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

Paredes S. Marco Patricio, Urbina G. Wilmer Marcelo, Espinosa O. Nikolai Daniel

Ingeniería Electrónica en Redes y Comunicación de Datos, Universidad de las Fuerzas Armadas ESPE

Sangolquí, Ecuador

marco1821paredes@hotmail.com

murbina@espe.edu.ec

ndespinosa@espe.edu.ec

***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, Protocolo EAP.

I. INTRODUCCIÓN

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 de 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. 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, en la actualidad la institución tiene implementado el protocolo.

II. ANALISIS ACTUAL DE LA RED

Actualmente la institución usa le protocolo LDAP (Protocolo compacto de acceso a directorio), tecnología que permite administrar a todos los usuarios acceder a la información de los mismos por medio de la base de datos, al mismo tiempo por medio de éste es posible administrar el hardware considerando que también funciona con el protocolo TCP/IP. La desventaja es que no muestra características de gran escalabilidad y flexibilidad, soporta algunas formas de acceso; pero no todas las formas de seguridad de los métodos de autenticación. Lo que se busca actualmente es dar solución a 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.

III. SERVIDOR AAA

A. *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, una contraseña, una huella dactilar, ocular u otras formas, las cuales fueron previamente almacenadas en una base de datos. Los métodos de autenticación son más complejos según el tipo de información que manejan.

B. *Autorización*

Este proceso entra en juego una vez que pasa la autenticación, lo que hace es brindar los permisos a los recursos de la red a cada uno de los usuarios basándose en privilegios que son dados por las políticas de seguridad y reglas de la institución, como el Ministerio es público tiene gran cantidad de usuarios y los privilegios se otorgan según el departamento al que pertenece el usuario, tratando de explotar al máximo todos los recursos, sin afectar a la información, aplicaciones, anchos de banda, archivos compartidos entre otros.

C. *Contabilidad*

Este proceso no es más que por medio de un log ir registrando cada uno de los eventos que cada usuario va generando dentro de la red este proceso sirve para detectar amenazas y ataques, la generación de los registros es personalizada se puede apreciar de forma gráfica o de alertas, sin duda se facilita la administración de la red porque el control es especifico detectando de forma sencilla el punto donde se genera un problema de la red y de esta forma dar soluciones puntuales y oportunas.

IV. ESTÁNDAR 802.1X

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

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, en la figura 1 podemos ver los componentes básicos en la topología del estándar 802.1X.

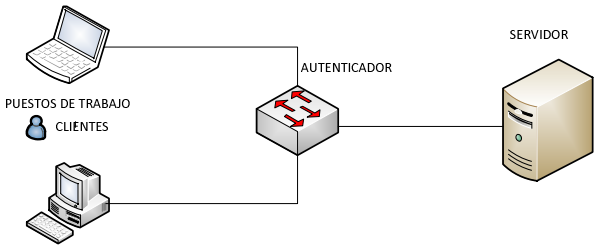

Figura 1. Conexión básica 802.1X fija

El estándar trabaja en la capa de enlace de datos del modelo OSI, 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 en español significa Protocolo de Autenticación Expandible.

Para entender el funcionamiento del estándar 802.1X vamos a observar el funcionamiento del mismo por medio del diagrama de flujo que se representa en la figura 2.

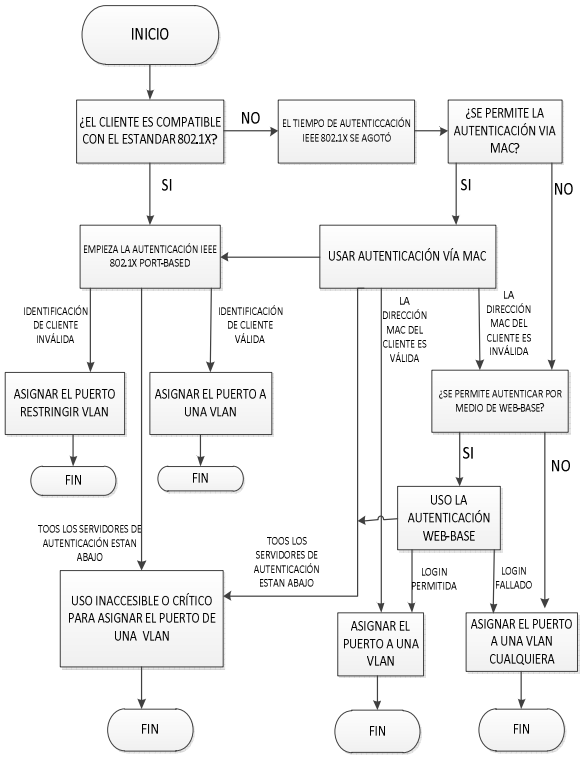

Figura. 2. Diagrama de Flujo de funcionamiento IEEE 802.1X

En la figura 3 representamos como es 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.

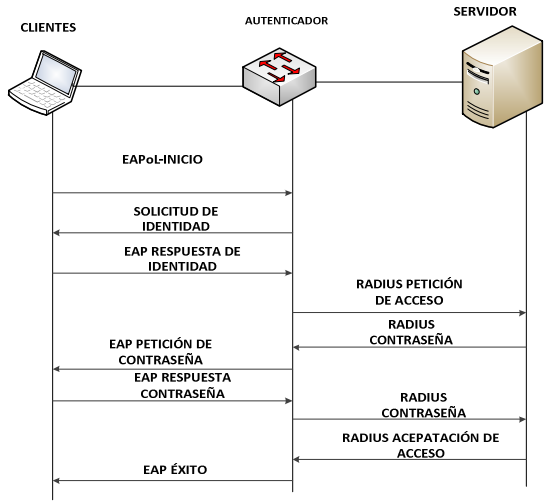

Figura 3. Funcionamiento del estándar

V. 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.

A. 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.

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

B. 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 es renviado al servidor RADIUS para repetir el procedimiento, si este proceso no tiene errores se da acceso a la red y sus recursos, una aplicación de este tipo es dado por el EAP-TLS 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 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 para cada dispositivo que quiere autenticarse, la que si usa encriptación en las tramas es empleada para WEP.

VI. ARQUITECTURA ESTÁNDAR 802.1X

El proceso de autenticación del estándar 802.1X se dá 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.

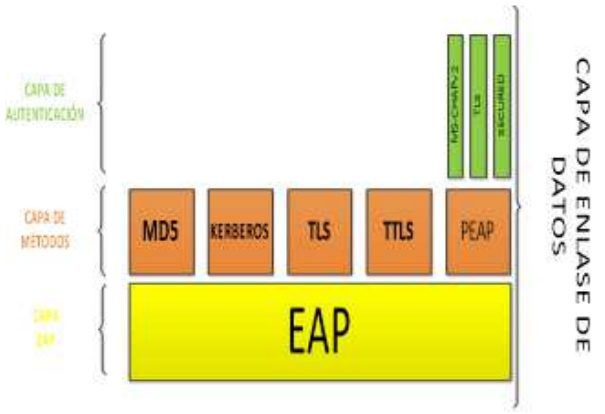

Figura 4. Arquitectura 802.1X por capas

En la figura 5 vamos a ver como es la trama generada por el estándar IEEE 802.1X y el análisis de cada uno de los campos.

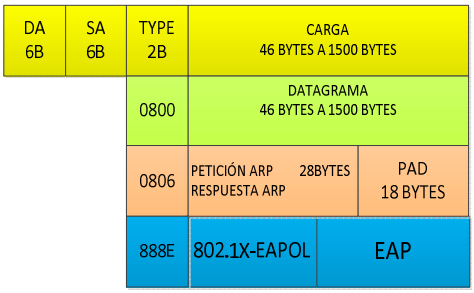

Figura 5. Trama estándar 802.1X

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 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.

A. Cabecera EAPOL/EAP

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.

En la tabla 2 vemos los campos que tiene el protocolo EAP en su trama.

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

Tabla 2 Campo tipo de paquete de la trama

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

B. Cabecera 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, en la tabla 3 mostramos el código y las acciones en el protocolo EAP.

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

Tabla 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.

VII. 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, 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, CHAP o el EAP.

A. Un solo host

En la figura 6 observamos la topología de un solo host donde a una interfaz solo va a reconocer un host.

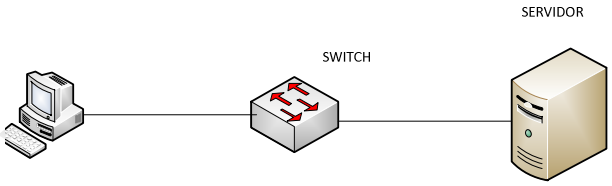

Figura 6. Conexión un solo host

B. Multihost

En la figura 7 observamos cómo se realiza la conexión multihost en la cual una interfaz puede reconocer varios dispositivos conectados a este.

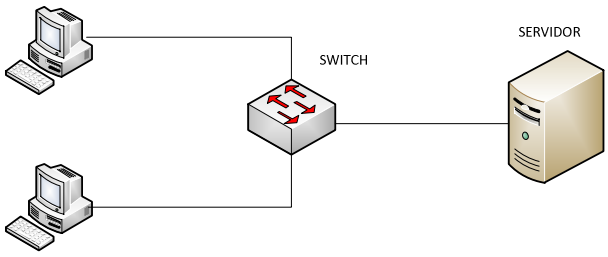

Figura 6. Conexión multihost

C. Multidominio

En este tipo de conexión debemos crear una Vlan de voz y una de datos en el switch como vemos en la figura 8 la conexión va del servidor al switch y este a un teléfono ip que manda los datos a un host.

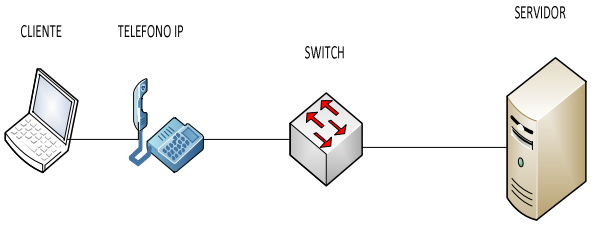

Figura 7. Conexión multidominio

VIII. CONFIGURACIONES SERVIDOR AAA

Las configuraciones para el servidor AAA 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, vamos a empezar con instalación de mysql cliente y servidor como en la figura 8

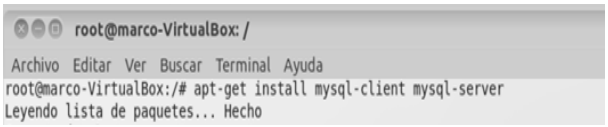

Figura 8. Instalación de mysql servidor y cliente

Vamos a instalar el phpmyadmin de la manera que lo indica la figura 9

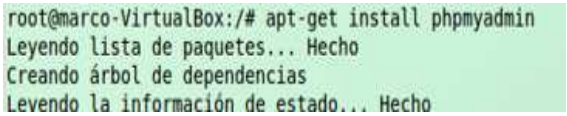

Figura 9. Instalación de phpmyadmin

Es necesario instalar apache2 fijarse en la figura 10 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.

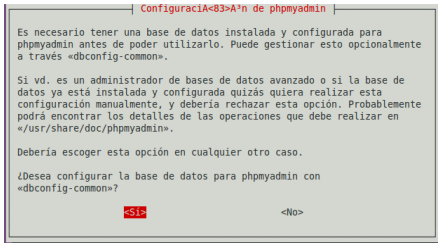

Figura 10. Configuración automática de phpmyadmin

Instalaremos los complementos de php con el siguiente comando apt-get install php5 php-pear php5-gd php-DBP, como en la figura 11.

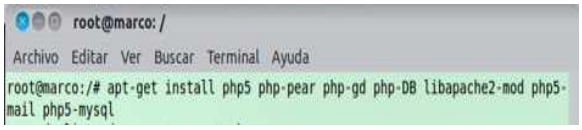

Figura 11. Instalación de todos los complementos de php

Seguimos con la instalación de freeradius para este 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 está vacía se genera una contraseña aleatoriamente, ver figura 12.

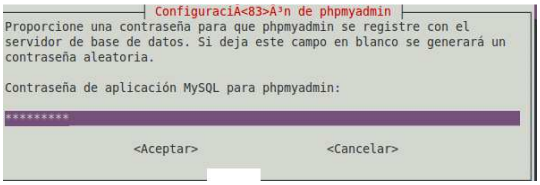

Figura 12. Ingreso de la contraseña de phpmyadmin que se vincula al servidor radius

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 intalado y configurado y su funcionamiento apropiado, si usamos un usuario que no esta 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, ver figura 13.

Figura 13. Radtest con usuariode prueba

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, como la figura 14.

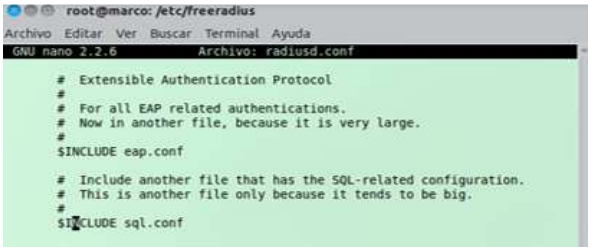

Figura 14. Descomentar include sql.conf

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, seguir la figura 15.

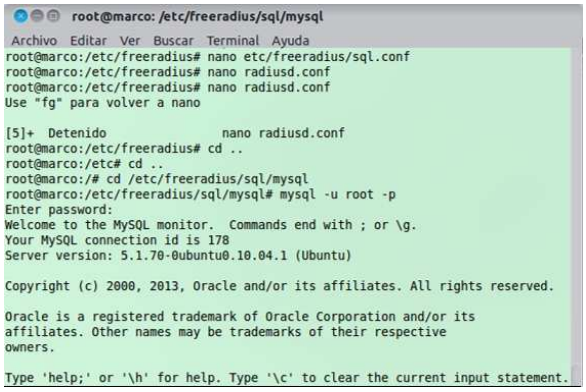

Figura 15. Ingreso a mysql con usuario y contraseña

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, ver figura 16 y 17

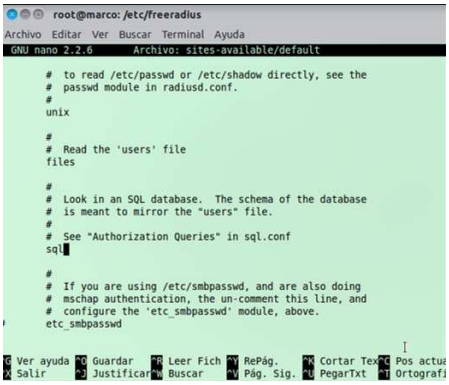

Figura 16. Descomentamos lineas con sql en autorización

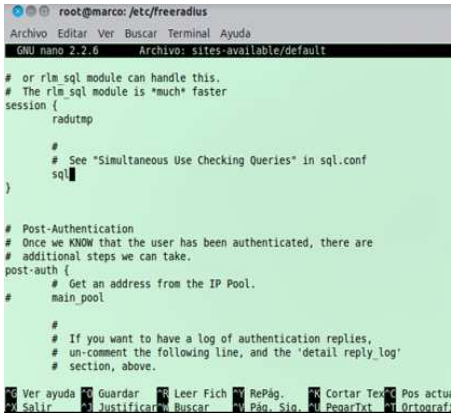

Figura 17. Descomentamos líneas con sql en sesión

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 red como se ve en la figura 18.

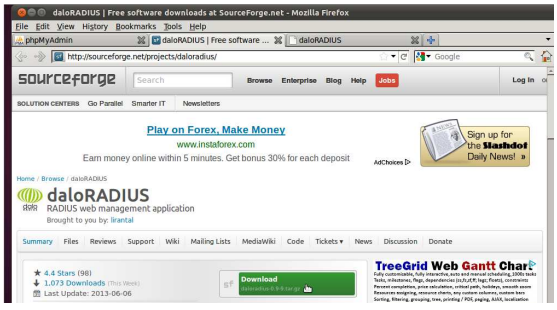

Figura 18. Página de descarga de Daloradius

Seguir la figura 19 para crear la base de datos que tendrá conexión con radius.

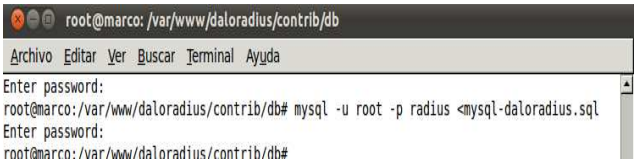

Figura 19. Ingreso de daloradius en la base de datos

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, ver figura 20.

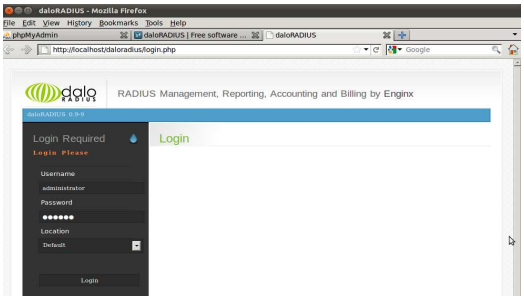

Figura 20.Ingreso a Daloradius

IX. CONFIGURACIÓN DEL AUTENTICADOR

Vamos a empezar con los comandos AAA new model como la figura 21.

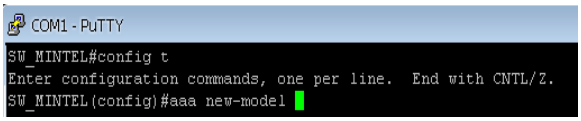

Figura 21.creación de modelo AAA en el switch

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. ver la figura 22.

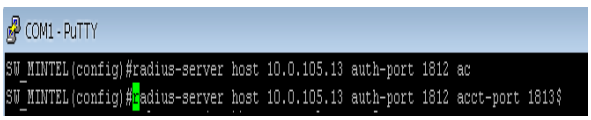

Figura 22. Apuntamiento al servidor radius

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, ver figura 23

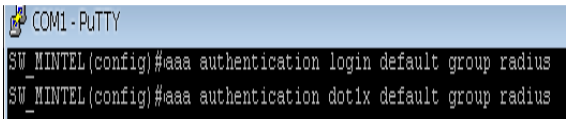

Figura 23. Poner al autenticador en modo de reconocimiento del estándar 801.X

El comando dot1x system-auth-control que indica la figura 24 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

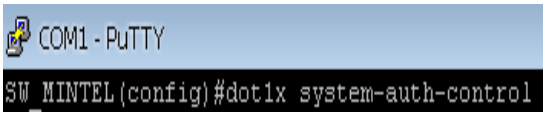

Figura 24. Configuración del reconocimiento al protocolo

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 ver figura 25.

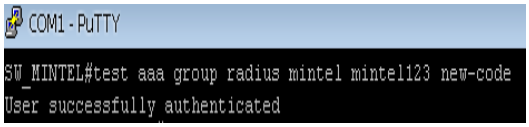

Figura 25. Auntenticación mediante usuario mintel

X. CONFIGURACIÓN DE HOST

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, 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, como indica la figura 26 de los usuarios con el fin de que la autenticación por medio del estándar 802.1X se pueda ejecutar sin problemas.

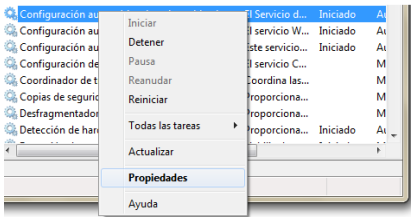

Figura 26. Configuración automatica de redes cableadas

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 como en la figura 27, en estado de servicio vamos a inicializarlo, nos aparecerá una ventana que indique el progreso de la inicialización.

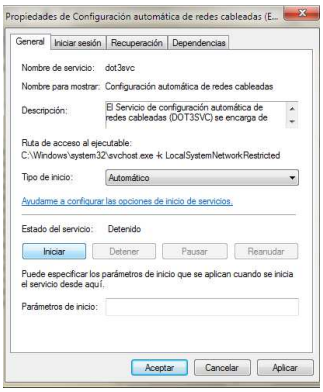

Figura 27. Propiedades de configuración de registros

Lo siguiente es entrar a las conexiones de red, ya en esta podemos ver todas las conexiones 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, ver figura 28.

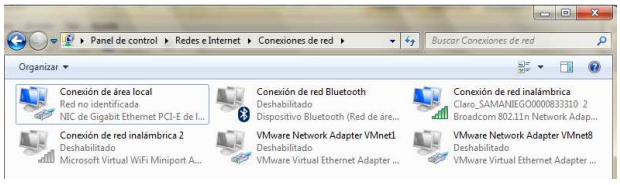

Figura 28. Ventana de conexiones de red.

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, ver figura 29.

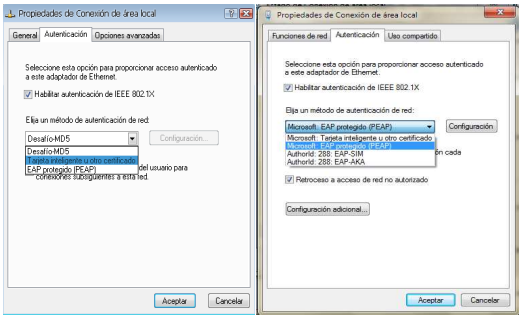

Figura 29. Método de autenticación 802.1X

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, ver figura 30.

Figura 30. 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,como lo indica la figura 31 si no elegimos esta opción no se podrá visualizar la opción en la cual se da la autenticación en el escritorio.

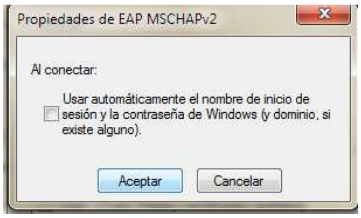

Figura 31. Deshabilirar el uso automático

XI. ANÁLISIS DE RESULTADOS DEL PROYECTO

Los resultados fueron los esperados dentro del plan piloto vamos analizamos 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 tabla 4 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 4. Comparación de métodos de autenticación 802.1X

El administrador web que usamos para el servidor RADIUS en nuestro caso DALORADIUS que 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.

XII. 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.

XIII. REFERENCIAS BIBLIOGRÁFICAS

[1] http://www.cisco.com/en/US/docs/switches/lan/catalyst2950

[2] http://es.kioskea.net/contents/126-criptografia-de-clave-privada-o-clave-secreta

[3] http://support.microsoft.com/kb/246071/es

[4] http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf

[5] http://cioperu.pe/articulo/10535/que-es-8021x

[6] http://es.scribd.com/doc/33983013/Manual-Servidor-Radius-Linux-Ubuntu

[7] http://es.scribd.com/doc/33983013/Manual-Servidor-Radius-Linux-Ubuntu

XIV. BIOGRAFÍAS

Marco P. Paredes S.

Nació el 28 de septiembre de 1988 en la ciudad de Ambato, sus estudios secundarios los culminó en el colegio San Luis Gonzaga ubicada en el en el Valle de los Chillos, obteniendo el título de bachiller en Físico-Matemático. Ingresa a la Escuela Politécnica del Ejército a realizar sus estudios superiores en Ingeniería en Electrónica y Comunicación de Datos, egresando en el año 2013.

Dr. Nikolai Espinosa, PhD

Obtuvo el título de MSc Física y PhD en Radiofísica, en la Universidad Rusa de Moscú, en el Departamento de Radiofísica y Electrónica, en 1990 y 1994, respectivamente. Se desempeña como Presidente para Ecuador de la International Commission for Optics, Docente del departamento de Eléctrica y Electrónica de la ESPE, desde 1995 hasta la fecha. Es miembro de la SPIE e IEEE, respectivamente.

Ing. Wilmer M. Urbina G.

Nació en Ambato, el 23 de Noviembre de 1979. Realizó sus estudios secundarios en el colegio “Instituto Técnico Superior Bolívar” de Ambato, obteniendo el bachillerato de Fisicomatemático. En el 2000 ingresó a la Escuela Politécnica del Ejército. En el 2007 se tituló en la carrera de Ingeniería Electrónica y Telecomunicaciones. Actualmente ejerce la docencia en la ESPE, en el departamento de Eléctrica Electrónica.