DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

IMPLEMENTACIÓN DE UN PLAN PILOTO DE SEGURIDAD BAJO EL PROTOCOLO IEEE 802.1X PARA EL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA DEL MINISTERIO DE TELECOMUNICACIONES Y SOCIEDAD DE LA INFORMACIÓN

MARCO PATRICIO PAREDES SAMANIEGO

SANGOLQUÍ – ECUADOR

2013

CERTIFICACIÓN

Certificamos que le presente proyecto de grado titulado: **IMPLEMENTACIÓN DE UN PLAN PILOTO DE SEGURIDAD BAJO EL PROTOCOLO IEEE 802.1X PARA EL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA DEL MINISTERIO DE TELECOMUNICACIONES Y SOCIEDAD DE LA INFORMACIÓN**, ha sido desarrollado en su totalidad por el señor MARCO PATRICIO PAREDES SAMANIEGO, bajo nuestra dirección.

Atentamente

_____	_____
ING.MARCELO URBINA	ING. NIKOLAI ESPINOSA
DIRECTOR	**CODIRECTOR**

AUTORÍA DE RESPONSABILIDAD

MARCO PATRICIO PAREDES SAMANIEGO

DECLARO QUE:

El proyecto denominado **"IMPLEMENTACIÓN DE UN PLAN PILOTO DE SEGURIDAD BAJO EL PROTOCOLO IEEE 802.1X PARA EL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA DEL MINISTERIO DE TELECOMUNICACIONES Y SOCIEDAD DE LA INFORMACIÓN"**, ha sido desarrollado en base a una investigación exhaustiva, respetando los derechos intelectuales de terceros conforme a las fuentes que se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud a esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 07 de Septiembre del 2013

Marco Patricio Paredes Samaniego

AUTORIZACIÓN

MARCO PATRICIO PAREDES SAMANIEGO

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la institución del trabajo **"IMPLEMENTACIÓN DE UN PLAN PILOTO DE SEGURIDAD BAJO EL PROTOCOLO IEEE 802.1X PARA EL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA DEL MINISTERIO DE TELECOMUNICACIONES Y SOCIEDAD DE LA INFORMACIÓN"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 07 de Septiembre del 2013

Marco Patricio Paredes Samaniego

DEDICATORIA

Primero a Dios y mi madre Dolorosa que ha hecho que todo salga como lo esperaba por darme todas las facilidades para realizar este proyecto, la paciencia necesaria para todos lo que me ayudaron a culminar la tesis y por haberme brindado la fortaleza y guía necesaria.

A mis padres que gracias a ellos puedo llegar a culminar mi carrera, gracias por darme todo su apoyo pese a todas mis fallas ustedes nunca me abandonaron en este camino, me dieron las fuerzas para cada día luchar por este objetivo que ahora es nuestro, Mamita mil gracias por tu sacrificio que lo valoro mucho y soportarme cada día, ser mi consuelo mi amiga y nunca dejar de preocuparte, a ti Papito que me has enseñado a luchar y sacrificarme por cada propósito de mi vida, por ser un ejemplo de esfuerzo y superación.

A todos mis familiares que cada día se preocuparon de mí y me dieron todo su apoyo, que me han brindado muchas lecciones y he podido aprender de cada uno de ustedes valores importantes de superación.

A mis amig@s que en este trayecto me dieron el ánimo necesario para lograr mi objetivo y que siempre estaré para todos como han estado a mi lado, los llevo en mi corazón.

AGRADECIMIENTOS

A Dios que me ha bendecido tanto y me dio los mejores padres y familia del mundo gracias por tantas bendiciones que he tendido y tendré en mi vida a mi madre Dolorosa que desde el día que me consagre la llevo en mi corazón y es mi guía en este camino.

A ti mami Paty y papi Guido gracias por tantos años de sacrificio, por todo el amor que me han dado siempre, cada palabra de motivación, gracias por enseñarme tantos valores y saber que la familia es lo primero como tú dices papi los tres siempre juntos, somos una familia pequeña pero con muchísimo amor, ustedes son el mejor ejemplo que podría tener de superación, esfuerzo y lucha, me han enseñado a no rendirme jamás hasta alcanzar un objetivo, gracias por creer en mí siempre los amo sobre todas las cosas.

Al MINTEL que desde que llegue me ha dado todo su apoyo en especial a personas que me ayudaron a cumplir mi objetivo, Wilson, Jorge, Oswaldo, a mi director ingeniero Marcelo Urbina y codirector ingeniero Nikolai Espinosa.

A mis abuelit@s Pia, Inesita, Clari, Romelia, Antonio por apoyarme cada momento de mi vida, por ser la personas que con amor me han dado una guía y siempre han querido lo mejor para mi vida, ustedes saben lo importantes que son para mi gracias por consentirme tanto.

A Toty y mi ñaño Pepé que nunca se han descuidado de mí, que son mis segundos padres que desde que tengo uso de razón han estado siempre a mi lado con sus acciones, palabras de aliento y enseñarme tantas cosas y querer que sea una gran ser humano los quiero mucho.

A mis ñañas que a la mayoría están lejos que las amo con todo mi corazón y las extraño mucho que gracias por el apoyo incondicional y tratarme como un hijo, ustedes son un ejemplo en mi vida Vero, Mashi, Anita, Pili, Yesy de una u otra forma siempre me han dado fortaleza y consejos para seguir adelante las extraño y tengo un vacío muy grande en mi corazón porque no las tengo a mi lado.

A mis tí@S son lo máximo Edi, Tato, Geovi, Sandra, Fany, son grandes seres humanos ejemplo de superación, responsabilidad gracias por todo su apoyo.

A mis amig@s que cada día compartí muchas experiencias gracias por aguantarme, Moni, Annie, Diana, Llango, Cristian, Diego, Anita son unos bacanes y espero siempre estar a su lado, Mishel gracias mi fea hermosa por ser incondicional conmigo te amo y eres la mejor amiga que alguien puede tener, gracias por tu cariño tus gestos juntos hasta viejos hija de la pelona, Andrea gracias por enseñarme tu más que nadie a valorar las cosas que Dios me ha dado y saber aprovechar todas las oportunidades de mi vida, Xime gracias por tu apoyo eres una bacana, parece que me olvido de alguien Alejo aunque no me dejabas estudiar gracias por estar en todo momento mijo y compartir tantas experiencias juntos eres un gran amigo.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Se realiza un análisis a la seguridad actual a la red del Ministerio de Telecomunicaciones y Sociedad de la Información y en la implementación de un plan piloto de seguridad para el acceso a la red, basándose en el estándar IEEE 802.1X, usando la plataforma Ubuntu 11.04 y herramientas como MYSQL para el manejo de la base de datos y FREERADIUS para el servidor AAA. La configuración del autenticador se realiza en un switch de marca Cisco con IOS 12.04 versión K9 que están a disposición y son compatibles con el estándar, también se indica como configurar los computadores de los usuarios con el sistema operativo Windows en sus versiones XP y 7. Basándose en un análisis preliminar se escogen los métodos de autenticación EAP-MD5 y PEAP como idóneos por la cantidad de usuarios dentro del Ministerio. Para la administración de la red se usan aplicaciones como Daloradius o el gestor actual WhatsApp para brindar control total sobre los recursos de la red.

Palabras claves.- Estándar 802.1X, Servidor AAA, RADIUS, FREERADIUS, Daloradius.

GLOSARIO

AAA: Autorización, Autenticación, Registro de Cuentas

AP: Punto de Acceso

ATM: Modo de Transferencia Asíncrono

CA: Autorización de Certificación

CHAP: Protocolo de autenticación por desafío mutuo

CNT: Corporación Nacional de Telecomunicaciones

CRC: Código de Corrección de Errores

CSMA: Acceso Múltiple con escucha de Portadora

CSMA/CA: Acceso Múltiple con escucha de Portadora, con Prevención de colisión

CSMA/CD: Acceso Múltiple con escucha de Portadora, con detección de colisión

BD: Servidor de Base de Datos

DAP: Protocolo de Acceso a Directorios

DGT: Departamento de Gestión Tecnológica

DIT: Árbol de información de directorio

DHCP: Protocolo de Configuración Dinámica de Máquinas

EAP: Protocolo de Autenticación Extensible

EAPOL: Protocolo de Autenticación Extensible sobre LAN

EAP-TLS: Protocolo de Autenticación Extensible con seguridad a nivel de Transporte

EAP-TTLS: Túnel mediante TLS para transmitir el nombre de usuario y la contraseña.

ETHERNET: Estándar de redes de área local

FDN: FortiProtect Distribution Network

FIREWALL: Sistema diseñado a bloquear acceso no autorizado

FREERADIUS: Servidor Radius

HP: Hewlett-Packard

HTTP: Protocolo de Transferencia de Hipertexto

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos

IMAP: protocolo de aplicación que permite en acceso a mensajes almacenados en un servidor

IP: Protocolo de Internet

IPSEC: Protocolo de Internet seguro

IPX: Intercambio de Paquetes interred

ISP: Proveedor de Servicios de Interne

LAN: Red de Area Local

LDAP: Protocolo Ligero de Acceso a Directorios

LEAP: Protocolo ligero de autenticación extensible

MAC: Control de Acceso al Medio

MD5: Algoritmo de Resumen del Mensaje 5

Mintel: Ministerio de Telecomunicaciones y Sociedad de la Información

MSCHAP: Variante de CHAP creada por Microsoft

MySQL: Sistema de gestión de base de datos relacional, multihilo y multiusuario

NAS: Servidor de Acceso a la Red

OSI: Modelo de referencia de Interconexión de Sistemas Abiertos

PAP: Protocolo de Autenticación de Contraseña

PDA: Asistente Digital Personal

PHPMYADMIN: Herramienta en PHP para manejar Mysql

PSK: Modulación por Desplazamiento de Fase

POE: Alimentación a través de Ethernet

POP3: Protocolo de Oficina de Correo o Protocolo de Oficina Postal

PPP: Protocolo Punto a Punto

QoS: Calidad de Servicio

RA: Campo de dirección del receptor este tiene consigo la dirección MAC

RFC: Request For Comment

RSA: (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública

SQL: Lenguaje de Consulta Estructurado

SENATEL: Secretaria Naciofnal de Telecomunicaciones

SSL: Capa de conexión segura

SW: Switch

TA: Campo de la dirección del transmisor es la dirección MAC

TCP: Protocolo de Control de Transmisión

Telconet: Proveedor de servicios

UBUNTU: Sistema operativo de Linux

UTM: Gestión Unificada de Amenazas

UNIX: Sistema operativo portable, multitarea y multiusuario

URL: Localizador de Recursos Uniforme

UTP: Par trenzado no apantallado **VBR:** Rata de bits de video

VLAN: Red de área Local Virtual

VPN: Red Privada Virtual

WEB: Red Global Mundial

WEP: Privacidad equivalente a Cableado

WIFI: Wireless Fidelity

WIMAX: Interoperabilidad mundial para acceso por microondas

WLAN: Red de área Local inalámbrica

WPA: Acceso Protegido WIFI

CAPÍTULO I

ESTUDIO DE LA IMPLEMENTACIÓN DE UN PLAN PILOTO DE SEGURIDAD BAJO EL PROTOCOLO IEEE 802.1X

1.1 OBJETIVOS

1.1.1 Objetivo General

Diseñar e implementar un plan piloto para la red de acceso del Ministerio de Telecomunicaciones y Sociedad de la información por medio del estándar 802.1X con la finalidad de garantizar la conexión a la red de los funcionarios autorizados, al mismo tiempo que brindamos mayor seguridad a la información que se maneja en la institución.

1.1.2 Objetivos Específicos

- Analizar las políticas a las cuales está sujeta la institución, para de este modo como administrador saber que restricciones debe tener cada departamento y funcionario del mismo.

- Realizar el respectivo estudio a cada uno de los dispositivos a los cuales vamos aplicar el estándar y servicios que necesita la aplicación.

- Implementar la autenticación dada por el estándar 802.1X a la red y realizar el respectivo análisis de la seguridad que este provee tano a nivel de los usuarios como a los administradores de la misma.

- Inspeccionar a los usuarios que acceden a los recursos de la red interna del ministerio para como administradores controlar y tener la mayor eficiencia de la misma.

- Analizar las mejoras que se dan en la seguridad y control de los recursos de la red a partir de la implementación del protocolo de acceso a la red por medio de puertos y comparar con los estudios realizados antes de la implementación del mismo.

- Inspeccionar conjuntamente con el administrador de la infraestructura de la red periódicamente la misma, de esta forma supervisaremos que la herramienta instalada está funcionando de forma óptima dentro de lo establecido.

1.2 DEFINICIÓN DEL PROYECTO

1.2.1 ANTECEDENTES

Los seres humanos somos sociables por naturaleza, necesitamos de la comunicación para mejorar las relaciones, sin embargo esto ha llevado consigo problemas de seguridad con la información que se manipula. A través del tiempo la tecnología ha mejorado en la comunicación y el traslado de la información entre las personas pero con esto también se ha desarrollado las formas para la obtención maliciosa o violación con la privacidad de la misma, pero también existe la evolución en la búsqueda en dar soluciones a estos problemas. Este proyecto se centra en como brindar la seguridad de una red corporativa donde se maneja gran cantidad de información y de usuarios, donde las redes son muy manipulables y tienen gran

cantidad de acceso ilegítimo por el tipo de información que se maneja al ser la institución un ministerio público. Para dar la necesaria confidencialidad, los administradores de la red deben tomar medidas de protección adecuada que permite garantizar a los usuarios un acceso seguro y con la debida privacidad en la información que maneja y comparte cada usuario.

Debido a esta necesidad de asegurar la confidencialidad a los servidores públicos, el Ministerio de Telecomunicaciones y Sociedad de la Información, ha requerido establecer una nueva normativa estándar que permita tanto la autenticación como el intercambio dinámico de contraseñas, de forma fácil y segura.

El estándar que se utilizará viene dado por la IEEE 802.1X, al cual permite implementar un acceso seguro empleando medios de comunicación como Ethernet[1], Token Ring[2] y LANs[3] inalámbricas 802.11[4], lo que hace al mismo compatible con la institución. Este estándar define el control de acceso a redes basadas en puertos, es decir permite la autenticación de dispositivos conectados a un puerto LAN estableciendo una conexión punto a punto o evitando el acceso por ese puerto si la autenticación falla, esto ocurre ya que se apoya en el protocolo de autenticación EAP (Extensible Autentication Protocol, Protocolo de Autenticación Expandible), aunque en realidad es EAPoL[5] (Extensible Autentication Protocolo over LAN, Protocolo de Autenticación Expandible sobre LAN).

[1] Ethernet: Estándar de redes de área local
[2] Token Ring: Arquitectura de red en anillo
[3] LAN: Red de área local

1.2.2 JUSTIFICACIÓN E IMPORTANCIA

El Ministerio de Telecomunicaciones y de la Sociedad de la Información requiere la implementación de un nuevo sistema de autenticación y de seguridad para la administración de la red, para lo cual el departamento de Gestión Tecnológica del Ministerio, quiere basarse en el sistema de acceso por medio del puertos dado por el estándar 802.1X, estableciendo al mismo como el más óptimo para sus necesidades; siendo compatible con la infraestructura de la red actual. Es por esto que se me han requerido trabajar en este proyecto que sería en beneficio de la institución y de la administración de cada uno de los usuarios de una forma más segura de la que se usa actualmente.

Se busca tener un control de acceso más seguro, por el cual se pueda como administrador, identificar, autenticar y autorizar, al mismo tiempo de permitir o denegar el uso de los recursos a la red, también se busca que este estándar permita llevar un registro sobre las vulnerabilidades que se pueden dar a cada uno de los usuarios o a cualquier dispositivo que forma parte de la infraestructura de la red.

Además con el proyecto se asegurará que los recursos de la red sean usados de la forma correcta por el usuario correcto optimizando el ancho de banda de la red entre Gotros recursos de la misma, también se va a trabajar para garantizar la seguridad en la información ya sea de tipo grupal o personal a la que puede acceder y manipular cada uno de los funcionarios de los departamentos que conforman el Ministerio.

1.2.3 ALCANCE DEL PROYECTO

La seguridad general en una red es imposible, lo que se realiza es una mejora continua para adaptar cada dispositivo de la red a métodos y estándares de seguridad que puedan mantener a la red en un nivel de seguridad aceptable de esta manera se reduce los riesgos en la misma a los ataques, si estos métodos son apoyados en políticas

y normas, que tiene la institución sobre el uso de los recursos informáticos, el presente proyecto brindará una seguridad muy confiable a los usuarios. El hecho que la institución posea esquemas de seguridad es imprescindible para proteger la información que circula por la red de la misma.

La implementación del estándar 802.1X controlará a los usuarios que acceden a la red interna de la institución otorgando acceso únicamente al usuario permitido.

Es por esto que se busca implementar un piloto en la red de acceso del Ministerio de Telecomunicaciones y Sociedad de la información por medio del estándar 802.1X, para mejorar la administración de la red lo cual es necesario en el presente de la institución, luego de los estudios pertinentes se busca implantarlo en todo el ministerio para tener un control total de la red, sabiendo que esto puede traer consigo muchos aspectos positivos en la administración, evitando conflictos, amenazas informáticas[6] que se han venido manejando a pesar de los controles que se suelen dar a la misma, el proyecto en un futuro con el debido mantenimiento y correcta administración traerá consigo a más de la confiabilidad de la información el uso óptimo de los recursos de la red.

El requerimiento de la institución es comprobar el correcto funcionamiento del estándar, como plan piloto de manera parcial en el departamento de gestión tecnológico del Ministerio de Telecomunicaciones y la Sociedad de la Información, teniendo en el mismo usuarios conectados de forma alámbrica como inalámbrica.

[4] 802.11: Protocolo de conexión inalámbrica
[5] EAPoL: Protocolo d autenticación extensible sobre LAN
[6] Amenazas informáticas: Vulnerabilidades de la red o de la información

Se debe usar por al menos cinco usuarios, incorporándolos a los componentes necesarios para el proceso de autenticación 802.1X EAP[7], que radica un suplicante, un autenticador como lo es un access point[8] o un switch[9] y un servidor de autenticación FREERADIUS, todo esto unido a infraestructura actual de la institución.

[7] EAP: Protocolo d autenticación extensible
[8] Access Point: Punto de acceso a la red
[9] Switch: Dispositivo para interconectar redes

CAPÍTULO II

ANÁLISIS ACTUAL DE LA RED DE ACCESO A LOS USURIOS DEL MINISTERIO DE TELECOMUNICACIONES Y SOCIEDAD DE LA INFORMACIÓN

2.1 FUNCIONAMIENTO DE LA RED DE ACCESO ACTUAL EN LA INSTITUCIÓN

2.1.1 TECNOLOGÍA

La tecnología de acceso al red del ministerio actualmente se maneja con el estándar LDAP[10] el cual permite administrar a todos los usuarios y acceder a la información de los mismos por medio de la base de datos, también por medio de este podemos administrar el hardware; este protocolo funciona con el protocolo TCP/IP[11].

El objetivo del protocolo LDAP, desarrollando en 1993 en la universidad de Michigan, y salió al mercado en el año de 1995 desplazando al protocolo DAP que su usaba hasta entonces servía para acceder a los servicios de directorio X.500 por OSI LPDA añade al TCP/IP.

[10] LDAP: Protocolo compacto de acceso a directorio
[11] TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet

Este protocolo es independiente y más sencillo al anterior es por esto que toma el nombre de protocolo compacto de acceso a directorios este lo que hace es definir métodos de acceso a los datos por medio del servidor a nivel cliente pero la manera de almacenamiento de la información era la misma. LDAP consta de tres versiones que ha sido estandarizada por la RFC[12].

Las ventajas que permite el protocolo LDAP son:

- Conectarse
- Desconectarse
- Buscar información
- Comparar información
- Insertar entradas
- Cambiar entradas
- Eliminar entradas

La última versión brinda para mayor seguridad mecanismos de cifrado por medio de SSL[13] y otros para su autenticación y la información que tenemos almacenada en la base de datos de la organización.

Estructura de árbol de la información de directorio

LDAP presenta la información bajo la forma de una estructura jerárquica de árbol denominada DIT[14] , en la cual la información, denominada entradas (o incluso DSE, Directory Service Entry), la misma que es representada por las bifurcaciones del

[12] RFC: Solicitud de comentarios
[13] SSL: Protocolo de seguridad de información de usuario
[14] DIT: Árbol de información de directorio

protocolo.

Una bifurcación ubicada en la raíz de una bifurcación se denomina entrada raíz. [1]

Cada entrada en el directorio LDAP corresponde a un objeto abstracto o real (por ejemplo, una persona, un objeto material, parámetros, etc.).

Cada entrada está conformada por un conjunto de pares clave/valor denominados atributos.

- **Atributos de entrada:** Cada entrada está compuesta por un conjunto de atributos (pares clave/valor) que permite caracterizar el objeto que la entrada define. Existen dos tipos de atributos.

- **Atributos normales:** Estos son los atributos comunes (apellido, nombre, etc.) que distinguen al objeto.

- **Atributos operativos**: éstos son atributos a los que sólo el servidor puede acceder para manipular los datos del directorio (fechas de modificación, etc.).

Una entrada se indexa mediante un nombre completo (DN) que permite identificar de manera única un elemento de la estructura de árbol, un DN se constituye tomando el nombre del elemento denominado Nombre distintivo relativo (RDN, es decir, la ruta de la entrada en relación con sus entradas superiores) y agregándole el nombre entero de la principal.

Se trata de utilizar una serie de pares clave/valor para poder localizar una entrada de manera única. [2]

Formatos de intercambio de datos de LDIF

LDAP brinda un formato de intercambio de datos LDIF[15], que permite importar y exportar datos desde un directorio mediante un archivo de texto simple. La mayoría de los servidores LDAP admiten este formato, lo cual permite una gran interoperabilidad entre ellos. [3]

LDAP configuration

Host **LDAP**: **ldap://micontroladordedominio.midominio.com**

LDAP Port: 389

Basedn: OU=Sectores,DC=midominio,DC=com (se debe respetar siempre las mayúsculas/minúsculas de ADSI Edit)

rootdn: una cuenta con derecho de únicamente leer el AD[16], del estilo CN=Juan

Perez,OU=Usuarios,OU=Sectores,DC=midominio,DC=com (se espetar siempre las mayúsculas/minúsculas de ADSI Edit)

Pass (para las conexiones no anónimas): * (su clave)

Filtro de conexión: (objectClass=user) (con los paréntesis)

Campo de login: samaccountname (en minúsculas). [4]

A continuación vamos a ver la topología tipo árbol que se maneja en el directorio del Ministerio de Telecomunicaciones y Sociedad de la Información

[15] LDIF: Formato de intercambio de datos de LDAP
[16] AD: Active Directory

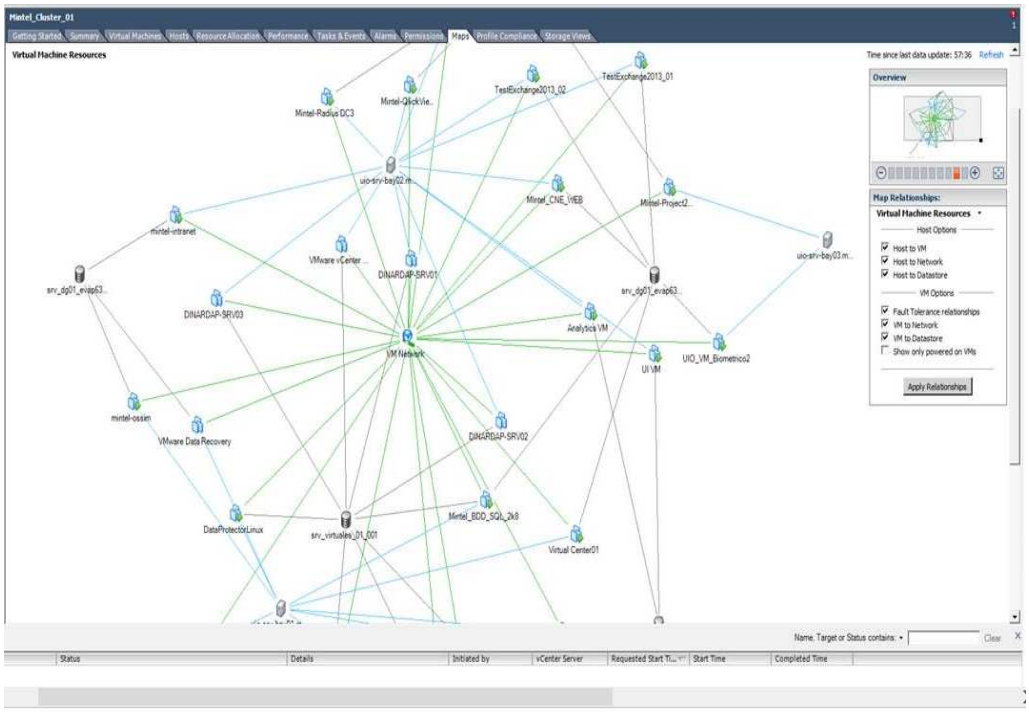

Figura. 2.1. Árbol LDAP del directorio del Ministerio de Telecomunicaciones y Sociedad de la Información

2.1.2 TOPOLOGÍAS DE LA RED

Se representa la red en el siguiente esquema:

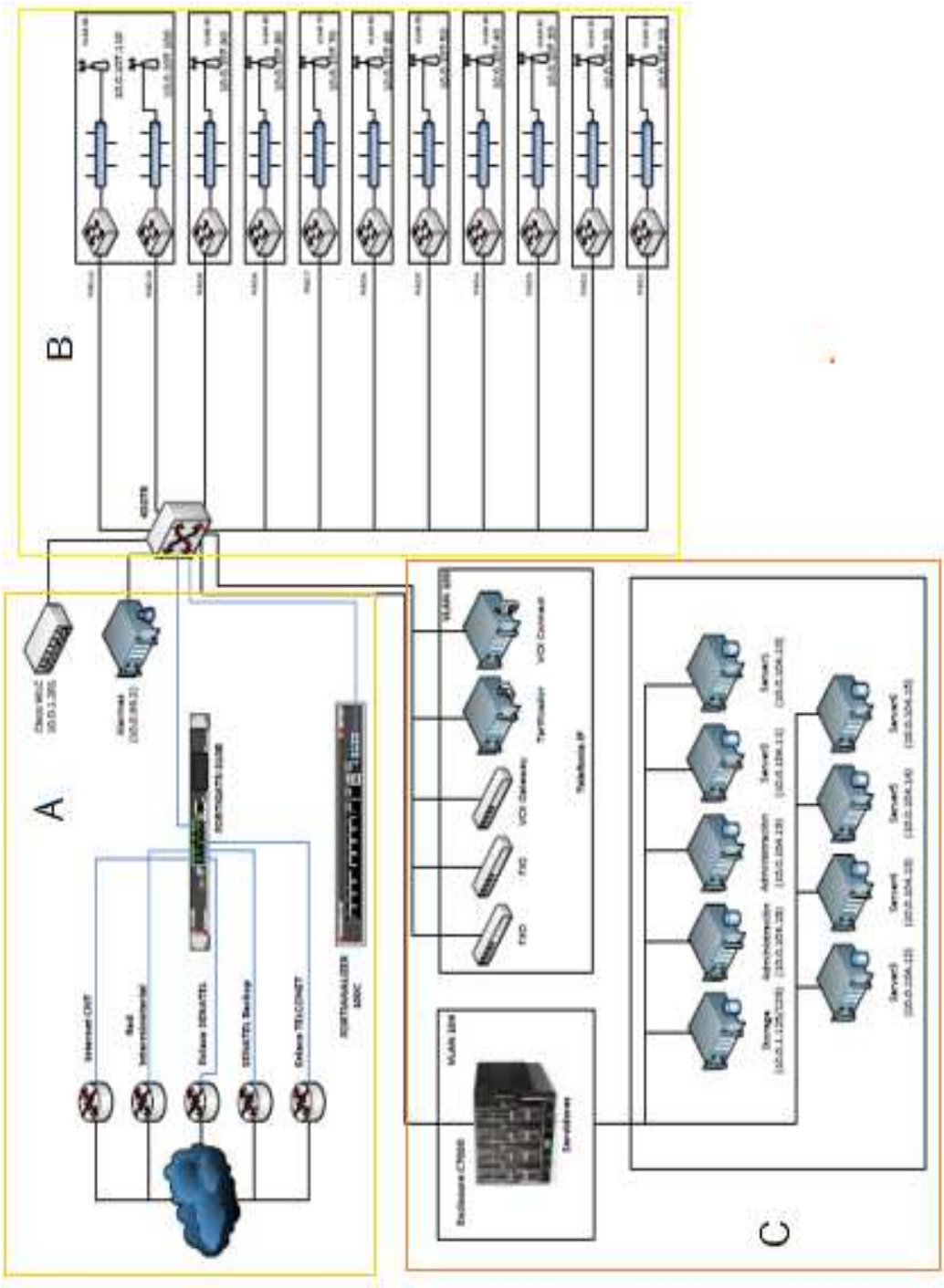

Figura. 2.2. Topología de la red completo del Ministerio de Telecomunicaciones y Sociedad de la Información

Vamos a explicar la topología de red de Mintel representada en la figura anterior, para lo cual hemos dividido la red en bloques A,B,C, empezamos la explicación con el bloque A que consta de la conexión a la nube por medio de los proveedores CNT[17], Telconet[18], tenemos salida por medio de la conexión interministerial y por el enlace a SENATAL y por último a un backup de SENATEL[19], las conexiones anteriormente descritas ingresan a la red de la institución encontrándose primero con un fortinegate 3200 para brindar seguridad, el Fortigate está directamente conectado a SWITCH CORE 4507R al mismo que se coneta también el Cisco WLC, alarmas, fortianalizer 100c.

El bloque B empieza en el Switch Core el cual tiene conexión por medio de fibra óptica a cada swittch de piso son 11 piso y cada uno tiene 2 switch Catalys Cisco 2960, que brinda conexión alámbrica a los empleados de la institución de este switch también tenemos conexión a un Access point por piso el cual también es de marca Cisco modelo 1300 que brindan acceso a la red vía inalámbrica a dispositivos móviles.

El bloque C tiene la conexión desde el Fortianalizer 100c al encloure 3700 que tiene control sobre los servidores como el storage, los dos servidores de uso de los administradores que veremos detalladamente en la topología de la figura 2.3, también tenemos en este bloque las conexiones de la central telefónica.

Para completar los conocimientos de la topología total de la red de la institución vamos ver la distribución de los servidores que están instalados y activos en la actualidad.

[17] CNT: Corporación Nacional de Telecomunicaciones
[18] Telconet: Proveedor de servicios
[19] Senatel: Secretaria Nacional de Telecomunicaciones

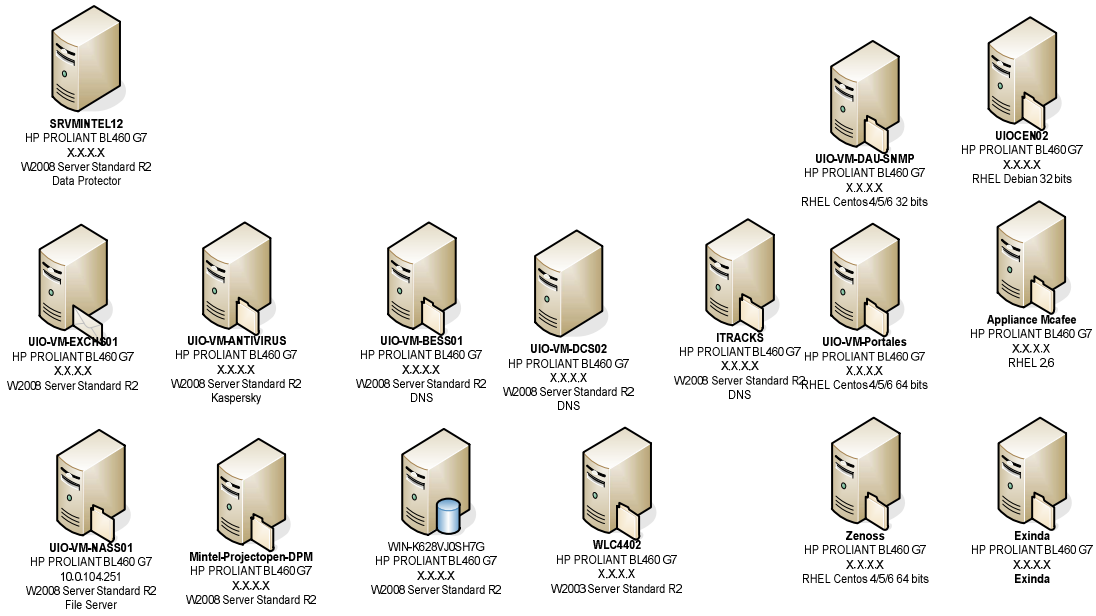

Figura. 2.3. Topología de los servidores instalados y activos en la actualidad de la institución.

2.1.3 Equipamiento

Switch Core 4507r

Figura. 2.4. Switch Core 4507R

El Catalyst series 4500 permite a las empresas y a los clientes con redes metro Ethernet desplegar redes convergentes con mayores niveles de desempeño, resistencia, seguridad y administración. Los clientes pueden converger y controlar más fácilmente los datos del Protocolo de Internet IP[20], streaming video, telefonía y aplicaciones basadas en Internet para una rentabilidad y productividad mejorada de la fuerza de trabajo.

El Catalyst series 4500 es óptimo en el wiring closet empresarial, donde se requieren servicios inteligentes, y donde niveles añadidos de resistencia entregan beneficios incrementados. El Catalyst series 4500 puede ser desplegado también como una solución integrada de oficina sucursal soportando datos, voz y video, junto con acceso WAN integrado.

El Catalyst series 4500 incluye el Catalyst series Supervisor Engine IV, el módulo de control que define y entrega todas las capacidades operativas de las plataformas del Catalyst 4000, ofreciendo entre mayor escalabilidad y desempeño a la red, redundancia integrada pero a la vez la misma es supervisada por los proveedores de todos los servicios.

Switches Catalyst Serie 2960

Figura.2.5. Switch Catalyst serie 2960

[20] IP: Protocolo de internet

Características destacadas:

- **Comunicaciones todas en uno:** Soporte de datos, voz y tecnología inalámbrica, por lo que cuando esté listo para implementar estos servicios disponga de una red que admita todas sus necesidades de negocio.

- **Inteligencia:** Ofrece prioridad al tráfico de voz o al intercambio de datos para alinear la entrega de información a sus requisitos de negocio.

- **Seguridad mejorada:** Proteja la información importante, mantenga a los usuarios no autorizados alejados de la red y consiga un funcionamiento ininterrumpido.

- **Fiabilidad:** Aprovéchese de las ventajas de los métodos basados en normas para conseguir una mayor fiabilidad y una rápida recuperación de errores. También puede agregar un suministro de energía redundante para obtener una fiabilidad adicional.

- **Fácil configuración:** Utilice Cisco Network Assistant para simplificar la configuración, las actualizaciones y la solución de problemas.

- Soporte para comunicaciones de datos, inalámbricas y voz que le permite instalar una única red para todas sus necesidades de comunicación.

- Capacidad de Power over Ethernet[21] para que puedan implementar nuevas funcionalidades como voz y tecnología inalámbrica sin tener que realizar un nuevo cableado.

[21] Power Over Ethernet: Alimentación por medio de ethernet

- Opción de Fast Ethernet (transferencia de datos de 100 Mbps) o Gigabit Ethernet (transferencia de datos de 1000 Mbps), dependiendo del precio y las necesidades de rendimiento.

- Múltiples modelos de configuración, con la habilidad para conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red.

- Capacidad de configurar LANs virtuales de forma que los empleados estén conectados a través de funciones de organización, equipos de proyecto o aplicaciones en lugar de por criterios físicos o geográficos.

- Seguridad integrada

- Funciones de monitorización de red y solución de problemas de conectividad mejoradas. [5]

Cisco Wireless lan Controller Serie 2100

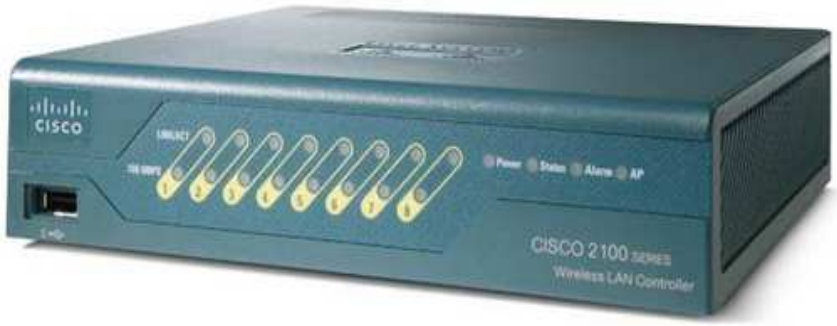

Figura. 2.6. Cisco wireless LAN Controller 2100

- **Tecnología inalámbrica:** Con dispositivos inalámbricos como Teléfonos IP, portátiles y teléfonos, los empleados se pueden comunicar y colaborar desde cualquier lugar con acceso a internet.

- **Amplia cobertura:** Con un soporte de hasta seis puntos de acceso, los empleados no están fuera de alcance ni desconectados.

- **Seguridad:** Soporte para la mayoría de estándares de seguridad, lo que significa que sus datos siempre están protegidos.

- **Integración:** Como parte de las soluciones de redes inalámbricas unificadas de Cisco, se integra perfectamente con productos de Cisco para gestión inalámbrica, puntos de acceso, puentes inalámbricos y productos de monitorización.

- Soporte para múltiples combinaciones de puntos de acceso y enlaces redundantes.

- Seguridad estándar, autenticación de identificación y protocolos de cifrado para obtener unos niveles de protección óptimos.

- Acceso de invitado seguro.

- Voz a través de WLAN.

- Integración con Cisco Wireless Control System para una configuración y monitorización de la red de área local inalámbrica completa.

- Cómodo montaje en escritorio o en rack, gracias a su pequeño tamaño. [6]

Enclosure C7000

Figura.2.7. Enclosure C7000

La marca con este dispositivo mejora considerablemente el rendimiento, la eficiencia y disponibilidad en entornos virtualizados en la nube que soportan los escritorios virtuales por servidor.

El BladeSystem c7000 Platinum con el nuevo conmutador Ethernet SX1018 ofrece la menor latencia de cualquier puerto de la hoja principal mercado del puerto, y es más de cuatro veces más rápido que las opciones anteriores.

HP[22] también es el primer fabricante que ofrece enlaces descendentes de 40 GB para cada servidor blade con un rendimiento casi en tiempo real. Con estos recursos nos enfrentamos interfaz de red ideal para clústeres de alto rendimiento y aplicaciones de servicios financieros, servidores blade ProLiant Gen8 como WS460c es la única infraestructura de hoja que apoya a los clientes gráficos 3D de alta densidad virtualizado ocho GPUs por blade de servidor, como se ha mencionado, soporta cuatro veces más usuarios por servidor y reduce los costes hasta en un 60% en comparación con la generación anterior, el WS460c ProLiant G6.

[22] HP: *Hewlett-Packard*

Cisco Aironet 1140 Series 802.11n

Figura.2.8. Access Point Cisco Aironet 1140

El éxito de su empresa depende de la capacidad de sus empleados para mantenerse conectados a las aplicaciones y los clientes, y para trabajar productivamente en cualquier lugar de las instalaciones de la empresa. Cada vez más empresas en crecimiento dependen de las redes inalámbricas para proporcionar a sus empleados una mayor movilidad y flexibilidad, y para brindar soporte a los grupos y usuarios temporales en las instalaciones de la empresa. Pero configurar, asegurar y administrar redes inalámbricas puede ser intimidante, especialmente para las empresas en crecimiento que no tienen un departamento de TI[23]. A medida que su empresa crece y necesita expandir su cobertura inalámbrica o agregar funciones nuevas, estos desafíos aumentan. Cómo pueden las empresas en crecimiento enfrentar estas demandas de una forma económica y disfrutar de los beneficios que proporciona una movilidad inalámbrica de clase empresarial Cisco ofrece Cisco.

Tiene varias características con las que viene implementado:

- Cable de alimentación (configurable).
- De 100 a 240 VCA[24] (AIR-PWR-A =) proporciona 48 VCC al inyector

[23] TI: Tecnología de la información
[24] VAC: Voltaje de corriente alterna

- 48 VCC[25] inyector de corriente (AIR-PWRINJ-BLR2 =)
- 1-pie de doble RG-6 conjunto de cable (Ethernet uplink de inyector de corriente)
- Kit de montaje en techo disponible por separado (AIR-ACCRMK1300 =)
- 12 a 40 VDC de alimentación Inyector (AIR-PWRINJ-BLR2T =) para las instalaciones de suministro de energía DC disponibles por separado.

2.1.5 Estudio de los requerimientos

Mediante la implementación a realizarse vamos a trabajar en los problemas que actualmente aquejan a la administración y la comodidad de casa usuario, a pesar que existen normas y políticas de seguridad internas para el manejo de recursos de la red e información no siempre se las respeta, siendo esto la principal desventaja teniendo muchas veces congestión en la red ministerial.

Son usuales las llamadas al Departamento de Gestión Tecnológica diariamente por mal manejo de claves, expiración de las mismas, la restricción a varias páginas web que consigo trae descontento a los funcionarios ya que no ven el riesgo que puede sufrir el mal uso de la nube, mucha gente que trabaja en la institución no es consciente de cuáles son los riesgos que puede traer consigo el mal uso de los mismos, pudiendo de esta forma tener accesos ilegítimos a la información que muchas veces es confidencial y de la institución, la administración se ve afectada por estos problemas para trabajar en contra de estos descontentos lo que se busca es que los usuarios manejen responsablemente sus claves de autenticación la seguridad en servicios y aplicaciones.

Control de servicios: Cumplir las políticas de la institución permitiendo a los usuarios control de recursos de la web necesaria para su trabajo para lo cual se maneja categorías de restricción.

[25] VCC: Voltaje de corriente continua

Control de aplicaciones: Es el tipo de software que va usar cada usuario según el departamento al cual pertenece y va a poder manejar para no gastar recursos innecesarios.

Autenticación: Acceder desde un dispositivo de manera segura a los recursos de forma alámbrica e inalámbrica.

Muchos usuarios de la institución tienen más de una manera de acceso a la red ya se de forma alámbrica como inalámbricas, lo cual también trae consigo problemas de confidencialidad de respuestas a los recursos que puede acceder ya que de forma alámbrica muchas veces tienen restricciones diferentes a la que tienen mediante su conexión inalámbrica, rompiendo cualquier norma de proteger los recursos de la red., tampoco se controla el ingreso a recursos de la web como a portales, servicios de correo vía Exchange[26] los cuales pueden traer problemas de acceso no permitido.

2.2 POLÍTICA DE SEGURIDAD INTERNA DEL MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN

2.2.1 Tipo de restricciones que se maneja en la institución

Potentially Liable
Abuso de Drogas
Hacking
Ilegales o inmorales
Discriminación
Violencia explícita
Evitar proxy
Plagio
Abuso Infantil

Tabla. 2.1. Potencialmente Responsable

[26] Exchange: Servidor de comunicación basado en correo

Adult/Mature Content
Otros Materiales adultos
Organizaciones de defensa
Juego
Desnudez y subido de tono
Pornografía
Armas (ventas)
Marihuana
Educación Sexual
Alcohol
Tabaco
Lencería y baño
Deportes de Caza y Juegos de Guerra

Tabla. 2.2. Contenido de Adultos

Bandwidth Consuming
Software libre y descargas de software
Uso compartido de archivos y almacenamiento
Streaming Media y Descargas
Peer-to-peer Intercambio de Archivos
Internet Radio
Internet TV
Telefónico por Internet

Tabla. 2.3. Consumidor de Ancho de Banda

Security Risk
Sitios Web maliciosos
Estafas cibernéticas
URL basura

Tabla. 2.4. Riesgos de Seguridad

General Interest – Personal
Publicidad
Corretaje y comercio
Juegos
Entretenimiento
Educación
Salud y Bienestar
Búsqueda de Empleo
Redes sociales
Organizaciones Políticas
Religión Global
Compras y Subastas
Vehículos personales
Contenido Dinámico
Contenido sin sentido
Chat web
Mensajeria Instantánea
Sitios web personales y blogs
Servidores de Contenido
Dominio parqueo
Intimidad Personal

Tabla. 2.5. Interés Personal

General Interest – Business
Finanzas y Banca
Buscadores y Portales
Organizaciones generales
Información y Seguridad Informática
Gobierno y organizaciones legales
Tecnología de la Información
Fuerzas Armadas
Sitios web seguros
Aplicaciones Web

Tabla. 2.6. Negocios interés general

2.3 ANALISIS DE LA SEGURIDAD ACTUAL

2.3.1 Seguridad a la red de acceso

Anivirus Kasperski

Protege contra todo tipo de virus, gracias a la combinación de una función basada en la nube y potentes tecnologías de seguridad que se ejecutan en tu ordenador, Kaspersky Anti-Virus 2013 te ofrece una seguridad única ante las amenazas actuales.

Detecta amenazas nuevas, emergentes y desconocidas, el servicio basado en la nube "Kaspersky Security Network" recopila datos de millones de sistemas de usuarios de todo el mundo que colaboran para ayudarnos a defenderte contra los últimos ataques de virus y malware[27]. Se supervisan y analizan las posibles amenazas en tiempo real, de modo que cualquier acción que resulte peligrosa queda completamente bloqueada antes de causar daños

Identifica sitios web sospechosos y de phishing, sus avanzadas tecnologías anti-phishing detectan de forma proactiva las URL fraudulentas y utilizan información en tiempo real procedente de la nube, para garantizar que nadie, mediante engaños, te haga revelar datos de valor en sitios web de phishing[28]. URL Advisor añade también etiquetas de distintos colores a todos los enlaces web para alertarte del nivel de peligrosidad del enlace así como de las páginas vinculadas.

Evita que el malware explote las vulnerabilidades de tu ordenador, si tu ordenador sufre vulnerabilidades en el sistema o en alguna aplicación y todavía no se han actualizado con correcciones recientes, es posible que sea vulnerable ante cibercriminales o malware.

Además de realizar análisis en busca de vulnerabilidades, Kaspersky Anti-Virus 2013 analiza y controla las acciones de los programas, de forma que no puedan causar ningún daño.

Funciones de descarga e instalación automática: ahorra tiempo y esfuerzo, ahora la instalación del producto requiere muchos menos pasos manuales. Cuando te descargues el producto por primera vez desde nuestro sitio web éste buscará automáticamente su versión más reciente, si es necesario desinfectará el malware existente, y, a continuación, comenzará con la instalación**.**

[27] Malware: Código maligno
[28] Phishing: Tipo d abuso informático

2.3.2 Seguridad de recursos

Fortinet

El fortinet publicación de servicios, webfilter para lo que es afuera,

Figura.2. 9. Dispositivo Fortinet

Las plataformas de seguridad FortiGate, líderes del mercado UTM[29], proveen una solución integrada de seguridad compuesta por las funcionalidades más necesarias para tener una protección completa de nuestras comunicaciones como son: Firewall[30], VPN[31] (IPSEC y SSL), Antivirus, Sistemas de Detección/Prevención de Intrusiones, Filtrado Web, Antispam, AntiSpyware, Control de Aplicaciones, Inspección de Contenido en SSL etc. Además, todas las funcionalidades de seguridad se integran de forma conjunta con funcionalidades añadidas como Traffic Shaping, Alta Disponibilidad, balanceo de carga, aceleración Wan[32], Enrutamiento dinámico RIP[33] (v1 y v2), OSPF[34], etc.

Fortinet ofrece de forma conjunta con su equipamiento servicios profesionales que garantizan el soporte, la actualización y el correcto mantenimiento de los niveles de servicio demandados.

[29] UTM: Dispositivo que permite la gestión unificada de amenazas
[30] Firewall: Contrfuego de seguridad de
[31] VPN: Red privada virtual
[32] WAN: Red de área amplia
[33] RIP: Protocolo de enrutamiento interno
[34] OSPF: Protocolo de enrutamiento jerárquico

Gracias a los equipos técnicos distribuidos a lo largo de todo el mundo, Fortinet es capaz de ofrecer soporte internacional con cobertura 24x7x365, actualizando en tiempo real las bases de datos de firmas de antivirus e IDS/IPS y los motores de estas aplicaciones, así como actualizando de forma continuada las bases de datos en las que se apoyan los servicios.

Fortiguard AntiSpam.

El Servicio FortiProtect Distribution Network (FDN) se encarga de la distribución de estas actualizaciones a lo largo de todo el mundo, existiendo el compromiso con aquellos clientes que contratan el servicio FortiProtect Premier Services de disponer de la firma correspondiente a cualquier nuevo ataque en menos de 3 horas.

Por otra parte, los equipos de soporte y desarrollo velan de forma continuada para dar respuesta a los servicios FortiCare de mantenimiento hardware, actualizaciones y desarrollo de nuevas versiones de firmware, y soporte vía telefónica o e-mail. Los centros de soporte y desarrollo están distribuidos por todo el mundo, si bien todos cuentan con un servicio 24x7, garantizándose de este modo que el soporte siempre se ofrece a nuestros clientes desde el punto más cercano regionalmente.

FortiMail

Seguridad Integral de correo electrónico es una potente y probada plataforma de seguridad de correo electrónico para organizaciones de cualquier tamaño, desde pequeñas empresas a operadoras, proveedores de servicios y grandes empresas.

Se trata de dispositivos específicamente diseñados para los sistemas de mensajería más exigentes, que aplican los años de experiencia de Fortinet en protección de redes contra spam[35], malware y otras amenazas que se propagan por el correo electrónico.

FortiMail permite impedir que los sistemas de mensajería se conviertan en sistemas de entrega de amenazas. Su motor de filtro de entrada bloquea el spam y el malware antes de que pueda infectar la red y afectar a los usuarios.

Modo transparente, cada interfaz de red incluye un proxy que recibe y transmite el correo electrónico. Cada proxy puede interceptar sesiones de SMTP[36] aunque el destino IP no sea el dispositivo FortiMail, lo que suprime la necesidad de cambiar el registro de DNS[37] MX o modificar la configuración existente de la red de servidores de correo.

Modo pasarela, ofrece servicios MTA de proxy[38] entrante y saliente para las pasarelas de correo electrónico existentes. Un simple cambio del registro de DNS MX redirige el correo electrónico a FortiMail con el fin de que realice exploraciones antispam y antivirus.

Modo servidor, proporciona la funcionalidad de un servidor de correo SMTP con todas las características, con soporte flexible para acceso seguro a POP3, IMAP y WebMail.

2.3.3 Seguridad brindada por cada dispositivo que conforma la topología de la red

Ya hemos considerado las características de cada uno de los dispositivos que conforman nuestra red nos vamos a enfocar un poco más en la red de cada piso como vemos en la figura siguiente.

[35] SPAN: Correo basura
[36] SMTP: Protocolo para la transferencia simple de correo electrónico
[37] DNS: sistema de nombres de dominio
[38] Proxy: ntermediario entre un navegador Web e Internet

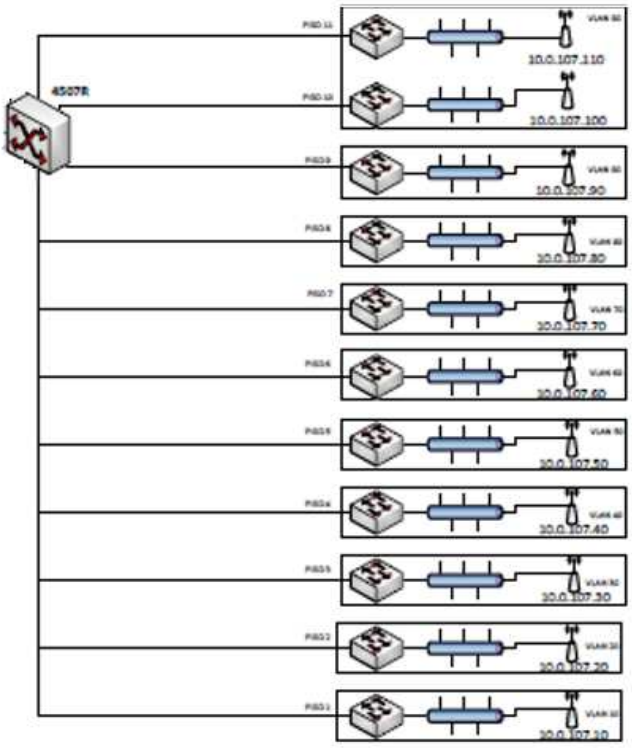

Figura. 2.10. Red de pisos conectado a switch Core

Esta es la red principales interna dentro de la institución y los dispositivos que la conforman comparten los recursos del medio físico, es decir, el ancho de banda proporcionado por el mismo.

Los switchs, lo que hacen dentro de nuestra red es mejorar el rendimiento y dar seguridad dentro de la misma estos son varios aspectos que podemos resaltar de los dispositivos que forman parte de casa piso.

Se brinda mayor seguridad física, puesto que si se desea conectar un dispositivo en un puerto que sea diferente al que se usa habitualmente este está cerrado sin que se le permita el uso indebido del mismo.

Proporciona el ancho de banda a cada uno de los puertos y, por lo tanto, a cada dispositivo conectado al mismo.

Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, esto asegura que otras máquinas no entren indebidamente.

VLAN por subredes de IP o IPX[39].

2.3.4 Seguridad de cada usuario o servidor público perteneciente a la institución

La seguridad que se le ofrece a cada uno de los usuarios de la red de la institución están el antivirus que se usa Kaspersky, que sus características ya las vimos anteriormente.

La forma de autenticación es dada por medio del Active Directory que funciona con el protocolo LDPA Permisos por usuarios, que es el controlador de dominio autentica y autoriza todos los usuarios y equipos que manejan el mismo dominio en el cual el administrador de la red lo que hace es asignar y hacer cumplir las políticas de seguridad que han sido establecidas anteriormente el cual no se cumple ya que por motivos de permisos por parte de los directores de cada área se hace una solicitud de recursos a la cual por medio de la política no tendría acceso pero se rompe muchas veces las reglas.

También brinda seguridad para que solo sea el administrador bajo su autenticación el que pueda instalar software en las máquinas para no tener programas que sean innecesarios para un usuario.

Toda esta información se guarda en una base de datos, hacienda que sea confidencial toda la información.

[39] IPX: Intercambio de Paquetes interred

Por necesidades que aparecieron en toda la institución ya que cada departamento puede trabajar con archivos compartidos los administradores de la red lo que hace es por medio del Active Directory crear una política para tener una carpeta compartida para cada uno de los departamentos en el cual se guarda solo información necesaria de cada departamento y el uso de los archivos del mismo son alterados con mucha frecuencia y el acceso solo es permitido por funcionarios que previamente fueron asignados por el director jefe de cada departamento de la institución ya que se puede manejar información confidencial.

2.3.5 Acceso a usuarios visitantes a la institución

Actualmente en el Ministerio de Telecomunicaciones y la Sociedad de la no se archiva las políticas a las cuales están sujetas las personas que no son funcionarios o sus máquinas no pertenecen a la institución, pero haciendo pruebas podemos ver que se tiene restricción a redes sociales, esto no es regulado debido a que las máquinas que llegan de esta forma al ministerio la red tiene que ser configurada con la autenticación de un administrador de la red, es decir no cualquier funcionario puede llevar consigo una computador y tener permisos diferentes a los que usualmente tiene con algún dispositivo de escritorio o inalámbrico que pertenece al Mintel[40].

El visitante ya sea por fines de trabajo dentro de la institución u otros parámetros no podrá ingresar a la red del ministerio sin previa autorización y aviso del director del departamento al cual acudió por algún motivo al Departamento de Gestión Tecnológica, el cual acudirá para autenticar la red de la misma, pero de igual forma los recursos usados por los mismos no deberán limitar el uso de los demás usuarios, sobrecargando la red.

[40] Mintel: Ministerio de Telecomunicaciones y Sociedad de la Información

CAPÍTULO III

ESTUDIO Y ANÁLISIS DEL ESTÁNDAR 802.1X EN LA RED

3.1 VENTAJAS DE LA IMPLANTACIÓN DEL ESTANDAR 802.1X DENTRO DEL MINISTERIO

3.1.1 Importancia de modificar la red de acceso actual

El Sistema utilizado actualmente es mediante cifrado y aunque sean cambiados cierto tiempo no son muy seguras ya sea por falta de educación a usuarios que no conocen de los peligros que puede contraer claves muy fáciles para descifrar, muchos usuarios usan contraseñas básicas por problemas de no olvidarse, a más de esto existen programas en los cuales se pueden descifrar la encriptación y muchas veces se puede ingresar de forma maliciosa a la información de los usuarios teniendo los conocimientos y herramientas necesarias para realizar esto.

La vulnerabilidad de la red es algo que se quiere trabajar por el Departamento de Gestión Tecnológica aunque no se ha tenido problemas grabes de intrusos, como administradores mejorar la seguridad es esencial en los dispositivos de la misma, las vulnerabilidades son más usuales aun de forma inalámbrica, por esto se requiere cambiar el sistema a un protocolo de autenticación como lo es 802.1X el cual da seguridad por los puertos de los dispositivos.

La cantidad de funcionarios que trabajan en la institución es grande y como pudimos ver no todos cumplen con las políticas de seguridad las cuales se las deniegan según necesidades que aparecen en curso, muchas veces no se respeta las políticas asignadas por los administradores a cada departamento de la institución ya que directores dan permisos por ciertos motivos a muchos funcionarios ya sea de forma permanente o momentánea, lo cual también puede contraer problemas a los recursos de la institución y problemas con otros usuarios de la red. Otro problema y uno de los más grabes es que un funcionario puede con su computador ir a otro piso y conectar a cualquier puerto es decir esta máquina entra en otra vlan[41] con permisos diferentes a la que este pertenece, esto es un problema grabe ya que puede acceder a recursos colapsar la red y otros problemas, la solución a estos problemas es de asignar los mismos permisos a usuarios por medio de los puertos de cada dispositivo de esta forma si un funcionario va a otra vlan de piso su máquina seguirá teniendo los mismos permisos ya que reconoce la dirección de su puerto no la ip, de esta forma damos seguridad tanto a la información ya que no se puede visualizar las carpetas compartidas que tiene cada departamento y tampoco a los recursos de la red que se puede usar de mala forma, esto es fundamental para lograr saber que dispositivo usa inadecuadamente la red y dar aviso.

3.2.1 Autenticación

La autenticación hace referencia al proceso en donde el cliente demuestra quien es por medio de una identidad frente a un sistema o frente a otro usuario de la red, este proceso se realiza por medio de un token[42], una contraseña, una huella dactilar, ocular u otras formas, las cuales fueron previamente almacenadas estas son más complejas según el tipo de información que se manipule.

Este proceso realiza la comparación de las formas de autenticar anteriormente mencionada emitidas en tiempo real con las almacenadas en un servidor de esta forma

[41] Vlan: Lan virtual
[42] Token: Autenticación criptográfica

permitiendo el ingreso a los servicios, si estas coinciden o denegando el ingreso si estas no coinciden.

3.2.2 Autorización

Este proceso entra en juego una vez que paso la autenticación, lo que aquí se ejecuta son los permisos a los recursos que cada uno de los usuarios puede acceder basándose en privilegios los cuales son dados por las políticas o reglas de la institución, como el mismo es un ministerio público con gran cantidad de funcionaros los privilegios son dados según el departamento a cual pertenece el mismo, tratando de explotar al máximo todos los recursos, sin afectar a la información, aplicaciones, anchos de banda, archivos compartidos entre otros.

3.2.3 Contabilidad

Este concepto se muchas veces mal entendido, pero este proceso no es más que por medio de un log ir registrando cada uno de los eventos que cada usuario de la red va ejecutando, dentro de la institución esto es muy importante para detectar amenazas, ataques que se pueden tener en forma gráfica o de alertas, sin duda este proceso facilita la administración de la red ya que el control de la misma es más específico ya que se puede tener el punto donde se origina cualquier problema de la red y de esta forma dar soluciones puntuales y oportunas.

3.3. TIPOS DE AMENAZAS DENTRO DE LA RED

3.3.1 Estudios de los tipos de amenazas a la que es sujeta la red

Las amenazas pueden ser generadas por varios aspectos que afecten de una u otra forma a la seguridad de la información, muchos de estos son inevitables pero se puede trabajar para contrarrestar contra ya sea daños, robos, entre otros.

Veamos cuales son los tipos de amenazas más comunes a la cual se somete la información dentro de una red.

3.3.1.1 AMENAZAS NATURALES

Estas amenazas se originan naturalmente y son inevitables siempre vamos a estar sujetos a que aparezcan estas son generadas por incendios, temblores, terremotos, inundaciones, etc.

Lo que se hace para protección es tener planes de contingencia aprobados basándonos en estándares probados con anterioridad y su efectividad esto para poder reducir el efecto que estos pueden ocasionar, muchos administradores lo que hacen es tener data center muy bien equipados y a la vez tener un data center remoto para aumentar la disponibilidad en este tipo de amenazas.

3.3.1.2 AMENAZAS LÓGICAS

Este tipo de amenazas viene dado por programas que son creados con la intención de dañar un sistema de información estos pueden ser unos más peligrosos que otros entre estos podemos encontrar lo que son códigos malicioso *malware* o simplemente errores como agujeros.

Código malicioso: Estos son partes o un programa completo que son construidos para generar un daño dentro de un sistema, estos debilitan el funcionamiento entre los códigos maliciosos tenemos:

Gusanos: Los cuales se multiplican y se dispersan alrededor de un sistema.

Troyano: Viene disfrazado con las características mismas del programa y se activan cuando el usuario los ejecuta.

Bombas lógicas: Siguen cierta lógica y se activan cuando se desarrollan dentro de un sistema.

Cookies: Es un tipo de texto que tiene en si la información que maneja el usuario dentro del internet y la confidencialidad del mismo muchas veces no son peligrosas dentro de un ordenador pero la acumulación de las mismas pueden volver lento el sistema.

Keyloggers: Estos son programas que se ejecutan y van guardando todas las teclas que el usuario va tipeando esto se hace para acceder a obtener usuarios, contraseñas de autenticación es muy peligroso por el tipo de información que se puede obtener.

Spyware: Estas son aplicaciones que almacenan las páginas web que accede un usuario, el tipo de conexión que tiene la duración de la misma entre otras, este pude obtener toda la información de la máquina la cual se está operando como es características generales sistema operativo, tipo de procesador, memoria, incluso pude decir si el sistema operativo es o no original.

3.3.1.3 Amenazas Humanas

Este puede ser el más preocupante ya que se puede generar por varios factores los cuales los presentamos a continuación:

Personal de la institución este es difícil de detectar ya que muchos de los empleados de la institución conocen la estructura de la red y teniendo usuarios y contraseñas necesarias puede obtener la información o recursos que desea, esto se puede dar por querer obtener información de forma no autorizada la cual es confidencial pero existen muchos casos en los cuales sustraer la misma para objetivos personales, con la gran cantidad de usuarios que puede tener una red el administrador no tiene muchas posibilidades de dar con el mismo, también estos problemas se dan por falta de educación de los empleados ya que

no pueden tener los conocimientos necesarios ya sea por querer experimentar o curiosidad puede generar ataques durante la navegación de internet porque se puede ejecutar cualquier tipo de aplicaciones maliciosas o aplicaciones que están encubiertas para causar daños, para lo mismo se debe instruir a todos los empleado de la red de los cuidados que debe tener para proteger la información no solo del usuarios sino de la institución con lo que se conoce como ingeniería social, muchas veces esta no se le da la importancia que se debe sin asumir todos los problemas que pueden generar los mismos a la red.

Existen usuarios de la institución que muchas veces para no olvidar sus datos de autenticación lo que hacen es pegarlo en un papel en su ordenador sin saber todos los problemas que esto puede causar, ingreso con un usuarios conocido y cambiar las configuraciones o manipular a su conveniencia la información.

A más de los empleados de la institución se dan casos que los ataques son generado por ex miembros de las instituciones causando muchos problemas debido a que tienen conocimientos de la estructura de la red del tipo de seguridad que la misma maneja muchas veces sus datos dentro de los servidores siguen vigentes como sus datos de autenticación y este puede usar la misma para poder obtener información, cambiar la configuración de la red, u otras formas de dañar la red, es por ello que algunas instituciones hacen contratos para en los cuales los empleados afirman el no divulgar la información interna de la institución este dentro o fuera de la misma, esto es útil pero muchas veces no es suficiente para obtenciones maliciosas, los administradores de la red deben de tener en cuenta de los ex empleados por esto en muchos casos las contraseñas son cambiadas con frecuencias de los dispositivos para no tener problemas de suspensión de recursos o que los mismos no funcionen como se los tenía configurados.

Tenemos también a los Hacker[43] que son conocidos como los piratas informáticos, estas son personas que tienen los conocimientos bastos para ingresar a la red de forma

[43] Hacker: Pirata de Información

remota de varias formas y realizar las configuraciones a su conveniencia son independientes en su forma de operar y casi nunca lo realizan de una ubicación fija sino que se cuidan en caso que estos puedan ser encontrados por las manipulaciones a los sistemas, páginas web entre otras.

Los Crackers[44] estas son personas que tienen los conocimientos necesarios para romper con las reglas de la seguridad, lo pueden hacer ya sea por diversión o para realizar de forma maliciosa para acceder modificar configuraciones de los dispositivos de la red y dañar la misma, esto debe ser tomado en cuenta por los administradores de la red ya que estas personas toman las vulnerabilidades de la red y acceden por las mismas pueden escanear equipos para ver cuáles son las deficiencias de la misma.

3.3.2 Tipos de Ataques

Vamos a comenzar definiendo al ataque como una acción que se da para causar problemas y daños dentro de un sistema informático que se las hacen para poder obtener información o manipularla se conocen algunos tipos de ataques como son por fuerza bruta, cartoneo, denegar servicios, captura de mensaje entre otros pero a continuación vamos a revisar las características de estos ataques que se los cataloga como los principales. [10]

3.3.2.1 Por fuerza bruta

Este ataque no necesariamente es realizado por una persona que tenga muchos conocimientos de accesos a sistemas de información porque lo que se hace es insistir varias veces adivinando combinaciones para romper la seguridad de la contraseña para acceder a una cuenta ilícitamente.

3.3.2.2 El cartoneo

[44] Cracker: Romper seguridad informática

También se lo conoce como trashing[45] que es causada por personas que dejan a la vista el usuario y contraseña para autenticarse y es tomada por algún individuo para acceder al sistema de forma maliciosa, esto se lo puede combatir instruyendo a los empleados de la empresa de los problemas que pueden ocasionar no solo con su información sino también con la de sus compañeros y la red en general.

3.3.2.3 Denegar servicios

Estos ataques lo que hacen es llenar el canal de comunicación con peticiones falsas a la red sobrecargándola entonces cuando un miembro de la red necesita hacer uso del canal sus peticiones son denegadas debido a la gran cantidad de mensajes falsos que están llegando a los dispositivos, haciendo que los mismos no lleguen a sus destino, esto es perjudicial ya que en instituciones y más si esta es pública manejan información que está constantemente viajando de un destino a otro de forma urgente.

3.2.3.4 Captura de mensaje

Esta es la intercepción de la información muchas veces usan software para obtener el mensaje aun cuando este viaja con encriptación y pude mandar a su destinatario pero muchas veces enmascarando código malicioso, en el cual es ejecutado por el destinatario sin saber que puede afectar a sus sistema de información, este tipo de ataque es realizado por individuos que tiene conocimientos en el tema para poder dañar un sistema de esta forma.

[45] Trashing: Recolectar información

3.4. ESTANDAR 802.1X

El estándar 802.1X es normado por la IEEE Instituto de Ingenieros Eléctricos y Electrónicos el cual define al 802.1X como el acceso seguro a la red por medio de puertos, los mismos que son de acceso público, el estándar trabaja cuando existe una conexión punto a punto donde existe un cliente o usuario que es el que realiza la petición a un servidor el cual restringe el acceso cerrando el puerto si la autenticación es invalida o abriendo el puerto si la autenticación se da de forma correcta, entre las facilidades de la implementación de este estándar está el ser combatible con diferentes medios como conexiones inalámbricas 802.11, Token Ring, Ethernet y FDDI[46].

Este estándar se creó para conexiones fijas, pero por las necesidades actuales se le adapto a que funcione también a conexiones inalámbricas dada por la IEEE 802.11 a continuación podemos ver cómo se realiza la conexión fija e inalámbrica como conexiones punto a punto, el proceso se realiza entre tres elementos que son los clientes o suplicantes, un autenticador que es dado por un switch o un acces point y por último un servidor de autenticación FREERADIUS[47].

El switch o Access point que funciona como dispositivo intermedio permite o deniega que las tramas procedentes del usuario al servidor se concreten o no. [11]

[46] FDDI: Interfaz de Datos Distribuida por Fibra
[47] Freeradius: Servido Radius

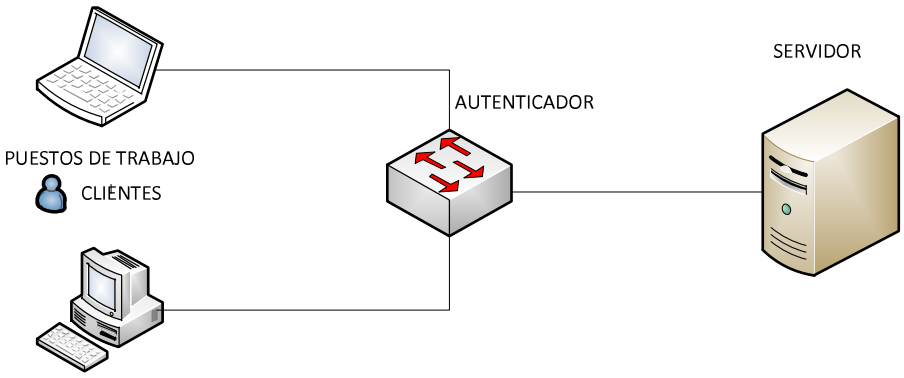

Figura. 3.1 Conexión básica 802.1X fija

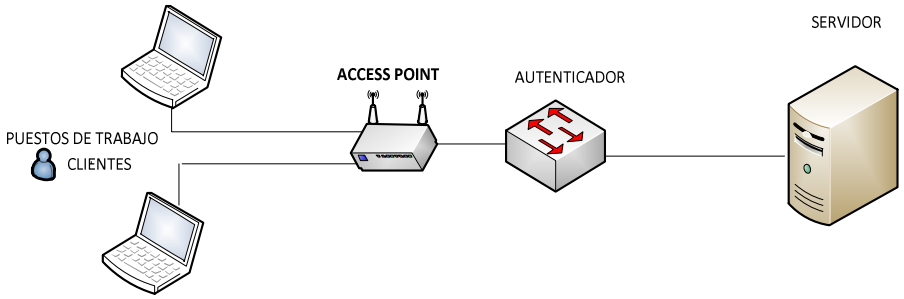

Figura. 3.2. Conexión básica 802.1X inalámbrica

El estándar trabaja en la capa de enlace de datos del modelo OSI[48], en donde se realizan el procesa de autenticación y autorización del uso de los diferentes dispositivos ya sea en conexiones fijas un switch o un punto de acceso para conexiones inalámbricas, este estándar trabaja conjuntamente con el protocolo de autenticación EAP que significa Extensible Autentication Protocol que en español significa Protocolo de Autenticación Expandible, sin embargo en realidad es EAPoL que significa Extensible Autentication Protocolo over LAN que significa Protocolo de Autenticación Expandible sobre LAN de esta forma que como lo dijimos anteriormente este estándar es compatible ya sea con

[48] OSI: Modelo de interconexión de sistemas abiertos

conexiones Ethernet, inalámbricas 802.11, Token-Ring y FDDI que significa Fiber Distributed Data Interface es decir Interfaz de Datos Distribuida por Fibra.

Ahora para entender el funcionamiento del estándar 802.1X vamos a observar el funcionamiento del mismo por medio del diagrama de flujo.

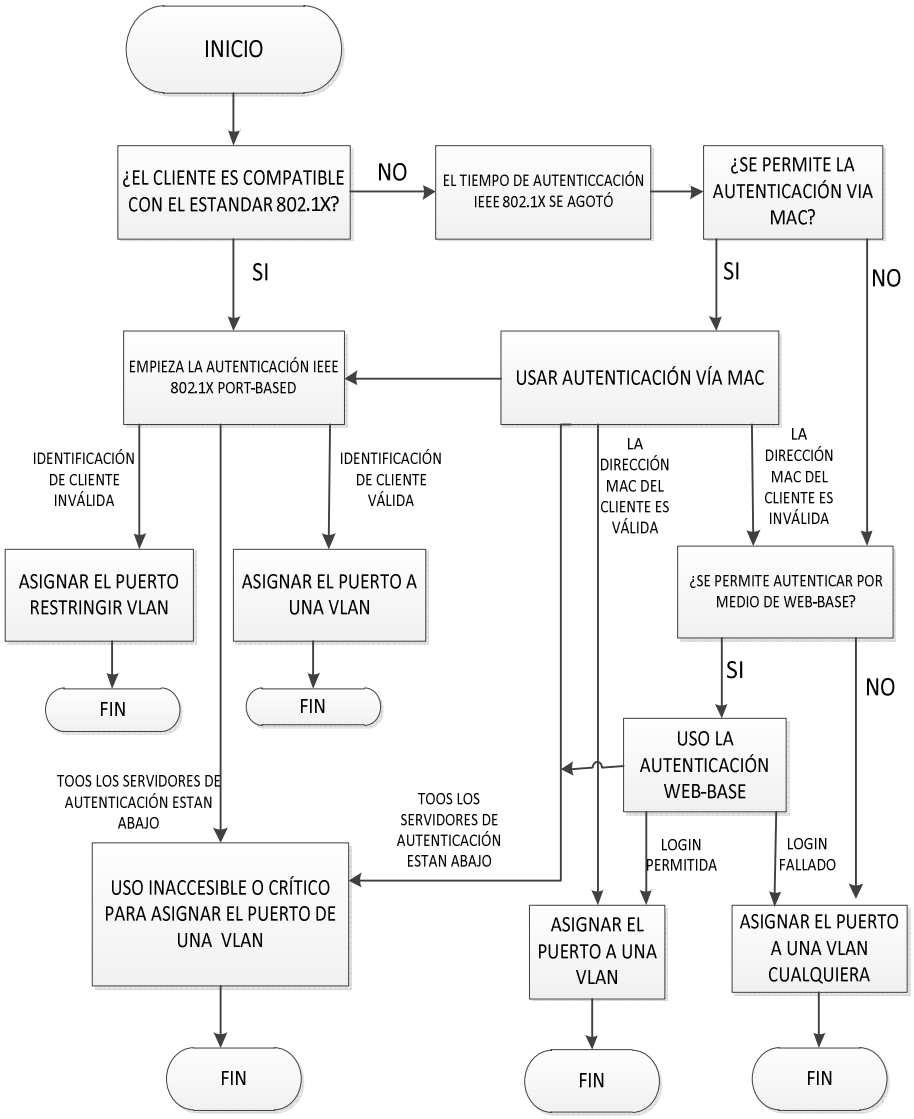

Figura. 3.3. Diagrama de Flujo de funcionamiento IEEE 802.1X

En la siguiente figura representamos como se realiza el proceso de autenticación por el estándar 802.1x para entender mejor el funcionamiento anteriormente mostrado en el diagrama de flujo cuando el sistema es compatible con el estándar y la respuesta es inmediata.

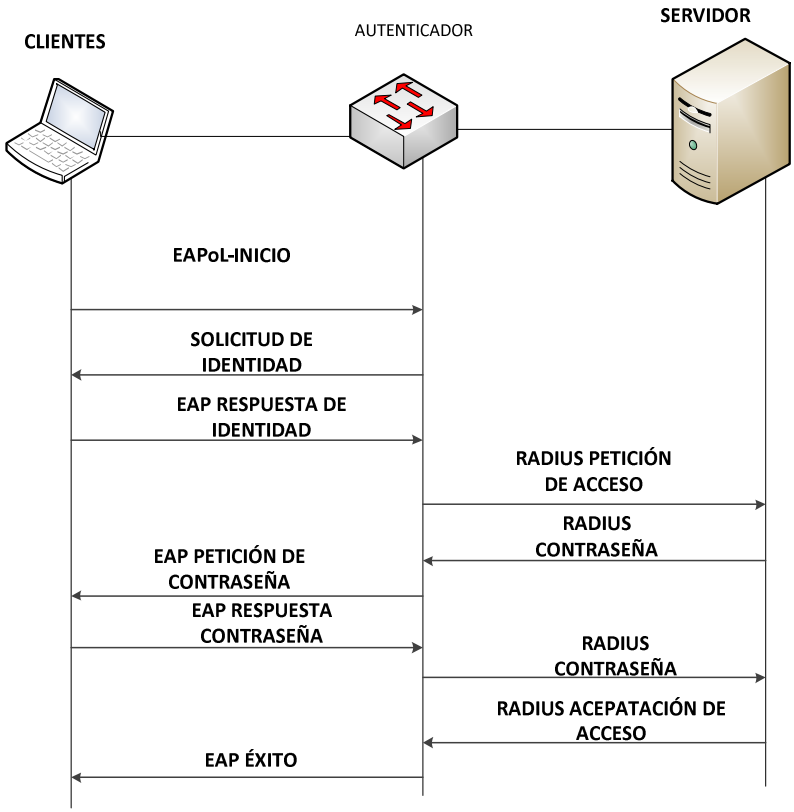

Figura.3.4. Funcionamiento del estándar

Ahora vamos a ver el caso en el cual el tiempo de espera de autenticación mediante el estándar 802.1X a la espera de un intercambio de mensajes EAPOL[49], y la omisión de autenticación MAC[50] está activado, el conmutador puede autorizar al cliente cuando el conmutador detecta un paquete Ethernet del cliente. El conmutador utiliza la dirección MAC del cliente como su identidad e incluye esta información en el marco RADIUS-

[49] EAPOL: Método de autenticación 802.1x
[50] MAC: Control de acceso al medio

access/request que se envía al servidor RADIUS[51]. Después de que el servidor envía el interruptor el marco RADIUS-access/accept cuando la autenticación tiene éxito, el puerto se abre permitiendo el acceso autorizado. Si la autenticación falla y los puertos permaneces cerrados y se especifica una VLAN de invitados, el conmutador asigna el puerto a la VLAN de invitados. Si el interruptor detecta un paquete EAPOL a la espera de un paquete Ethernet, el interruptor detiene el proceso de omisión de autenticación MAC y comienza la autenticación 802.1X.

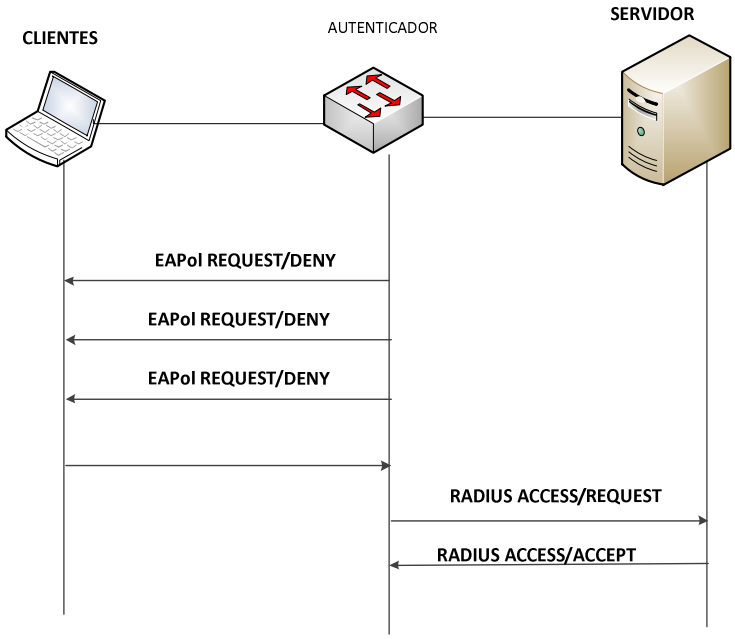

Figura. 3.5. Funcionamiento EAPOL

Ahora vamos a observar el proceso que se realiza en redes inalámbricas la que no cambia con la vista anteriormente.

[51] Radius: Servidor 802.1x

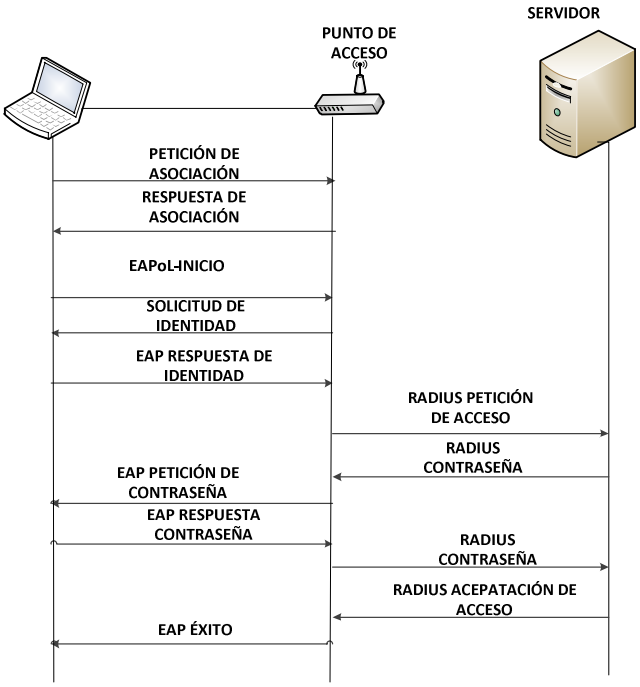

Figura 3.6. Proceso de funcionamiento inalámbrico del estándar

Existen varios modos en los cuales el estándar 802.1X funciona de forma correcta, vamos a revisar qué pasa cuando son varios clientes los que van a querer autenticarse en el puerto y como el estándar funciona para que esto se cumpla eficazmente, los modos son los siguiente:

Modo de un solo host

Como se entiende es en el cuál que existe un solo usuario o cliente el que es detectado por el switch mediante el envío de la trama EAPOL, cuando la autenticación se hace de forma correcta el dispositivo puede acceder al puerto, cuando este cierra sesión el puerto se cierra se pone en estado no autorizado y espera la siguiente autenticación correcta es decir a otro cliente.

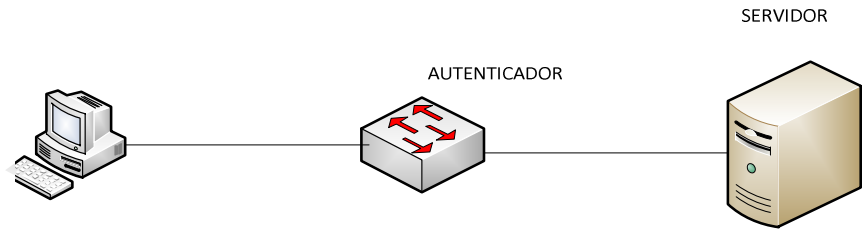

Figura. 3.7. Modelo un solo host

Multimodo Hosts

En este puede conectarse varios hosts a un solo puerto habilitado para el estándar 802.1X, lo que hace este modo es que solo un usuario o cliente de los conectados tienes autorización para 6todos los dispositivo conectados a la red, si el puerto no se autentica de la forma correcta con el cliente se deniega el acceso a todos los dispositivos conectados a la red, como podemos ver en la figura lo que sucede aquí el dispositivo que autentica a los clientes es el Access Point y este actúa a su vez como un cliente del interruptor o switch, además se usa la seguridad portuaria para gestionar el acceso a la red por medio de las direcciones MAC, incluyendo la dirección MAC del access point que actúa como cliente en este caso.

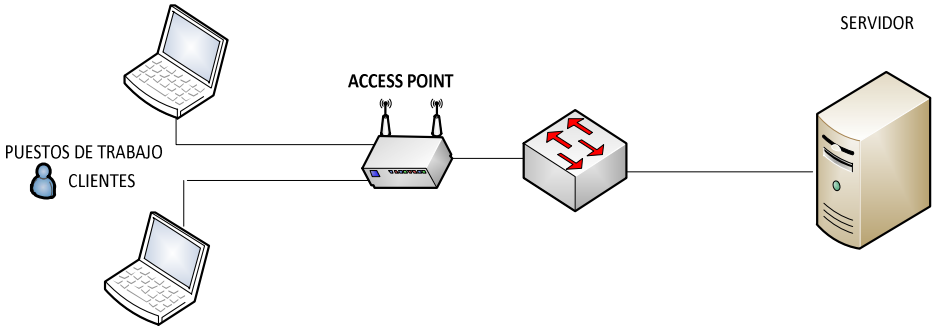

Figura. 3.8. Modelo inalámbrico

Modo de autenticación multidominio

Esta es admitida no para todas las marcas la versión Cisco IOS[52] 12.2 SXI y posteriores este modo lo que hace es que el teléfono ip de cualquier marca y solo un host detrás de este se autentique de forma independiente al estándar 802.1X, ya que se va a tener dos dominios el uno de datos y el otro de voz y solo se permite el acceso a los puertos mediante las direcciones MAC de este modo cada dispositivo es configurado en una vlan diferente el host en la vlan de datos y el teléfono en la vlan de voz, aunque como podemos ver en la figura siguiente solo tiene acceso a un puerto del switch, las vlans se diferencia según los atributos del proveedor los cuales se obtienen el momento en que se autentican en el servidor AAA

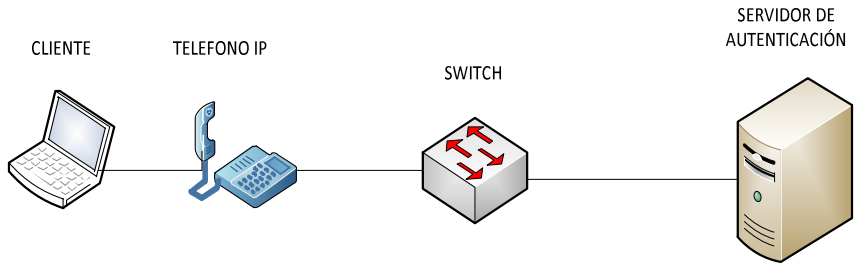

Figura. 3.9. Modelo multimedio

Modo Multiautenticación

Al igual la modo anterior es dado en los switch Cisco los cuales si tiene la institución donde realizaremos la implemantación con IOS 12.2 o posteriores a este, lo que permite a diferencia de los anteriores lo que hace es que un cliente al estándar que este adherido por la vlan de voz y varias autenticaciones en la vlan de datos, cuando tenemos un punto de acceso o un switch conectados al puerto del estándar 802.1X, este modo brinda un sistema

[52] IOS: Imagen del sistema operativo cisco

de seguridad sobre los multiples hosts una vez que se da la auntenticación de cada uno de los clientes de forma correcta, para los que no son usuarios 802.1X/MAB se usa otro método el cual esta basado en la reserva que después serán autenticados de forma individual a este proceso se lo conoce como autenticación basado en la web, esto permite que este método pueda hacer que varios hosts puedan ser autenticados de forma diferente por medio de un solo puerto.

3.4.1. Análisis del protocolo EAP

Conocido como protocolo de autenticación extensible, este protocolo lo que hace es cambiar la información del cliente con un servidor para poder autenticarse desde un punto de acceso, este protocolo trabaja conjuntamente con el protocolo RADIUS Servicio de autenticación remota de llamada de usuarios, este protocolo apoya a los métodos en la cual la conexión sea punto a punto, entre los métodos de autenticación que maneja este protocolo se pueden encontrar, autenticación de clave pública, tarjetas de identificación, contraseñas de un solo uso, tarjetas inteligentes y certificados, cada uno de estos dan un tipo de seguridad diferente el uno mejor que el otro frente a los ataques que se pueden generar.

Ahora vamos a describir las implementaciones que se puede tener por medio del protocolo EAP entre las cuales las principales son las claves secretas y criptografía asimétricas.

Las claves secretas

Se da por claves compartidas entre el usuario y el servidor, donde el servidor usa esta clave para comparar con la contraseña del suplicante para permitir el acceso a los servicios, es por eso que esta no es segura está sujeta a innumerables ataques entre como Man in the Middle.

La aplicación más conocida es la EAP-MD5[53] en la cual se usa un usuario y una contraseña este tipo de aplicación es poco usada en redes inalámbricas debido a los ataques. [12]

Cifrado asimétrico

En este método existe una autoridad que maneja las claves públicas del cliente como del servidor, lo que se hace es enviar dentro del texto la clave en forma cifrada para el solicitante de la misma, el cual teniendo conocimiento de la clave pública puede descifrar de forma privada este mensaje y luego es renviado al servidor RADIUS para repetir el procedimiento, si este proceso no tiene errores se da acceso a la red y sus recursos. [13]

Una aplicación de este tipo es dado por el EAP-TLS[54] Transport Layer Security , que utiliza el algoritmo de cifrado asimétrico RSA, de forma bidireccional, a partir de este nace el EAP-TTLS el mismo que establece un túnel encriptado por el que se manejan el transporte de los datos de la autenticación.

También se conoce el PEAP que significa protección EAP que usa el túnel encriptado descrito anteriormente los cuales los certificados del servidor que funciona como autenticador son necesario no así los EAP-TTLS y EAP-PEAP.

Por último se conoce el EAP-MSCHAPv2, el cuál funciona con un usuario y contraseña y se encapsulan en el EAP de MS-CHAP-v2.

El estándar 802.1X con autenticación EAP también funciona para redes inalámbricas para ello se usa lo conocido como WPA que significa Wifi Protected

[53] EAP-MD5: Método de autenticación 802.1X
[54] EAP-TLS: Capa de transporte seguro

Access para ello tenemos diferentes tipos de administración y autenticación de claves que funcionan conjuntamente con el estándar 802.X/EAP para permitir la autenticación y acceso a la red, ya vimos las características del 802.1X/EAP y sabemos que trabaja con el servidor RADIUS, el estándar WPA puede o no funcionar conjuntamente con RADIUS, el modelamiento para no usar el Servidor RADIUS es dado por el WPA-PSK que no usa la encriptación en las tramas trabaja con una cadena de código ASCII[55] para cada dispositivo que quiere autenticarse, la que si usa encriptación en las tramas es empleada para WEP[56].

La conexión que genera más seguridad en redes inalámbricas es dada por WPA[57] empleando RADIUS, después se la cataloga como la más segura es WPA-PSK y por último la menos segura es WEP. [14]

3.4.2 Servidor RADIUS

El significado de mismo es Remote Autentication Dial in User Server, este es un protocolo de autenticación de seguridad basado en un cliente y un servidor, el cual es usado para proporcionar servicios de autenticación, autorización y administración AAA, usa para la conexión usa el puerto 1812 UDP para los mensajes de autenticación y el puerto 1813 para los mensajes de administración de cuentas.

Una de las principales característica del protocolo RADIUS está en que puede notificar cuando se realiza el inicio y fin de una sesión siendo útil para llevar unas estadísticas de la conexión de cada usuario.

[55] ASCII: Digo Estándar Estadounidense para el Intercambio de Información
[56] WEP: Privacidad Equivalente a cableado
[57] WPA: Acceso wifi protegido

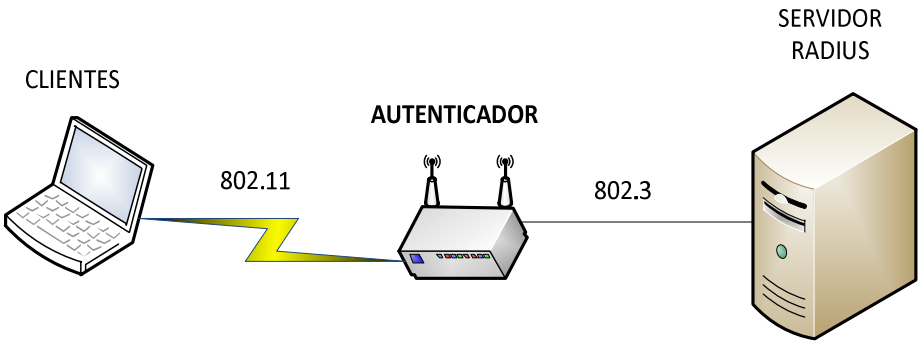

Figura 3.10. Modelo de autenticador RADIUS

Como vemos en la figura anterior el cliente puede ser un servidor de acceso telefónico, un servidor VPN o un punto de acceso inalámbrico el cual envía los parámetros establecidos de autenticación al servidor RADIUS como un mensaje, el servidor RADIUS es el cual autentica y autoriza la petición del suplicante, después el mismo envía la respuesta al cliente si es posible o no la conexión para esto se usa los protocolos PAP[58], CHAP[59] o el EAP.

El autenticador usa una variante de EAP para pasar de un lado al otro de la arquitectura propuesta, el funcionando del autenticador es precisamente como un puente. Desde el suplicante al autenticador, el protocolo es EAP sobre LAN (EAPOL) o EAP sobre WLAN (EAPOW). En el otro lado, el protocolo usado es RADIUS.

3.4.3. Arquitectura 802.1X

Ya hemos visto cuales son los protocolos que se manejan en el estándar 802.1X y cuáles son sus características, ahora vamos a ver cómo es su arquitectura para que se pueda dar el cambio de información correctamente entre un cliente y un servidor atravesando por un autenticador y así llegar a autenticarse.

[58] PAP: Protocolo de autenticación con contraseña
[59] CHAP: *Protocolo* de autenticación por desafío mutuo

Recordemos que EAP puede trabajar con diferentes tipos de autenticación como lo son las claves secretas o cifrado asimétrico, como MD5, contraseñas de un solo uso, Kerberos, o los diferentes tipos de encriptación como son PKE, etc que ya los estudiamos anteriormente, ahora solo vamos a ver cómo se distribuyen, encapsulan para su funcionamiento.

El proceso de autenticación del estándar 802.1X se da en la capa 2 de OSI que es la capa de en enlace de datos, para completar con éxitos el proceso se realiza en 3 capas conocidas como capas EAP, capa de métodos, capa de autenticación como indica la figura y vemos que EAP es un encapsulado de la capa de enlace. [16]

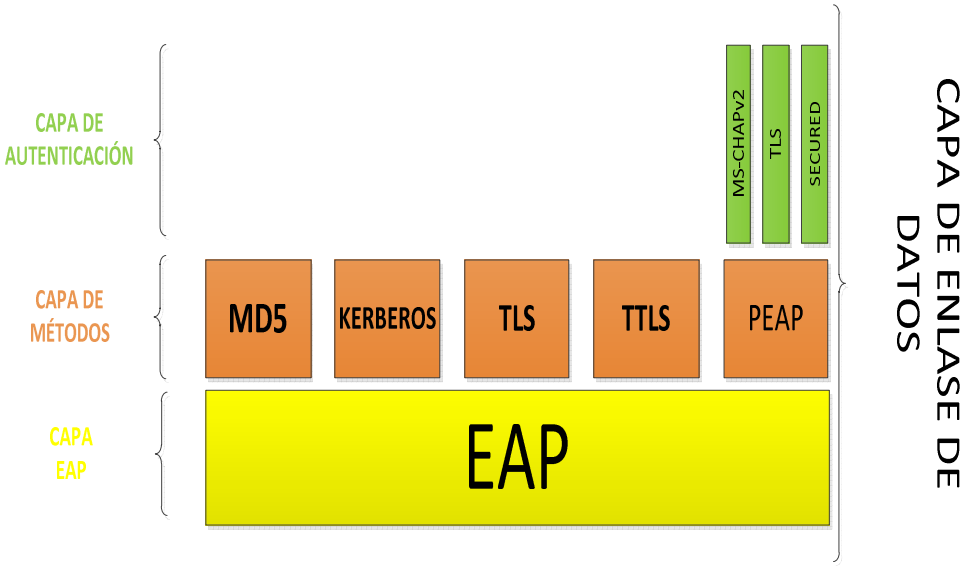

Figura. 3.11. Arquitectura 802.1X por capas

3.4.4 Estudio de la trama del estándar 802.1X

Por lo general los datos que se envían están siendo enviado por dos tipos de conexiones ya sean de forma alámbrica e inalámbrica las cuales son manejadas por los protocolos

802.11 para inalámbricas y la conexión alámbrica por medio del protocolo 802.3[60] como vemos en la siguiente figura.

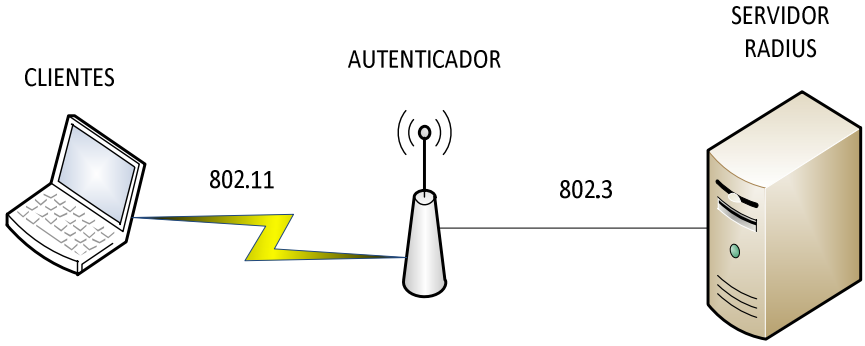

Figura. 3.12. Modelo de conexiones

Vamos a estudiar cada una de estas tramas y su funcionamiento dentro del estándar 802.1X, empezaremos por el protocolo 802.3 o Ethernet que es el que maneja las conexiones cableadas. [17]

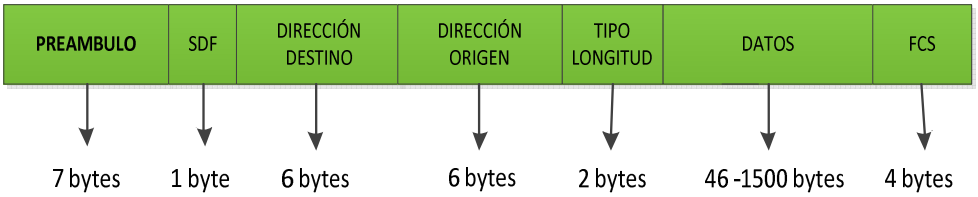

Figura. 3.13. Trama Ethernet

Preámbulo: Es el campo que sincronizan los bits

SDF: Es el que indica el tiempo de inicio de la trama si este no tiene sincronismo con el final de la trama puede perder parios bits de preámbulo para esto se agrega un 11 al fin de la misma

[60] 802.3 Estándar paraconexión cableada

Dirección Destino: Es la dirección MAC del equipo donde se quiere llegar en la comunicación.

Dirección Origen: Es la dirección MAC del equipo emisor en la conexión.

Tipo/Longitud: Las conexiones Ethernet usan el campo como tipo, y las conexiones 802.3 usan el campo longitud.

Datos: Es el campo más grande esto se debe a que a más de llevar la información del usuario lleva la cabecera de transporte y la cabecera de red.

Relleno: Este es usado ya que según el estándar 802.3 se sabe que los datos deben tener un tamaño que vaya desde los 64 bytes y cuando es pequeño el tamaño del campo Datos es completado con bytes de este campo.

FCS: Calcula CRC de la trama que se está enviando esta da la Secuencia de chequeo de trama.

Ahora vamos a ver la trama dada por la conexión inalámbrica 802.11 y la función que cumple cada uno de sus campos. [18]

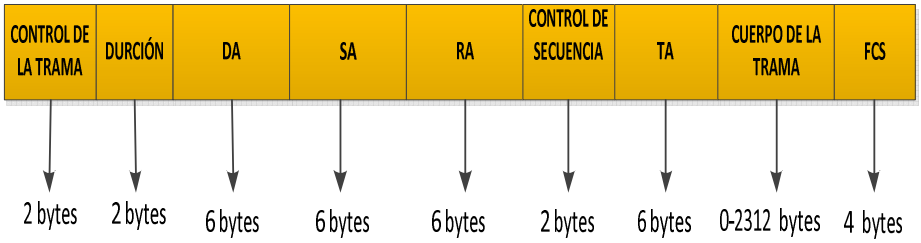

Figura. 3.14 Trama del estándar 802.11

Control de trama: Tiene varios parámetros dentro del mismo y es el que maneja a la trama y su funcionamiento.

Duración: Este es el tiempo en milisegundos en el que se va a transmitir la trama para conexión.

DA: Es el campo de la dirección de destino es decir este tiene la dirección MAC a la cual se quiere enviar los datos.

SA: Es el campo de la dirección origen es decir este tiene la dirección MAC es decir de donde se va a empezar la conexión.

RA: Campo de dirección del receptor este tiene consigo la dirección MAC del access point o dispositivo inalámbrico donde va a llegar la comunicación.

TA: Campo de la dirección del transmisor es la dirección MAC del Access pointo o dispositivo inalámbrico que empezó a transmitir la trama.

Cuerpo de la trama: Es donde se lleva la información que se está transmitiendo es decir todos los datos están en este campo.

FCS: Calcula CRC de la trama que se está enviando esta da la Secuencia de chequeo de trama.

Una vez conociendo las tramas de los diferentes tipos de conexión que existen vamos a detallar las tramas conocidas por el estándar IEEE 802.1X en cada uno de sus campos con la ayuda del siguiente gráfico. [19]

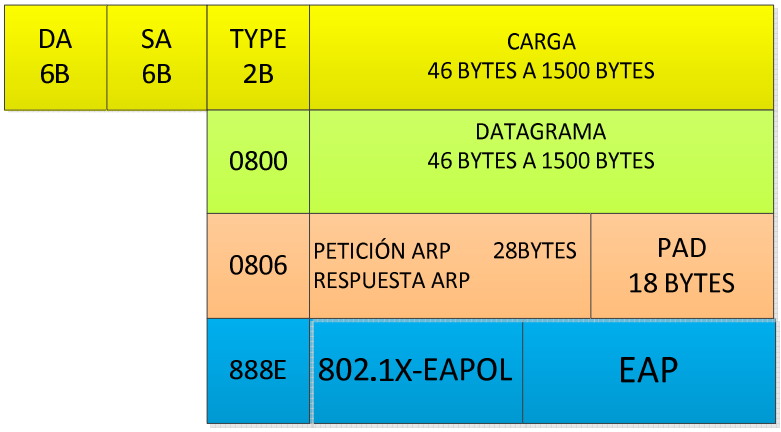

Figura.3.15. Trama estándar 802.1X

DA: En este campo lo que se tiene es la dirección MAC de destino, es decir la dirección del dispositivo que va a finalizar la conexión.

SA: En este campo lo que se tiene es la dirección MAC de origen.

TYPE: Este puede variar indica tipo de conexión existe puede ser cualquiera de los siguientes:

TIPO	NOMBRE
0800	DATAGRAMA IP
8006	ARP
8035	RARP
888E	802.1X
8863	TRAMA DE

Tabla 3.1 Campo tipo de la trama

Como vemos el que maneja el estándar IEEE 802.1X viene con el tipo 888E que observamos en la parte azul de la figura anterior, entonces vamos a estudiar el tipo 888E que tiene dos cabeceras la una de EAPOL y la otra por la cabecera EAP.

CABECERA EAPOL/EAP

Al lado derecho del tipo tenemos el campo EAPOL/EAP el que contiene 4 octetos.

Versión de Protocolo: Es el tipo de versión que está siendo usada por EAPOL la cual es tomada según el que envía los datos el valor por default es 0000 0001 el tamaño de este campo es 1 byte

Tipo de Paquete: Existen 4 parámetros en este campo los cuales podemos ver en el cuadro.

TIPO	NOMBRE
PAQUETE EAPOL	0000 0000
INICIO EAPOL	0000 0001
LOGOFF EAPOL	0000 0010
CLAVE EAPOL	0000 0011

Tabla 3.2 Campo tipo de paquete de la trama

Longitud del Paquete: Aquí va el cuerpo del paquete su tamaño es de 2 bytes.

CABEZERA EAP

Código: Vamos a representar en el siguiente cuadro el número de código y que hace cada uno de ellos, siendo en total 4 códigos, su tamaño es de 1 byte.

CÓDIGO	ACCIÓN
CÓDIGO 1	PETICIÓN
CÓDIGO 2	RESPUESTA
CÓDIGO 3	EAP EXITOSO
CÓDIGO 4	EAP NO EXITOSO

Tabla 3.3 Campo código EAP

Identificador: Es el campo que asocia las respuestas con las peticiones que le llegan, su tamaño es de 1 byte.

Longitud: Es el tamaño del paquete EAP este es de 2 bytes.

3.4.5 Mejoras que se espera a partir de la implementación

Este plan piloto se realiza con la expectativa de ver sus resulta dos para brindar en futuro una buena seguridad en la red de la institución, en este Ministerios existen gran cantidad de dispositivos unidos a la red, actualmente en su mayoría de dispositivo se conectan de forma alámbrica a la red predominando sobre la conexión de tipo inalámbrica, pero es este estándar válido para las dos formas de conexión como ya lo hemos visto y analizado anteriormente.

No solo se usan host de escritorio por sus costos y el tipo de conexión que manejan, a más de ello se piensa en la seguridad que los mismos por su forma de unirse a la red brinda a la información que maneja cada uno de los funcionarios que muchas veces se cataloga de confidencial, los dispositivos inalámbricos son vistos como no seguros para esta información pero con el estándar analizado vamos a dar mayor seguridad a este tipo de dispositivos que en el futuro serán los más usados no solo en la institución por las ventajas

de movilidad y comodidad que brinda a los usuarios, en un tiempo futuro las conexiones remotas van a predominar, en especial con funcionarios que se desplazan, no olvidemos en la actualidad el Ministerio de Telecomunicaciones y Sociedad de la Información trabaja con muchos proyectos en todo el país entre ellos los Infocentros en los cuales los encargados del mismo trabajan en diferentes ciudades capacitando e implementando estos proyectos, pero ellos por seguridad a los datos que manejan muchas veces sus equipos están fuera de los dominios de la institución, ya que los permisos a recursos que pueden usar son innumerables, por medio de este estándar se puede llevar el control y estadísticas de los recursos que usa y como los utiliza favorablemente o no para seguridad del sistema que manejan.

Una vez que el mismo se la implante en toda la institución y en sus servidores vamos a ver que los ataques, amenazas de todo tipo disminuirán, tendremos portales web más seguros, los accesos remotos a la red de la misma forma, la autenticación no será muy notoria en los usuarios de la red, pero si será de gran ayuda a todos los recursos de la red de la institución.

3.4.6 Estudio de implantación del protocolo con los dispositivos físicos que posee la institución.

Ya hemos visto los dispositivos que forman parte de la red de Ministerio de Telecomunicaciones y Sociedad de la Información, lo que necesitamos es que sean compatibles con el nuevo estándar de autenticación a implementar, estos equipos son el Switch core 4507R, los dos switch por cada piso Switches catalyst serie 2960 y el access point cisco aironet 1310 cada uno de estos en sus características internas están que soportan el estándar IEEE 802.1X de autenticación.

Como hemos visto anteriormente podemos tener conexiones ya sean de tipo alámbrico como inalámbrica, respetando todos las normativas y políticas internacionales y de la institución.

Todos los equipos que maneja en ministerio son Cisco tanto alámbrico como inalámbricos y este fue uno de los pioneros en el uso del estándar, por lo cual no tendremos ningún problema de compatibilidades, los servidores pueden ser configurados en cualquier host que dispongan el administrador de la red.

Al ser un plan piloto las configuraciones que vamos a realizar son con equipos que están disponibles en la institución, los ISOs que están instalados en cada uno de los switch son aceptables y no dan ningún problema si las configuraciones internas en los mismos se dan sin errores, los usuarios a instalarlos son de prueba y se instalarán con equipos que pertenezcan al Departamento de Gestión Tecnológica, y están activos para los administradores de la red.

CAPÍTULO IV

ADMINISTRACIÓN DE LA RED A PARTIR DEL ESTANDAR 802.1X

4.1 Configuración de los dispositivos.

Vamos a configurar los dispositivos anteriormente en la topología de la red como es un switch que actúa como autenticador, el servidor para el mismo vamos a usar el sistema operativo Ubuntu y los dispositivos de cada usuario de la red.

4.1.1 Configuración de servicio AAA

Las configuraciones para el servidor AAA[61] que vamos a mostrar las realizaremos en el sistema operativo Ubuntu 11.04 ya que muestra estabilidad en comparación a otras versiones, aquí instalaremos el servidor de código abierto FREERADIUS que es uno de los más populares que nos ofrece RADIUS ya que tiene gran versatilidad, el mismo va a tener una base de datos para los usuarios y capacidad de responder a las peticiones de los usuarios para acceder a la red. [21]

[61] AAA: Servidor Autenticación, Autorización y Contabilización

Antes de empezar la instalación vamos a ingresar al archivo sources.list para actualizar o cambiar el repositorio, esta vez utilizaremos el siguiente:

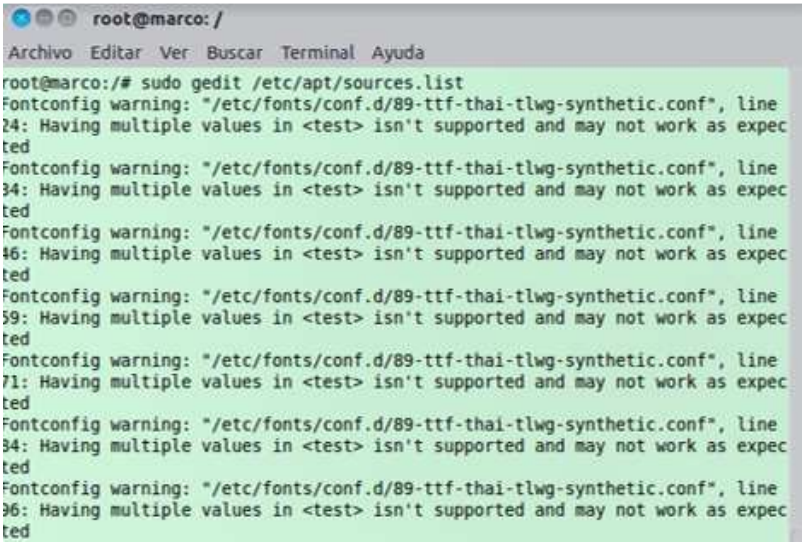

Figura 4.1. Ingreso al archivo sources.list

Lo guardamos con el mismo nombre.

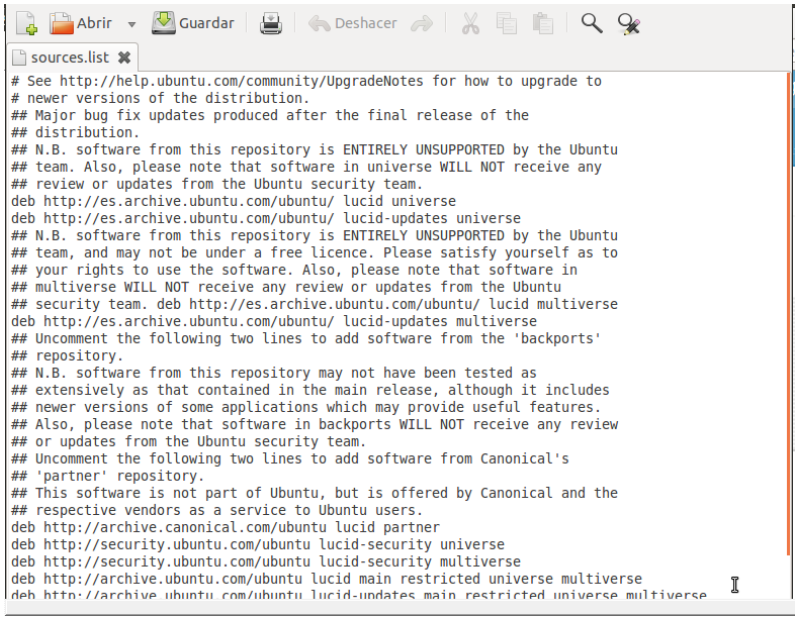

Figura 4.2. Nuevo repositorio con librerias necesarias

Para terminar actualizamos con el comando apt-get update y podremos empezar con la simulación, vamos a ir instalando todos los programas que se necesitan para el correcto funcionamiento de radius, empezaremos con mysql tanto como servidor como del cliente.

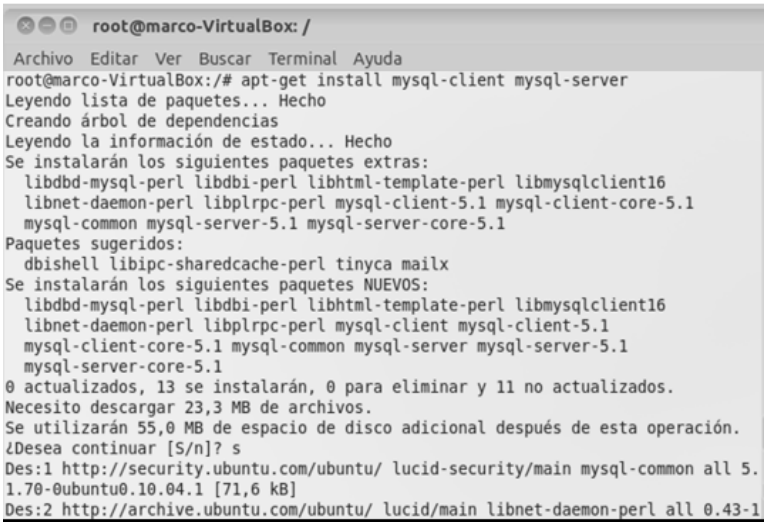

Figura 4.3. Instalación de mysql servidor y cliente

El espacio que ocupa este programa en el disco es de aproximadamente 55 MB si estamos de acuerdo aprobamos la instalación con un S.

Para seguir con la instalación nos pregunta la contraseña que va a tener el usuario root en el servidor.

Figura 4.4. Ingreso contraseña del servidor mysql

En la siguiente imagen confirmamos la contraseña para evitar errores en el acceso al usuario root, si esta no se la configura de forma correcta la instalación se ve interrumpida.

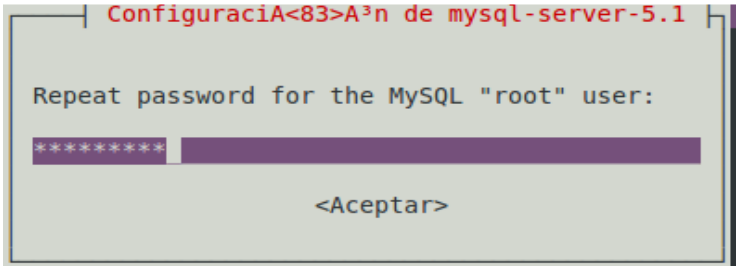

Figura 4.5. Confirmación de contraseña usada

Si no tenemos ningún problema de instalación esta figura representa la finalización del mismo donde se hace la configuración con la ultima verión de este caso Ububtu que estamos usando y comienza a correr el programa.

Figura 4.6. Progreso de funcionamiento de mysql

Continuamos con la instalación de phpmyadmin el cual nos va a servir como base de datos y almacenamiento de datos de los usuarios, ese usa 40,2 MB en el disco para su instalación si deseamos la instalación colocamos la S.

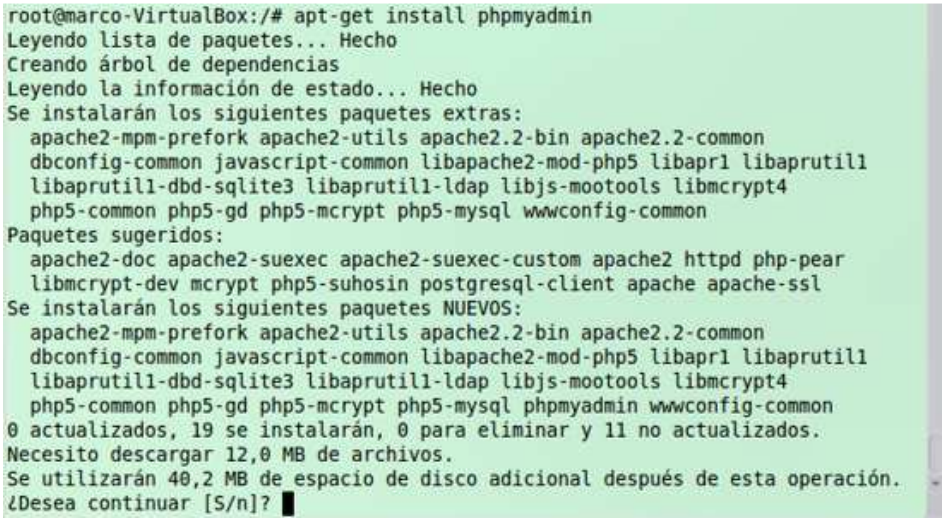

Figura 4.7. Instalación de phpmyadmin

Es necesario instalar apache2 para su funcionamiento y damos la opción aceptar, después de esto, confirmamos si la instalación que deseamos va hacer de forma manual o de forma automática, en nuestro caso vamos a configurar la base de datos por medio del dbconfig-common y aceptamos la misma.

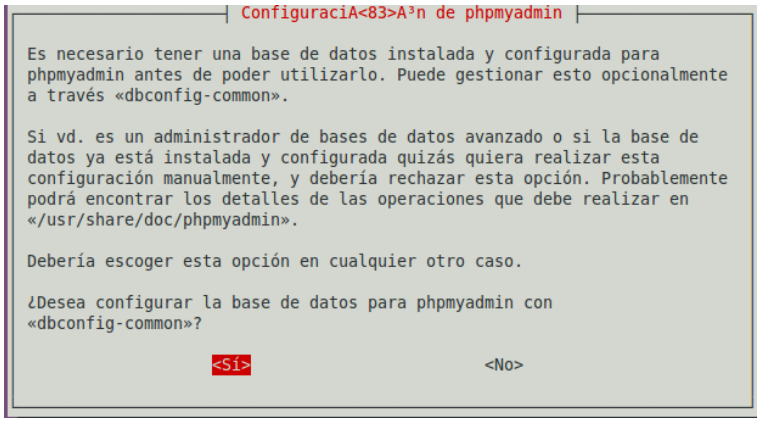

Figura 4.8. Configuración automática de phpmyadmin

Instalaremos los complementos de php con el siguiente comando apt-get install php5 php-pear php5-gd php-DBP.

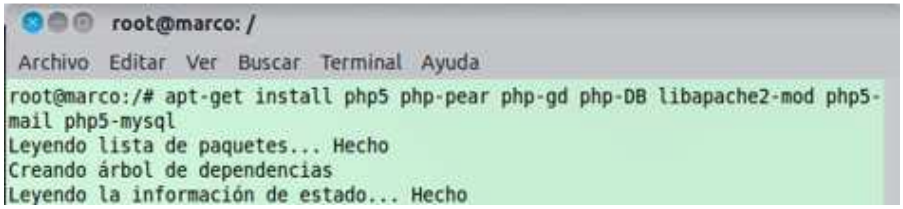

Figura 4.9. Instalación de todos los complementos de php

Seguimos con la instalación de freeradius para esto tenemos que instalar el mysql del mismo y la utilidades que el mismo maneja esto se lo puede a partir de un solo comando como es apt-get install freeradius freeradius-mysql freeradius-utils

Vamos a dar la contraseña por la que vamos a ingresar a phpmyadmin si se deja esta vacía se genera una contraseña aleatoriamente.

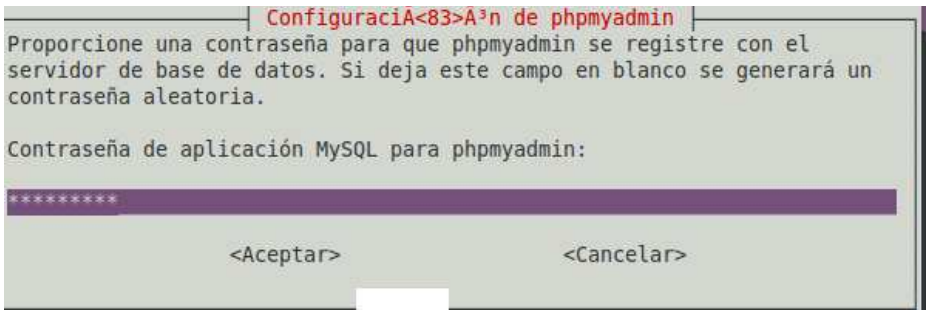

Figura 4.10. Ingreso de la contraseña de phpmyadmin que se vincula al servidor radius

Confirmamos la contraseña de ingreso, esta contraseña nos servirá para acceder vía browser para configuración del mismo gráficamente.

Ahora vía browser vamos a ingresar como empezamos la instalación localmente ponemos la dirección http://localhost/phpmyadmin/, si nos da el siguiente error de Not Found con error de apache 2.2.16.

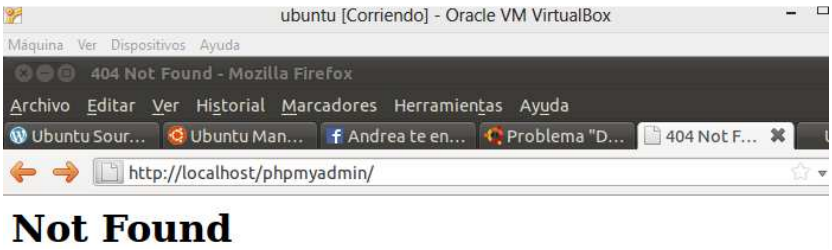

Figura 4.11. Ingreso a phpmyadmin vía browser

Esto no quiere decir que está mal configurado e instalados los programas anteriores sino que necesitamos aumentar en la lista de control una línea para acceder al mismo, para ellos ingresamos al archivo apache2.list por medio del comando sudo /etc/apache2/apache.conf.

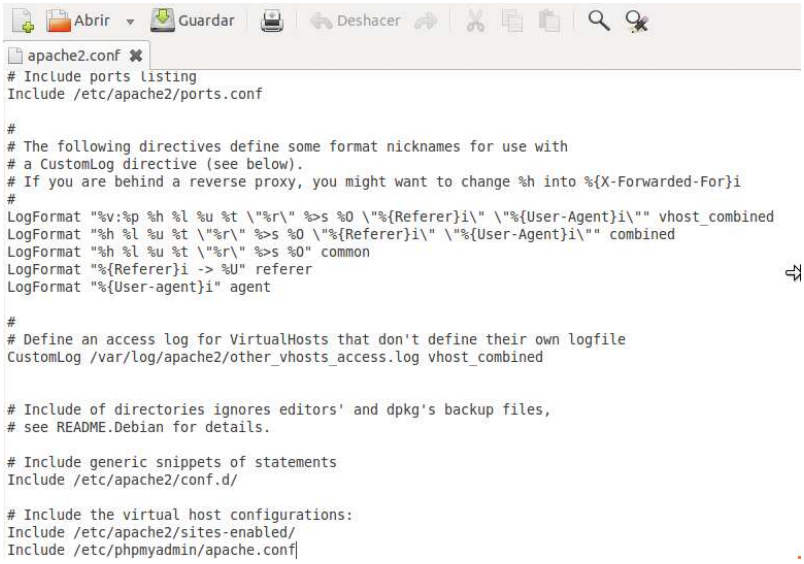

Figura 4.12. Ingreso al archivo sources.list

Si acudimos a un navegador de preerencia y colocamos nuevamente http://localhost/phpmyadmin y vemos que se abre la aplicación correctamente, aquí ingresamos los datos manualmente de usuario y contraseña los que ya pusimos el momento de la instalación.

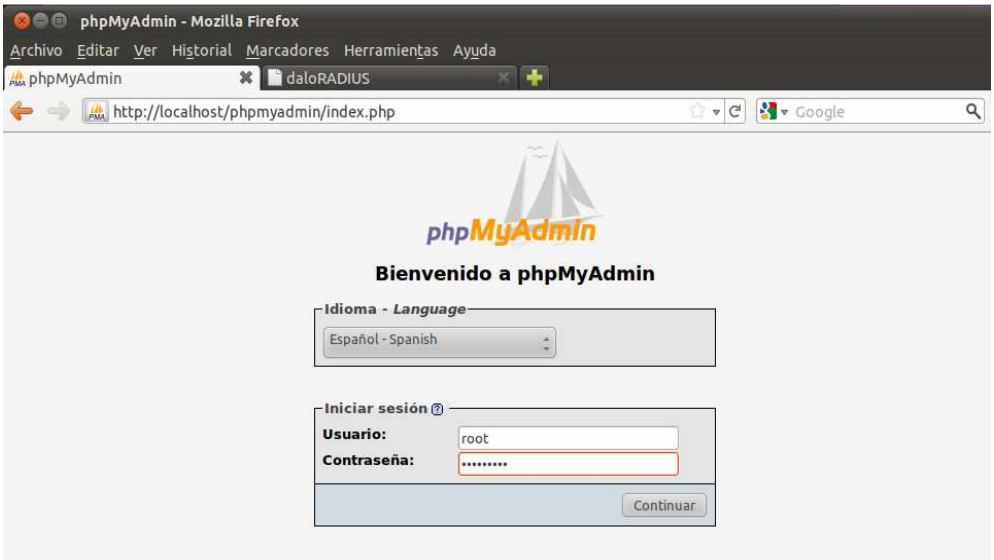

Figura 4.13. Pantalla de phmyadmin vía browser

Vamos a comprobar le funcionamiento del servidor por medio de un usuario de tipo local para esto usamos el comando radtest, la estructura del funcionamiento del mismo es el siguiente: rastest “usuario” “contraseña” “local host” “puerto” testing123.

Si al final mos aparece **rad_recv: Access-Accep packet** este esta correctamente instalado y configurado y su funcionamiento apropiado, si usamos un usuario que no está dentro de este servicio local el resultado que arooja es **rad_recv: Access-Reject packet,** también nos da la dirección del host el puerto un id que usa y el tamaño.

Figura 4.14. Radtest con usuario de prueba

Para que funcione el servidor radius debemos configurar nuevas instancias que son las siguiente: entramos a la carpeta que se creo con la instalación de freeradius esto con desde la raíz colocando el comando cd/etc/freeradius.

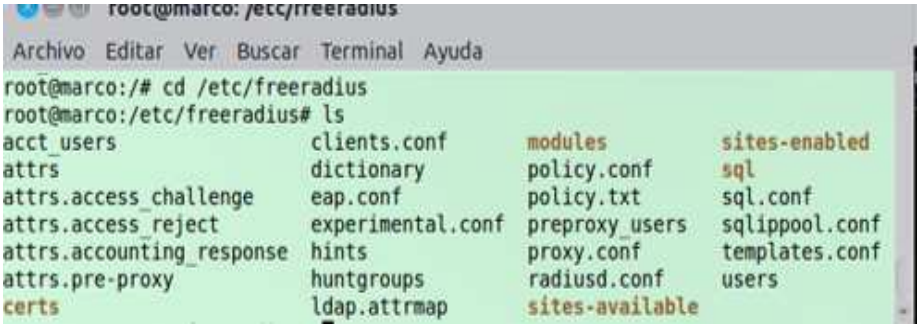

Figura 4.15. Ingreso a la carpeta freeradius

Lo siguiente es entrar a la opción radiusd.conf en forma de editor esto se hace con el comando nano radius.conf, dentro de este descomentamos quitando el símbolo # de la línea INCLUDED sql.conf de la siguiente manera.

Figura 4.16. Descomentar include sql.conf

Cuando ya descomentamos tenemos que guardar mediante ctrl+0 aceptamos el mismo nombre y para salir crtl+x, tenemos que crear la base de datos de radius para eso debemos ingresar mysql si estamos en la raíz ponemos el comando cd etc/freeradius/sql/mysql, ya adentro de mysql lo que debemos hacer es ingresar el comando mysql –u root –p aquí ingresamos la contraseña anteriormente colocada, si esto se hace correctamente entonces entramos a configurar el mysql.

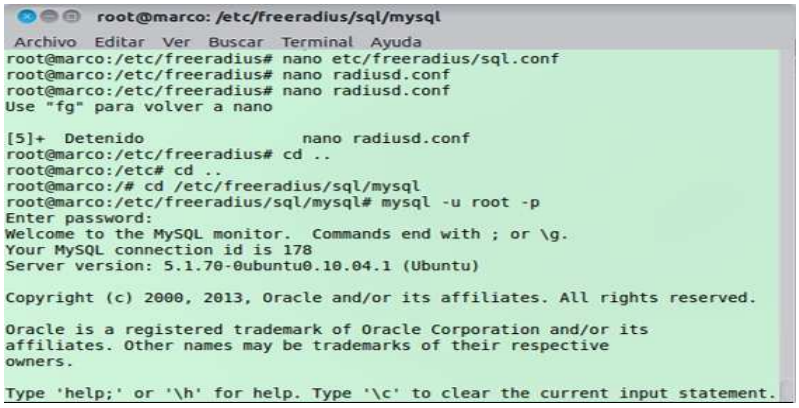

Figura 4.17. Ingreso a mysql con usuario y contraseña

Lo siguiente es la creación y configuracion de la base de datos que le vamos a poner el nombre de radius con por medio del comando create database radius, el la figura que presentamos a continuación muestra un error en nuestro caso porque la base de datos ya fue creada pero esto no ocurrira en una configuración nueva, lo siguiente en la configuración es colocar el comando grand all on radius.* to radius@localhost identifiel by ‘contraseña’ si esto es correcto saldra ok, si es asi salimos por medio del comando quit.

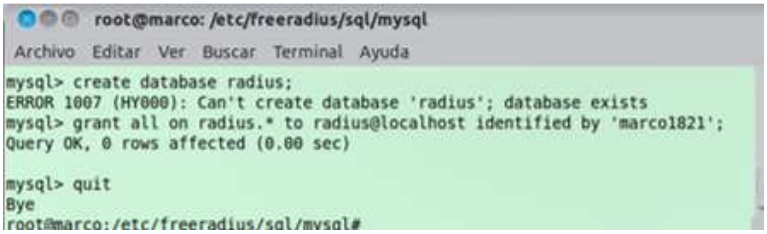

Figura 4.18. Creación de la base de datos y sus tablas

Si queremos cambiar la contraseña anteriormente configurada lo podemos hacer ingresamos al archivo sql.conf por medio del comando nano sql.conf una vez aquí podemos editar el archivo, cuando este realizado el cambio podemos guardar crtl+O, aceptamos y salimos.

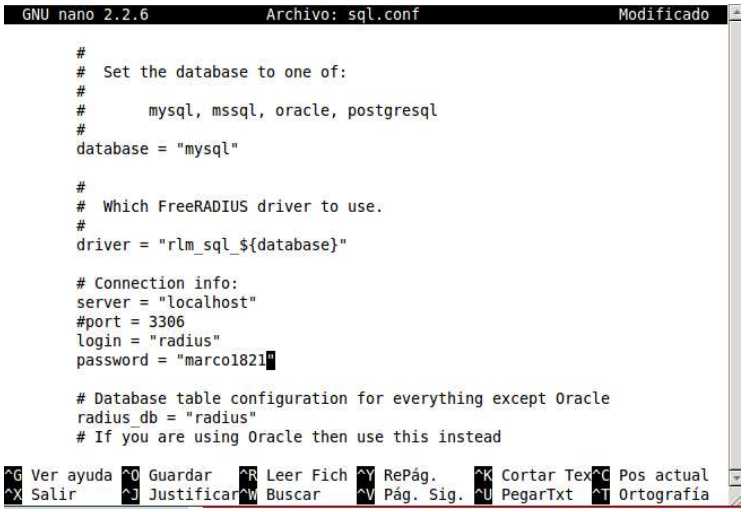

Figura 4.19. Cambio de la contraseña de radius

Lo último que queda para terminar estas configuraciones es el ingresar a freeradius, ya estando aquí vamos a editar el default de sites-available con el comando nano sites-available/defaul, estando dentro del mismo vamos a editar este archivo quitando el comentario borrando el numeral en el sql de authorize y accounting, una vez borrados damos ctrl+o para guardar damos enter par que el archivo tenga el mismo nombre y por último salimos con un ctrl+x, para facilitar la búsqueda usamos ctrl+w y una palabra que este cerca al sql buscado.

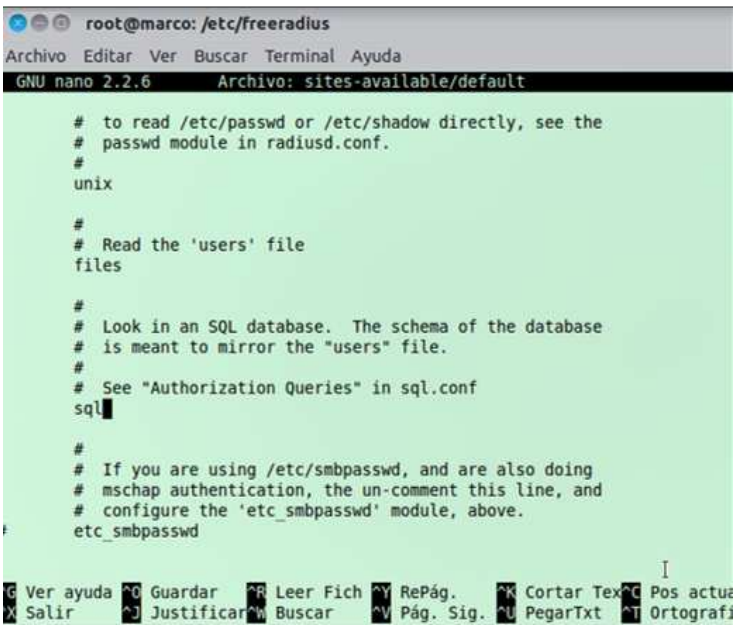

Figura 4.20. Descomentamos lineas con sql en autorización

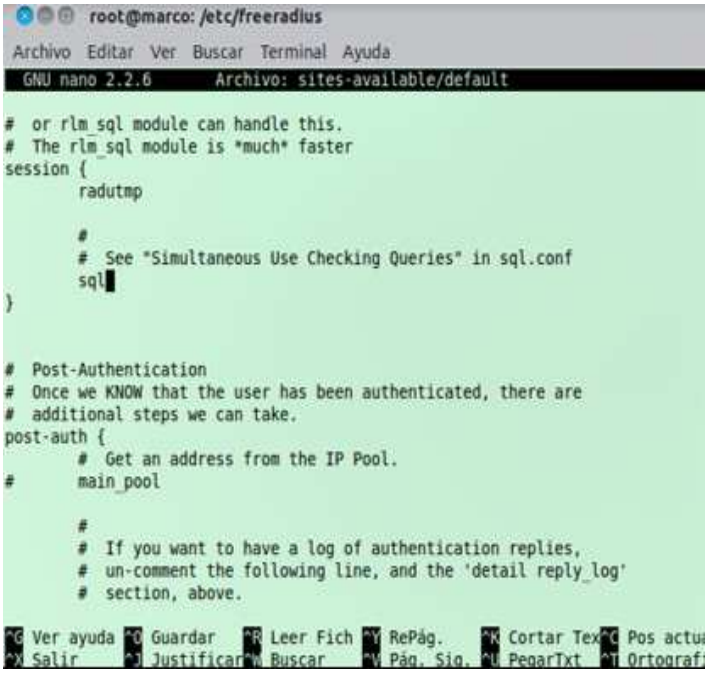

Figura 4.21. Descomentamos líneas con sql en sesión

Para seguir veremos como ingresar usuarios en el phpmyadmin que ya lo abrimos anteriormente pues bien ahora vamos a ir al costado izquierdo e ingresar a la base de datos que creamos con el nombre de radius.

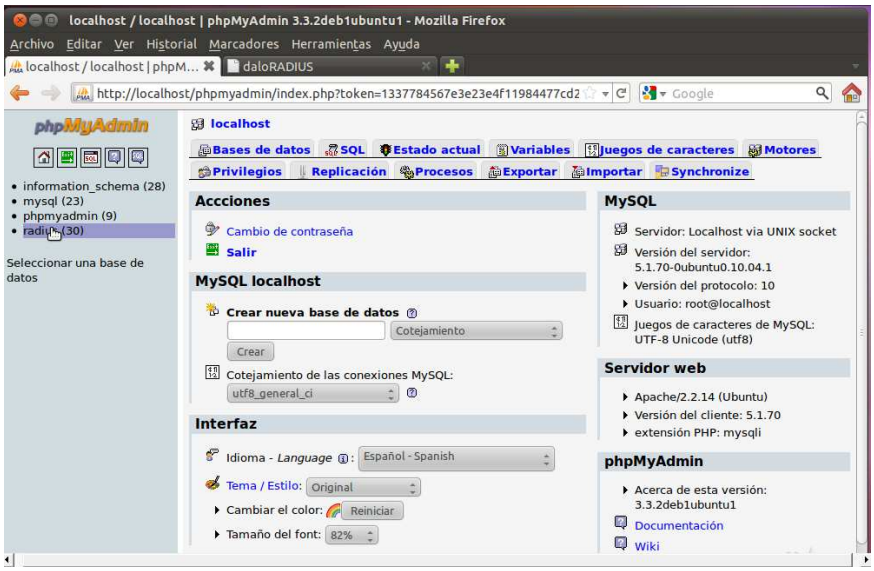

Figura 4.22. Ingreso base de datos de radius

Ahora ingresamos al radcheck ubicado en la parte inferior izquierda escogiéndola, esta es creada para colocar los usuarios que van a poder acceder a la red posteriormente, si no tenemos esta opción algún tendremos que corregir este error.

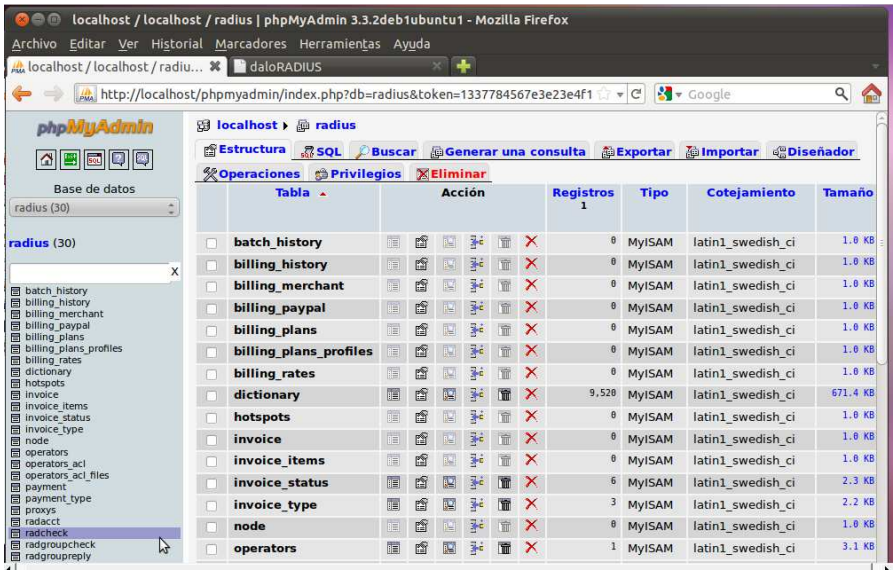

Figura 4.23. Tabla radcheck donde se crean usuarios

Vamos a la opción insertar

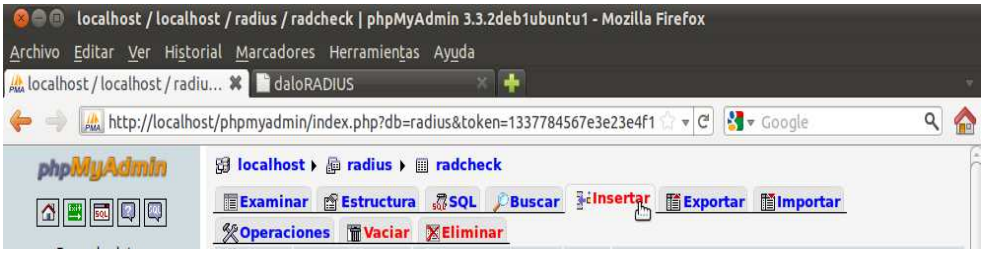

Figura 4.24. Opción insertar un nuevo usuario

Aquí ingresamos los datos del usuario como nombre atributos y contraseña, ingresaremos el nombre “patricio” con atributo “password” y value “marco1821” e ingresamos el dato en la base.

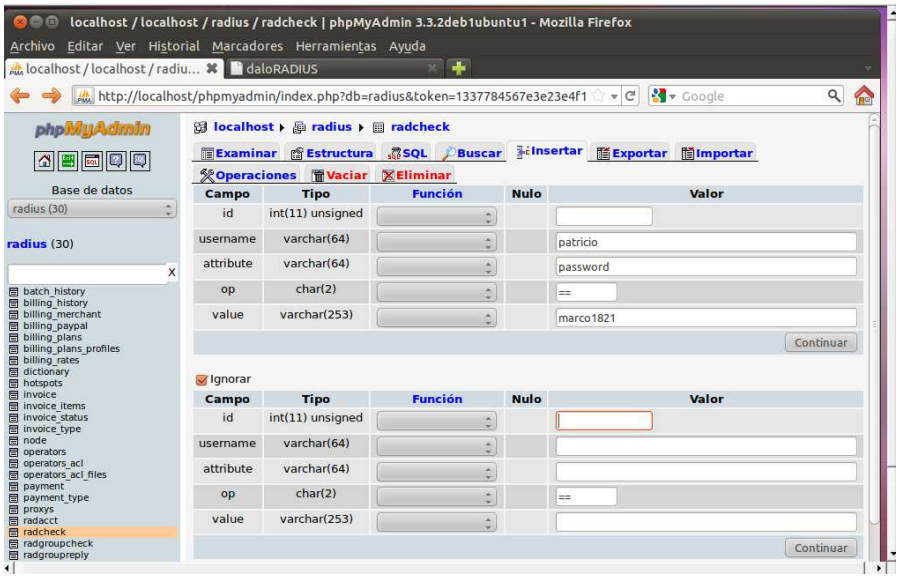

Figura 4.25. Campos de datos para creación de usuarios

Ya insertada nos aparece una tabla que indica esta situación si se muestra algún problema también nos indica esta opción.

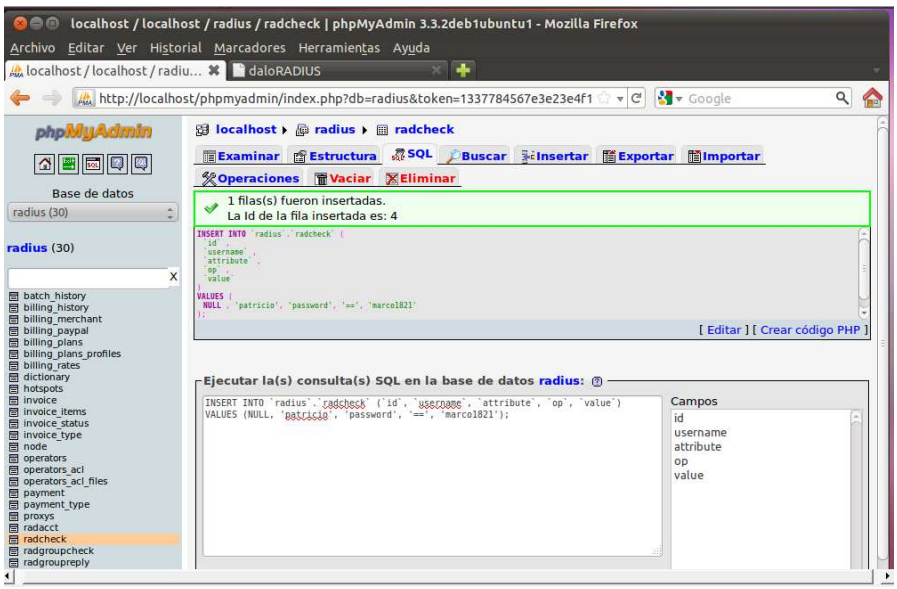

Figura 4.26. Visualización nuevo usuario

Colocamos ahora la opción examinar en esta opción se nos presentan todos los usuarios que con anterioridad fueron modificado o cambiados.

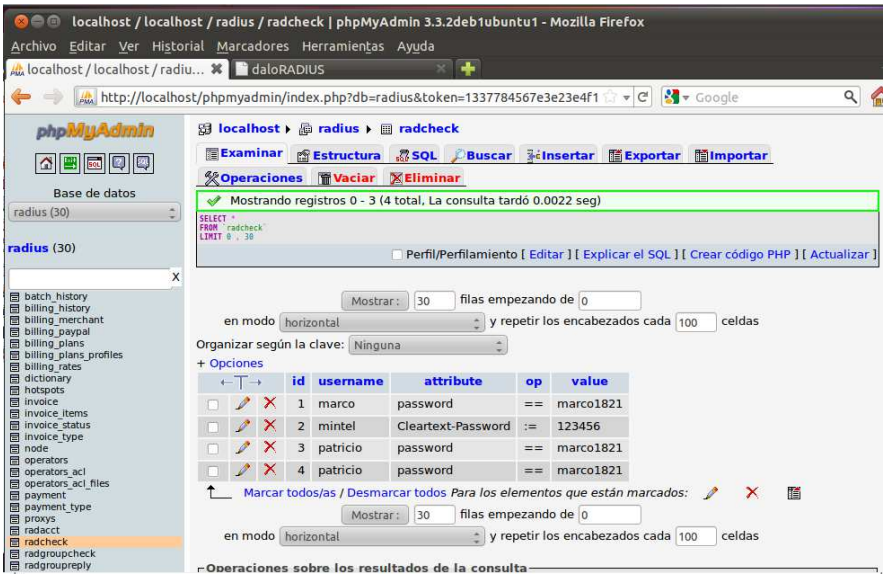

Figura 4.27. Lista de usuarios dentro de la base de datos

Podemos cambiar las opciones o atributos del mismo con la opción de estructura como se lo representa a continuación.

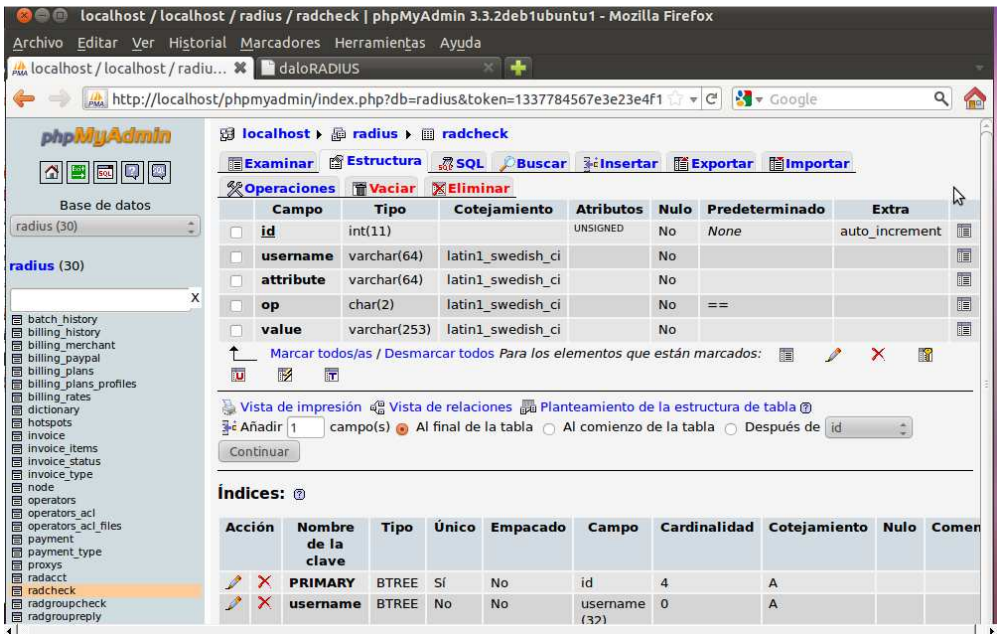

Figura 4.28. Examinación de campos de usuario

Comprobando el correcto funcionamiento del phpmyadmin y creando usuarios para comprobar el mismo, empezaremos con la configuración de DALORADIUS.

Vamos a acceder a la página de descarga de Daloradius y sus paquetes del siguiente link: http://sourceforge.net/projects/daloradius, descargamos una aplicación para la administración web de RADIUS que gestiona los puntos de acceso y las implementaciones del ISP.[62]

[62] ISP: Proveedor de Servicios de Internet

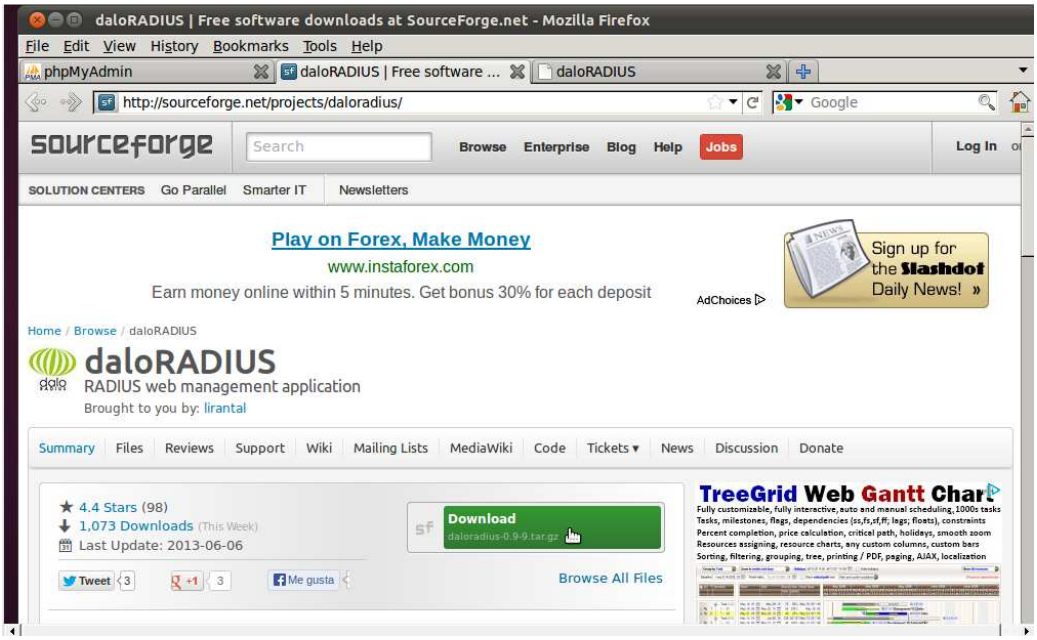

Figura 4.29. Página de descarga de Daloradius

Realizamos la descarga y ahora acudimos donde se realizó la misma, ahora vamos de extraer la carpeta comprimida y para facilidades del nombre dejamos a la carpeta descomprimida con el nombre daloradius.

Figura 4.30. Carpeta de descargas realizadas por Ubuntu

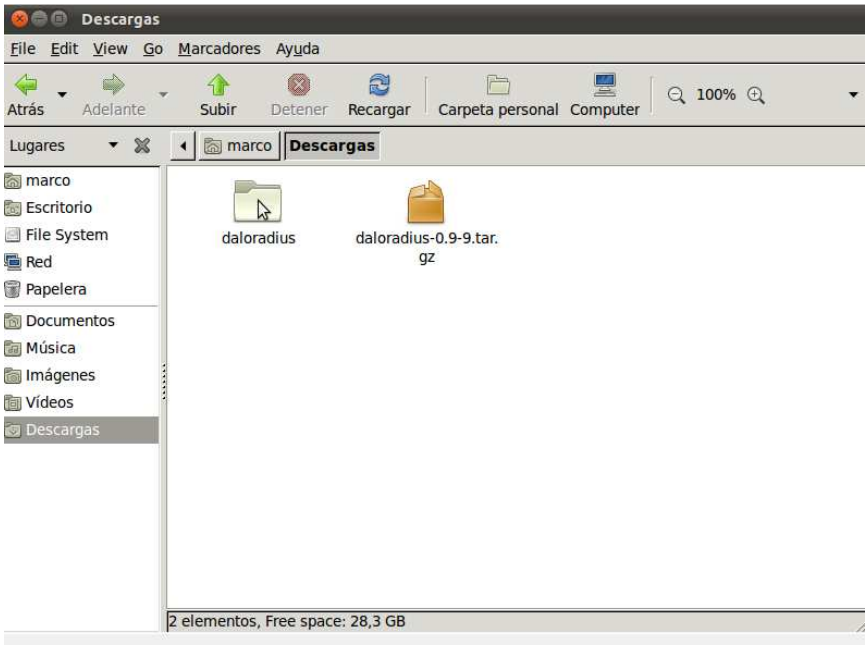

Figura 4.31. Descomprimimos la carpeta daloradius

Ahora vamos a copiar mediante el terminal la carpeta daloradius a servidor web www, esto se logra introduciendo el comando cp/home/marco/Descargas/daloradius/var/www -R

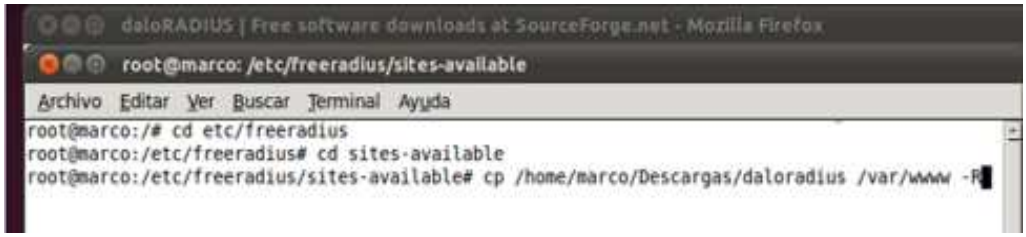

Figura 4.32. Copia de la carpeta a la carpeta del root

Después del paso anterior colocamos el comando chown –R wwwdata:wwwdata/var/www/marco/dalordius

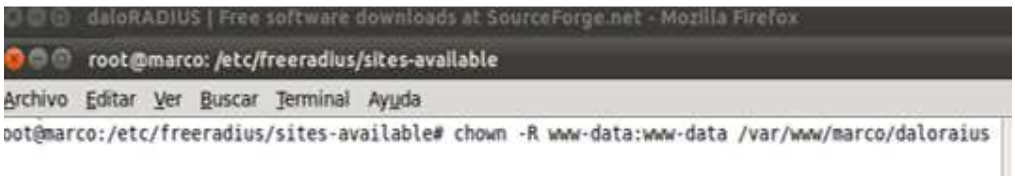

Figura 4.33. Pegamos de la carpeta a la carpeta del root

Vamos a ver si todos los paquetes se instalaron de la forma correcta dentro de daloradius para ver esto ingresamos el comando cd /var/www/daloradius/libray y dentro del mismo desplegamos los contenidos con el comando ls

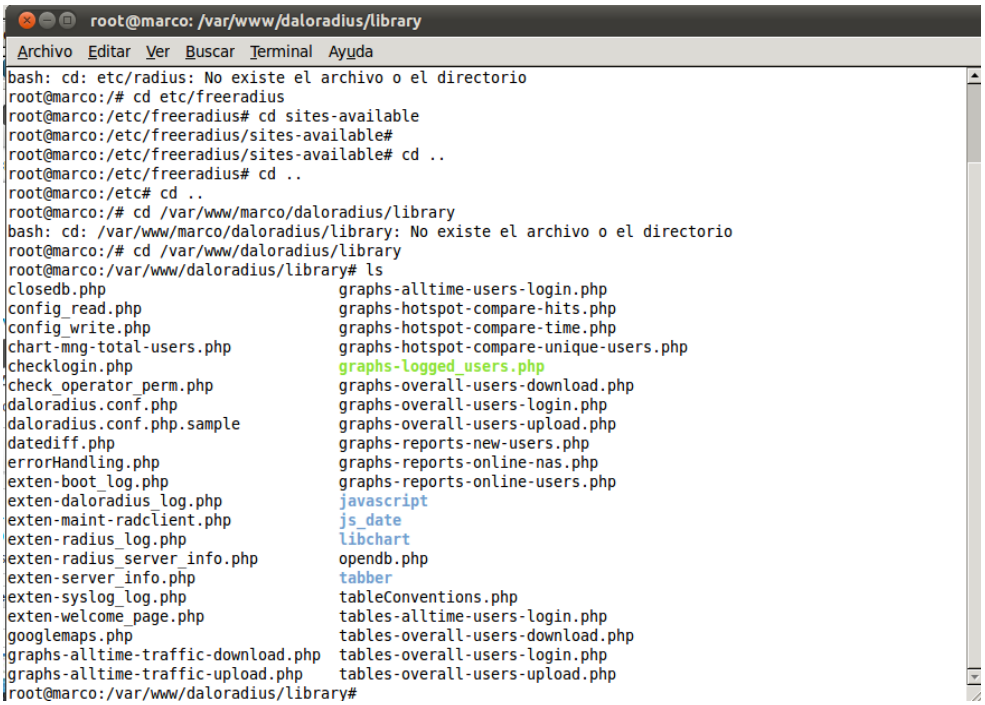

Figura 4.34. Visualización del contenido de la librería de daloradius

Ahora entraremos al archivo daloradius.conf.php y editaremos la contraseña que deseamos para el funcionamiento del mismo una vez alterado este parámetro debemos guardar con ctrl+o aceptar el nombre del archivo alterado con el mismo y por ultimo salimos con ctrl+w.

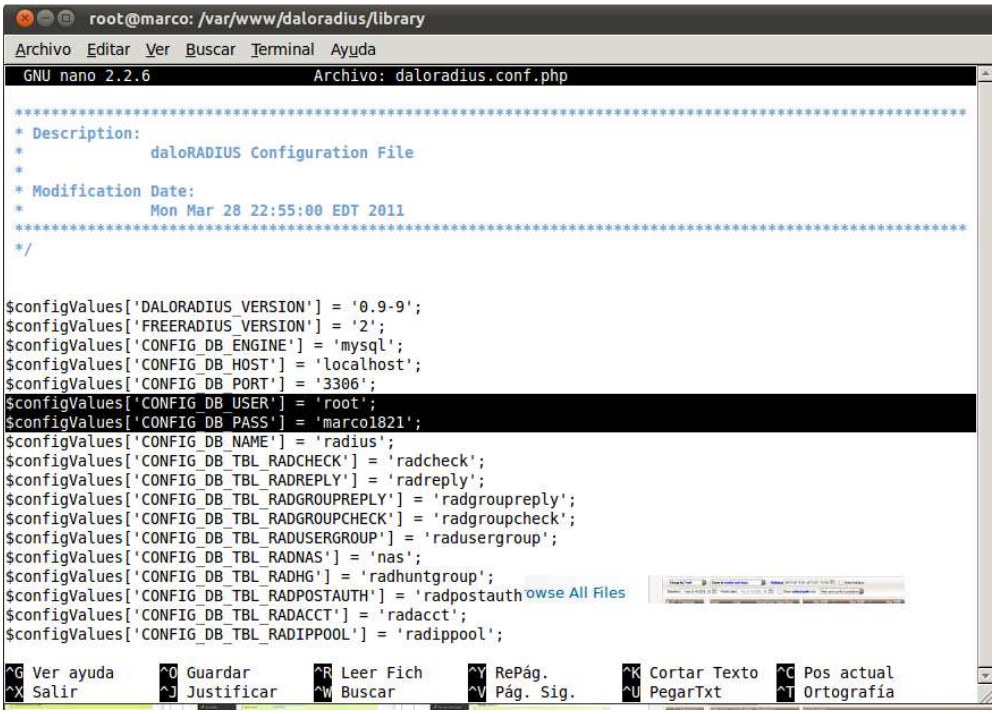

Figura 4.35. Configuración de contraseña de Daloradius

Lo siguiente es estando en la raíz ingresar a db por medio del comando cd/var/www/daloradius/contrib/db ya dentro vamos a comprobar la contraseña antes cambiada por medio del comando mysql root –u radis –p <mysql-daloradius.sql y ponemos la contrasña anteriormente modificada si logramos un acceso correcto entonces fue bien configurado.

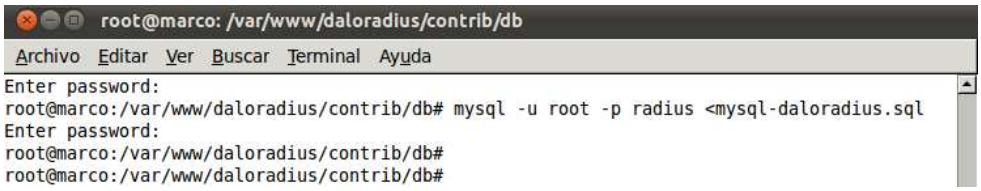

Figura 4.36. Ingreso de daloradius en la base de datos

Ya configurado todos estos archivos y su comprobación vamos a ver si la aplicación web esta lista para ser usada para esto debemos ingresar la dirección

http://localhost/daloradius en cualquier navegador como lo presentamos a continuación, el usuario y contraseña por defecto es Administrador y radius.

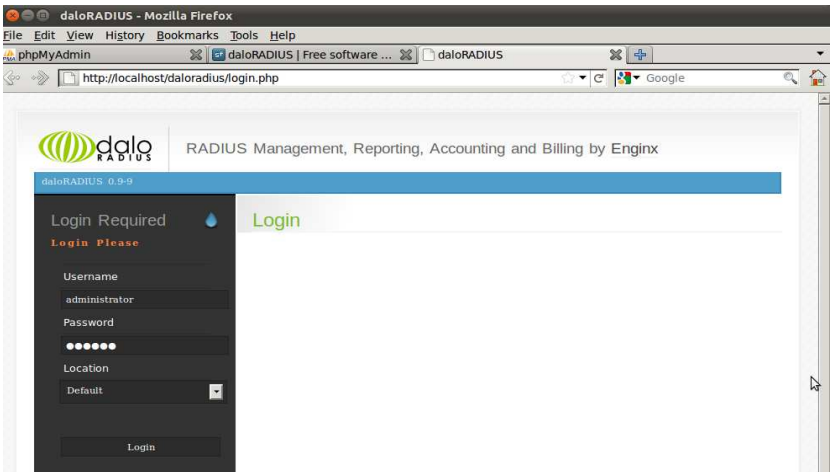

Figura 4.37.Ingreso a Daloradius

Lo siguiente es ingresar a colocar los usuarios esto se lo logra entrando Managment y nuevo usuario esto se lo puede hacer de varias maneras una de estas son con el nombre y contraseña.

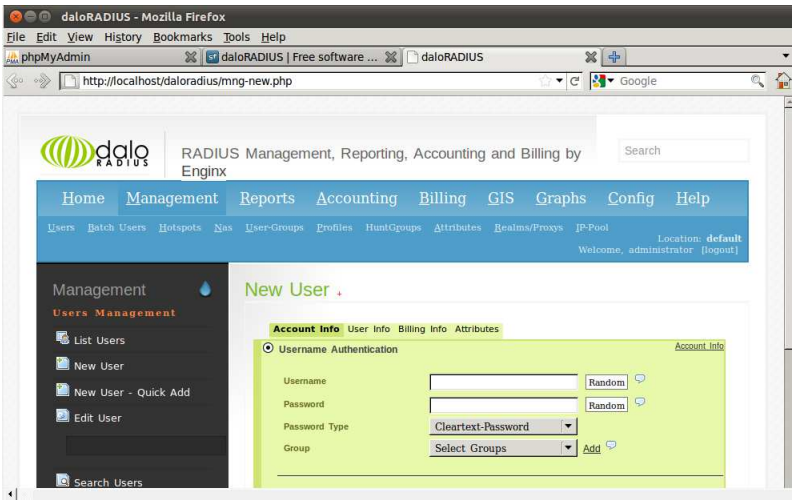

Figura 4.38. Creación de usario primordial

Podemos ingresar un usuario especificando la dirección MAC del mismo por medio de la siguiente tabla o por medio del pin.

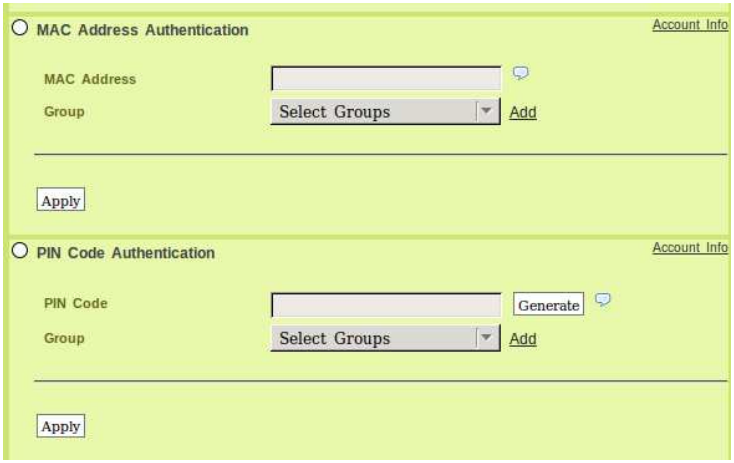

Figura 4.39. Formas de creación de usuarios

Podemos ver la lista de usuarios que vamos añadiendo en la base

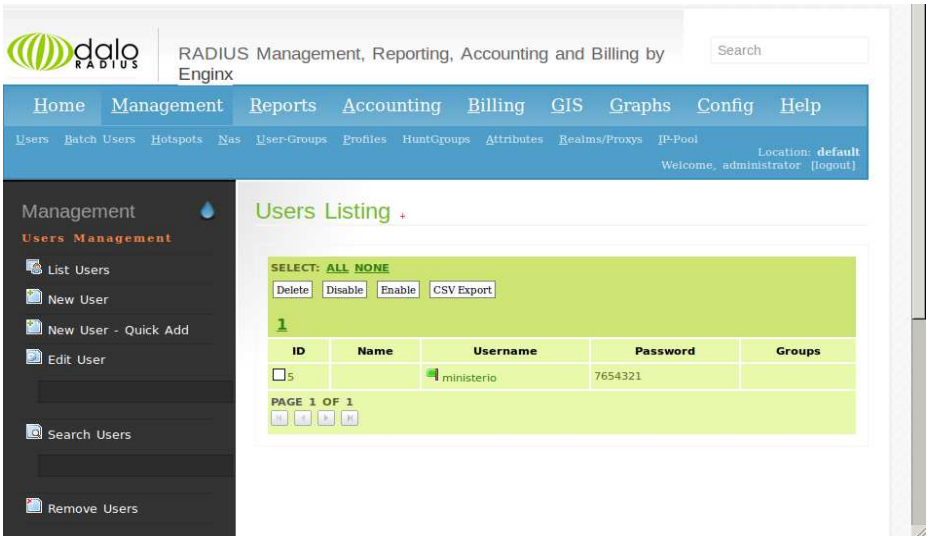

Figura 4.40. Usuario creado y su contraseña

Podemos ver un gráfico con la cantidad de usarios en la base de datos como se representa a continuación.

Figura 4.41. Lista de usuarios creados

4.1.3 Conectividad de máquina virtual y física

Para lograr la conectividad entre las máquinas virtuales vamos a empezar a poner direcciones estáticas en las dos máquinas correspondientes a la vlan que vamos a configurar posteriormente, vamos a empezar con la configuración de la máquina virtual para lo cual ingresamos a la opción de red colocada en la barra superior, y entramos en la opción editar la conexión.

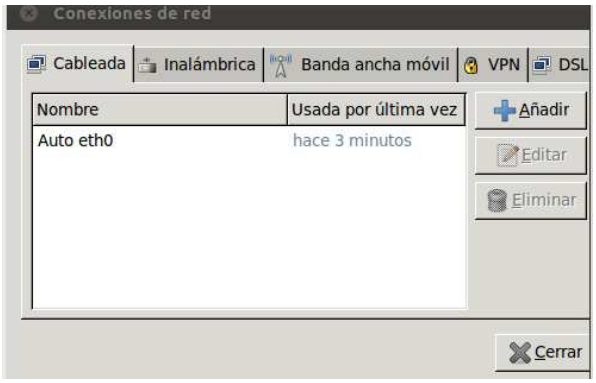

Figura 4.42. Configuraciones de conexión de red

Escogemos la conexión cableada entramos ajuste de IPV4 con método manual y añadimos en la dirección colocamos la dirección que escogimos para nuestro servidor y su máscara.

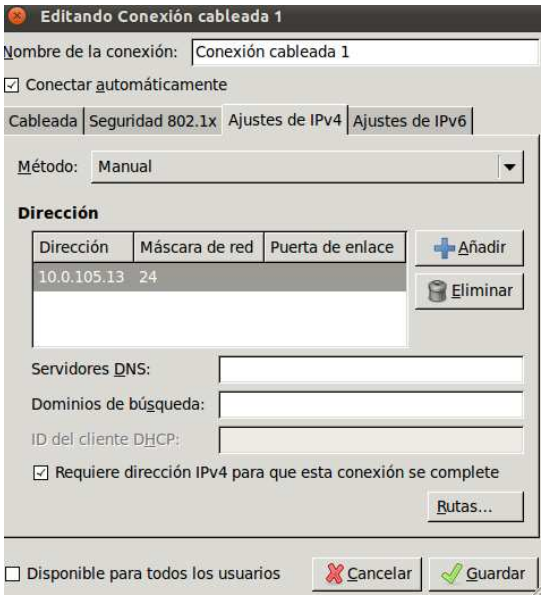

Figura 4.43. Configuración de dirección ip Ubuntu

También se puede hacer esta configuración mediante comandos en el terminal, y después de configurarla podemos usar el comando ifconfig para ver la configuración.

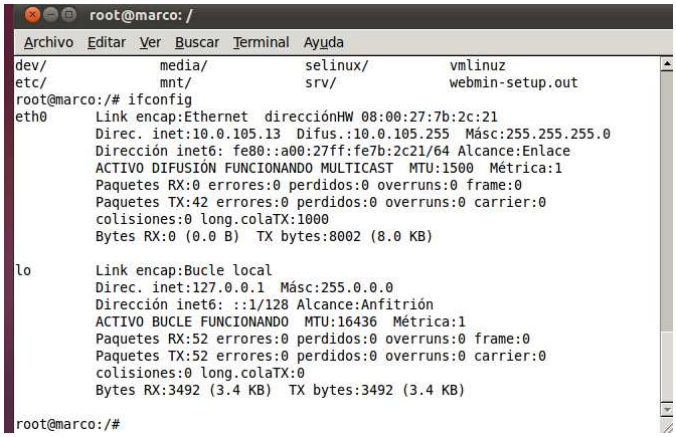

Figura 4.44. Confirmación de direccion ip configurada

También configuramos la dirección local de la maquina física con su conexión Ethernet con una dirección en el mismo segmento de red.

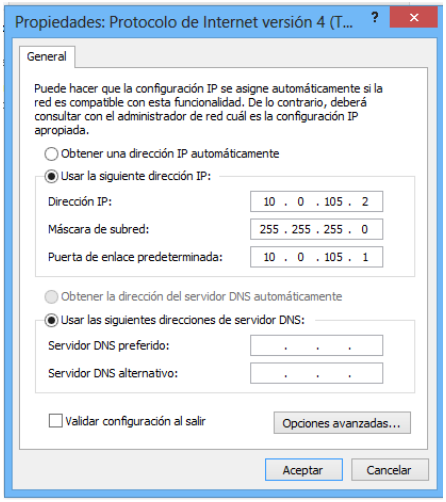

Figura 4.45. Configuración dirección ip windows

Ahora acudimos a la configuración de Ubuntu y escogemos la opción de red en el adaptador 1 configuramos de la siguiente forma, en conectado a escogemos Adaptador puente y el nombre puede ser el que se ve en la figura.

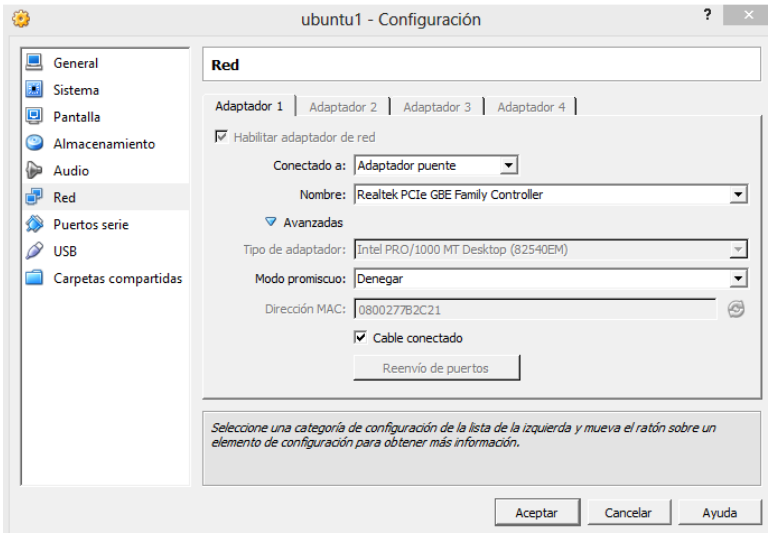

Figura 4.46. Configuración de adaptador de red en puente deUbuntu

4.1.3 Configuración del autenticador

Vamos a realizar la configuración del switch paso a paso para que funcione como autenticador de la mano de nuestro servidor configurado anteriormente, como ya vimos nuestro switch es un cisco 2960 con iso 12.2 versión K9 el que es compatible con la configuración que vamos a realizar.

Ya que nuestro switch es operativo dentro de la institución vamos a realizar una vlan a la cual la vamos a poner como nombre AUTENTICADOR, para ello en método de configuración global vamos a poner vlan 100, después con el comando name AUTENTICADOR damos el nombre a la vlan.

Figura 4.47. Creación y nombramiento de vlan

Vamos a colocar una dirección de administración en la vlan para ellos dentro de la configuración global colocamos interface vlan 100 y accedemos a la misma y colocamos la dirección que vamos a usar para administrar el dispositivo con el comando ip address 10.0.105.18 255.255.255.0 y no shutdown para activar la dirección.

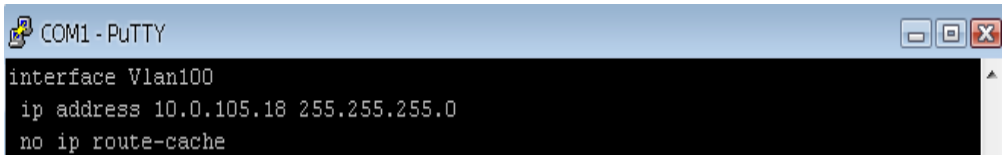

Figura 4.48. Configuración de dirección ip del autentitcador

Ahora separamos los puertos que vamos a usar en nuestra vlan y vamos a disponer para la configuración del plan piloto nos basta con 6 puertos usamos el comando interface range FastEthernet0/1-6, entramos al rango y aquí colocamos a los puertos en modo de acceso

y dentro de la vlan 100 con los siguientes comandos switchport mode access, y después switchport Access vlan 100.

Figura 4.49. Configuración del rango y acceso de la vlan

Salimos a la raíz y colocamos el comando show vlan brief para ver cómo está configurando la vlan su nombre y los puertos que estamos usando en el mismo, podemos hacer pruebas de conectividad desde el switch al servidor y nuestra máquina física para ver si está configurado de manera correcta.

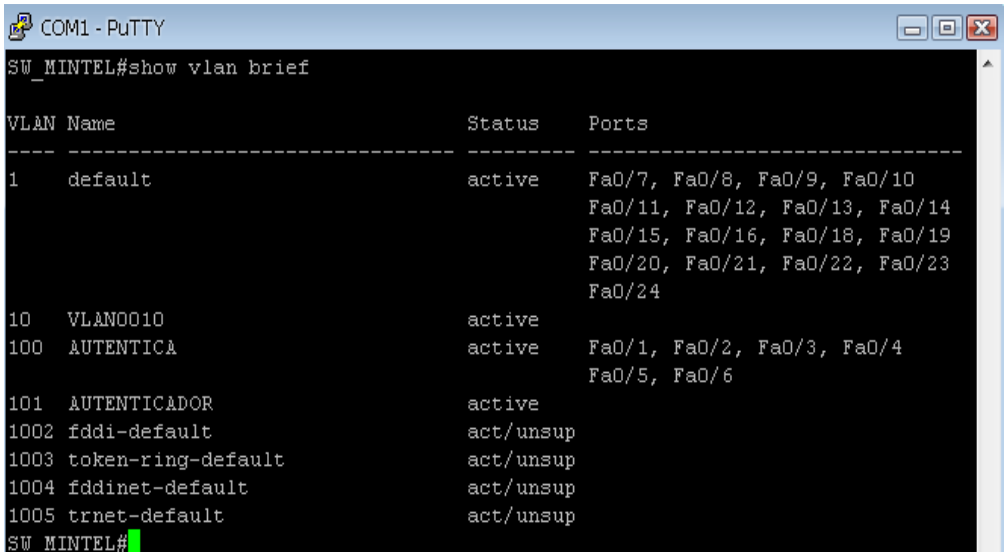

Figura 4.50. Visualización de la vlan creada su estado y puertos

Empezamos la configuración del autenticador para ello en modo de configuración global colocamos el comando aaa new-model, para que reconocer el autenticador aaa que tenemos configurado en el servidor podemos usar un usuario encriptado para acceder al mismo por medio del comando username mintel secret …..

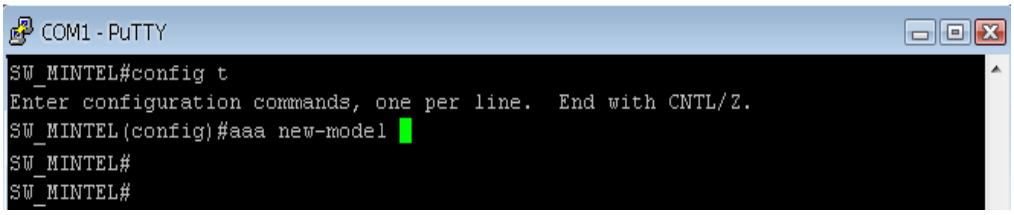

Figura 4.51.creación de modelo AAA en el switch

Ahora haremos el apuntamiento desde el autenticador al servidor por medio del siguiente comando radius-server host 10.0.105.13 auth-port 1812 acct-port 1813 key testing123, donde el host es la dirección de nuestro servidor radius, auth-port el cual se refiere a que la autorización se la haga por medio del Puerto 1812 y el accounting por medio del puerto 1813 el key es la clave compartida entre el servidor y el autenticador en nuestro caso es testing123.

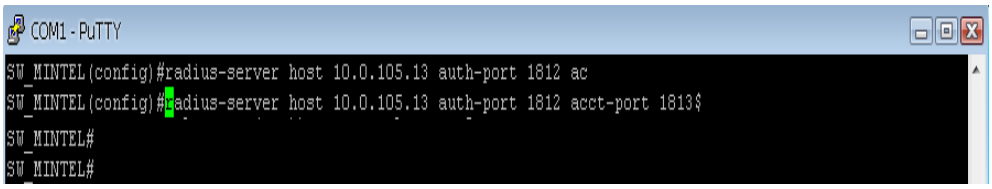

Figura 4.52. Apuntamiento al servidor radius

Ahora configuramos el comando aaa authentication dot1x default group radius, dot1x es el comando que usa 802.1x para la seguridad y escogemos el grupo radius este comando se usa para la autenticación de los dispositivos que se pegan al mismo., si usamos el mismo comando pero con login este nos permite que el switch nos pida autenticación y con los configurados en el servidor podemos realizar el ingreso correcto al mismo aaa authentication login default group radius,

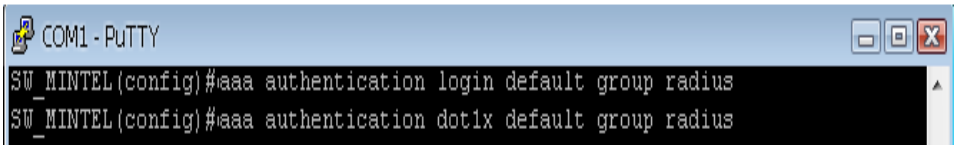

Figura 4.53. Poner al autenticador en modo de reconocimento del estándar 801.X

El comando dot1x system-auth-control es el que hace que cuando conectemos un ordenador aparezca la opción donde nos autenticaremos, sin este comando el ordenado no puede reconocer que va autenticar por medio del estándar 802.1X

Figura 4.54. Configuración del reconocimiento al protocolo

Para comprobar que nuestro autenticador funciona correctamente vamos a usar el comando test aaa group radius mintel mintel 123 new-code donde group radius es el grupo del servicio configurado, mintel uno se los usuarios configurados en el servidor y mintel123 como la contraseña del mismo, como vemos en la figura usuario fue autenticado con éxito, si no es así es usuario es rechazado.

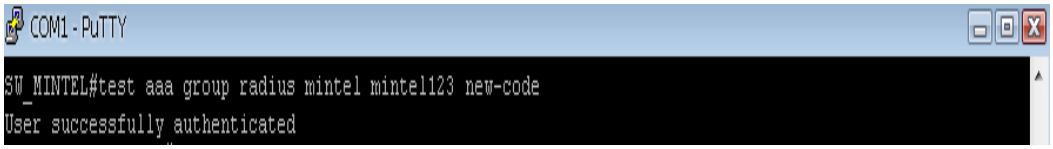

Figura 4.55. Auntenticación mediante usuario mintel

Figura 4.56. Auntenticación mediante usuario ministerio

4.1.4. Configuración del servidor radius.

Para configurar nuestro servidor radius ya instalamos la aplicación daloradius la que es una interfaz gráfica que nos ayuda a la configuración del servicio de forma más simple vamos a ver cómo está esta interfaz y cómo podemos configurar sus opciones y como las mismas ayudan a la administración del mismo, la primera opción que vamos a configurar es la creación de un nuevo usuario que será el que se puede autenticar, para esto vamos a la opción Gestión y después User.

Figura 4.57. Menú de configuración Daloradius

En la parte izquierda de esta ventana podremos escoger la opción que deseamos ver el listado de los usuarios, nuevo usuario, usuario modo expreso, buscar algún usuario que ya fue creado anteriormente, se puede editarlo o borrarlo.

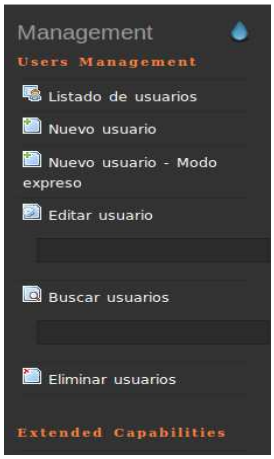

Figura 4.58. Opción de administración de Daloradius

Para crear el usuario lo podemos hacer de tres formas, creando con usuario y contraseña, con alguna dirección mac o por medio de un pin como vemos en la siguiente figura.

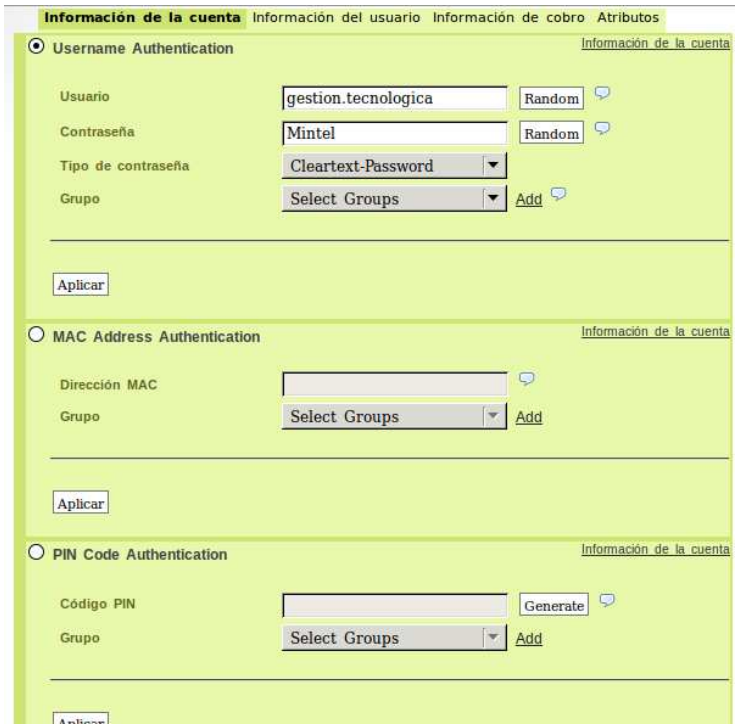

Figura 4.59. Manipulación de información de usuario

Ya que creamos un usuario podemos ver un listado de todos los creados y una gráfica del número total de usuarios para tener mayor control del mismo, como administrador podemos tener una lista con la contraseña y grupo al que pertenece cada uno.

Figura 4.60. Lista de usuarios ambiente Daloradius

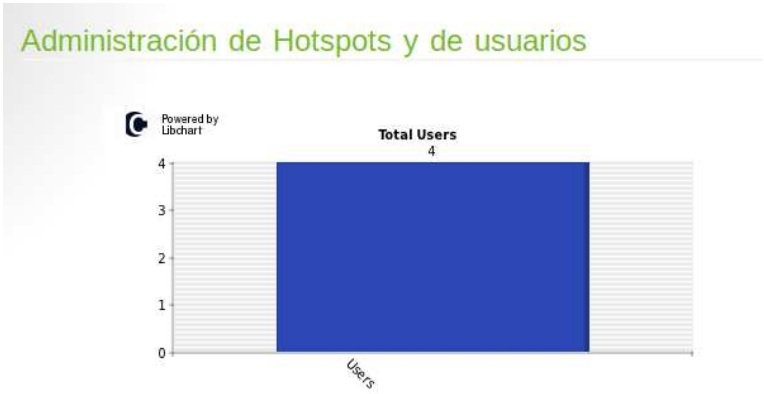

Figura 4.61. Grafica de administración de usuarios

Los usuarios que creamos en la aplicación daloradius y tenemos en la lista de usuarios también los podemos ver de forma momentaea que se van colocando en el servidor phpmyadmin.

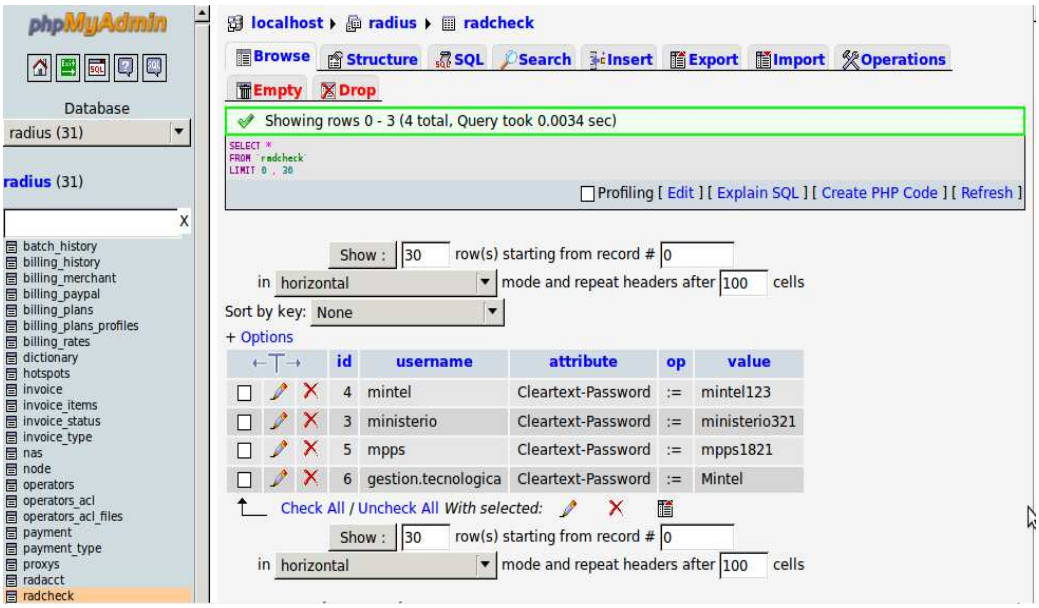

Figura 4.62 . Visualización d eusuarios en la base de datos

Podemos enlistar los nas con las direcciones ip que van a acceder con nuestro servidor radius para que sean los que tienen acceso y mayor seguridad en el mismo ya que aquí se contiene la clave compartida entre el usuario y el servidor, al igual que en los usuarios se puede crear nuevos nas, borrarlos editarlos, si deseamos hacer algo más complejo podríamos ubicarlos en una comunidad o que tenga control sobre determinado puerto, la opción está sobre el menú de gestión.

Figura 4.63. Listado de los nas creados

Realizaremos una breve explicación de los reportes que se pueden obtener con la aplicación gráfica Daloradius, en esta podemos ver información general, los logs que se crean al generar autenticación o falla de la misma el estado del mismo, entre otros,el primer reporte que vamos a observar el que genera el historial, aquí muestra las últimas acciones realizadas en secuencia desde la última como anteriormente creamos el usuario gestion.tecnologica la acciones nos muestran la creación y que fue realizada por el administrador.

Figura 4.64. Acciones de usuarios

Los reportes pueden ser más específicos con fechas de donde a donde queremos buscar, los usuarios que están en línea, intentos de conexión igual especificados por fecha o

también para ver específicamente por el usuario y sus accesos aceptados o rechazados como lo vemos en la figura.

Esta opción es muy importante para los administradores de la red para ver el tipo de acceso que se da si es rechazado aceptado, esto se puede controlar los ataques o ingresos no deseados a la red por fecha y si la misma pudo o no acceder con éxito, y como se refleja el servidor ante la autenticación.

Figura 4.65. Intentos de conectividad al servidor

El funcionamiento de los estados se da de la siguiente forma y en la misma opción de reportes, en este podemos ver si los servidores están o no activos, la característica del servidor, podemos configurar UPS, CRON, RAID, en el siguiente gráfico vamos a ver la información que nos da del servidor y su estado actual.

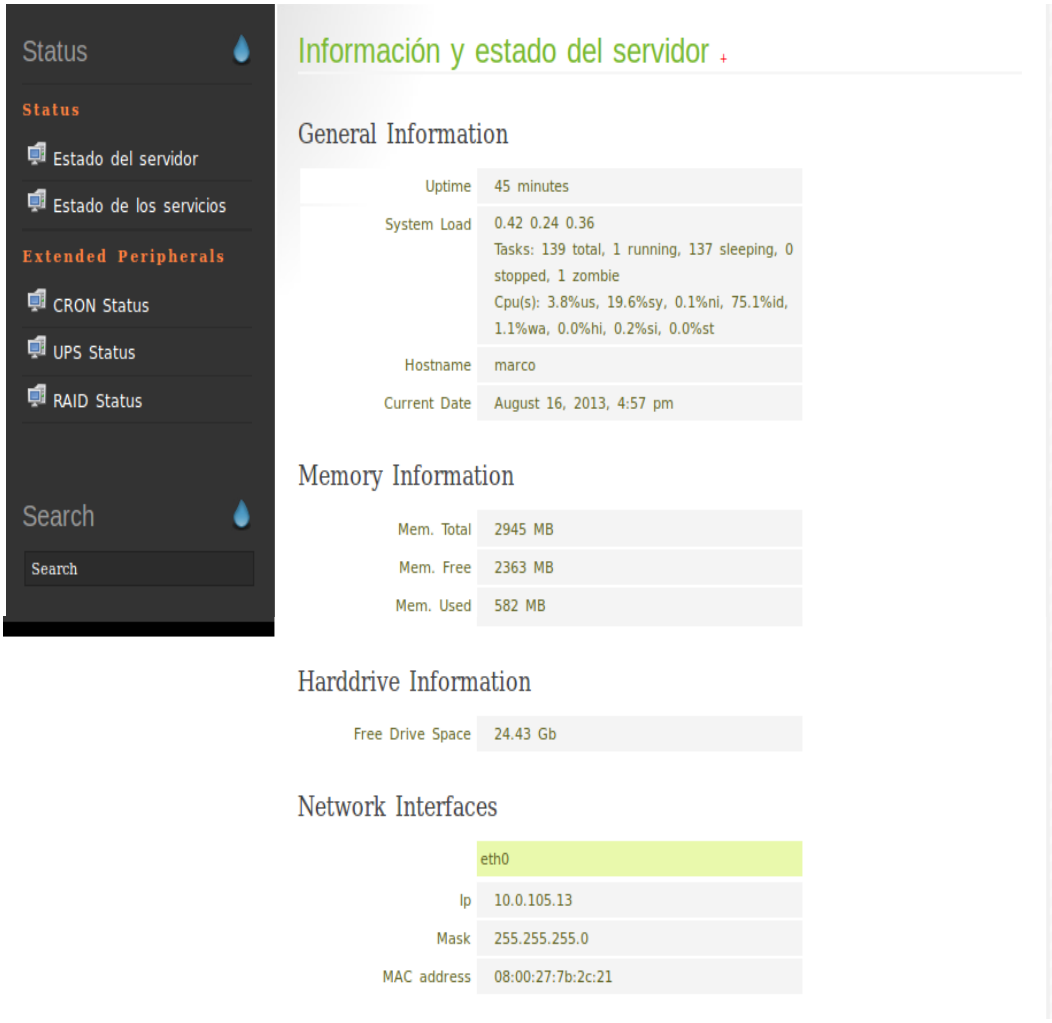

Figura 4.66. Información estado del servidor

Para administrar a los usuarios y controlar su funcionamiento de la red, tenemos que acceder a la función gráfico y aquí podremos ver la cantidad de acceso del usuario, descargas, subidas, y estadísticas de todos los usuarios.

Figura 4.67. Opción de gráficos que se pueden obtener

En configuración podemos entrar a cambiar la información de los registros y como queremos que se den los mismos, podemos ver los ajuste de las bases de datos, idiomas, el acceso, en esta opción podemos ver la instancias a registrar como puede ser las páginas que el usuario visita, las consultas, las acciones que este realiza, información de depuración de páginas.

Figura 4.68. Configuración de registros

4.1.5. Configuración de dispositivos de los usuarios.

Para comenzar la configuración de los usuarios vamos a ir a la máquina y en la opción de inicio colocamos Servicios, en esta opción tenemos los servicios locales y podemos configurarlos para activar o desactivarlos, ya dentro de la ventana de Servicios vamos a buscar la opción Configuración automática de redes cableadas.

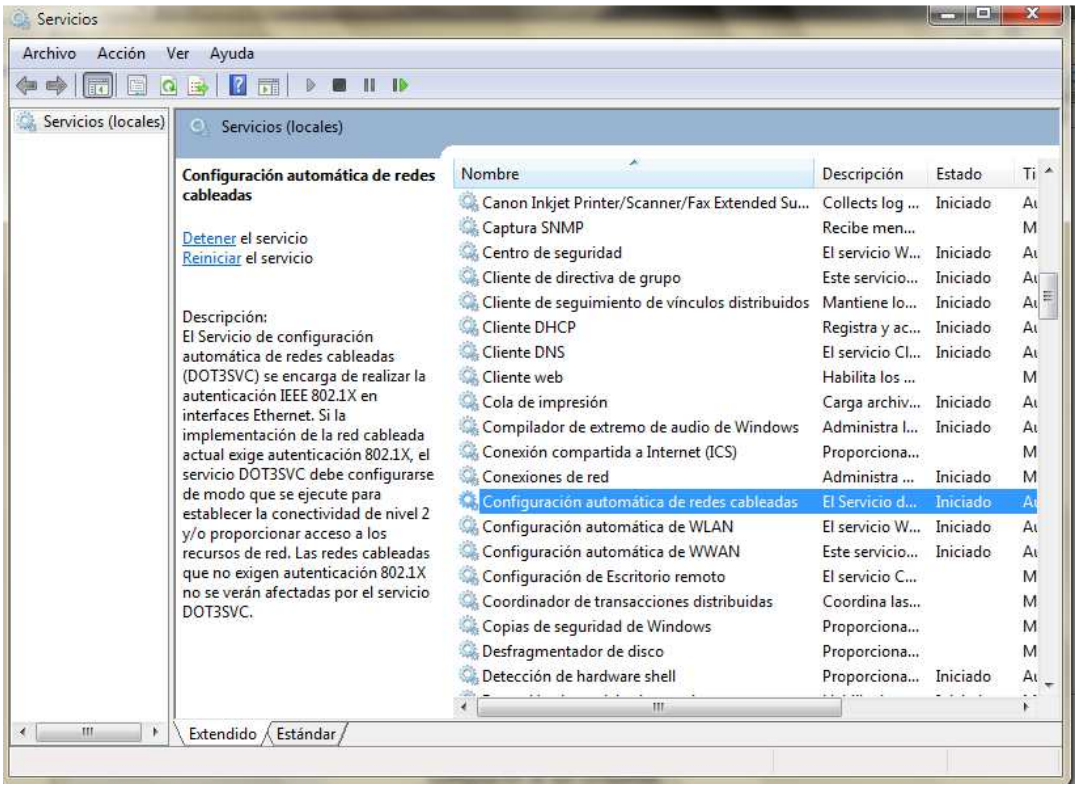

Figura 4.69. Servicios del sistema operativo windows

Una vez en encontrada la opción vamos a ingresar a Propiedades dando clic izquierdo sobre el mismo, aquí podremos cambiar la opciones que vienen predeterminadas en la máquina de los usuarios con el fin de que la autenticación por medio del estándar 802.1X se pueda ejecutar sin problemas.

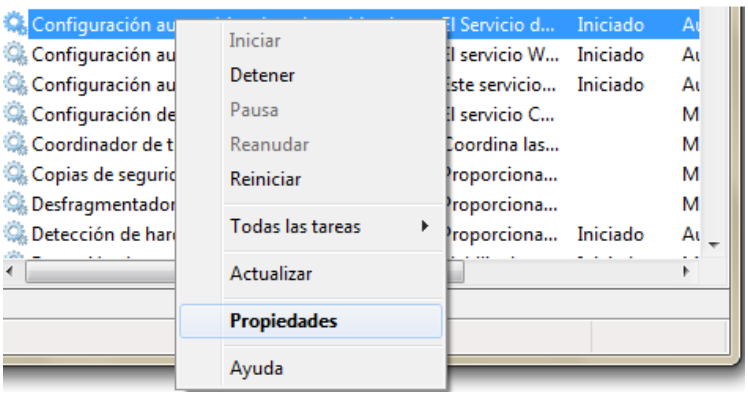

Figura 4.70. Configuración automatica de redes cableadas

Dentro de las propiedades de configuración automática de redes cableadas vamos a generar el tipo de inicio que vamos a utilizar en nuesto caso vamos a colocar como automático, en estado de servicio vamos a inicializarlo, nos aparecerá una ventana que indique el progreso de la inicialización.

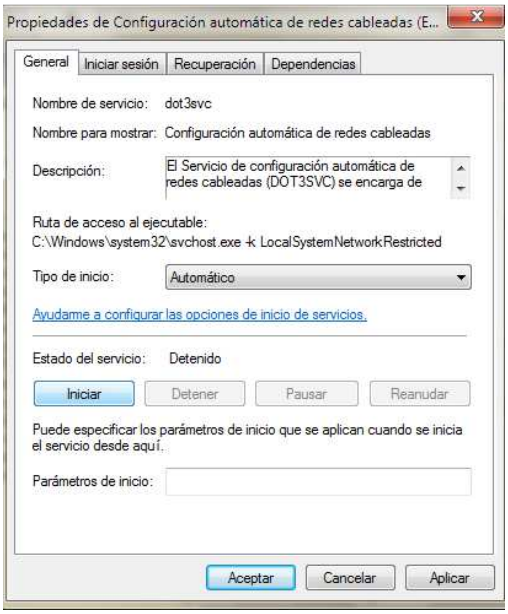

Figura 4.71. Propiedades de configuración de registros

Entre otras aconfiguraciónes podemos encontrar el de inicio de seción que nos indica si queremos que el usuario se autentique automáticamente o no, tener interacción en el escritorio para la autenticación, la opción de recuperación y el de dependencia que nos indica los componentes del sistema donde vemos los protocolos que trabajan con el mismo, colocamos aplicar y aceptar y el servicio se inicializará.

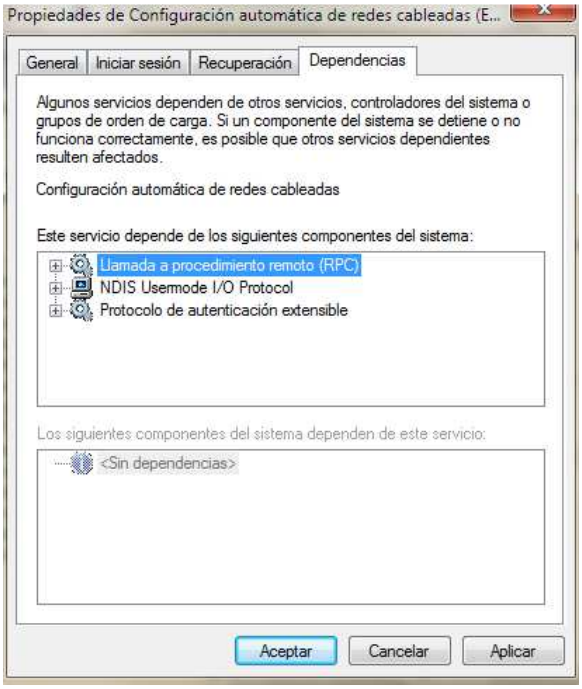

Figura 4.72. Dependendia de las propiedades de configuración

Lo siguiente es entrar a las conexiones de red, ya en esta podemos ver todas las conexiones que tenemos activas o inactivas en las máquinas tanto alámbricas como inalámbricas, como estamos configurando una conexión alambrica vamos al icono de conexión de área local que en el momento antes de la configuración va a estar sin conexión a una red, vamo a dar clic izquierdo sobre este icono e ingresamos en la opción de propiedades, en la misma que vamos a configrar el tipo de autenticación que vamos a usar que pueden ser varias dependiendo de las necesidades de la institución, pero indicaremos como funciona cada una de las configuraciones posibles.

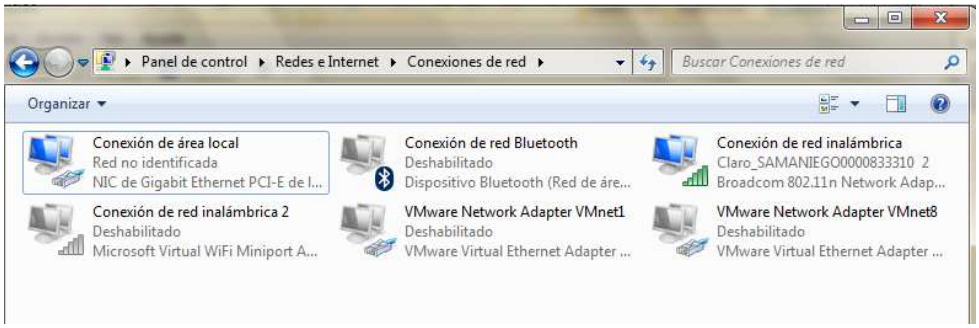

Figura 4.73. Ventana de conexiones de red.

Lo primero es habilitar la opción de autenticación de IEEE 802.1X, después podemos elegir uno de los métodos de autenticación, en la versión de sistema operativo que posee el usuario el mismo puede variar.

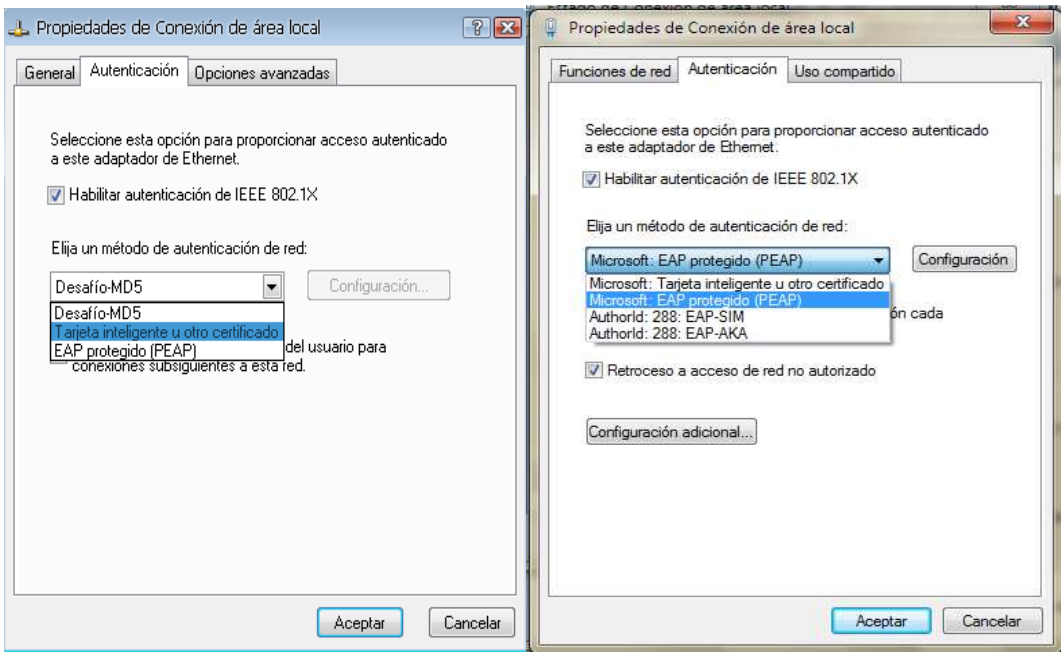

Figura 4.74. Método de autenticación 802.1X

Estas opciones son las que se pueden usar si elegimos el método Desafío—MD5 en este no se usan los certificados para cada usuario que como administrador es lo más complejo de manejar en este tipo de autenticación, para usar certificados se lo puede

realizar mediante el uso de tarjetas inteligentes u otros certificados, a más de esto tenemos la opción de EAP protegido (PEAP), que es uno de lo más usados por la diversidad de configuración que este nos brinda, podemos usar en sistemas operativos más actuales la opción de EAP-SIM, y EAP-AKA, si usamos la opción EAP protegido (PEAP) vamos a la opción de configuración, aquí podemos validar un certificado para esto se puede realizar una validación o no de certificados y si deseamos escoger la opción de conectarnos a un servidor en la cual debemos colocar el nombre completo del servidor, a más de esto podemos escoger la entidades de certificación raíz de confianza, si escogemos esta opción podemos también elegir el método de autenticación preferido como es EAP-MSCHAP v2, aquí nos da una diversidad de opciones como habilitar la conexión rápida, poder proteger el acceso a la red entre otras.

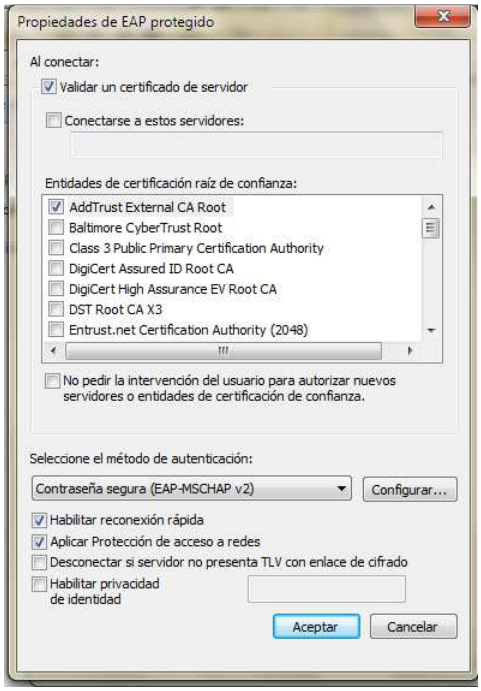

Figura 4.75. Propiedades de EAP

Podemos solo escoger el método de autenticación que vamos a usar en el caso de no usar ningún certificado, al momento que elegimos el tipo de autenticación al lado izquierdo del mismo podemos escoger la opción de configuración del método si

escogemos el método EAP-MSCHAP v2, se nos abrirá una ventana de Propiedades de EAP-MSCHAP v2 y quitamos la opción que viene habilitada por default de usar automáticamente el inicio de la sesión y la contraseña de Windows, si no elegimos esta opción no se podrá visualizar la opción en la cual se da la autenticación en el escritorio.

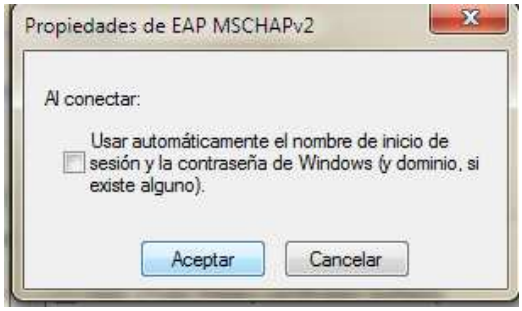

Figura 4.76. Deshabilirar el uso automático

Si la configuración hasta este punto son correcta en la parte inferior izquierda de nuestra pantalla nos aparecerá un cuadro de dialogo donde nos dice que se necesita información para conectarse a una red y que demos clic sobre este aviso, como se lo ve en la siguiente imagen.

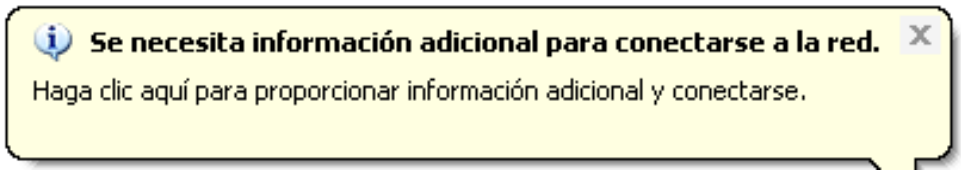

Figura 4.77. Dialogo de autenticación

4.2 Funcionamiento de la implementación

Ya que colocamos autenticación por medio del estándar IEEE 802.1X, tanto para el autenticador como para los usuarios de la red, cabe decir que el que tiene acceso al dispositivo que funciona como autenticador en este caso nuestro switch tiene que ser uno de los administradores de la red, vamos a ver como se da el este tipo de autenticación en

los diferentes dispositivos, vamos a empezar con el autenticador podemos ingresar remotamente por medio de protocolos que lo permitan y para acceder al mismo debemos ingresar los datos del administrador previamente creado en el servidor radius,

Lo primero en aparecer a la inicialización del dispositivo nos pedirá tanto el usuario y la contraseña y si son colocadas de manera correcta vamos a poder ingresar en el dispositivo y configurarlo.

En la siguiente imagen vemos que el switch se autentica con el usuario mintel y su respectiva contraseña de la siguiente manera.

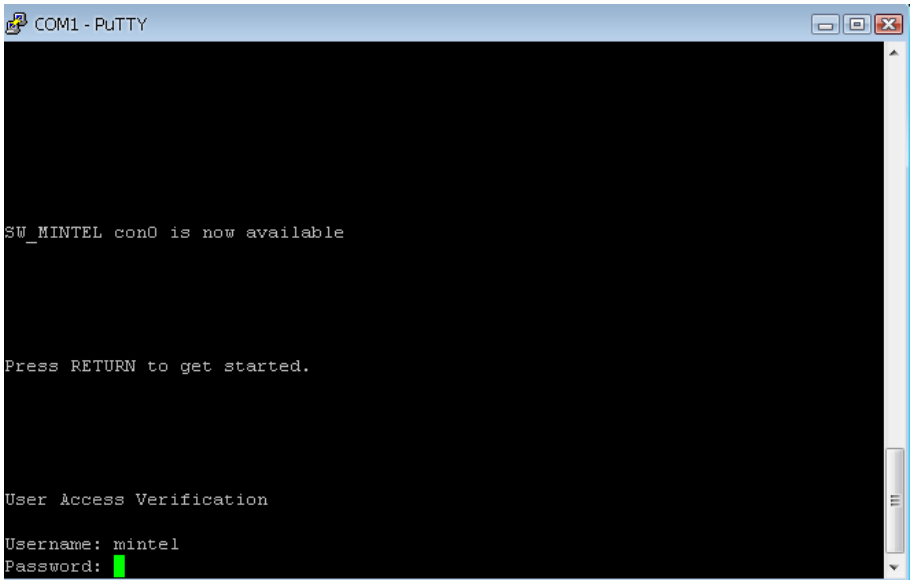

Figura 4.78. Autenticación en el switch

Como no se dieron inconvenientes en la misa accede al switch si colocamos mal la contraseña nos volverá a pedir la contraseña para tener un poco más de seguridad podemos configurar el número de intentos fallidos que puede tener un usuario no solo en el auntenticador, sino en todos los dispositivos configurados.

Para el ingreso de los usuarios es de la misma forma vamos a tener un cuadro de dialogo que nos pide el ingreso de la autenticación y dependiendo del sistema operativo el formato del cuadro de autenticación va a variar en las últimas versiones no nos aparece el domino de inicio de sesión del usuario, y solo pedir usuario y su respectiva contraseña en la cual vamos a ingresar los datos ya activos en nuestro servidor radius 802.1X, en este caso vamos a configurar el usuario ministerio y su respectiva clave.

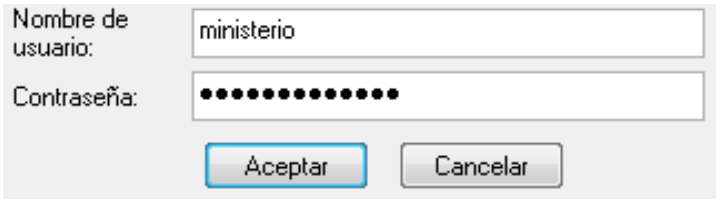

Figura 4.79. Autenticacion de usuario

Si la autenticación no tiene problema en el usuario o contraseña el servidor acepta al usuario dentro de nuestra red.

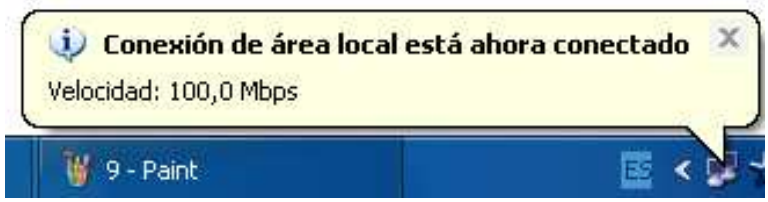

Figura 4.80. Conexión del usuario

Podemos ver el estado de la red por medio del estado de conexión de área local en donde podemos ver el estado conectado, desconectado, la duración de la conexión y la velocidad que al ser cableada es de 100 Mbs, a más de esto podemos visualizar la actividades en forma gráfica para ver la interactividad con la red.

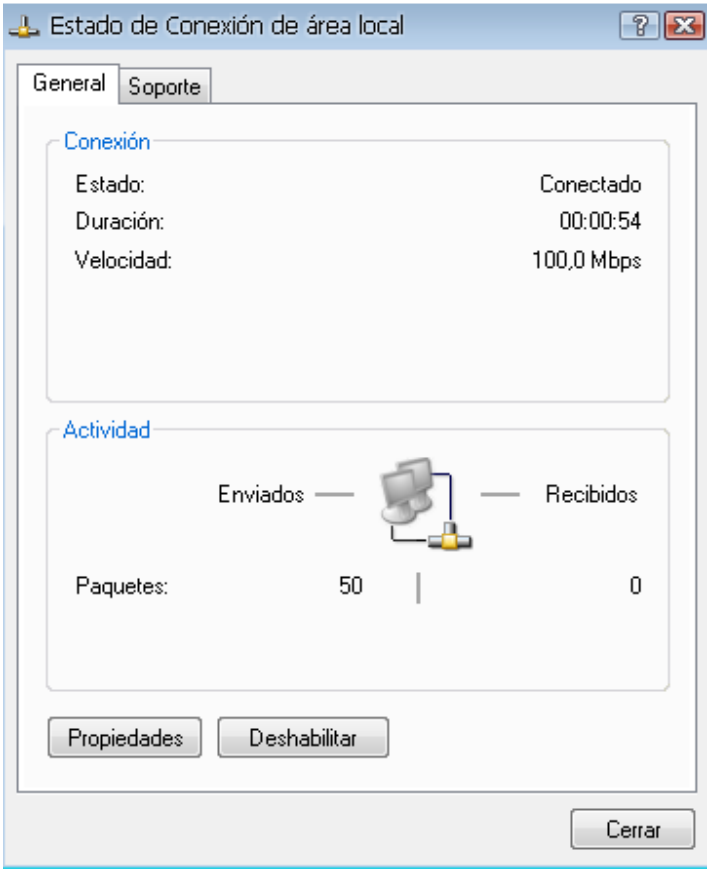

Figura 4.81. Estadk de la conexión de área local

4.3 Control de acceso a la red

El control de acceso a la red lo hace el administrador de la red por medio del terminal por medio de los logs o como instalamos la aplicación web para controlar el servidor por medio de Daloradius, si vamos a la opción de reportes podemos observar la cantidad de usuarios que ingresan a la red y si los mismos son o no aceptados por el servidor, esto se lo hace en la opción en usuarios intentos de conexión, podemos escoger la opción que muestra todos, solamente los aceptados o solo los rechazados.

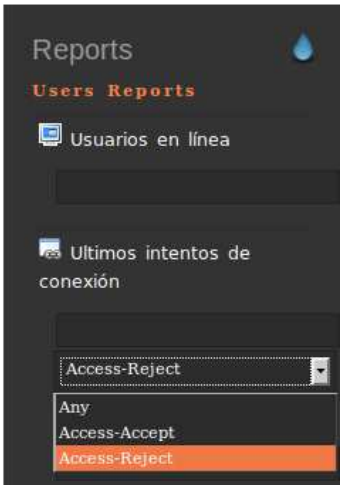

Figura 4.82. Reportes de intentos de conexión

Tambien podemos ver los usuarios que estan conectado en la actualidad dentro de la red, para esto escogemos la primera opción de reportes podemos poner el nombre del usuario en el buscador, esta opción nos muestra los usuarios que actualemente estan en la red con la hora del inicio con fecha complenta.

CSV Export

1 2 3 4

Usuario	Contraseña	Hora de inicio	Respuesta del servidor RADIUS
ministerio		2013-08-14 12:23:17	Access-Accept
mintel		2013-08-14 12:22:39	Access-Accept

Figura 4.83. Lista de usuarios conectados

Podemos tener mayor control de usuarios para administrar si buscamos por fechas esto ayuda a monitorear problemas que ocurrieron en cierta fecha o en un rango de fechas que ocurrió el problema u otras cosas que se estén buscando, según la conexión de usuarios.

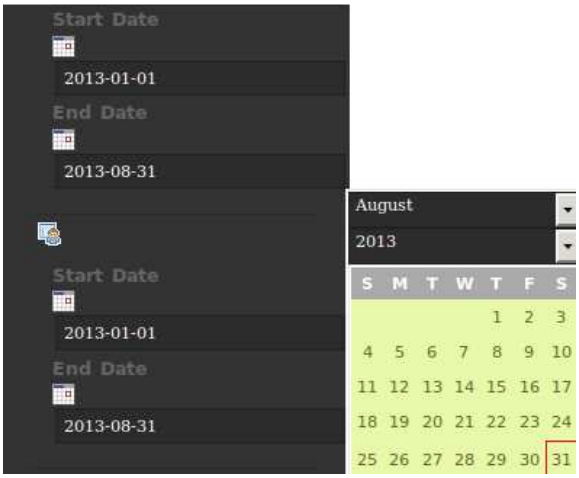

Figura 4.84. Menú de reportes por fechas

Podemos usar la opción de usuario tope para visualizar los más logeados con el sistema para el caso también podemos filtrar por el nombre de usuario y tener un reporte claro de las actividades del mismo en conveniencia del administrador, esta opción también nos brinda la búsqueda con rango de fechas para facilidad.

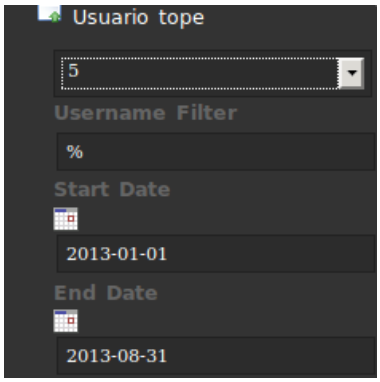

Figura 4.85. Reporte por usuario tope

Si la búsqueda es por el ancho de banda o tiempo del consumo de un usuario también es posible obtener un reporte del mismo, con esto podemos tener un control del manejo de los servicios y como el usuario maneja los mismos, esto da un reporte con la hora en que se excedió los límites de ancho de banda, el administrador usa esta herramienta para

poder ver que usuario consume los recursos de manera desmedida y poder corregir el problema inmediatamente.

Figura 4.86. Reporte por ancho de banda o tiempo

También tenemos la posibilidad de obtener reporte del historial de las últimas actividades realizadas sobre el servidor con fecha y hora de manipulación y que creo dicha acción si fue actualización muestra la fecha y hora de la actualización realizada y también el usuario que realizó la misma.

iHistorial de acciones

1

Sección	Item	Fecha de creación	Creado por	Fecha de actualización	Actualizado por
userinfo	gestion.tecnologica	2013-08-16 16:09:34	administrator		
userinfo	mpps	2013-08-08 11:45:00	administrator		
userinfo	mintel	2013-08-08 11:44:28	administrator		
userinfo	ministerio	2013-08-06 23:43:46	administrator		
operators	administrator	2009-12-07 20:12:33	admin	2009-12-07 20:14:01	administrator

PAGE 1 OF 1

Figura 4.87. Reporte de historial de acciones

Otras configuraciones pueden darse vía terminal como la visualización de los log un reporte del servidor completo colocando el comando freeradius –X en a raíz, la respuesta da en su totalidad la configuración del servicio, para poder restaurar el servicio podemos colocar el comando service freeradus restart y aquí nos indicara si es o no correcto, podemos parar el servicio colocando el comando en la raíz service freeradius stop e iniciarlo con el comando serivce freeradius star en todos estos casos nos da un aviso que si se realizó el mismo con un ok o si fallo con un fail, en la siguiente imagen visualizamos la restauración del sistema, si se paró correctamente y con el nuevo inicio correctamente.

Figura 4.88. Restauración del servidor freeradius

Podemos configurar los registros que los usuarios a freeradius utilizaran como las páginas usadas, registro de consultas, registro de las acciones como envío de información, registro de información o de dependencias.

Figura 4.89.Configuración de registros

Por último vamos a observar los log que se generan el el radius para lo caul vamos a ingresar el comando tail-f /var/log/freeradius/radius.log donde observamos el comportamiento de nuestro servidor, a las diferentes configuraciones de administración o de usuarios de la red.

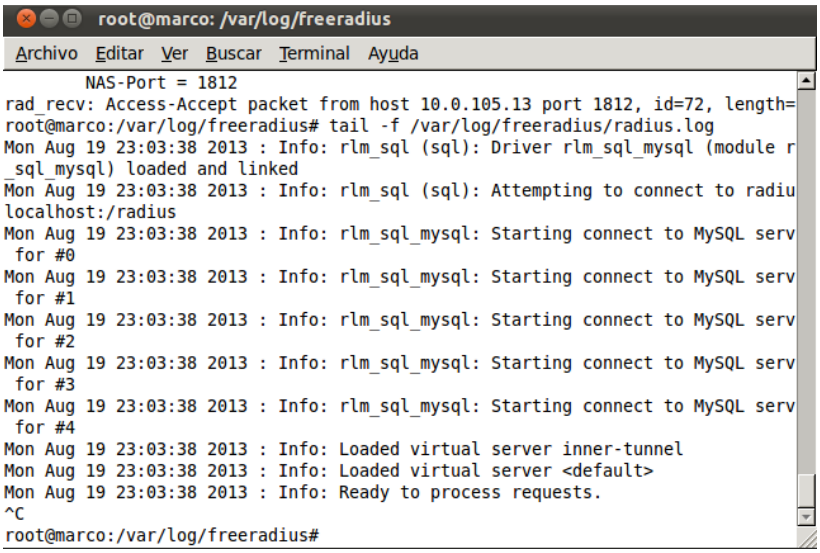

Figura 4.90.Visualización de los logs generados

CAPÍTULO V

PRUEBAS Y RESULTADOS

5.1 PRUEBAS

5.1.1 Funcionalidades

La implementación funciona de la siguiente manera para un puesto de trabajo, si se tiene un nuevo usuario que quiere acceder a la red el administrador puede crear su perfil dentro del servidor RADIUS usando la aplicación de Daloradius, antes de ello debemos ver que el estado de los servicios y del servidor deben estar habilitados como se lo muestra en la figura, esto significa que se pueden hacer configuraciones exitosamente.

Figura. 5.1. Estado de los servicios servidores

Ingresamos el nuevo usuario el cual la creamos con usuario y contraseña para mayor seguridad podemos crear una contraseña randomca o cambiar el tipo de la contraseña como ClearText-Password, Chap-Password como este caso, Usr-Password, Md5-Password, entre otras la cuales tienes que ser modificadas dentro de la configuración del ordenador de cada uno de los usuarios.

Figura. 5.2. Creación de usuario y tipo de contraseña

La configuración de los usuarios pueden ser en todas las versiones del sistema operativo de Windows que se le modifica en las propiedades de la conexión local como en el tipo de contraseña podemos escoger MD5-Password, entonces deberíamos escoger el método de autenticación de Desafío-MD5 si el tipo de contraseña es ClearText-password que es la que se configura por default es compatible con el método de Desafio-MD5, si el anterior tipo de contraseña se configura como CHAP entonces el método de autenticación de red debe configurarse como EAP protegido PEAP.

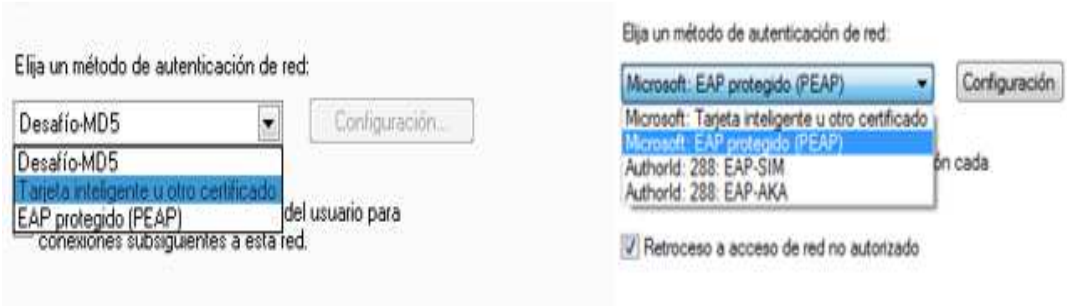

Figura. 5.3. Elección del método de autenticación de la red

Si la opción de método escogida fue EAP protegido PEAP, debemos ingresar a las configuraciones del mismo aquí debemos desactivar todas las características que requiere el uso de certificados en la forma de autenticación como es desactivar la opción de validar un certificado al servidor, y conectarse a cierto servidor, aquí se desactivan las entidades de certificación raíz de confianza, esta configuración es la habitual a sistema operativo d WINDOWS superiores a XP, como Vista o 7 ya que la institución posee máquinas en versiones XP o 7 entonces la configuración es la que estamos observando, en el caso de escoger CHAP, la última configuración en el estado de los usuarios es selecciona el método de configuración dentro de las mismas propiedades de EAP protegido y configuramos una contraseña segura como EAP-MSCHAP, las demás configuraciones son secundarias como el habilitar conexión rápida Protección de acceso a la red, Privacidad de identidad, las últimas opciones de configuración son opcionales y se activan solo si el administrador quiere un funcionamiento adicional al que ya hemos analizado con los métodos de autenticación, en nuestro caso solo habilitamos las dos primeras opciones como se muestra en la figura siguiente.

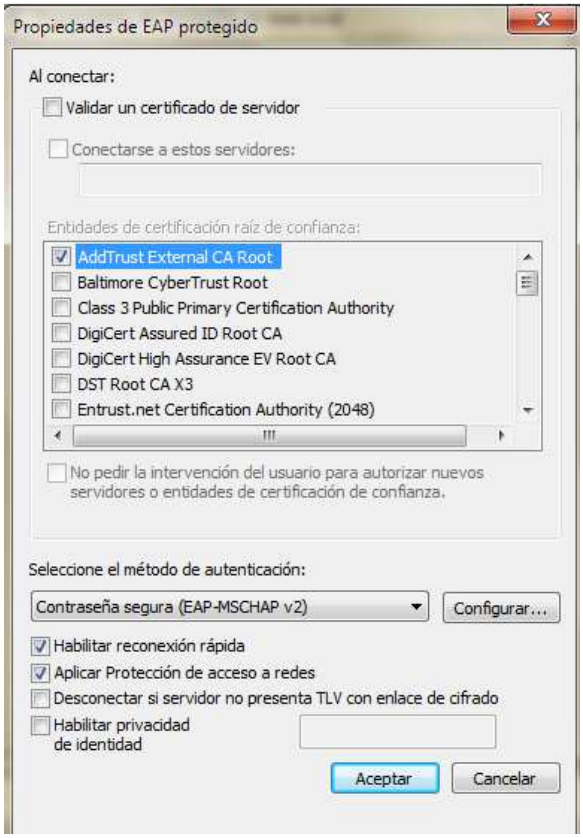

Figura. 5.4. Propiedades de EAP

Si como administradores de la red queremos saber si nuestro usuario creado no va a tener problemas en el momento de su autenticación vamos a ver el reporte el historial de su creación, como vemos en la figura siguiente.

Figura. 5.5. Historial de las acciones

La prueba de que este correctamente saliendo es un radtest desde el terminal de la consola como ya hemos visto con el radtest Marco.Paredes Mintel4321 10.0.105.13 1812 testing123, el cual el servidor va a realizar un proceso de aceptación o de rechazo.

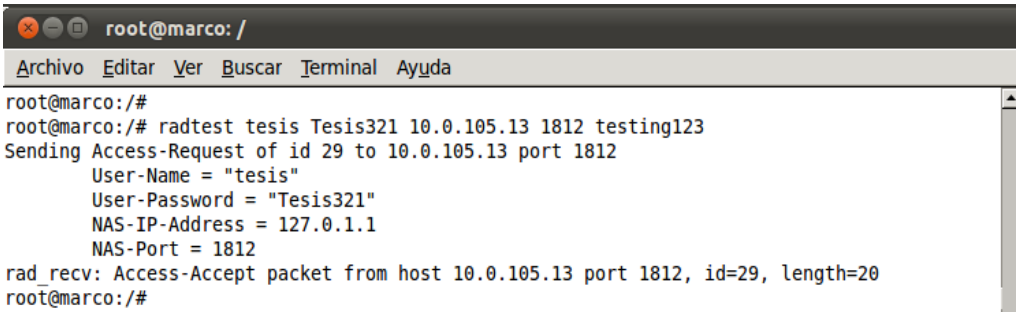

Figura. 5.6. Radtest del nuevo usuario

El Daloradius en sus reportes menciona los últimos 50 reportes si el nuevo usuario ingreso o no ingreso, es decir el reconocimiento del servidor ante este usuario en la figura podemos ver la hora de inicio de sesión del usuario en mención y la respuesta de servidor Radius ante la petición.

Figura. 5.7. Lista de intentos de conexión al servidor

Una vez que autentiquemos nuestro usuario en el sistema operativo vamos a ingresar los datos del usuario y su contraseña según la seguridad que hayamos escogido para la misma.

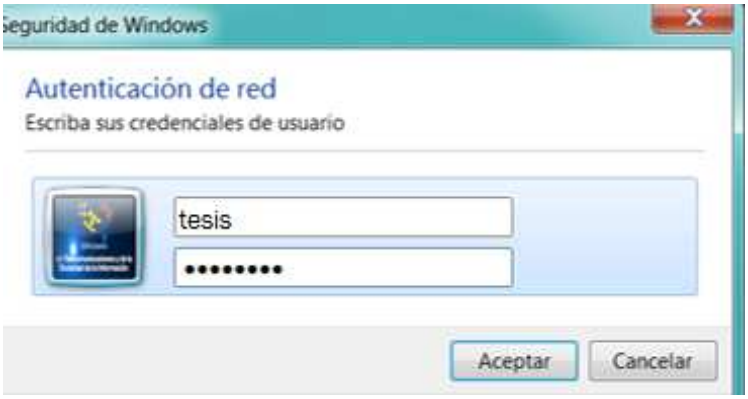

Figura. 5.8. Autenticación a la red con usuario creado

5.2 RESULTADOS

5.2.1 Análisis de Resultados

Los resultados fueron los esperados dentro del plan piloto vamos a analizar los diferentes métodos de autenticación que se pueden dar en la ejecución del estándar y se pueden dar en la implementación vamos a empezar con el método de MD5, la que es una encriptación unidireccional es decir que se puede encriptar pero no se la puede desencriptar, esto no quiere decir que no se la puede crackear, MD5 trabaja con una encriptación la misma que encriptar una contraseña en 32 caracteres pero muchas combinaciones pueden llegar a la misma encriptación por lo cual no es posible desencriptarla, existen varias páginas web donde se coloca el código encriptado y este lo descifra o por fuerza bruta puede ser descifrado, como vemos tiene un cierto tipo de seguridad pero resulta conveniente trabajar en redes cableadas, debido a que si esta se da de forma inalámbrica capturar su tráfico es más sencillo y obtener el código encriptado de igual manera, después la persona puede entrar a la web y aquí usar un programa para

descifrar el código que esta encriptado y de esta forma tener la contraseña de cierto usuario por más compleja que la misma sea ya usando mayúsculas, minúsculas o caracteres especiales, pero es viable si lo que queremos es autenticar redes cableadas donde es más difícil obtener el ruptura de una de las contraseñas de un usuario.

Si vemos ahora el uso de EAP que significa Protocolo de autenticación extensible y el PEAP es Protocolo de autenticación extensible protegido, no siempre van de la mano con el estándar IEEE 802.1X, esta lo que hace es dar mayor seguridad en las contraseñas que se asignan a un usuario de una manera más óptimas que otro tipo de seguridad inalámbrica como lo es WEP, funciona con certificados, o con CHAP su funcionamiento es intercambiar su clave con el servidor en este caso RADIUS y está según el método escogido rota las claves de forma rápida, este tiempo es corto haciendo que la captura y ruptura de la misma sea muy difícil de realizar, si usamos esta forma de autenticación tendremos mayor seguridad en la información que se intercambia, a más de esto el uso de certificados en tarjetas inteligentes nos puede brindar una mayor seguridad pero a la vez tiene contras como el manejo de tanto certificado en la red, y por la cantidad de funcionarios en la institución incontrolable por el administrador de la red y generación de costos si son tarjetas inteligentes.

En la siguiente tabla vemos una comparación entre los diferentes métodos de autenticación que ofrece el estándar 802.1X.

Tema	EAP-MD5	EAP-PEAP	EAP-TLS	EAP-TTLS
Solución de seguridad	Estándar	Estándar	Estándar	Estándar
Certificados-cliente	NO	NO(opcional)	SI	NO(opcional)
Certificados-servidor	NO	SI	SI	SI
Soporta autenticación de base de datos	Requiere borrar la base de datos	Active Directory	Active Directory	Active Directory, Tokens, SQL,LDAP
Intercambio de llaves dinámicas	NO	SI	SI	SI
Autenticación mutua	No	SI	SI	SI

Tabla 5.1. Comparación de métodos de autenticación 802.1X

El administrador web que usamos para el servidor RADIUS en nuestro caso DALORADIUS nos permite tener un control eficaz en la red por medio de gráficas o visuales para ver el consumo de ancho de banda el tiempo, ver la cantidad de usuarios que tenemos en la red, los grupos a los cuales pueden pertenecer cada uno de ellos, los permisos que pueden tener dentro de la red, el administrador puede visualizar las página que está intentando ingresar para controlar los recursos de mejor manera con esta herramienta que indica el usuario exacto la hora fecha en que está ocupando la red y más detalles.

También podemos tener control del servidor vía comandos en la terminal de Ubuntu donde realizamos la instalación de nuestro servidor, aunque este tiene que tener mayor

conocimiento debido a la dificultad pero si queremos parar el servicio, resetearlo, o inicializarlo se lo puede hacer como lo hemos observado anteriormente, la dificultad que este ofrece es el que hace que la administración web sea la mejor para el control total de la red y si trabaja de la mano con la seguridad que mantiene la institución como lo son los antivirus y gestores de red podremos tener una administración óptima y eficiente.

Las diferentes formas de usar el estándar que estamos estudiando IEEE 802.1X son óptimos ya sea en forma cableada o en forma inalámbrica darán una mayor seguridad en la información de la institución que es lo que se buscaba, vamos a ver a continuación el proceso de funcionamiento de lo descrito anteriormente y pruebas de conectividad entre los dispositivos para probar una conectividad total de la red que implementamos para realizar el plan piloto que es viable dentro del ministerio.

Para realizar las pruebas de nuestro plan piloto vamos a comenzar haciendo pruebas de conexión desde los dispositivos que forman parte de nuestra topología servidor, autenticador, usuario, vamos a empezar con conectividad al local host de nuestro servidor para ello hacemos ping a la dirección 10.0.105.13.

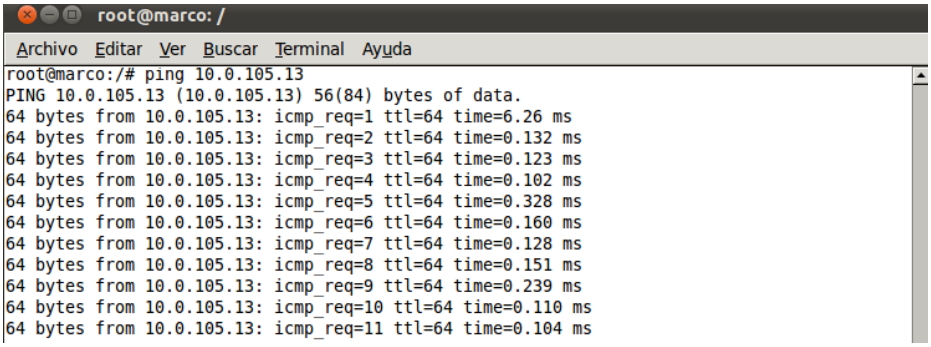

Figura. 5.9. Conectividad local

Vamos a realizar una prueba de conectividad al switch que actúa como autenticador este tiene como dirección ip 10.0.105.18.

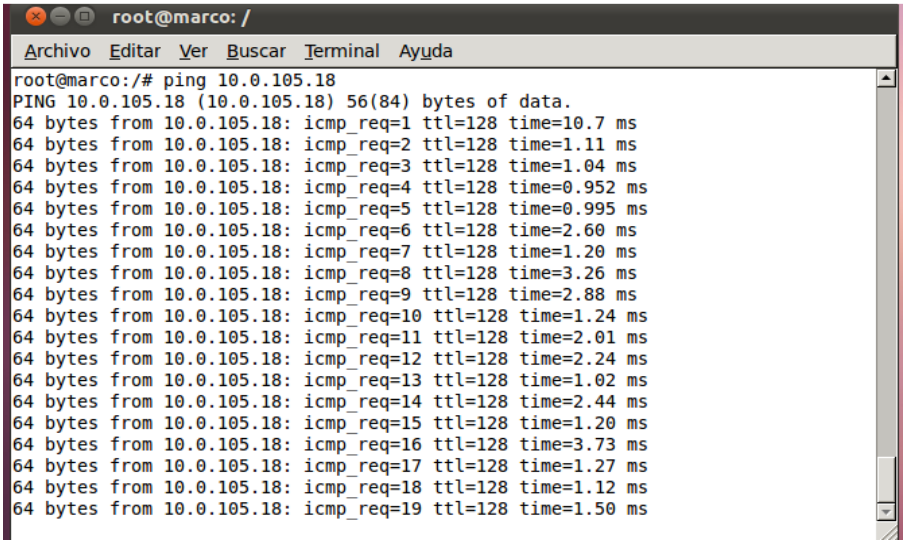

Figura. 5.10. Conectividad con el autenticador

Realizamos preuba de conexión a la máquina física desde la virtual la que salimos por la direción ip 10.0.105.2.

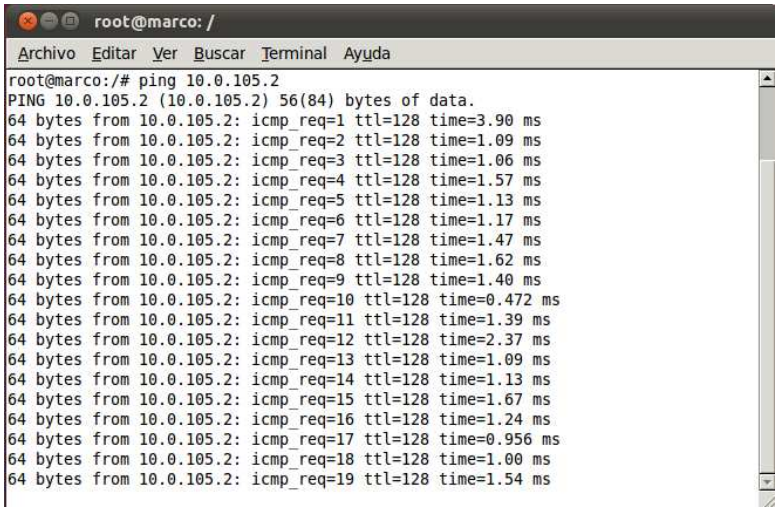

Figura. 5.11. Conectividad con máquina física

Seguimos haciendo pruebas de conectividad entre nuestro servidor y los usarios que fueron autenticados de forma correcta.

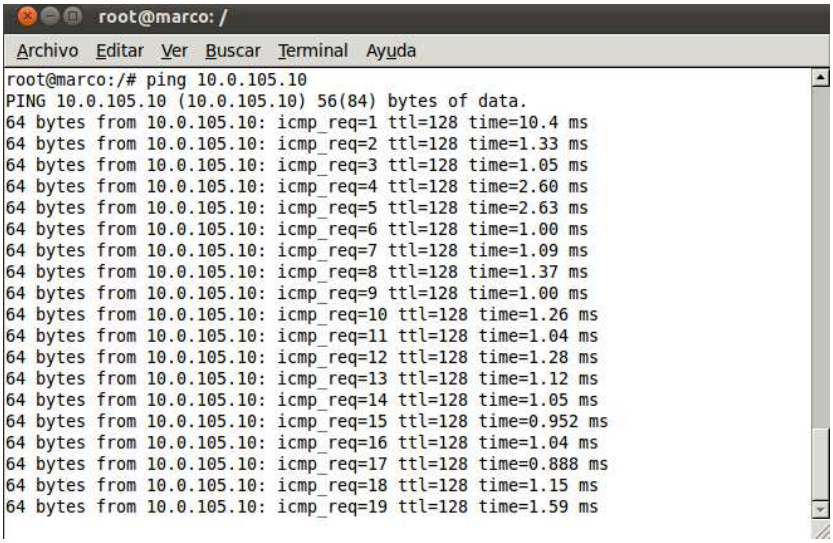

Figura. 5.12. Conectividad con el usuario

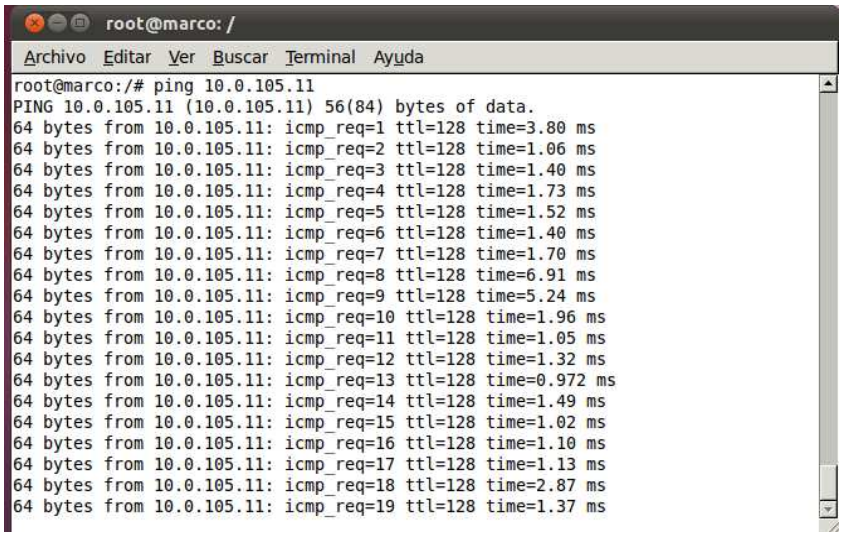

Figura. 5.13. Conectividad con eldiferente usuario

Podemos hacer las pruebas localmente de los usuarios mediante radtest y ver los log que se generan después del mismo para comprobar su correcto funcionamiento.

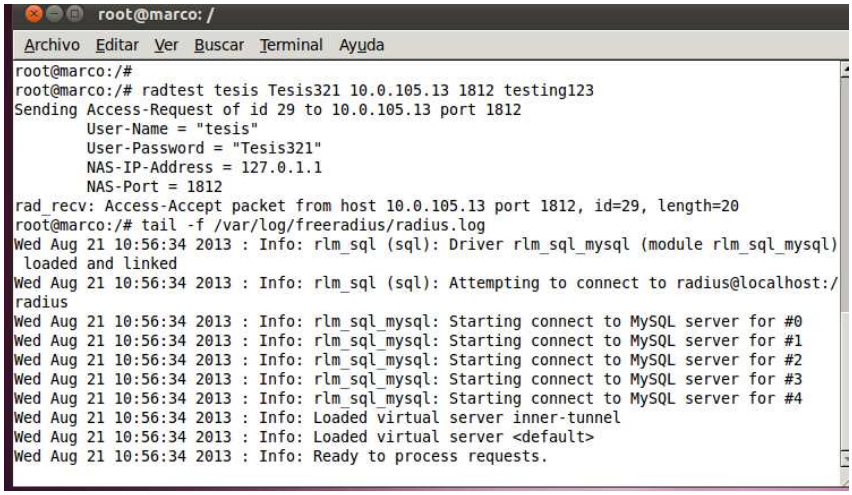

Figura. 5.14. Log de generación de usuario

El autenticador en su interfaz antes de la actualización está en down aun estando conectado a la interfaz a un ordenador hasta antes de su autenticación, una vez que logeamos el usuario correctamente la interfaz pasa a estado up.

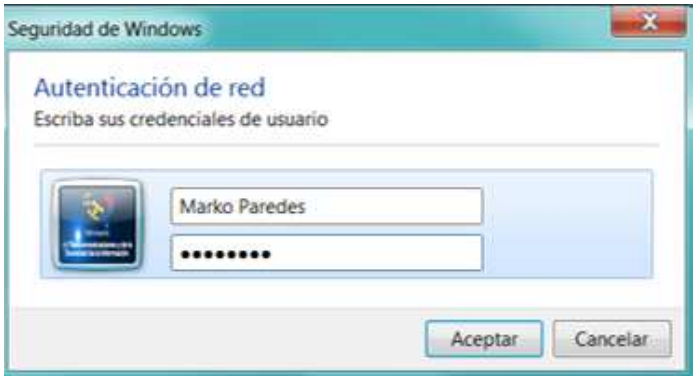

Figura. 5.15. Auntenticación válida

En la siguiente imagen observamos el compartamiento antes descrito de estado down a up de la interfaz a la cual esta conectada el ordenanor que se auntentica al sistema, después en el switch para ver el estado de la autenticación podemos colocar el comando show dot1x interface fastethernet 0/2 dependiendo de al interfaz a la cual tenemos conectado el ordenador, este comando no sa información como puerto el modo que fue

configurado el sistema el tipo de configuración del estándar como la protección el periodo de tiempo de reconocimiento del servidor, el número de autenticaciones fallidas que puede soportar el servidor, esi ha esta interfaz se puede conectar a más de un ordenador como multi host, entre otros.

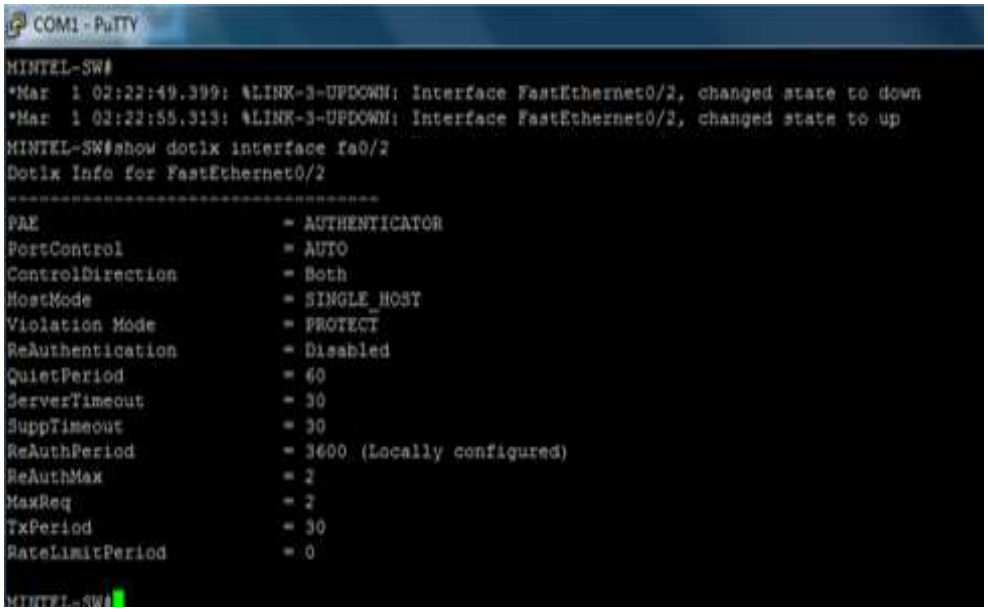

Figura. 5.16. Visualización del estado de la interfaz de switch

Entonces una vez la interfaz arriba nosotros podremos hacer pruebas de conexión entre el ordenador conectado al autenticador en este caso el switch que tiene configurado una dirección de administración con la vlan creada.

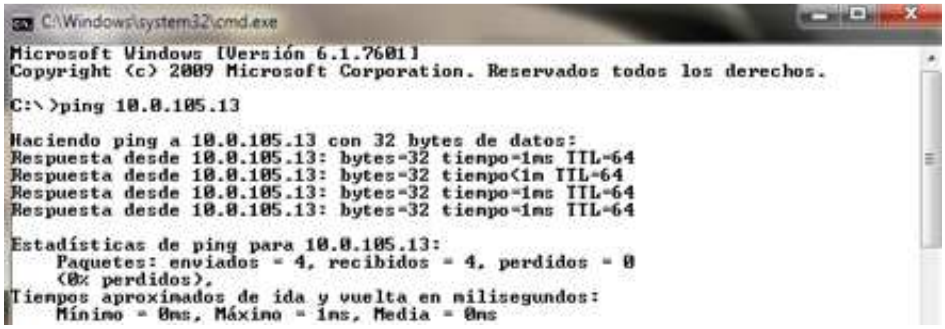

Figura. 5.17. Conectividad al servidor

Una vez arriba varias interfaces reconocidas por el switch autenticador podremos tener conexión entre diferentes dispositivos reconocidos por el servidor y pertenecientes a un mismo grupo.

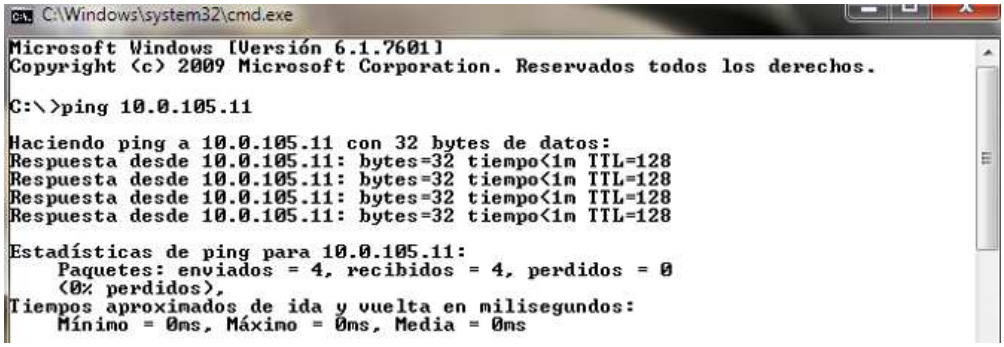

Figura. 5.18. Conectividad al usuario

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Se logró con la implementación del estándar IEEE 802.1X mayor seguridad a los recursos que forman parte de la red de la institución, sabemos que todo sistema es vulnerable y no existe un sistema cien por ciento seguro, si complementamos a la nueva implementación con las herramientas de seguridad que actualmente se encuentran en funcionamiento en la institución tendremos un nivel de seguridad aceptable y apta para información muchas veces confidencial que se maneja en una institución pública.

- El uso de software libre no genera costos en licenciamiento y cada día tiene mayor acogida, la implementación del servidor está configurada en la plataforma Ubuntu escogido por su estabilidad y versatilidad, su configuración vía comandos es una de las más conocidas y existen herramientas web como Webmin, phpmyadmin, Daloradius que ayudan al manejo y configuración de los programas y servicios instalados en el sistema operativo.

- El servidor instalado AAA funciona de acuerdo a los parámetros configurados, dando acceso a todos los usuarios que se encuentran dentro de la base de datos y denegando el ingreso a los servicios a los usuarios que no lo están, la autenticación se realiza mediante usuario y contraseña, por motivos de seguridad no realizamos la autenticación vía MAC por la facilidad que actualmente existe para clonar estas direcciones usando software especializado para este fin.

- El servidor no permite una autenticación combinada mediante usuario, contraseña y la dirección MAC, lo que se hizo es configurar la interfaz a la que está conectado un dispositivo y ponerla en modo un solo host dando el mismo efecto y evitando de esta forma que usuarios conecten su máquina en otro punto de red para obtener permisos a los que no están autorizados.

- La base de datos es compartida entre los dos servicios Radius y Mysql, las configuraciones se pueden realizar en uno de ellos y los cambios se reflejan simultáneamente en los dos, para facilidad de administración se instalaron las aplicaciones web Daloradius y phpmyadmin herramientas en las cuales la configuración de la base de datos como es la creación de usuarios o el cambio de esta información es sencilla.

- Daloradius permite una configuración personalizada, cada usuario puede tener su método de autenticación, grupo al que pertenece dentro de la red, su propia generación de logs y registros, a más de esto la aplicación brinda un ambiente gráfico que permite que el administrador tenga facilidad de controlar la red, y solucionar problemas si es el caso.

- Los métodos de autenticación que nos permite el estándar 802.1X son varios, cada uno con cierto tipo de seguridad adicional, después de un análisis con los miembros del Departamento de Gestión Tecnológica se escoge como los métodos ideales por sus características de configuración y seguridad en encriptación y

cifrado a EAP-MD5 y PEAP, que pueden ser implementadas en conexiones alámbricas e inalámbricas.

- El manejo de tarjetas inteligentes o certificados digitales pueden brindar mayor seguridad a la red, pero generan costos y mayores inconvenientes en la administración por la cantidad de usuarios que forman el sistema, queda a consideración de la institución el poder implementar estos métodos de autenticación en el futuro.

- Se entregó al director del Departamento de Gestión Tecnológica un manual de administración que muestra paso a paso la configuración en los diferentes dispositivos que forman parte del estándar 802.1X a nivel de usuario y a nivel de administrador.

- Todos los dispositivos que forman parte de la topología de la red del ministerio son compatibles con el estándar IEEE 802.1X, la mayor cantidad de equipos son switch de marca Cisco modelo 2960 haciendo que la integración con la nueva forma de autenticación sea posible y todos estos pueden tener el acceso seguro a la red.

- El sistema de seguridad actual del Mintel maneja antivirus, fortigate, fortimail los que son compatibles con la implementación, si estos trabajan conjuntamente brindan mayor fortaleza a la seguridad de la información y los recursos que puede tener cada funcionario, respetando las políticas de seguridad que el ministerio tiene para cada departamento y usuario.

- Para facilitar la gestión de la red el administrador puede acceder a Daloradius o a la vez puede seguir usando software que lo tiene contratado como lo es la herramienta Whatsapp para gestionar de mejor manera la red, crear alarmas de avisos para la seguridad y monitorear la saturación del uso del internet y con el servidor instalado podemos detectar el usuario exacto que está afectando a los

recursos, la cantidad de excesos y a la vez el mismo puede visualizar las páginas que están siendo visitadas, y poner correctivos de forma oportuna.

6.2 RECOMENDACIONES

- La instalación del servidor Radius sus utilitarios y programas que se utilizan para el funcionamiento correcto de los servicios instalados en la plataforma Ubuntu deben estar considerados en las últimas versiones que estén disponibles para no generar errores de instalación, o errores de funcionamiento cuando estén activos los servicios.

- Es de gran ayuda las aplicaciones web que se instalaron como son phpmyadmin, Daloradius para que las configuraciones en los servicios sea muy sencilla debido a que el sistema operativo Ubuntu manejado vía comandos requiere un alto grado de conocimientos para realizar cualquier configuración de forma correcta, estas aplicaciones nos dan la facilidad de controlar administrar de forma visual por medio de gráficas el funcionamiento de los servicios, también contamos con el uso de Webmin con el que podemos manejar la plataforma Linux instalada de forma sencilla desde cualquier tipo de browser de Windows, en este podemos controlar, manipular ya se carpetas, archivos, y los servicios requeridos entre otros, el único requerimiento que tiene es el correcta autenticación que hicimos en el momento de la instalación del sistema operativo en este caso Ubuntu.

- Es necesario tener en cuenta antes de inicializar las configuraciones las políticas de seguridad que maneja la institución para no ir en contra de la misma tanto en las configuraciones del administrador como la de cada usuario que va acceder a los servicios instalados.

- Es necesario que el administrador sepa cómo generar los logs ya que estos informan cómo está funcionando el servicio y en caso de error en que parte de la

configuración tenemos la falla y el poder solucionarlo de forma oportuna, los registros que se manejan de los usuarios los podemos manipular de forma más sencilla con aplicación Daloradius, el cual nos muestra ya sea por fechas, o historiales como el usuario accede a los recursos de la red para facilidad de la administración.

- La ingeniería social es vital cuando se implemente totalmente el servidor y este en vigencia, para que cada funcionario no tenga problema en su forma de acceso a la red y sepa cómo manejarse ya que el monitoreo que se va a obtener sobre cada uno es más sólida.

- Se debe monitorear periódicamente no solo el servidor AAA instalando sino también los servicios como MYSQL que funcionan de la mano con el servicio AAA, a más de esto se recomienda tener monitoreado los dispositivos que forman parte de la red como son los switch, Access point, ordenadores esto se puede hacer mediante un gestor de red como Wathsapp que actualmente maneja el Ministerio y también manualmente para ver que las interfaces configuradas no se vean afectadas.

- Es necesario que se tenga implementado el estándar IEEE 802.1X no solo en los ordenadores de los usuarios a la red sino también en los dispositivos que forman parte de la topología de la institución los cuales no tendrán problema en pegarse al mismo que son de la misma marca, si se piensa instalar dispositivos de una marca diferente también es posible por la versatilidad que ofrece el estándar y su capa.

- El uso de certificados dentro de los métodos de autenticación en PEAP pueden ser demasiado costosos por la gran cantidad de usuarios que se tienen en la institución lo cual queda en consideración de análisis posteriores si estos se realizan o no posteriormente, pero se recomienda PEAP sin certificados como

método seguro de autenticación o a su vez el método MD5 también es recomendado aunque se lo realiza más en redes cableadas que son la que más se maneja en la institución.

REFERENCIA BIBLIOGRÁFICA

[1] Jorge, M. (31 de agosto de 2011). , Configurar un servidor Controlador de Dominio con Samba y OpenLDAP en Ubuntu Server Hardy 8.04. Obtenido de http://tuxjm.net/docs/Configurar_Servidor_Controlador_de_Dominio_con_Samba_y_OpenLDAP/Ubuntu/html-multiples/el-arbol-de-directorio-dit.html

[2] Protocolo LDAP. (junio de 2012). Obtenido de http://es.kiokera.net /contents/269-protocolo-ldao

[3] Lázaro, R. (febrero de 2010). Implementación de un Servidor Samba con autenticación LDAP. Obtenido de http://www.monografias.com/trabajos-pdf4/implementacion-servidor-samba-autenticacion-ldap/implementacion-servidor-samba-autenticacion-ldap.pdf

[4] Samba PDC en Debian. (28 de abril de 2009). Obtenido de http://www.improvisa.com/28-04-2009/samba-pdc-en-debian

[5] Switches Cisco Catalyst serie 2960,2960-C y 2960-S. (marzo de 2009). Obtenido dehttp://www.cisco.com/web/LA/soluciones/comercial/products/routers_switches/catalyst_2960_series_switches/index.html

[6] Cisco Wireless LAN Controller Serie 2100. (septiembre de 2010). Obtenido de http://www.cisco.com/web/ES/solutions/smb/products/wireless/2100_series_wireless_lan_controller/index.html

[7] Aironet 1140 Serie de acceso. (enero de 2011). Obtenido de http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/datasheet_c78502793.html&prev=/search%3Fq%3DCisco%2BAironet%2B1140%2BSeries%2B802.11n%26biw%3D1241%26bih%3D606

[8] Seguridad Informatica. (mayo de 2005). Obtenido de http://www.seguinfo.com.ar/fisica/

[9] Normatividad para seguridades inalámbricas.(diciembre del 2007). Obtenidod de http://redesseguridad-wikipaces.com

[10] Ataque de autenticación captura de handshake wpa . (05 de febrero de 2010). Obtenido de http://www.aircrack.es/foro/aircrack-ng-linux/127-ataque-0-deautenticacion-captura-del-handshake-wpa.html

[11] Configuración de la autenticación basada en puerto 802.1X. (abril de 2010). Obtenido de http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/Sw8021x.html&prev=/search%3Fq%3D802.1x%2Bcisco%26biw%3D1241%26bih%3D606

[12] Criptografía de clave privada (o clave secreta). (2007). Obtenido de http://es.kioskea.net/contents/126-criptografia-de-clave-privada-o-clave-secreta

[13] Descripción de cifrado simétrico y asimétrico. (2008). Obtenido de http://support.microsoft.com/kb/246071/es

[14] Revista It Now. (25 de septiembre de 2012). Obtenido de http://revistaitnow.com/2012/09/SEGURIDAD/mas-alla-del-firewall-y-la-seguridad-perimetral

[15] Instalación y configuración de un servidor radius. (2010). Obtenido de http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

[16] Configuración de la autenticación basada en puerto 802.1X. (2011). Obtenido de http://translate.google.com.ec/translate?hl=es19&sl=en&u=http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/Sw8021x.html&prev=/search%3Fq%3D8

[17] Formato de la trama Ethernet. (2006). Obtenido de http://www.itescam.edu.mx/principal/sylabus/fpdb/recursos/r93145.PDF,

[18] Seguridad en WIFI. (junio de 2009). Obtenido de http://redesseguridad.wikispaces.com/Normatividad

[19] Entender lo que es el estándar IEEE 802.1X . (17 de octubre de 2012). Obtenido de http://cioperu.pe/articulo/10535/que-es-8021x

[20] Guillermo, I. (julio de 2010). Aspectos de Seguridad en Redes Locales e Inalámbricas : Acceso Red controlado por puerto (IEEE 802.1X). Obtenido de http://cita2003.fing.edu.uy/articulosvf/59.pdf

[21] Manual radiuslinux_ubuntu, . (octubre de 2011). Obtenido de http://es.scribd.com/doc/33983013/Manual-Servidor-Radius-Linux-Ubuntu

[22] Jimmy, V. (2012 de agosto). Seguridad avanzada en redes wireless 802.1x. Obtenido de http://www.jacksecurity.com/files/publications/Jack42.pdf