
Total			**108.309.38**
Elaborado por: Diego Mendoza			

1.2.24.4.2. Costo de infraestructura

Dentro la Infraestructura se considera los costos de Kits de montaje, herramientas, equipos de subministro de Energía, cables, adaptadores de fibra. En la tabla XXVII se puede observar los costos totales para la implementación de la red mallada.

TABLA XXVII

Costos de infraestructura

Equipo	Descripción	Cantidad	Precio Unitario	Subtotal
Aironet 1500 Pole Mount Kit	**Accesorios de montaje de radios.**	**17**	**117.57**	**1.998.76**
Herramientas de Instalación	**Accesorios del equipo de Instalación**	**17**	**454.80**	**7.731.85**
AC Power Cord	**Cables para conexiones eléctricas**	**17**	**252.72**	**4.632.79**
Power Injector	**Dispositivo de subministro de energía**	**17**	**226.95**	**3.858.08**
1000Base-T SFP	**Transceptor de fibra óptica intercambiable**	**2**	**360.01**	**720.02**
Total Precio				**18.941.50**
I.V.A 12%				**2.272.98**
Total				**21.214.48**
Elaborado por: Diego Mendoza				

1.3. FASE 3: IMPLEMENTACIÓN DE LA APLICACIÓN WEB PARA LA ADMINISTRACIÓN DEL SERVIDOR RADIUS

1.3.1. DaloRADIUS

Figura 34. Logo de daloRADIUS

Es una aplicación avanzada de gestión de RADIUS web destinadas a la gestión de puntos de acceso y las implementaciones de proveedor de internet para fines generales. Es una interfaz web que permite configurar y administrar mi servidor FreeRADIUS.

daloRADIUS está escrito en PHP y JavaScript, y utiliza una capa de abstracción de base de datos lo que significa que es compatible con muchos los sistemas de bases de datos, entre ellos el popular MySQL, PostgreSQL, SQLite, MSSQL, y muchos otros.

1.3.2. Módulos de daloRADIUS

daloRADIUS esta compuesto de diferentes módulos dentro de ellos se va a detallar los más importantes:

a. **Módulo de Gestión:** este módulo permite la gestión de usuarios, hotspot, NAS, Perfiles etc.

   Es importante mencionar que la opción de gestión de usuarios permite al administrador de la herramienta web crear usuarios, es decir que cuando no exista un usuario dentro de la base de datos del SGA y se requiera el uso del

sistema de seguridad implantado se puede utilizar esta opción para crear una cuenta con un nombre de usuario y una contraseña.

b. **Módulo de Reportes:** permite ver a todos los usuarios en línea, intentos de conexión, Registro del arranque, registro del sistema, registro de FreeRADIUS, registro de daloRADIUS, estado del servidor y estado de los servicios.

c. **Módulo de Gráficos:** permite ver estadísticas por usuario de los accesos, descargas y subidas, y los accesos totales al sistema.

d. **Módulo Configuración:** este módulo permite la configuración de la conexión a la base de datos, cambiar el lenguaje de la herramienta, ajustes de acceso y ajustes de la interfaz.

1.4. FASE 4: PRUEBAS DE VALIDACIÓN

Una adecuada planificación de pruebas es absolutamente indispensable para lanzar al entorno de producción una nueva versión con razonables garantías de éxito.

Para el desarrollo de esta etapa se comprobó que se cumplen con las especificaciones y que se cumplen los objetivos planteados.

Para la realización de las pruebas se planificaron tanto pruebas automatizadas con software como pruebas con usuarios en un escenario real.

1.4.1. Pruebas del servidor RADIUS

Como punto de partida para las pruebas correspondientes del sistema de seguridad se empezó comprobando los aspectos importantes del servidor RADIUS.

1.4.1.1. Conexiones simultáneas

Para las pruebas automatizadas se utilizó el software radLogin como se observa en la figura 35, el cual es un simulador de solicitudes de acceso simultáneas para comprobar carga de los servidores.

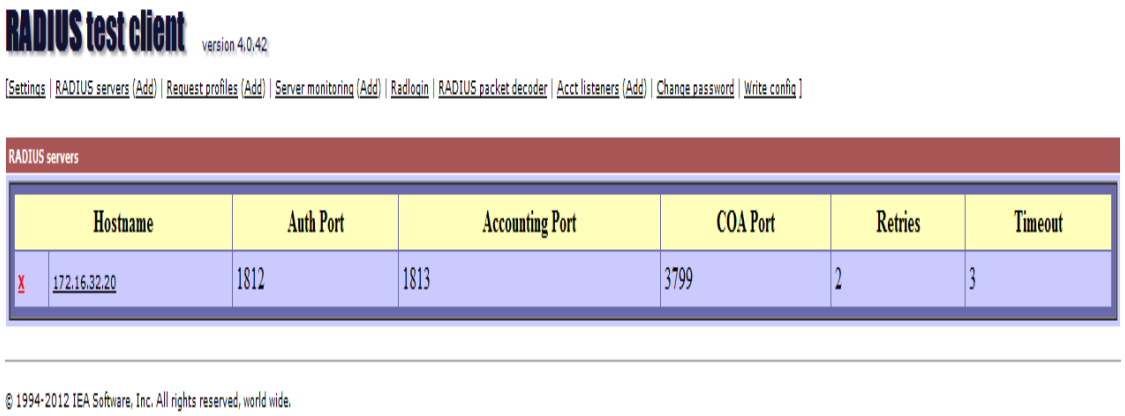

Figura 35. Respuesta del RadLogin

RadLogin permite simular conexiones simultáneas hacia el servidor RADIUS. La interfaz es amigable y nos devuelve el tiempo promedio de respuesta del servidor RADIUS como se puede ver en la figura 36.

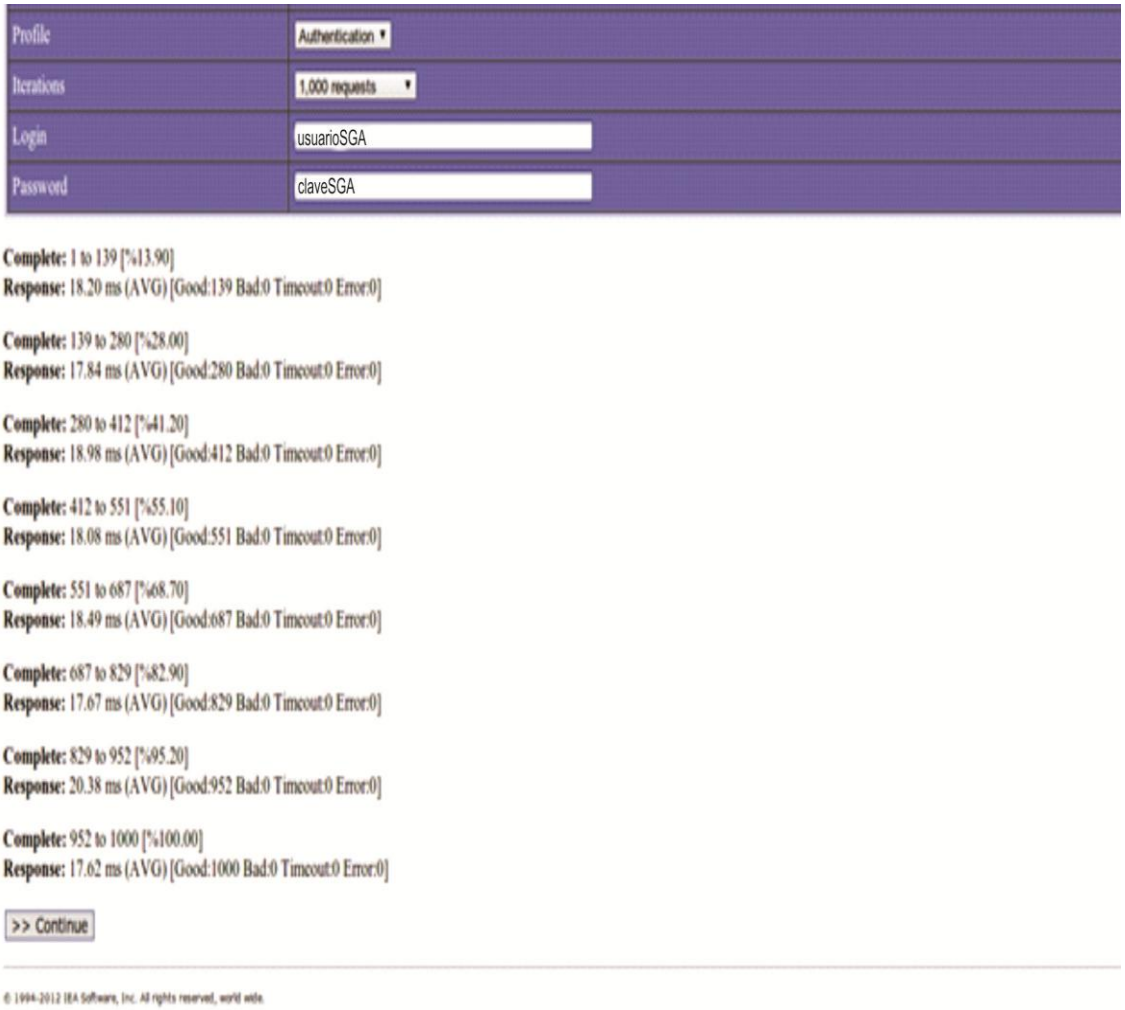

Figura 36. Respuesta de conexiones simultáneas

Al realizar 1000 solicitudes concurrentes se obtuvieron los siguientes resultados que se detallan en la tabla XXVIII.

TABLA XXVIII

Resultados de las conexiones simultáneas

Cantidad Solicitudes	Promedio de solicitudes total	Promedio de solicitudes individual	Solicitudes respondidas correctamente	Solicitudes respondidas erróneamente	Solicitudes excedidas tiempo
1000	17.62 ms	0.01762 ms	1000	0	0

Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo

Fuente: Unidad de Telecomunicaciones e Información

Además, en cuanto al uso de CPU y memoria del servidor durante las 1000 solicitudes se obtuvieron los siguientes datos que se encuentran en la tabla XXIX.

TABLA XXIX

Uso de memoria del servidor

%CPU	**10%**
MEMORIA RAM	20 MB

Elaborado por: Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo

Fuente: Unidad de Telecomunicaciones e Información

1.4.1.2. Solicitud de acceso con usuario del SGA

Para la validación de los usuarios se utilizó el comando radtest el cual permite simular una solicitud de acceso RADIUS y comprueba tanto conectividad como parámetros de envío.

Una vez enviada la solicitud de acceso, FreeRADIUS se encarga de receptar esta solicitud y dar una respuesta.

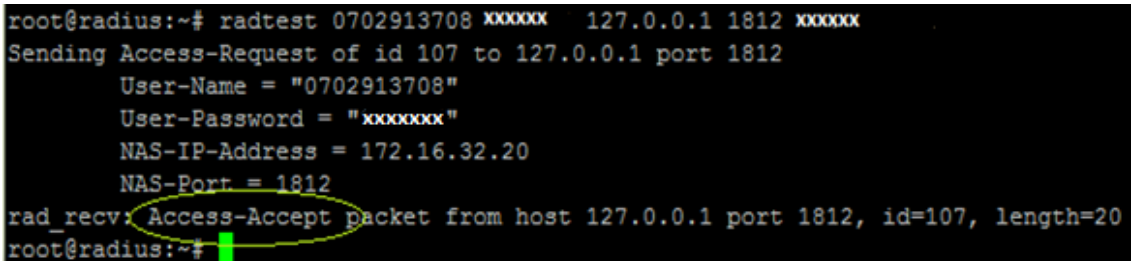

Figura 37. Respuesta del comando radtest

Como se ve en la figura 37 al ser correctas las credenciales da una respuesta de Access-Accept.

1.4.2. Pruebas del portal cautivo CoovaChilli

Las pruebas del portal cautivo permitió comprobar los aspectos básicos de coovachilli para lo cual se hicieron las siguientes pruebas.

1.4.2.1. Asignación de IP y parámetros de la red

En la figura 38 se muestran los parámetros de configuración de la red obtenidos mediante la ventana de detalles de la conexión de red en Windows 7. Con esto se comprueba que el dhcp del CoovaChilli esta funcionando correctamente ya que asigna una dirección IP dentro del rango previamente configurado, el DNS configurado es el de la universidad el cual es 172.16.32.2.

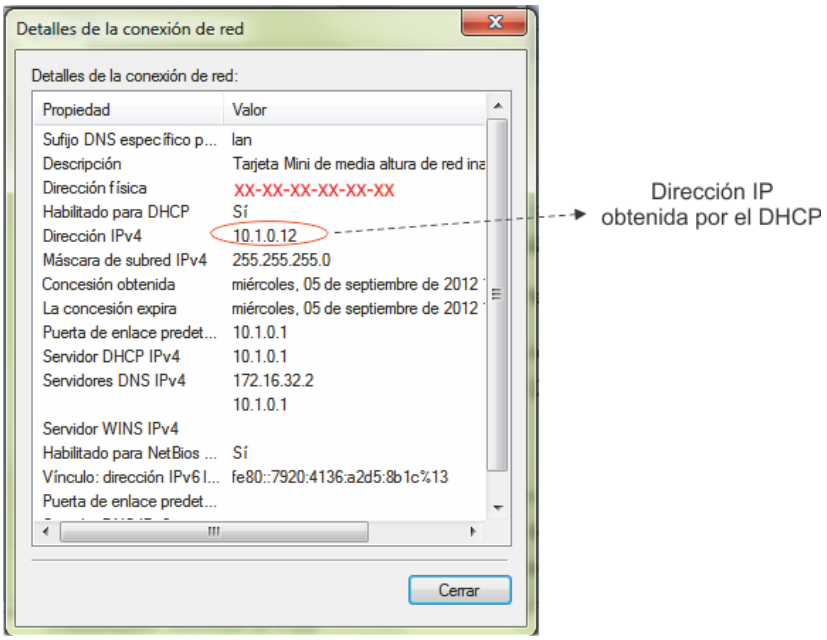

Figura 38. Ventana detalles de la conexión de red

1.4.2.2. Intercepción de trafico http

Esto nos permite comprobar que después de conectarnos al punto de acceso inalámbrico y querer navegar en cualquier dirección http CoovaChilli redirecciona a la página de inicio de sesión como se muestra en la figura 39.

Figura 39.Ventada de redirección

1.4.2.3. Verificación de datos correctos de usuario del SGA

Se ingresó datos correctos de un usuario del SGA y también datos incorrectos esto permitió comprobar que el script de perl el cual hace la consulta al webservice esta funcionando ya que al ingresar los datos del SGA se hace una consulta interna con la base de datos del SGA y si son correctas el servidor RADIUS las acepta y almacena en su base de datos y autoriza a navegar como se muestra en la figura 40.

Figura 40. Ventana principal de inicio de sesión

Al ser correctas las credenciales ingresadas el servidor autorizó a que ese usuario navegue y se le asignó el tiempo de sesión ya configurado en el CoovaChilli el cual es de 2 Horas como se ve en la figura 41.

Figura 41. Ventana de sesión iniciada

Cuando se ingreso los datos incorrectos el servidor RADIUS no autoriza a navegar y en el portal cautivo nos mostró que el registro esta fallido como observa en la figura 42.

Figura 42. Ventana de registro fallido

1.4.3. Escenario de pruebas

Para las pruebas con usuarios del S.G.A. en un escenario real, se utilizó un Access Point D-Link DAP-1360 con el servicio de DHCP deshabilitado y dispositivos portátiles con tarjeta de red inalámbrica (laptops, smartphones, tablets) con diferentes sistemas operativos.

Para demostrar la compatibilidad con diferentes equipos se usaron diferentes sistemas operativos y diferentes dispositivos para hacer uso del servicio de Internet a través de un portal cautivo.

Las pruebas se las realizaron en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja y en la biblioteca del Área de la Energía, las Industrias y los Recursos Naturales no Renovables.

La primera prueba fue a los administradores de la herramienta web de administración del servidor RADIUS que en este caso fue daloRADIUS utilizando la técnica del cuestionario para la recolección de información, lo que permitió comprobar la facilidad de uso de la misma ver anexo 5.

El otro perfil fue orientado a la utilización del portal cautivo a todo el personal que se encontraba en ese lugar (estudiantes y docentes) ver anexo 6.

1.4.3.1. Configuración de los puntos de acceso

Coovachilli provee una red diferente para que los usuarios se autentiquen. Así, es necesario que todos los usuarios que se requiere que se autentiquen estén en una red diferente. La Universidad Nacional de Loja implantará una red inalámbrica en la cual va a funcionar el presente proyecto de fin de carrera. La única configuración a tener en consideración es deshabilitar el servidor DHCP puesto a que Coovachilli se encarga de la asignación de IPs.

Para las pruebas se configuró un punto de acceso con el servidor DHCP deshabilitado. Al no haber un DHCP en el punto de acceso pasa la solicitud de broadcast directo al servidor, y éste le asigna una IP dentro de la red de Coovachilli, y bloquea e intercepta todo el tráfico hasta que no se autentique.

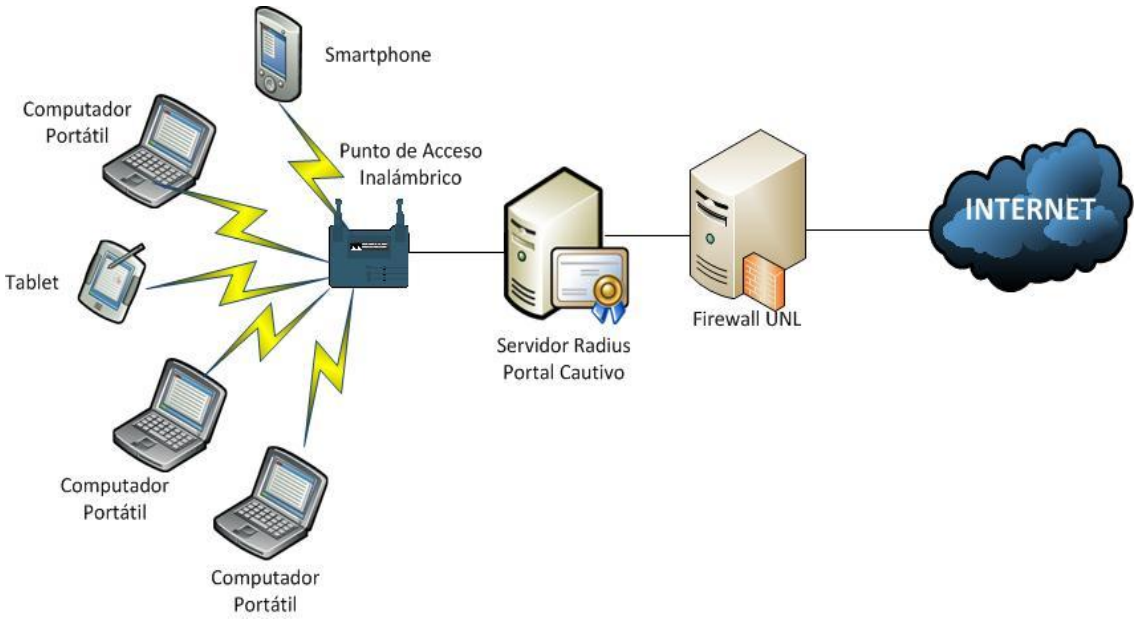

Figura 43. Diagrama del ambiente de pruebas

1.4.3.2. Pruebas en el Área de la Energía las Industrias y los Recursos Naturales no Renovables.

Se seleccionó como escenario la biblioteca del AEIRNNR para realizar las respectivas pruebas del sistema de seguridad. Se procedió a establecer un periodo de duración de las pruebas correspondientes.

El periodo de pruebas empezó desde el día lunes 22 de Octubre hasta el día viernes 26 de Octubre. El horario que los usuarios podían establecer la conexión con el punto de acceso inalámbrico iniciaba desde las 8:00 am hasta 6:00 pm aproximadamente, lo que permitió que los usuarios se familiaricen con el uso del portal cautivo y el procedimiento de agregar certificados de seguridad ver anexo 7.

Los resultados de las pruebas fueron los siguientes:

1.4.3.2.1. Usuarios en línea

Los usuarios en línea son todos aquellos que se encuentran conectados en ese momento al servidor RADIUS.

A través del uso de la herramienta wed de administración del servidor RADIUS (daloRADIUS) se pudo obtener los usuarios en línea que se conectaron el día lunes 22 de Octubre, obteniendo la información de cada usuario en línea como lo es: Usuario (Cédula de Identidad), Nombre, Dirección IP y Dirección MAC, Hora de inicio de sesión, el tiempo total de conexión y el total en Mb de subida y descarga de archivos como se puede observar en la figura 44.

Listado de usuarios en línea

Statistics Graph Online Nas

SELECT: ALL NONE

Limpiar sesiones | CSV Export

1

Usuario	Nombre	Dirección IP	Hora de inicio	Tiempo total	
0702913708	Lisset Alexandra Neyra Romero	IP: 10.1.0.74 MAC: 78-E4-00-DE-CC-14	2012-10-22 09:42:38	30 minutes	Subida: 9.45 Mb Descarga: 2.2 Mb : 11.65 Mb
invitado	Invitado	IP: 10.1.0.77 MAC: 40-FC-89-38-D0-B1	2012-10-22 09:48:24	25 minutes	Subida: 1.72 Mb Descarga: 10.76 Mb : 12.48 Mb
1104015936	Fabricio Alejandro Flores Gallardo	IP: 10.1.0.78 MAC: C4-17-FE-1E-BC-5D	2012-10-22 09:59:51	10 minutes	Subida: 16.43 Mb Descarga: 1.3 Mb : 17.73 Mb
1104706922	Lenin Capa	IP: 10.1.0.80 MAC: 0C-60-76-4C-0E-DE	2012-10-22 10:06:02	5 minutes, 1 seconds	Subida: 5.48 Mb Descarga: 934.33 Kb : 6.39 Mb
1104617053	Cristian Leonardo Calderon Ordoñez	IP: 10.1.0.82 MAC: 74-E5-0B-07-AC-FE	2012-10-22 10:09:23	0 seconds	Subida: 0 B Descarga: 0 B :
0705183986	Stalin Alfonzo Gomez Eras	IP: 10.1.0.84 MAC: E0-2A-82-A8-DD-69	2012-10-22 10:11:18	0 seconds	Subida: 0 B Descarga: 0 B :

Figura 44.Usuarios en línea de la biblioteca del AEIRNNR

1.4.3.2.2. Conteo de usuarios

El conteo de usuarios es la cantidad de usuarios que se conectaron al servidor RADIUS durante un periodo de tiempo.

Utilizando la opción de conteo de daloRADIUS se pudo obtener un conteo de usuarios ordenado por fecha desde el 22/10/2012 hasta el 26/10/2012 lo que arrojo la siguiente información que se detalla en la figura 45.

Información ordenado por fecha

PLAN INFORMATION

SUBSCRIPTION ANALYSIS

SESSION INFO

CSV Export

1 2 3 4

ID	Hotspot	Usuario	Dirección IP	Hora de inicio	Hora de finalización	Tiempo total	Subida (Bytes)	Descarga (Bytes)
481		0702913708	10.1.0.74	2012-10-22 09:42:38	2012-10-22 11:42:41	2 hours, 3 seconds	35.1 Mb	6.3 Mb
482		invitado	10.1.0.77	2012-10-22 09:48:24	2012-10-22 10:37:34	49 minutes, 11 seconds	1.93 Mb	10.82 Mb
483		1104015936	10.1.0.78	2012-10-22 09:59:51	2012-10-22 11:59:53	2 hours, 3 seconds	191.85 Mb	13.31 Mb
484		1104706922	10.1.0.80	2012-10-22 10:06:02	2012-10-22 12:06:02	2 hours, 1 seconds	444.08 Mb	18.21 Mb
485		1104617053	10.1.0.82	2012-10-22 10:08:42	2012-10-22 10:08:58	16 seconds	2.42 Kb	1.6 Kb
486		1104617053	10.1.0.82	2012-10-22 10:09:23	2012-10-22 11:23:20	1 hours, 13 minutes, 57 seconds	10.39 Mb	1 Mb
487		0705183986	10.1.0.84	2012-10-22 10:11:18	2012-10-22 11:40:39	1 hours, 29 minutes, 21 seconds	27.54 Mb	5.48 Mb
488		0706246436	10.1.0.87	2012-10-22 10:35:22	2012-10-22 11:00:55	25 minutes, 34 seconds	44.53 Mb	2.86 Mb
489		1104679038	10.1.0.88	2012-10-22 10:37:25	2012-10-22 12:37:26	2 hours, 1 seconds	4.74 Gb	241.94 Mb
490		1103805501	10.1.0.93	2012-10-22 11:03:34	2012-10-22 11:43:13	39 minutes, 39 seconds	40.06 Mb	3.52 Mb
491		invitado	10.1.0.94	2012-10-22 11:06:21	2012-10-22 12:42:24	1 hours, 36 minutes, 3 seconds	3.69 Mb	33.93 Mb
492		pruebas	10.1.0.95	2012-10-22 11:09:03	2012-10-22 11:38:45	29 minutes, 43 seconds	14.94 Mb	403.06 Kb
493		1105148942	10.1.0.100	2012-10-22 11:37:56	2012-10-22 13:14:32	1 hours, 36 minutes, 36 seconds	25.8 Mb	6.31 Mb
494		1104992118	10.1.0.101	2012-10-22 11:38:22	2012-10-22 12:54:04	1 hours, 15 minutes, 43 seconds	44.61 Mb	1.78 Mb

Figura 45. Conteo de usuarios de la biblioteca del AEIRNNR

1.4.3.2.3. Total de acceso

El total de acceso es la gráfica estadística de todos los accesos al servidor RADIUS durante un mes determinado distribuidos por días y la cantidad de accesos respectivamente.

Al utilizar la opción de gráficos de daloRADIUS se pudo obtener un gráfico estadístico de todos los accesos totales del mes de octubre del 2012 como se muestra en la figura 46 y así determinar la cantidad de accesos durante el periodo del 22 al 26 de octubre lo que se detalla en la tabla XXX.

TABLA XXX

Accesos totales del mes de octubre

Fecha	Número de Acceso
Lunes 22/10/2012	31
Marte 23/10/2012	25
Miércoles 24/10/2012	16
Jueves 25/10/2012	15
Viernes 26/10/2012	22
Total	99

Como se ve en la figura 46 se resaltó el periodo de los días en que se realizaron las pruebas en la biblioteca del área.

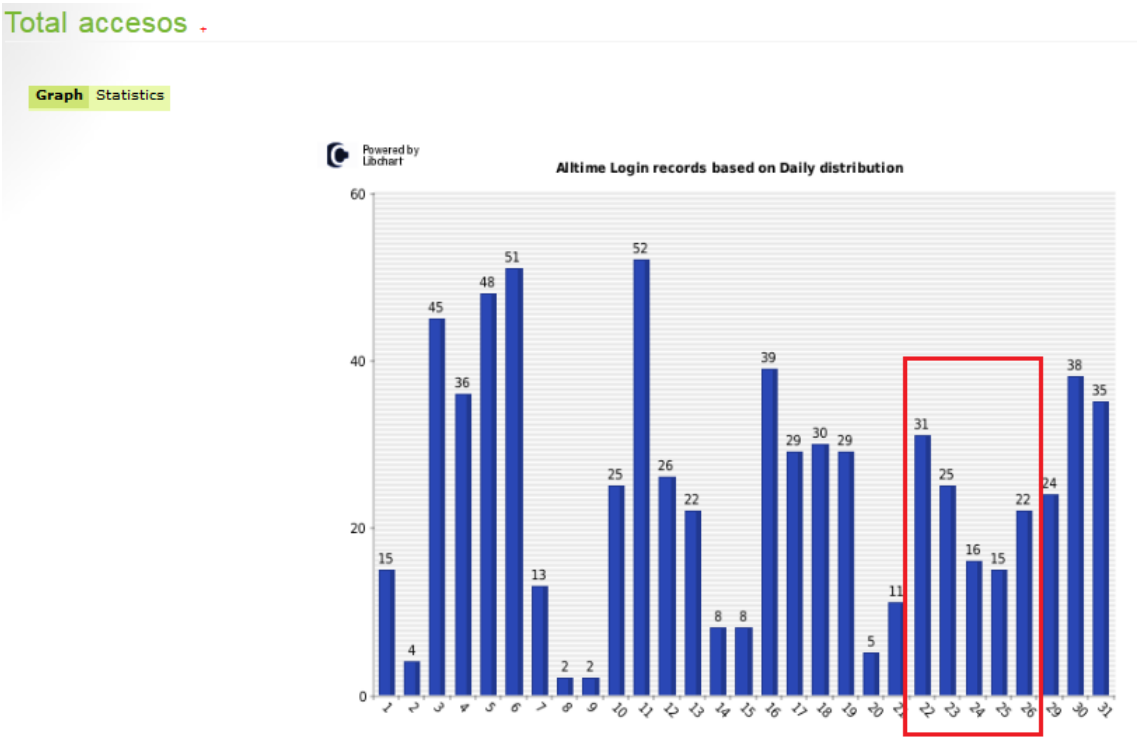

Figura 46. Accesos totales de usuarios de la biblioteca del AEIRNNR

1.4.3.3. Presentación de resultados administradores

En la tabla XXXI y XXXIII se presentan los resultados de la evaluación que se realizaron a los dos administradores del portal cautivo (tabla 1) y en la tabla XXXII y XXXIV los resultados de la administración de la herramienta web del servidor RADIUS llamada daloRADIUS (tabla 2) para comprobar el correcto funcionamiento del sistema.

TABLA XXXI
Respuesta tabla 1 del administrador 1
ADMINISTRADOR 1
ADMINISTRADOR 1 TABLA 1

Elemento que se prueba	Descripción de la funcionalidad	Descripción del caso de prueba	No Cumple	Parcialmente	Cumple	Observaciones
Validación	Ingreso a la interfaz de administración de RADIUS.	Verificar que se pueda ingresar a la interfaz de administración	0	0	1	-
	Ingreso a la interfaz de administración de RADIUS.	Comprobar que al ingresar credenciales incorrectas no deje ingresar.	0	0	1	-
Administración	Administración de usuarios.	Permitir ingresar un nuevo usuario en la BD del servidor RADIUS	0	0	1	-
	Administración de usuarios.	Permitir modificar un usuario en la BD del servidor	0	0	1	-
	Administración de usuarios.	Permitir eliminar un usuario en la BD del servidor RADIUS	0	0	1	-
Reportes	Visualización de reportes	Permites ver reportes del servidor RADIUS.	0	0	1	-
RESULTADOS			0	0	6	-

TABLA XXXII

Respuesta tabla 2 del administrador 1

ADMINISTRADOR 1 TABLA 2

Elemento que se prueba	Descripción de la funcionalidad	Descripción del caso de prueba	No Cumple	Parcialmente	Cumple	Observaciones
Validación	Ingreso a través del portal cautivo implantado	Verificar que se pueda iniciar sesión luego de ingresar las credenciales correctas	0	0	1	-
	Ingreso a través del portal cautivo implantado	Comprobar que al ingresar credenciales incorrectas no deje iniciar sesión.	0	0	1	-
Navegación	Navegación	Navegación sin contratiempos luego de iniciar sesión	0	0	1	-
	Navegación	Descarga correcta de archivos luego de iniciar sesión	0	0	1	-
RESULTADOS			0	0	4	-

TABLA XXXIII

Respuesta tabla 1 del administrador 2

ADMINISTRADOR 2 TABLA 1

Elemento que se prueba	Descripción de la funcionalidad	Descripción del caso de prueba	No Cumple	Parcialmente	Cumple	Observaciones
Validación	Ingreso a la interfaz de administración de RADIUS.	Verificar que se pueda ingresar a la interfaz de administración	0	0	1	-
	Ingreso a la interfaz de administración de RADIUS.	Comprobar que al ingresar credenciales incorrectas no deje ingresar.	0	0	1	-
Administración	Administración de usuarios.	Permitir ingresar un nuevo usuario en la BD del servidor RADIUS	0	0	1	-
	Administración de usuarios.	Permitir modificar un usuario en la BD del servidor	0	0	1	-
	Administración de usuarios.	Permitir eliminar un usuario en la BD del servidor RADIUS	0	0	1	-
Reportes	Visualización de reportes	Permites ver reportes del servidor RADIUS.	0	1	0	-
RESULTADOS			0	1	5	-

TABLA XXXIV

Respuesta tabla 2 del administrador 2

ADMINISTRADOR 1 TABLA 2

Elemento que se prueba	Descripción de la funcionalidad	Descripción del caso de prueba	No Cumple	Parcialmente	Cumple	Observaciones
Validación	Ingreso a través del portal cautivo implantado	Verificar que se pueda iniciar sesión luego de ingresar las credenciales correctas	0	0	1	-
	Ingreso a través del portal cautivo implantado	Comprobar que al ingresar credenciales incorrectas no deje iniciar sesión.	0	0	1	-
Navegación	Navegación	Navegación sin contratiempos luego de iniciar sesión	0	0	1	-
	Navegación	Descarga correcta de archivos luego de iniciar sesión	0	1	0	-
RESULTADOS			0	1	3	-

1.4.3.3.1. ANÁLISIS DE RESULTADOS

De acuerdo a la información obtenida se puede realizar un análisis reflejado en los siguientes resultados.

ADMINISTRADOR 1 TABLA 1

Cumple= 6

Parcialmente= 0

No Cumple= 0

Representado en porcentajes se obtuvieron los siguientes datos que se muestran en la tabla XXXV.

TABLA XXXV

Resultados de la tabla 1 del administrador 1

VALORACIÓN	PORCENTAJE
Cumple	100 %
Parcialmente	0 %
No Cumple	0 %

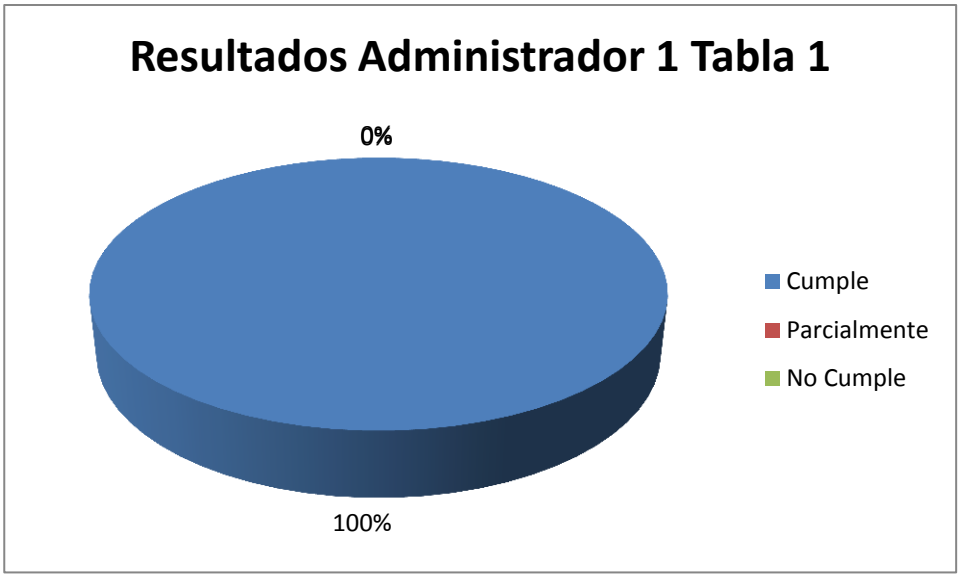

Figura 47. Resultados de la tabla 1 del administrador 1

Realizado el análisis de los resultados obtenidos, se deduce que el Administrador 1 considera que el sistema es funcional respecto a Validación, Administración y Reportes del mismo.

ADMINISTRADOR 1 TABLA 2

Cumple= 4

Parcialmente= 0

No Cumple= 0

Representado en porcentajes se obtuvieron los siguientes datos que se muestran en la tabla XXXVI.

TABLA XXXVI

Resultados de la tabla 2 del administrador 2

VALORACIÓN	PORCENTAJE
Cumple	100 %
Parcialmente	0 %
No Cumple	0 %

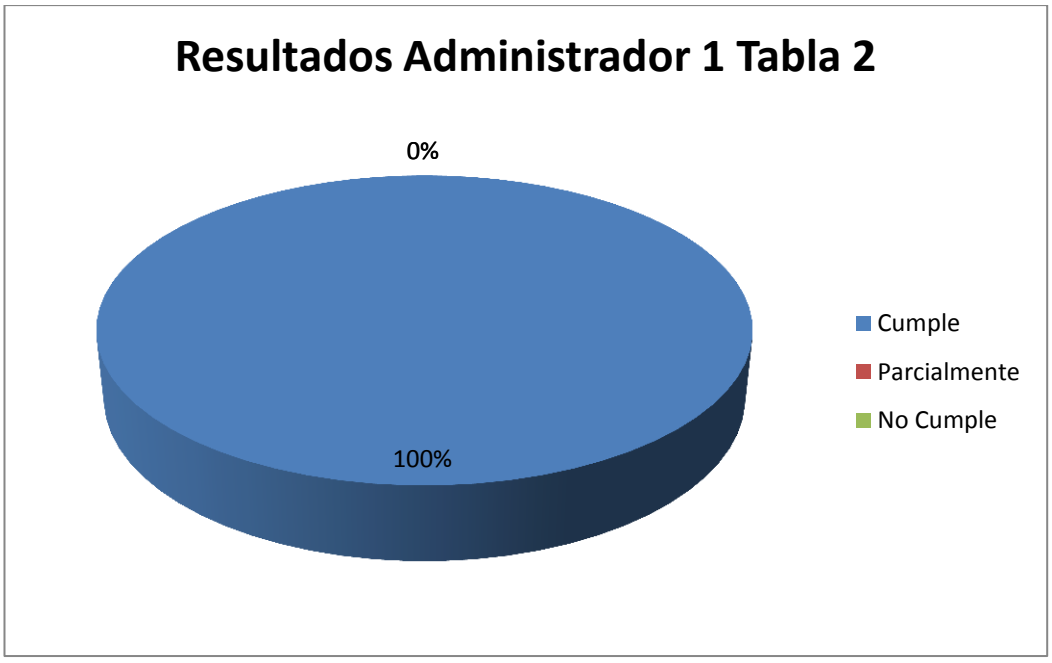

Figura 48. Resultados de la tabla 2 del administrador 1

Realizado el análisis de resultados, se deduce que el Administrador 1 considera que el sistema es funcional respecto a Validación y Navegación.

ADMINISTRADOR 2 TABLA 1

Cumple= 5

Parcialmente= 1

No Cumple= 0

Representado en porcentajes se obtuvieron los siguientes datos que se muestran en la tabla XXXVII.

TABLA XXXVII

Resultados de la tabla 1 del administrador 2

VALORACIÓN	PORCENTAJE
Cumple	83.33 %
Parcialmente	16.67 %
No Cumple	0 %

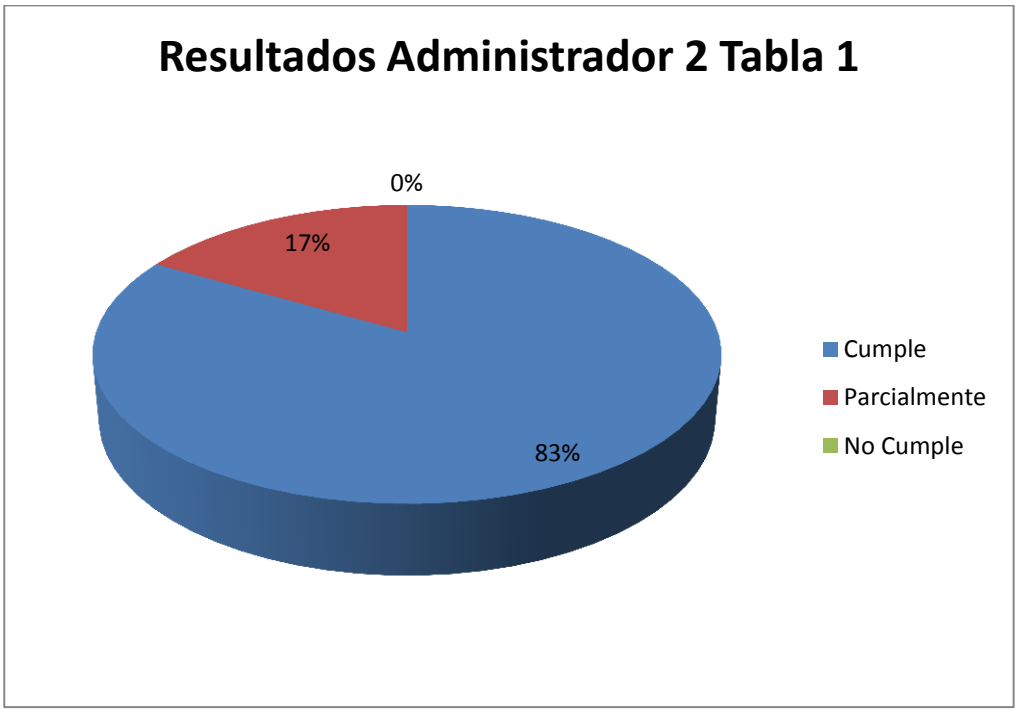

Figura 49. Resultados de la tabla 1 del administrador 2

Realizado el análisis de los resultados obtenidos, se deduce que el Administrador 2 considera que el sistema es funcional respecto a Validación, Administración, pero encuentra falencias en la presentación de Reportes del Sistema.

ADMINISTRADOR 2 TABLA 2

Cumple= 3

Parcialmente= 1

No Cumple= 0

Representado en porcentajes se obtuvieron los siguientes datos que se muestran en la tabla XXXVIII.

TABLA XXXVIII

Resultados de la tabla 2 del administrador 2

VALORACIÓN	PORCENTAJE
Cumple	75 %
Parcialmente	25 %
No Cumple	0 %

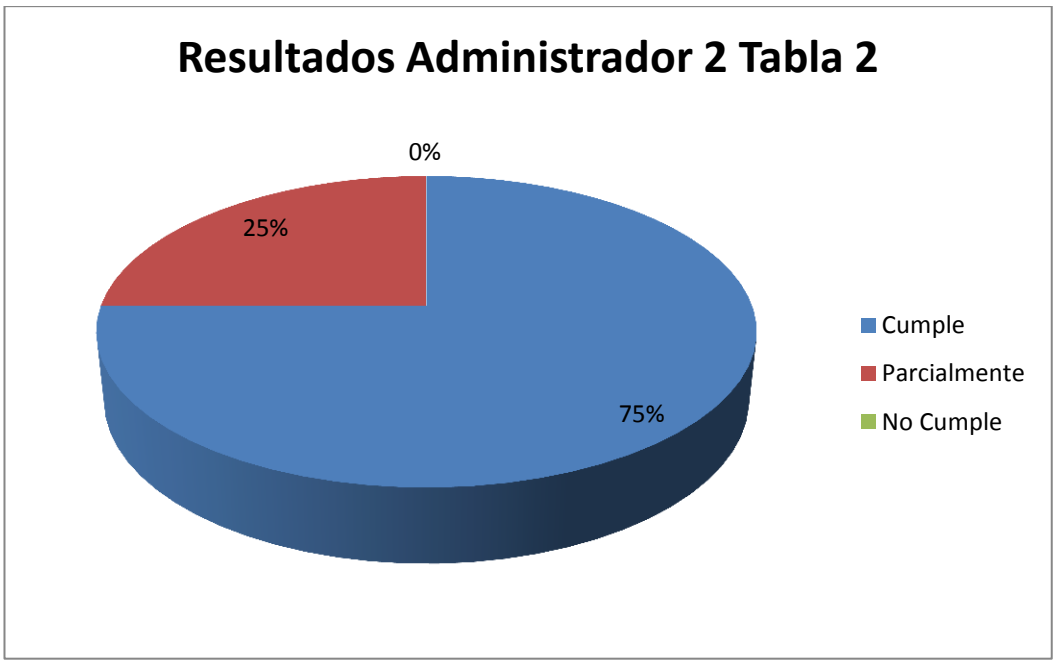

Figura 50. Resultados de tabla 2 del administrador 2

Realizado el análisis de los resultados obtenidos, se deduce que el Administrador 2 considera que el sistema es funcional respecto a Validación, pero encuentra falencias en la Navegación, concretamente en la descarga de archivos.

1.4.3.4. Presentación de resultados usuarios

Para realizar las pruebas a usuarios, se consideró realizarla en un escenario real, y se la realizó en la biblioteca del Área de la Energía, las Industrias y los Recursos Naturales no Renovables. Se colocó un Access Point con autenticación mediante el portal cautivo. Durante en transcurso de las pruebas se conectaron un total de 99 usuarios, de los cuales se realizó una entrevista a 67 usuarios. La encuesta permitió obtener los siguientes resultados expuestos en la tabla XXXIX.

TABLA XXXIX

Respuestas de usuarios

Elemento que se prueba	Descripción de la funcionalidad	Descripción del caso de prueba	No Cumple	Parcialmente	Cumple	Observaciones
Validación	Ingreso a través del portal cautivo implantado	Verificar que se pueda iniciar sesión luego de ingresar las credenciales correctas	1	0	66	-
	Ingreso a través del portal cautivo implantado	Comprobar que al ingresar credenciales incorrectas no deje iniciar sesión.	7	0	60	-
Navegación	Navegación	Navegación sin contratiempos luego de iniciar sesión	2	5	60	-
	Navegación	Descarga correcta de archivos luego de iniciar sesión	7	4	56	-

1.4.3.4.1. ANÁLISIS DE RESULTADOS

De acuerdo a la información obtenida se puede realizar un análisis reflejado en los siguientes resultados.

VALIDACIÓN 1: Verificar que se pueda iniciar sesión luego de ingresar las credenciales correctas

Cumple= 66

Parcialmente= 0

No Cumple= 1

Representado en porcentajes se obtuvieron los siguientes datos que se muestran en la tabla XL.

TABLA XL

Resultados de validación 1 usuarios

VALORACIÓN	PORCENTAJE
Cumple	98.50 %
Parcialmente	0 %
No Cumple	1.5 %

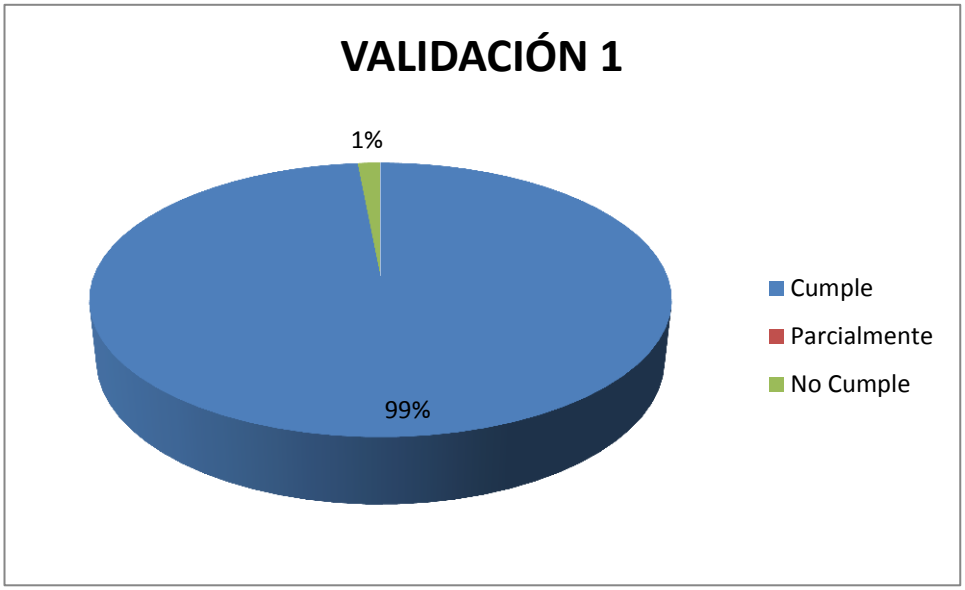

Figura 51. Resultados de validación 1 usuarios

Al realizar un análisis de los resultados, se obtuvo que el 98.50 % de usuarios realizó en proceso de autenticación a través del portal cautivo.

VALIDACIÓN 2: Comprobar que al ingresar credenciales incorrectas no deje iniciar sesión.

Cumple= 60

Parcialmente= 0

No Cumple=7

Representado en porcentajes se obtuvieron los siguientes datos que se muestran en la tabla XLI.

TABLA XLI

Resultados validación 2 usuarios

VALORACIÓN	PORCENTAJE
Cumple	89.55 %
Parcialmente	0 %
No Cumple	10.45 %

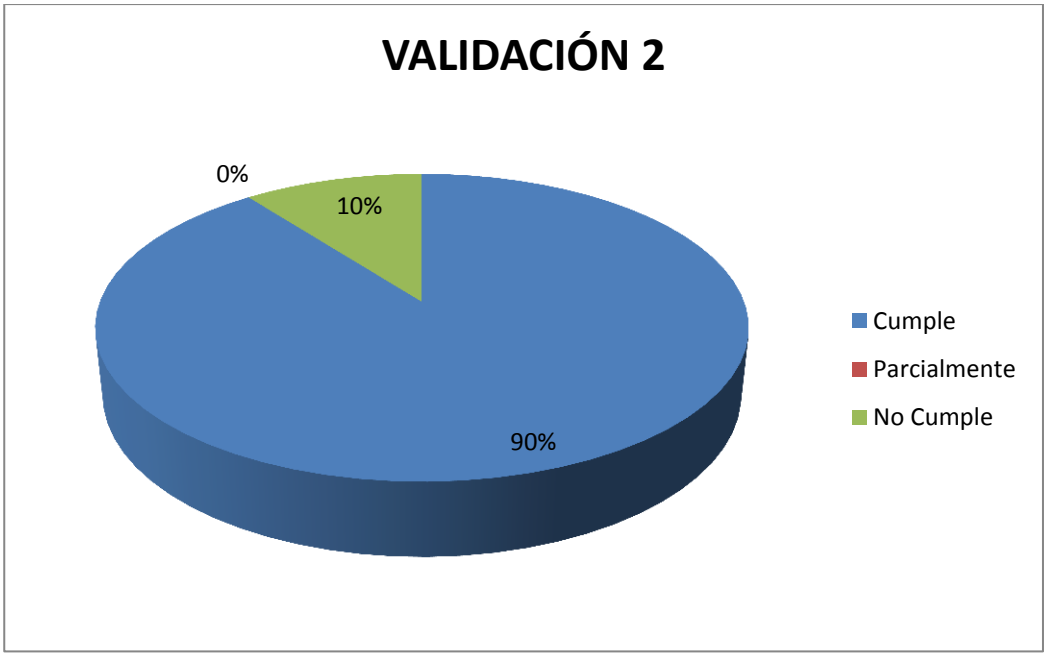

Figura 52. Resultados validación 2 usuarios

Al realizar un análisis de los resultados, se obtuvo que el 89.55 % de usuarios comprobó que al ingresar credenciales incorrectas no se permite la autenticación. El principal inconveniente que encontraron los usuarios es que el navegador no mostraba la opción de cerrar sesión (pop up bloqueado) razón por la cual no podían cerrar sesión e intentar con credenciales incorrectas.

NAVEGACIÓN 1: Navegación sin contratiempos luego de iniciar sesión

Cumple= 60

Parcialmente= 5

No Cumple= 2

Representado en porcentajes se obtuvieron los siguientes datos que se muestran en la tabla XLII.

TABLA XLII

Resultados navegación 1 usuarios

VALORACIÓN	PORCENTAJE
Cumple	89.55 %
Parcialmente	7.46 %
No Cumple	2.98 %

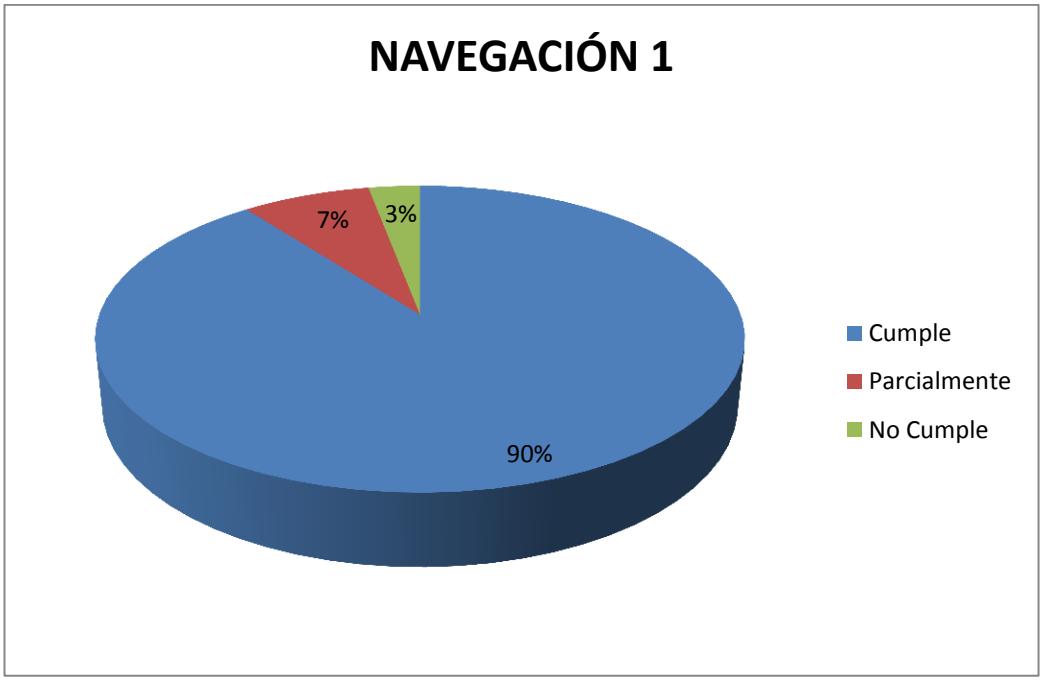

Figura 53. Resultados navegación 1 usuarios

Al realizar un análisis de los resultados, se obtuvo que el 89.55 % de usuarios navegó en internet sin inconvenientes. El principal inconveniente fue que, al no encontrarse en un área de cobertura inalámbrica suficientemente buena existe pérdida de paquetes.

NAVEGACIÓN 2: Descarga correcta de archivos luego de iniciar sesión

Cumple= 56

Parcialmente= 4

No Cumple= 7

Representado en porcentajes se obtuvieron los siguientes datos que se muestran en la tabla XLIII.

TABLA XLIII

Resultados navegación 2 usuarios

VALORACIÓN	PORCENTAJE
Cumple	83.58%
Parcialmente	5.97 %
No Cumple	10.44 %

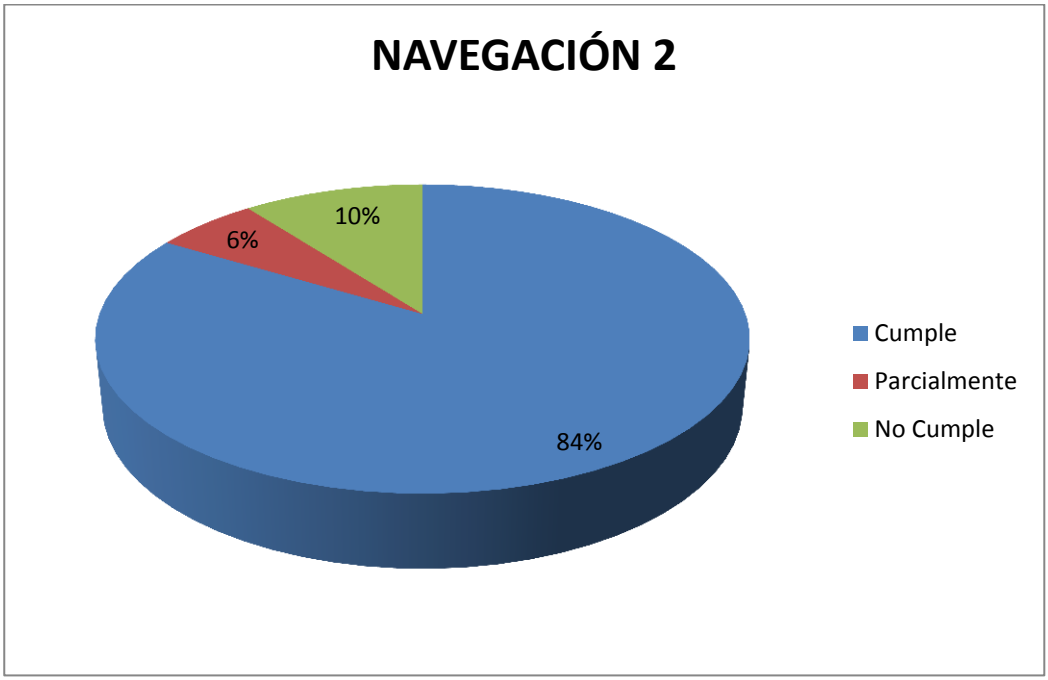

Figura 54. Resultados navegación 2 usuarios

Al realizar un análisis de los resultados, se obtuvo que el 83.58 % de usuarios realizó descarga de archivos de manera correcta. El principal inconveniente fue que, al no encontrarse en un área de cobertura inalámbrica suficientemente buena existe pérdida de paquetes.

2. VALORACIÓN TÉCNICA ECONÓMICA AMBIENTAL

2.1. Valoración técnica económica

El desarrollo del presente PFC desde el punto de vista técnico, es factible puesto que es una necesidad dentro de la administración de la red de datos de la Universidad Nacional de Loja, ya que al ser un sistema de seguridad, se controla que únicamente las personas autorizadas puedan hacer uso del servicio de internet. Así también el software implementado fue de fácil configuración y la interfaz gráfica que se usa para el portal cautivo es de fácil manejo y amigable al usuario. La herramienta web de administración del servidor RADIUS es completamente configurable y se adapta a los requerimientos del servidor RADIUS.

Económicamente el proyecto también se ha considerado factible porque la Universidad cuenta con el hardware que cumple con todas las especificaciones técnicas para el buen funcionamiento del servidor RADIUS, además todos los programas que se utilizan poseen licencias libres y el sistema operativo también cuenta con licencias de software libre.

Por lo antes mencionado se concluye que fue totalmente factible la ejecución del proyecto cumpliendo con los objetivos planteados al inicio de la investigación. Los materiales utilizados para el desarrollo del proyecto se detallan a continuación:

TABLA XLIV

Valoración económica de recursos humanos

Recursos Humanos				
Recursos	Cantidad	Horas c/u	Costo / Hora	Costo Total
Director de Tesis (Docente de la Carrera de Ingeniería en sistemas de la UNL)	1	100	7	$700.00
Investigadores	2	1920	5	$9,600.00
Asesores Unidad de Telecomunicaciones e Información	3	100	5	$ 500.00
Asesor externo con conocimientos en RADIUS	1	10	$ 20.00	$ 200.00
SUBTOTAL				**$ 1,1000.00**

TABLA XLV

Valoración Económica de Recursos Materiales

Recursos Materiales	
Recurso	**Costo Total**
Resmas de papel	$ 20.00
Tinta para impresora	$ 50.00
Empastados	$ 50.00
Discos Compactos	$ 10.00
SUBTOTAL	**$ 130.00**

Recursos Técnicos y Tecnológicos

TABLA XLVI

Valoración Económica de Hardware

HARDWARE		
Recurso Tecnológico	**Cantidad**	**Costo Total**
Computador personal	2	$ 0.00
Impresora	1	$ 0.00
Servidor	1	$ 400.00
Puntos de Acceso para pruebas (DLink DAP 1360)	4	$ 320.00
SUBTOTAL		$ 720.00

TABLA XLVII

Valoración Económica de Software

SOFTWARE	
Recurso	**Costo Total**
FreeRADIUS	$ 0.00
Coovachilli	$ 0.00
radLogin	$ 0.00
Ubuntu 12.04	$ 0.00
DIA	$ 0.00
OpenOffice	$ 0.00
SUBTOTAL	$ 0.00

TABLA XLVIII

Valoración Económica de Comunicaciones

COMUNICACIONES			
Recurso	**Cantidad**	**Costo / Mes**	**Costo Total**
Celular	2 (12 meses)	$ 10.00	$ 240.00
Internet	2 (12 meses)	$20.00	$ 480.00
SUBTOTAL			**$720.00**

TABLA XLIX

Valoración Económica Técnica y Tecnológica

RECURSOS TÉCNICOS Y TECNOLÓGICOS	
Descripción	**Costo Total**
Hardware	$ 720.00
Software	$ 0.00
Comunicaciones	$ 720.00
SUBTOTAL	**$ 1440.00**

TABLA L

Aproximación del Costo Real del Proyecto

SUBTOTALES	VALOR
Subtotal Recursos Humanos	$ 1100.00
Subtotal Recursos Materiales	$ 130.00
Subtotal Recursos Técnicos y Tecnológicos	$ 1440.00
SUBTOTAL	$ 2670.00
IMPREVISTOS 10%	$ 267.00
TOTAL	**$ 2937.00**

2.2. Valoración Ambiental

Es factible porque los equipos utilizados para la implementación del presente proyecto se encuentran ubicados en una zona adecuada dentro de la Unidad de Telecomunicaciones e Información, de tal forma que no afecta al medio ambiente.

G. DISCUSIÓN

DESARROLLO DE LA PROPUESTA ALTERNATIVA

Al haber culminado con el desarrollo del presente proyecto fin de carrera es importante realizar una evaluación de todos los objetivos planteados y determinar si se ha logrado cumplir con cada uno de ellos, lo cual se detalla a continuación:

- **Objetivo Especifico 1:** Realizar el análisis de la situación actual de la red de la UNL para determinar los problemas reales de seguridad informática que atraviesa nuestra institución.

  La primera fase que corresponde a determinar como se encuentra en la actualidad la red de datos de la universidad se la llevó a cabo aplicando algunas técnicas de investigación como lo es la entrevista a los especialistas de la Unidad de Telecomunicaciones e Información. Del mismo modo aplicando la técnica de la observación directa se obtuvo una idea general de los equipos de networking con los que cuenta actualmente la Universidad ver anexo 9. Luego de haber realizado estas actividades se procedió a realizar diseños de la red de datos y de la ubicación y distribución de los puntos de acceso inalámbricos (*Ver sección resultados apartado 1.1 FASE 1: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL*).

  El alcance de este objetivo fue laborioso debido a la gran cantidad de información recolectada y privada lo que hizo de esta fase una de las más complicadas en la organización y estructuración del contenido.

- **Objetivo Especifico 2:** Implantar y Configurar un servidor RADIUS en la Unidad de Telecomunicaciones e Información con la utilización de FreeRADIUS para el acceso inalámbrico a la red de la Universidad Nacional de Loja.

  Para el desarrollo de esta etapa se procedió a la recolección de la documentación apropiada y se hizo uso de la técnica de la lectura comprensiva lo cual permitió conocer las especificaciones técnicas y requisitos para la implementación del servidor RADIUS (*ver sección resultados apartado 1.2.1.Análisis de las características del servidor a adquirir*).

El desarrollo y cumplimiento de este objetivo se logró mediante la colaboración de las personas que laboran en la unidad de telecomunicaciones e información que facilitaron el equipo donde se instaló y configuró el servidor RADIUS. Es importante mencionar que el proceso de configuración del servidor fue progresivo y con algunas dificultades técnicas leves que se resolvieron durante el proceso de aprendizaje.

- **Objetivo Especifico 3:** Garantizar el acceso a la red a través de los puntos de acceso mediante la autenticación de cada usuario con un portal cautivo.

  Para lograr este objetivo se hizo un análisis para la selección de un portal cautivo que cumpla con los requerimientos del servidor RADIUS, (*ver sección resultados apartado 1.2.10. Análisis del portal cautivo a elegir*) lo que permitió escoger a CoovaChilli, ya que una de sus ventajas más importantes es que es de código abierto y se acopla con todas las características del servidor RADIUS.

  Es importante resaltar que en el alcance de este objetivo hubieron complicaciones con respecto a la compatibilidad de CoovaChilli con la distribución que en un inicio fue Centos 5 la cual tuvo que ser cambiada a Ubuntu Server 12.04, este proceso permitió conocer alguna de las dificultades al elegir sobre que plataforma iba a funcionar el conjunto de software que conforman al sistema de seguridad.

- **Objetivo Especifico 4:** Implementar una aplicación web que lleve un registro de la ocupación del sistema, que sea una solución modular y permita monitorear la utilización del ancho de banda.

  En esta fase del proyecto fin de carrera se procedió a la selección de la aplicación web DaloRADIUS la cual trae una interfaz grafica amigable para la configuración del servidor RADIUS y administración de la misma (*ver sección resultados apartado 1.3. FASE 3: IMPLEMENTACION DE LA APLICACIÓN WEB PARA LA ADMINISTRACIÓN DEL SERVIDOR RADIUS*).

Durante la utilización de la herramienta web para la administración del servidor RADIUS hubo algunos problemas en la visualización de algunos registros los que se llegó a solucionar a través de la investigación realizada.

- **Objetivo Especifico 5:** Realizar pruebas de validación y autentificación de usuarios de la red de la Universidad Nacional de Loja a través de los puntos de acceso inalámbricos.

  Se procedió a realizar la autenticación a los usuarios en un escenario de pruebas, donde estudiantes, tesistas, técnicos, y otros usuarios de la Unidad de Telecomunicaciones e Información y de la Biblioteca del AEIRNNR procedieron a utilizar el portal cautivo. También se realizó las respectivas encuestas para comprobar el buen funcionamiento del portal cautivo y de la herramienta web de administración del servidor RADIUS (*Ver sección resultados apartado 1.4.3. Escenario de pruebas*).

  El cumplimiento de este objetivo no tuvo contratiempos debido a la apertura de las personas que laboran en la biblioteca del AEIRNNR y la colaboración de los usuarios que se acoplaron rápidamente al proceso de autenticación a través de la página de autenticación, permitiendo así medir el funcionamiento del sistema de seguridad.

H. CONCLUSIONES

- Con la presente solución se logró implantar un Sistema de seguridad en la unidad de telecomunicaciones e información para el acceso inalámbrico a la red de la Universidad Nacional de Loja utilizando software libre el cual permite controlar de manera efectiva el acceso a los recursos de la red, lo que se pudo constatar mediante las pruebas de validación realizadas en la biblioteca del AEIRNNR. Este sistema es totalmente adaptable y configurable cuando la Universidad Nacional de Loja implemente una red inalámbrica.

- La solución propuesta al implantar un servidor RADIUS con el uso de un portal cautivo es una alternativa eficiente ya que permite controlar el acceso a personal no autorizado a la red de la Universidad Nacional de Loja. Además consume recursos disponibles actualmente, como el Web Services del Sistema de Gestión Académico.

- Realizar el análisis de la situación actual de la red de datos apoyada de técnicas y métodos científicos ayudó a encontrar las falencias en cuanto a la seguridad en el acceso inalámbrico lo que permitió aplicar la solución adecuada.

- Con la implantación del portal cautivo se logró interceptar todo el tráfico de internet y hacer más amigable el proceso de autenticación por parte de los usuarios, además de tener mayor seguridad al usar HTTPS en el momento de acceder. Al utilizar certificados de seguridad ssl en el inicio de sesión, se proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía protegiendo así la clave del usuario.

- Para que el personal de la Unidad de Telecomunicaciones e Información pueda tener una administración amigable se implementó una aplicación Web, la cual permite llevar un registro de la ocupación del sistema, administración de usuarios y adicionalmente permite monitoreo de la utilización del ancho de banda.

- La realización de pruebas de validación del sistema de seguridad en escenarios reales permitió que los usuarios se habitúen al uso de certificados de seguridad, activación de ventana emergente del navegador. Obteniendo así una adecuada adaptación al sistema de seguridad implantado.

I. RECOMENDACIONES

- Previa a la instalación y configuración de herramienta de software, analizar la compatibilidad del Sistema Operativo con las aplicaciones escogidas y con las librerías adicionales que se vaya a utilizar, tomando en cuenta que el portal cautivo CoovaChilli versión 1.2.6 no funciona correctamente en la distribución de Centos 5.

- Realizar una evaluación técnica detallada es importante para la selección de la alternativa de software que mejor se acople a las necesidades y requerimientos del PFC, ya sea privativa o libre.

- Utilizar tipos de autenticación del protocolo EAP que garanticen la seguridad de todo el tráfico en la red, ya que el **EAP-MD5 CHAP** que se utilizó en este proyecto fin de carrera no es adecuado por que requiere que las contraseñas se almacenen de forma que se puedan descifrar.

- La Unidad de Telecomunicaciones e Información debería implementar políticas de seguridad para un correcto funcionamiento de todos los aspectos fundamentales de las secciones que pertenecen a la misma.

J. BIBLIOGRAFÍA

Referencias Bibliográficas

[1] GUZMÁN, Norma. Modelo e Infraestructura de Seguridad basado en Identificación y Autentificación para Redes. Distrito Federal. México. 2011. Tesis para obtener el grado de: Maestro en Ciencias en Ingeniería de Telecomunicaciones.

[2] LUQUE, Jorge. Diseño e Implementación de un Sistema de Autenticación, Autorización y Acceso a una Red Inalámbrica vía FreeRADIUS y Active Directory. Distrito Federal. México. 2011. Tesis para obtener el grado de: Maestro en Ciencias en Ingeniería de Telecomunicaciones.2004. Ingeniería Informática.

[3] RUBIO, Esteban de la Fuente. Redes Inalámbricas - Laboratorio de Seguridad. 2012.

[4] MÁRQUEZ, Alonso; VADILLO, Fanny; GARCÍA, Santiago; LING, Sergio; ZORRILLA, Paulette; PINEDA, Luis; PELÁEZ, Gustavo. RADIUS (Remote Access Dial-in User Service). Monterrey. México. 2007.

[5] BARRIOS, Joel. Configuración básica de Freeradius con soporte de LDAP. http://www.alcancelibre.org/staticpages/index.php/como-freeradius-basico. 2012.

[6] Servidor FreeRadius. http://cayu.com.ar/wiki/doku.php?id=manuales:servidor_freeradius. 2012.

[7] SOLANO, Johanna. OÑA, Mercedes. Estudio de Portales Cautivos de Gestión de Acceso Inalámbrico a Internet de la ESPOCH. Riobamba. Ecuador. 2009. Tesis de grado previa a la obtención del título de Ingeniero en Sistemas Informáticos.

[8] CRUZ, David. Diseño e Implementación de un Portal Cautivo que permita la Venta de Tickets de Internet para un Hotspot, empleando Herramientas de Software Libre. Quito. Ecuador. 2011. Proyecto previo a la Obtención del Título de Ingeniero en Electrónica y Redes de Información.

[9] CoovaChilli. http://coova.org/CoovaChilli. 2012.

[10] MENDOZA, Diego. Análisis Para El Diseño De Una Red Mesh En La Universidad Nacional De Loja Y Su Implementación En Administración Central. Loja. Ecuador. 2012. Tesis previa a optar por el grado de Ingeniero en Sistemas.

[11] STALLMAN, Richard M. Software libre para una sociedad libre. Diciembre 2004. Versión 1.0.

K. ANEXOS

ANEXO 1.

CERTIFICACIÓN

UNIVERSIDAD NACIONAL DE LOJA
UNIDAD TELECOMUNICACIONES E INFORMACIÓN

ING. MILTON PALACIOS

C E R T I F I C A:

Que se ha implementado en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja un servidor de seguridad para el acceso inalámbrico de la red, el mismo que es parte para dar cumplimiento con un objetivo del proyecto de investigación que titula **"Implantación de un Sistema de Seguridad para el Acceso Inalámbrico a la Red de la Universidad Nacional de Loja utilizando software libre"** de los egresados Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo aspirantes a obtener el Título de Ingeniero en Sistemas. Este proyecto fue desarrollado en los términos que fue planteado en la propuesta, y actualmente se encuentra prestando el servicio de acceso inalámbrico mediante el servidor RADIUS utilizando un portal cautivo bajo CoovaChilli en la Unidad antes mencionada.

Es cuanto puedo certificar en honor a la verdad.

Loja, 13 de septiembre de 2012

Lo certifica,

Ing. Milton Palacios M.
DIRECTOR TELECOMUNICACIONES E INFORMACIÓN

UNIVERSIDAD NACIONAL DE LOJA
JEFATURA DE INFORMATICA

Tnlgo. Daniel Reyes T.
RESPONSABLE SECCIÓN REDES

ANEXO 2.

ENTREVISTA N°1

Dirigida a: Ing. Milton Palacios – Director de la UTI – UNL

Fecha: 2011-10-13

Cuestionario:

1. ¿Cómo afecta a la red de la UNL la falta de control de los usuarios que se conectan a los puntos de acceso inalámbricos?

Afecta mucho en control de contenido que realizan los estudiantes así como no se puede identificar que usuarios navegan por los diferentes sitios de la web. Así mismo tenemos una disminución del ancho de banda por la gran cantidad de computadores conectados a los diferentes wireless.

2. ¿Cree usted que beneficiaría la implantación de una página de autenticación para los puntos de acceso inalámbricos de la red de la UNL? ¿Cómo?

En el control de usuarios que acceden a la red, y se sabrán exactamente la información necesaria de las actividades que realiza el estudiante.

3. Reglas y políticas del acceso al internet de los usuarios y con qué criterio se escogieron dichas reglas y políticas.

Por ser la primera semana en la que mi persona está al frente de la Unidad de Telecomunicaciones, estoy poniéndome al tanto de todas las políticas para el acceso al internet por parte de los usuarios. Pero cabe recalcar que estas políticas y reglas son muy importantes porque así contribuiremos a un desarrollo adecuado del consumo de internet y formaríamos una cultura en el uso del internet.

ANEXO 3.

ENTREVISTA N°2

Dirigida a: Tnlg. Daniel Reyes– Encargado de la Sección Redes - UTI – UNL

Fecha: 2011-10-13

Cuestionario:

1. ¿Cuáles son los problemas de seguridad más sobresalientes que existen cuando los usuarios se conectan a los puntos de acceso inalámbrico?

- Duplicidad de ip´s
- Software q vulnera los proxy

2. Marca y características de los puntos de acceso

Dwl-2100ap marca DLINK

3. ¿Cuántos usuarios se conectan diariamente a los puntos de acceso inalámbrico de la red de la UNL?

784 usuarios

4. ¿Cuáles son las políticas de uso y mecanismos de restricción para los usuarios que la Universidad tiene?

- Control de contenido a través de dansguardian
- Control de puertos a través de iptables

5. ¿Cuántos tipos de usuario tiene la UNL y cuáles son los privilegios de cada tipo de usuario?

- Estudiantes con control de contenido a través de dansguardian
- Dirección de telecomunicaciones sin restricción y salida directa a través de firewall
- Usuarios con permisos especiales a través de excepción del dansguardian

ANEXO 4.

ENTREVISTA N°3

Dirigida a: Ing. Patricio Valarezo – Encargado de la Sección Desarrollo de Software - UTI – UNL

Fecha: 2011-10-13

Cuestionario:

1. ¿Cuantos Usuarios Tiene la Base de Datos del SGA?

El sistema de gestión registra a la fecha 64164 usuarios, de los cuales: 63221 son estudiantes registrados, matriculados, egresados, 1207 docentes activos, contratados y 943 administrativos.

2. Políticas del Web Service del SGA

Si son políticas para el uso del webservice, no se han especificado realmente, puesto que no ha existido abuso del sistema, por otro lado, el WebService soporta lo que soporte el hardware directamente, la mayoría de llamadas se realizan por autenticación. Desde el punto de vista administrativo, se tiene como política que se solicite el acceso a los servicios del webservice por medio de un oficio a la dirección de informática o al departamento de desarrollo de software.

3. Políticas de seguridad del departamento del SGA

Nuestra tarea es desarrollar el Software y cuidar los procesos desde el punto de vista de funcionamiento, no es tanto nuestra función la seguridad informática de toda la Unidad de Telecomunicaciones.

Para el SGA exclusivamente se ha creado una red isolada que aísle mediante firewall las redes potencialmente peligrosas, esto como medida precautelar. La construcción de toda la solución tiene como centro la seguridad.

4. ¿Cómo se realiza la solicitud de servicio a través del Web Services?

El webservice esta construido usando el protocolo SOAP, aunque en algunas partes se ha seguido estándares como REST, los datos en su mayoría son retornados usando el formato JSON.

En el sitio oficial del webservice (ws.unl.edu.ec) existe un breve manual de funcionamiento dependiendo de la plataforma.

5. ¿Cree que es factible la adaptación del servidor Radius con el Web Service?

Es posible, sin embargo, un mejor acercamiento sería el uso del SSO (Single Sign On) que es parte del proyecto de migración de Auth de los sistemas del Departamento de Desarrollo de Software usando LDAP.

ANEXO 5.

CUESTIONARIO ADMINISTRADORES
UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía y las Industrias y los Recursos Naturales No Renovables

Instrucciones: Favor sírvase contestar el siguiente cuestionario relacionado con la funcionalidad del servidor RADIUS con el portal cautivo implantado en la Unidad de Telecomunicaciones e Información, responda a las preguntas presentadas a continuación solo marcando una de las opciones entre las representadas en cada apartado.

Nombre: …….

Cargo: ……

PERSONAL DE ADMINISTRACIÓN

Elemento que se prueba	Descripción de la funcionalidad	Descripción del caso de prueba	No Cumple	Parcialmente	Cumple	Observaciones
Validación	Ingreso a la interfaz de administración de RADIUS.	Verificar que se pueda ingresar a la interfaz de administración				
	Ingreso a la interfaz de administración de RADIUS.	Comprobar que al ingresar credenciales incorrectas no deje ingresar.				
Administración	Administración de usuarios.	Permitir ingresar un nuevo usuario en la BD del servidor RADIUS				
	Administración de usuarios.	Permitir modificar un usuario en la BD del servidor				
	Administración de usuarios.	Permitir eliminar un usuario en la BD del servidor RADIUS				
Reportes	Visualización de reportes	Permites ver reportes del servidor RADIUS.				

USUARIOS

Elemento que se prueba	Descripción de la funcionalidad	Descripción del caso de prueba	No Cumple	Parcialmente	Cumple	Observaciones
Validación	Ingreso a través del portal cautivo implantado	Verificar que se pueda iniciar sesión luego de ingresar las credenciales correctas				
	Ingreso a través del portal cautivo implantado	Comprobar que al ingresar credenciales incorrectas no deje iniciar sesión.				
Navegación	Navegación	Navegación sin contratiempos luego de iniciar sesión				
	Navegación	Descarga correcta de archivos luego de iniciar sesión				

Firma: _____

ANEXO 6.

CUESTIONARIO USUARIOS

UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía y las Industrias y los Recursos Naturales No Renovables

Instrucciones: Favor sírvase contestar el siguiente cuestionario relacionado con la funcionalidad del servidor RADIUS con el portal cautivo implantado en la Unidad de Telecomunicaciones e Información, responda a las preguntas presentadas a continuación solo marcando una de las opciones entre las representadas en cada apartado.

Nombre: …….

Elemento que se prueba	Descripción de la funcionalidad	Descripción del caso de prueba	No Cumple	Parcialmente	Cumple	Observaciones
Validación	Ingreso a través del portal cautivo implantado	Verificar que se pueda iniciar sesión luego de ingresar las credenciales correctas				
	Ingreso a través del portal cautivo implantado	Comprobar que al ingresar credenciales incorrectas no deje iniciar sesión.				
Navegación	Navegación	Navegación sin contratiempos luego de iniciar sesión				
	Navegación	Descarga correcta de archivos luego de iniciar sesión				

Firma: _____

ANEXO 7.

PRUEBAS REALIZADAS EN LA BIBLIOTECA DEL AEIRNNR

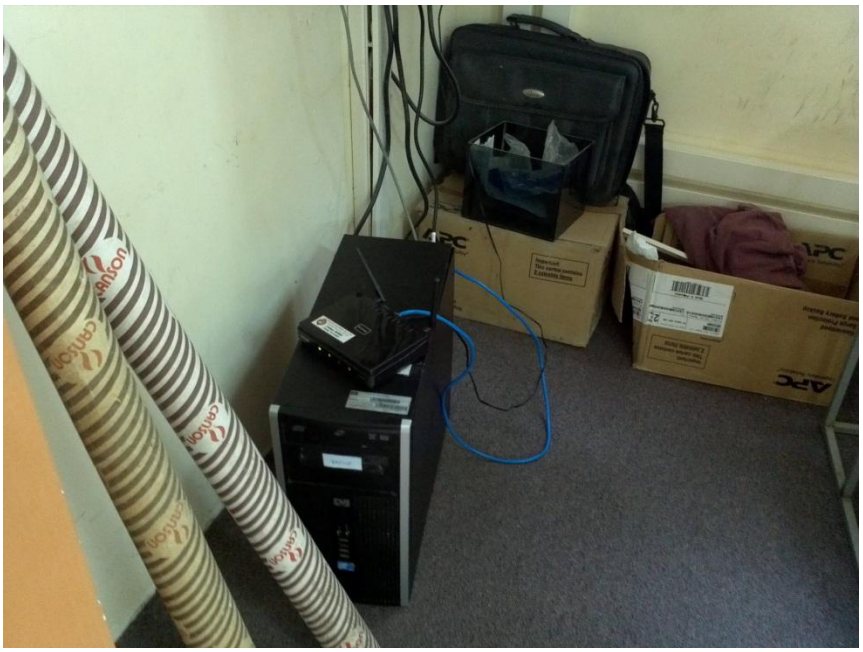

Figura 55. Ubicación del servidor RADIUS

Figura 56. Estudiantes del AEIRNNR

Figura 57. Selección del SSID SIRadius

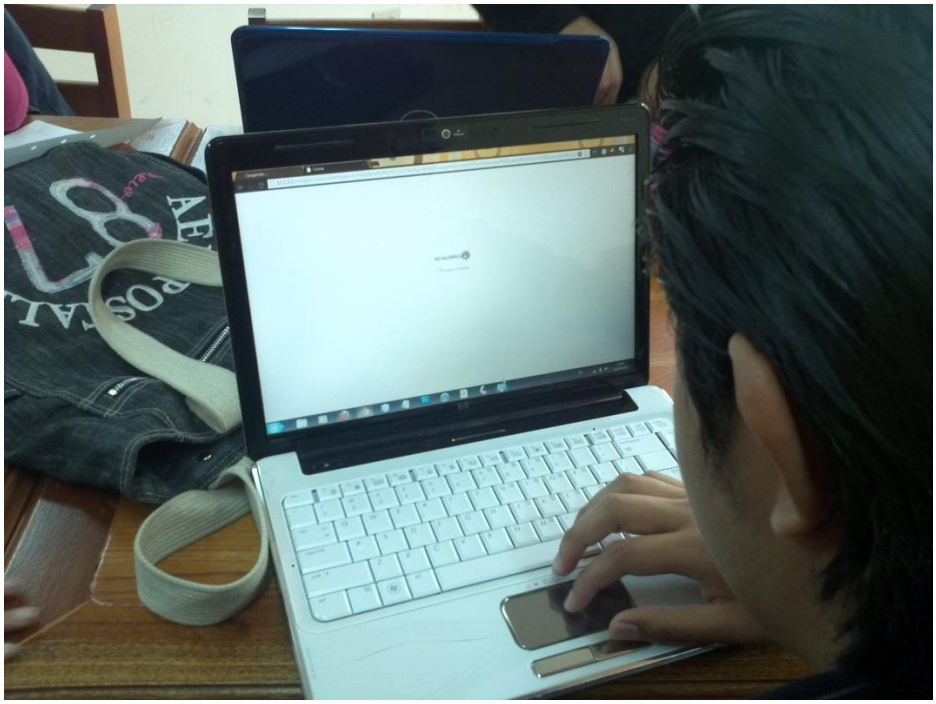

Figura 58. Captura del trafico Http del portal cautivo

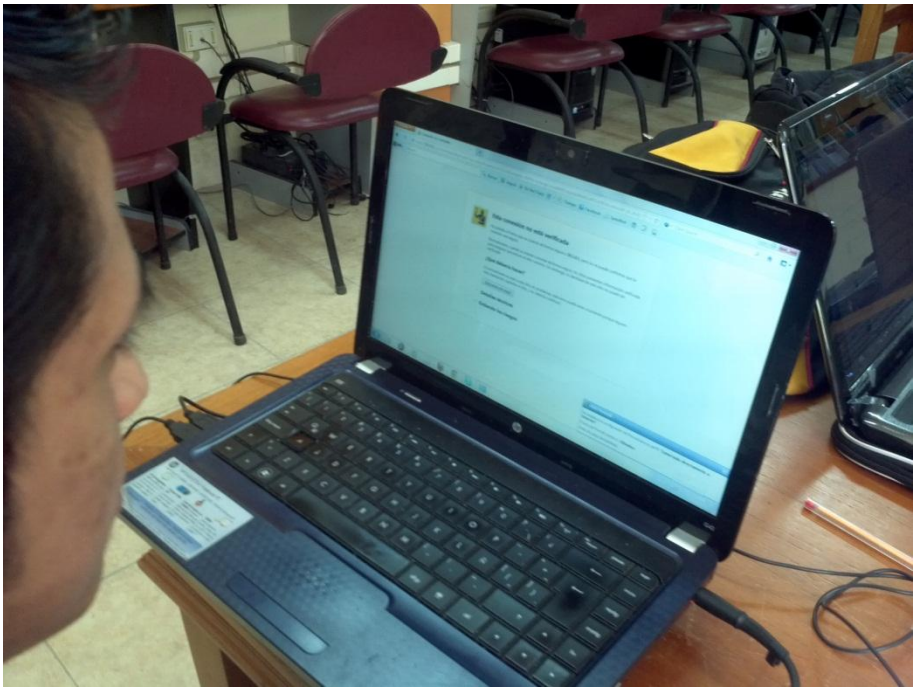

Figura 59. Aceptación de Certificados de Seguridad

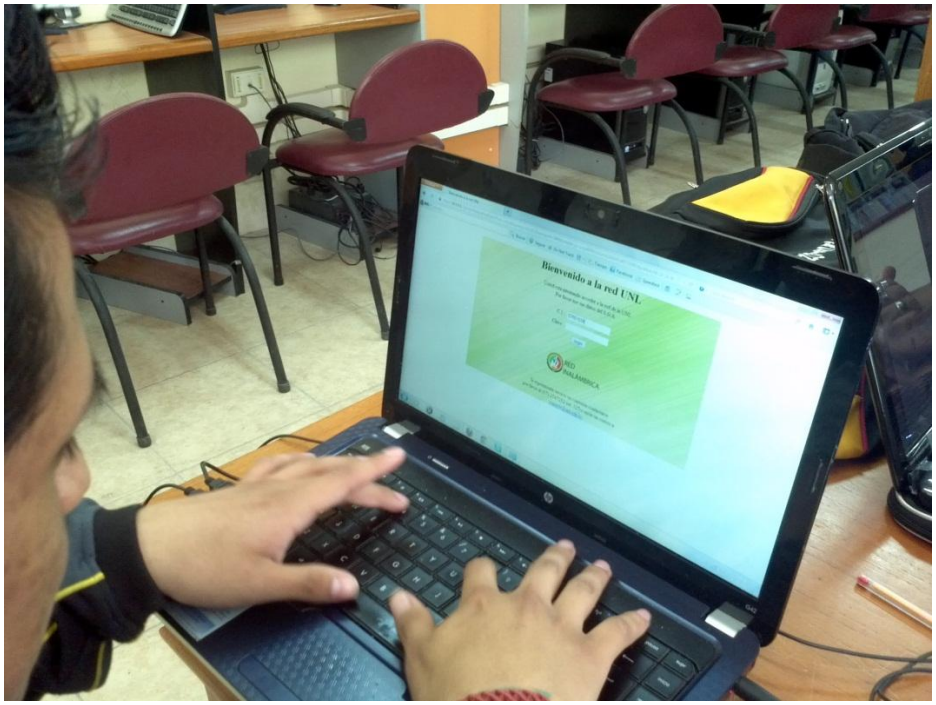

Figura 60. Ingreso de Credenciales (Cédula de Identidad y Contraseña SGA)

Figura 61. Usuarios utilizando el portal cautivo.

ANEXO 8.

GNU General Public License

La Licencia Pública General de GNU pretende garantizar la libertad de compartir y modificar software libre para asegurar que el software es libre para todos sus usuarios. Esta Licencia Pública General se aplica a la mayor parte del software de la Free Software Foundation y a cualquier otro programa si sus autores se comprometen a utilizarla [11].

Cuando hablamos de software libre, estamos refiriéndonos a la libertad, no al precio. Nuestra Licencia Pública General está diseñada para asegurarnos de que tenga la libertad de distribuir copias de software libre —y cobrar por ese servicio si quiere—, de que reciba el código fuente o de que pueda conseguirlo si así lo desea, de que pueda modificar el software o utilizar fragmentos del mismo en nuevos programas libres, y de que sepa que puede hacer todas estas cosas [11].

Para proteger sus derechos, necesitamos algunas restricciones que prohíban negarle a usted estos derechos o pedirle que renuncie a ellos. Estas restricciones se traducen en ciertas obligaciones que le afectan si distribuye copias del software, o si modifica software [11].

Por ejemplo, si distribuye copias de uno de estos programas, ya sea gratuitamente, o a cambio de unos honorarios, debe dar a los receptores todos los derechos que posee. Debe asegurarse de que ellos también reciben, o pueden conseguir, el código fuente. Y debe mostrarles estas condiciones de forma que conozcan sus derechos [11].

Protegemos sus derechos por medio de la combinación de dos medidas: (1) ponemos el software bajo copyright y (2) le ofrecemos esta licencia, que le da permiso legal para copiar, distribuir y/o modificar el software [11].

También, para proteger a cada autor y a nosotros mismos, queremos asegurarnos de que todo el mundo comprende que no se proporciona ninguna garantía para este software libre. Si el software es modificado y distribuido, queremos que sus receptores sepan que lo que tienen no es el original, de forma que cualquier problema introducido por otros no afecte a la reputación de los autores originales [11].

Por último, cualquier programa libre está constantemente amenazado por las patentes de software. Queremos evitar el peligro de que los distribuidores de un programa libre

lo patenten por su cuenta, convirtiendo así el programa en propietario. Para evitar esto, hemos dejado claro que cualquier patente debe ser registrada para el libre uso, o no ser registrada de ninguna manera [11].

ANEXO 9.

Figura 62. Equipos del Networking principales en el cuarto de telecomunicaciones de la UTI.

Figura 63. Servidores de la UTI 1

Figura 64. Servidores de la UTI 2

Figura 65. Servidores de la UTI 3

ANEXO 10.

CERTIFICACIÓN DE COBERTURA INALÁMBRICA AEIRNNR

UNIVERSIDAD NACIONAL DE LOJA
UNIDAD TELECOMUNICACIONES E INFORMACIÓN

ING. MILTON PALACIOS M.

C E R T I F I C A:

Que el estudio realizado de la Cobertura Inalámbrica en el Are de la Energía, las Industrias y Recursos Naturales no Renovables por los estudiantes Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo dentro del proyecto de tesis " IMPLANTACION DE UN SISTEMA DE SEGURIDAD PARA EL ACCESO INALAMBRICO A LA RED DE LA UNIVERSIDAD NACIONAL DE LOJA UTILIZANDO SOFTWARE LIBRE ha sido revisado y aprobada por parte de la Unidad de Telecomunicaciones.

Es cuanto puedo certificar en honor a la verdad.

Loja, 8 de Noviembre de 2012

Lo certifica,

Ing. Milton Palacios M.
DIRECTOR TELECOMUNICACIONES E INFORMACIÓN

ANEXO 11.

DECLARACIÓN DE CONFIDENCIALIDAD

Lisset Alexandra Neyra Romero y Fabricio Alejandro Flores Gallardo (en adelante: "los declarantes"), con C.I. 0702913708 y 1104015936 respectivamente DECLARAN lo siguiente:

PRIMERO: Antecedentes

1) Los declarantes van a participar o han participado en el proyecto de fin de carrera "Implantación de un sistema de seguridad para el acceso inalámbrico a la red de la Universidad Nacional de Loja utilizando software libre", dirigido por Ing. Juan Manuel Galindo Vera, en calidad de director del proyecto.

2) Por el presente documento se regula el tratamiento que los declarantes han de dar a la información a la que pueda tener acceso en el desarrollo de las tareas de investigación que se realicen en dicho proyecto, el cual se regulará por las disposiciones contenidas en las cláusulas siguientes.

SEGUNDO: Información Confidencial

La información referida a materiales, métodos y resultados científicos, técnicos y comerciales utilizados u obtenidos durante la realización del proyecto de investigación o una vez realizado el mismo, se considerará siempre Información Confidencial.

TERCERO: Excepciones

No será considerada como Información Confidencial:

a) La información que los declarantes pueda probar que tenía en su legítima posesión con anterioridad al conocimiento de la Información Confidencial.

b) La información que los declarantes puedan probar que era de dominio público en la fecha de la divulgación o pase a serlo, con posterioridad, por haberse publicado o por otro medio, sin intervención ni negligencia de los declarantes.

c) La información que dichos declarantes pueda probar que corresponde en esencia a información facilitada por terceros, sin restricción alguna sobre su divulgación, en virtud de un derecho de los declarantes a recibirla.

CUARTO: Secreto de la Información Confidencial

Los declarantes se comprometen a mantener totalmente en secreto la Información Confidencial recibida en relación con el proyecto referido anteriormente y no divulgarla a terceros durante la vigencia de esta Declaración de Confidencialidad.

Asimismo, los declarantes se comprometen a emplear la Información Confidencial, exclusivamente, en el desempeño de las tareas que tenga encomendadas en dicho proyecto.

QUINTO: Duración

La obligación de los declarantes respecto al mantenimiento del compromiso de secreto de la Información Confidencial, será indefinido para fines de investigación a partir de la fecha de la recepción de la Información Confidencial.

Loja, 8 de noviembre de 2012

Lisset Alexandra Neyra Romero

Fabricio Alejandro Flores Gallardo

ANEXO 12.

ANTEPROYECTO