SERVIDOR RADIUS CON WPA2 MEDIANTE EL PROTOCOLO DE AUTENTICACIÓN EXTENSIBLE (EAP)

EDUARD FELIPE CARDOZO LINARES

000209220

LUIS FELIPE FORERO CASTAÑEDA

000208636

ING. EFRAIN MÁSMELA

DIRECTOR DE TECNOLOGIA EN INFORMATICA

UNIMINUTO GIRARDOT

CORPORACION UNIVERSITARIA MINUTO DE DIOS

SEDE GIRARDOT

TECNOLOGIA EN INFORMATICA

GIRARDOT, 2014-II

PÁGINA DE ACEPTACIÓN

_____

_____

_____

_____

_____

JURADO

_____

JURADO

_____

JURADO

_____

JURADO

Girardot, _____ de _____ del 2014

AGRADECIMIENTOS

Los autores de este trabajo expresamos los agradecimientos:

A la Universidad Minuto de Dios.

A el Ingeniero Efraín Másmela, Coordinador de Tecnología en Informática.

A el Ingeniero Fabio Cárdenas, Docente de Diplomado.

A los Docentes de Tecnología en Informática.

Y a todas las demás personas que de una u otra forma colaboraron en la realización del presente trabajo.

DEDICATORIA

Este trabajo está dedicado a mis padres quienes me apoyaron incondicionalmente para que pudiera lograr mis sueños, por motivarme y levantarme cuando ya no podía y mis docentes quienes fueron los que me guiaron con sus lecciones y experiencias para culminarlo enteramente, muchas gracias.

RESUMEN

Con el pasar de los años, las redes inalámbricas han sido vulneradas, debido a la aparición de complejas técnicas de ataques, por lo tanto es importante para las empresas contar con protocolos de autentificación y seguridad modernos que sean capaces de no permitir amenazas a los recursos de la red por parte de usuarios no autorizados.

Con la realización de esta monografía, se pretende incentivar el uso del servidor **Radius** con **WPA2** mediante el protocolo de autentificación **EAP** y el estándar de encriptación avanzada **AES** dentro de las empresas.

Así mismo realizaremos una apreciación más profunda de lo que es una red inalámbrica, Servidor Radius, autentificación, WPA2, EAP, criptografía simétrica y asimétrica, los diferentes métodos de encriptación y algoritmos de cifrado de datos como el AES entre otros.

Finalmente veremos el paso a paso de la configuración de nuestro servidor Radius con OpenWRT con la creación de certificados de seguridad informática, mediante open-SSL, la posterior creación y autentificación de usuarios, como también del protocolo de autentificación EAP. Todo esto gracias a herramientas gratis que se encuentran en la red como Putty e Inssider.

ABSTRAC

With the passing of years, wireless networks have been violated due to the emergence of sophisticated technical attacks, therefore it is important for companies to have authentication protocols and modern security are able to not allow threats to resources network by unauthorized users.

With the completion of this monograph is to encourage the use of **Radius** Server with **WPA2** with **EAP** authentication protocol and advanced encryption standard **AES** within companies.

Also we will have a deeper appreciation of what a wireless network, Radius Server, authentication, WPA2, EAP, symmetric and asymmetric cryptography, the different methods of encryption and data encryption algorithms such as AES and others.

Finally we see the step by step configuration of our Radius server with OpenWRT with the creation of computer security certificates through open-SSL, the subsequent creation and authentication of users, as well as EAP authentication protocol. All this thanks to free tools found on the net as Putty and Inssider.

ÍNDICE GENERAL

Tema **Pag**

Contenido

ÍNDICE DE FIGURAS

Tema **Pag**

2. INTRODUCCIÓN

El uso de las redes inalámbricas WIFI dentro de las empresas ha venido creciendo considerablemente en los últimos años, debido a su movilidad, economía, instalación, espacio, etc. Lo cual garantiza dentro de las empresas ventajas tanto empresariales como operativas, por lo tanto se obtiene mejoramiento de la productividad con disminución de gastos administrativos y de capital.

En toda empresa las redes inalámbricas aportan una mayor eficacia en relación a los todos los procesos de negocios, también mejora la movilidad, mantiene la ventaja competitiva e incrementa los ingresos.

La seguridad de la información dentro de las empresas siempre ha sido un desafío para los líderes de estas, por lo tanto con el desarrollo de esta monografía queremos recalcar la importancia de las redes inalámbricas, así mismo de que estas estén protegidas con protocolos de seguridad robustos y modernos. Ya que las redes Wifi se ven afectadas por problemas de seguridad ante amenazas de intrusos maliciosos.

Por lo tanto escogimos al servidor Radius con WPA2 con el protocolo de autenticación extensible “AEP” por ser uno de las más seguros y robustos en la actualidad, ya que cuenta con autenticación, autorización y administración de usuarios remotos.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 FORMULACION DEL PROBLEMA

¿Para qué implementar dentro de una empresa un servidor Radius con WPA2 mediante protocolo de autenticación extensible (EAP)?

3.2 DESCRIPCION DEL PROBLEMA

En la actualidad, muchas empresas no cuentan con una red WIFI que tenga un sistema de autenticación que garantice la seguridad de los datos, es por esto que buscan soluciones efectivas que les garantice que la información no pueda ser accedida ni modificada, por usuarios no autorizados. Por lo tanto las empresas deberían optar por un protocolo de autenticación y cifrado de datos que cumplan con las necesidades de dichas instituciones.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Implementar un servidor Radius en una red wifi acorde a las necesidades de seguridad de las empresas.

4.2 OBJETIVOS ESPECIFICOS

- Instalar el servidor radius bajo openwrt
- Crear certificados de seguridad informática, mediante open-SSL
- Configurar una red inalámbrica con encriptación WPA2 y protocolo EAP
- Implementar el algoritmo de cifrado simétrico AES
- Recalcar la importancia de utilizar un protocolo de seguridad viable para las empresas

5. MARCO TEORICO

En este punto se integran todas las teorías, estudios y antecedentes, que dan peso al proyecto y demuestran la validez de este. El marco teórico integra todos los conceptos esenciales para aprobar un proyecto, lo que hace necesario su desarrollo. Estos son los siguientes

5.1 RADIUS

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

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

El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

5.2 AUTENTICACIÓN

Autenticación (authentication) hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso. Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario nos permite acceder a determinados recursos. El nombre de usuario es nuestra identidad, que puede ser públicamente conocida, mientras que la contraseña se mantiene en secreto, y sirve para que nadie suplante nuestra identidad. Otros tipos más avanzados de credenciales son los certificados digitales.

5.3 CRIPTOGRAFIA

La criptografía es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: criptografía y criptoanálisis. La criptografía se ocupa del diseño de procedimientos para cifrar; es decir, para enmascarar una determinada información de carácter confidencial. El criptoanálisis se ocupa de romper esos procedimientos para así recuperar la información. Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su criptoanálisis correspondiente.

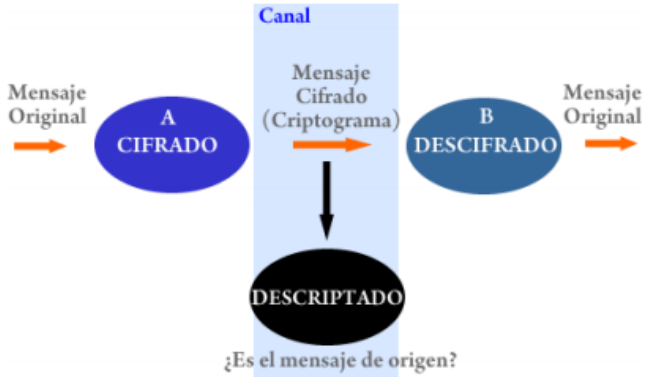

Ilustración 1-Esquema de un proceso criptográfico Fuente: http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Criptograf%C3%ADa%20I.pdf?sequence=1

5.3.1 criptografía de clave simétrica

Esta forma de cifrado utiliza una clave secreta, denominada secreto compartido, compartida por emisor y receptor. El receptor necesita la clave secreta para desbloquear los datos, esto lo hace por medio de un algoritmo de cifrado. Se denomina criptografía simétrica porque tanto para cifrar como para descifrar se necesita la misma clave.

Dentro de los sistemas simétricos distinguimos dos tipos de algoritmos:

- **Cifrado por bloque:**

  Es aquel en el que se cifra el mensaje original agrupándolo en bloques de tamaño fijo, por ejemplo 64 bits.

- **Cifrado por flujo**:

  Es aquel en el que se cifra el mensaje original bit a bit o byte a byte.

Por otro lado, los sistemas de cifrado simétrico presentas dos grandes desventajas: la distribución de las claves (en un medio público, el cual puede ser interceptado) y la dificultad de almacenar y proteger muchas claves diferentes.

5.3.2 criptografía de clave asimétrica

Esta forma de cifrado utiliza dos claves: una clave es secreta y una clave pública.

El mensaje lo ciframos con la clave pública del destinatario. Este puede descifrar a continuación con su propia clave privada. La diferencia de este sistema es que nadie necesita la clave privada de otro para poder enviar un mensaje en forma segura. Utilizamos su clave pública, la cual no necesita mantenerse segura. Al utilizar la clave pública del destinatario, sabemos que sólo esa persona puede cifrar utilizando su propia clave privada.

Este sistema tiene algunas desventajas: para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso, las claves deben ser de mayor tamaño que las simétricas y el mensaje cifrado ocupa más espacio que el original.

Por otro lado, teniendo en cuenta el tipo de operación que es usado para transformar el mensaje original en un mensaje cifrado, podemos distinguir dos métodos criptográficos:

- **Cifrado por sustitución**

  Este método consiste en establecer una correspondencia entre las letras del alfabeto en el que está escrito el mensaje original y los elementos de otro conjunto, que puede ser el mismo o distinto alfabeto. De esta forma, cada letra del texto original se sustituye por un símbolo correspondiente en la elaboración del criptograma. El receptor por su parte, conoce la correspondencia establecida, y sustituye cada símbolo del criptograma por el símbolo correspondiente del alfabeto original, recuperando así el mensaje emitido originalmente.

- **Cifrado por transposición**

  Consiste en reorganizar los símbolos del mensaje original colocándolos en un orden diferente, de tal forma que el criptograma contengan los mismos elementos del mensaje original, pero colocándolos de tal forma que resulten incomprensibles. El receptor, con conocimiento de la transposición, organiza los símbolos desordenados del criptograma en su posición original.

5.3.3 algoritmos de cifrado

Los algoritmos de cifrados son programas que realizan el proceso de criptografía basándose en los tipos de cifrado. A continuación mencionaremos los algoritmos de cifrado más usados para el proceso de encriptación.

- **DES (Data Encryption Standard):** Es un algoritmo de cifrado por bloques de 64 bits. Fue ideado por IBM y aceptado por el NIST (National Institute of Standars and Technology) en 1976. Se trata de un algoritmo de 64 bits de clave de los cuales 56 bits componen la clave de cifrado propiamente dicha, mientras los 8 restantes son de paridad y se usan para corrección de errores.

  Su principal ventaja es la rapidez de cálculo y la sencillez de su implementación. Sus principales desventajas son la poca longitud de clave que maneja y la incapacidad de manejar claves de longitud variable.
- **Triple-DES (Triple - Data Encryption Standard):** dada la capacidad de cómputo actual y la relativa facilidad que supone romper el algoritmo DES, se desarrolló DES TRIPLE, el cual consiste en aplicar tres veces el algoritmo DES en un orden específico. Primero se cifra el dato con una clave, el resultado de esto es descifrado con otra clave y por último el resultado del descifrado es cifrado nuevamente. La clave que se emplea en este último paso puede ser la primera clave utilizada o puede ser una nueva clave.Mediante este sistema se obtiene un cifrado de 192 bits (168 efectivos y 24 de paridad) con tres claves que resulta mucho más complejo de vulnerar.
- **AES (Advanced Encryption Algorithm):** también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado para el gobierno de los Estados Unidos. Actualmente es uno de los algoritmos más populares usados en criptografía simétrica.

.

- **IDEA (International Data Encryption Algorithm):** fue creado por Xuejia Lai y James Massey en 1990. Es un cifrado de bloque, que opera sobre mensajes de 64 bits con una clave de 128 bits. Consiste en ocho

transformaciones idénticas (cada una llamada una ronda) y una transformación de salida (llamada media ronda). Gran parte de la seguridad de IDEA deriva del intercalado de tres operaciones: Operación O-exclusiva (XOR) bit a bit, suma módulo 216 y multiplicación módulo 216+1.

5.3.4 Principales algoritmos de cifrado

Fue emitido por el NIST en 1999 como una versión mejorada de DES. Realiza tres veces el cifrado DES utilizando tres claves.
Cuando se descubrió que una clave de 56 bits (utilizada en el DES) no era suficiente para evitar un ataque de fuerza bruta, el DES3 fue elegido para agrandar la clave sin la necesidad de cambiar el algoritmo de cifrado.

Con tres claves distintas, DES3 tiene una longitud de clave efectiva de 168 bits con lo que se tiene una longitud de clave efectiva de 112 bits

Actualmente el DES3 sigue siendo utilizado pero cada vez más está siendo sustituido por el algoritmo AES que ha demostrado ser muy robusto y más rápido.

5.4 CERTIFICADO DIGITAL

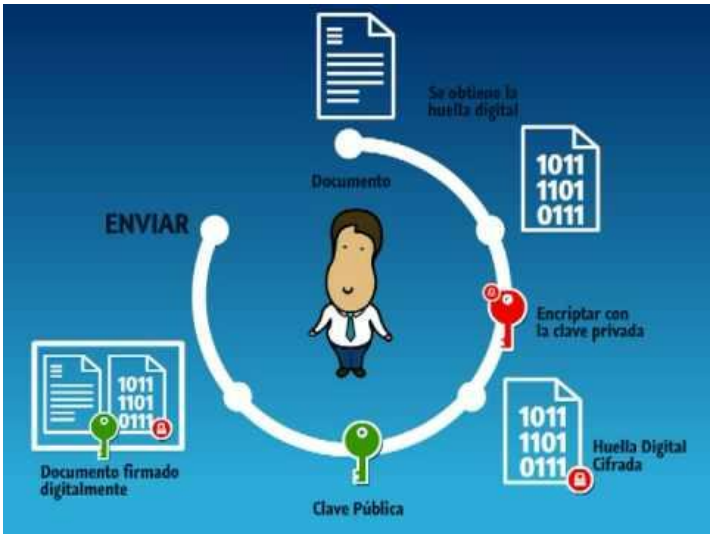

Ilustración 2-encriptación y des encriptación de un certificado digital Fuente: http://i.ytimg.com/vi/EU6vgU077xU/0.jpg

Un certificado es un conjunto de credenciales de autentificación cifradas. Los certificados se autentican mediante una clave pública que comprueba la firma digital incluida. Los certificados pueden residir en el almacén de certificados del equipo o en una tarjeta inteligente. Una de las principales utilidades de los certificados consiste en proporcionar a los servidores una capa criptográfica para evitar la circulación de información en claro por la red, particularmente cuando se intercambian datos importantes.

Las tres partes más importantes de un certificado digital son:

- Una clave pública
- La identidad del implicado: nombre y datos generales

5.5 RED INALÁMBRICA

Es aquella que permite a sus usuarios conectarse a una red local o la internet, sin la necesidad de usar cables, debido a que las transacciones realizadas o paquetes de información, se transmiten mediante ondas electromagnéticas, propagadas utilizando como medio de transmisión el aire.

Esto quiere decir que una red inalámbrica, es aquella en la cual, voz y datos pueden ser transmitidos de un punto a otro sin la necesidad de utilizar de utilizar un medio físico, como es el caso del cable de cobre o fibra óptica, lo cual, la hace muy atractiva para los usuarios finales.

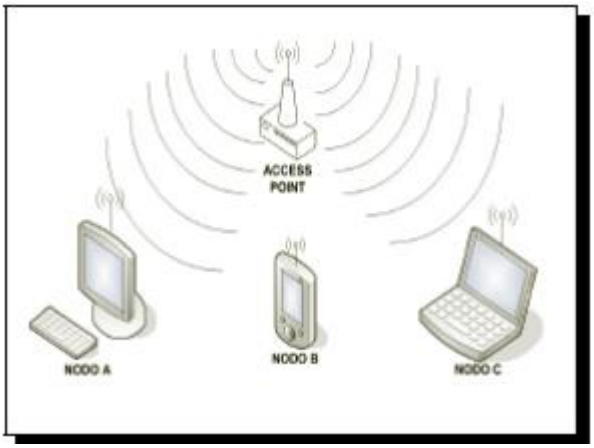

Ilustración 3-Red Inalámbrica de Área Local (WLAN) Fuente: http://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf

Dentro de las WLAN existen varios mecanismos de seguridad de los cuales los más utilizados son:

- **SSID (Service Set Identifier):** consiste en que el cliente debe de tener configurado el mismo SSID que el Access Point.
- **WEP (Wired Equivalet Piracy):** Su objetivo principal consiste en proveer la confidencialidad de transmisión de la información, tal como se ofrece en las LAN.
- **Filtrado por dirección MAC:** El Access Point está configurado para aceptar solo las peticiones de ciertos nodos de la red.
- **WPA (Wi-Fi Protected Access):** Distribuye claves diferentes a cada usuario mejora la integridad de la información, igual que WEP, los usuarios malintencionados pueden obtener su clave, otra de sus desventajas es que

al tener una contraseña de al menos 20 caracteres, la cual es difícil que los usuarios la recuerden.

WPA soluciona gran parte de las debilidades conocidas de WEP y se considera suficientemente seguro, WPA se distingue por tener una distribución dinámica de claves, utilización más robusta del vector de inicialización y nuevas técnicas de integridad y autentificación.

- **WPA2 o IEEE 802.11i:** incluye un algoritmo de cifrado AES (Advanced Encriptyon Standard), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque con claves de 128 bits. El cual, requiere un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos anteriores a su publicación no poseen las capacidades suficientes de proceso para incorporarlo, para aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter- Mode 7 Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

5.6 PROTOCOLO EAP

Con el Protocolo de autenticación extensible (EAP), un mecanismo de autenticación arbitrario autentica una conexión de acceso remoto. El esquema de autenticación exacto que se va a usar se negocia entre el cliente de acceso remoto y el autenticador (el servidor de acceso remoto o bien el servidor del Servicio de autenticación remota telefónica de usuario [RADIUS]). Enrutamiento y acceso remoto incluye compatibilidad con EAP-TLS de forma predeterminada. Puede conectar otros módulos EAP al servidor que ejecuta Enrutamiento y acceso remoto para proporcionar otros métodos EAP.

EAP permite conversaciones abiertas entre el cliente de acceso remoto y el autenticador. La conversación se compone de solicitudes de información de autenticación por parte del autenticador y de respuestas del cliente de acceso

remoto. Por ejemplo, si se utiliza EAP con tarjetas de token de seguridad, el autenticador puede consultar al cliente de acceso remoto el nombre, el NIP y el valor de token de la tarjeta por separado. Con cada consulta realizada y respondida, el cliente de acceso remoto pasa por otro nivel de autenticación. Una vez que se ha respondido correctamente a todas las preguntas, se autentica al cliente de acceso remoto.

5.6.1 EAP-Radius

EAP-RADIUS no es un tipo de EAP, sino el paso de cualquier tipo de EAP a un servidor RADIUS realizado por un autenticador de mensajes EAP para su autenticación. Por ejemplo, si se configura un servidor de acceso remoto para la autenticación RADIUS, los mensajes EAP enviados entre el cliente y el servidor de acceso remoto se encapsulan y formatean como mensajes RADIUS entre el servidor de acceso remoto y el servidor RADIUS.

EAP-RADIUS se usa en entornos en los que RADIUS se usa como proveedor de autenticación. La ventaja de utilizar EAP-RADIUS es que no es necesario instalar los tipos de EAP en todos los servidores de acceso remoto, sino sólo en el servidor RADIUS. En el caso de los servidores que ejecutan el Servidor de directivas de redes (NPS), sólo debe instalar tipos de EAP en el servidor NPS.

6. IMPLEMENTACIÓN DEL SERVIDOR DE AUTENTICACIÓN

6.1 HARDWARE

Para la implementación se utilizó un Router Model: TP-LINK TL-WDR3600/4300/4310 con un Firmware Versión: OpenWrt Attitude Adjustment 12.09 / LuCI 0.11.1 Release (0.11.1) Kernel Linux Versión: 3.3.8, estándares inalámbricos EEEI 802.11 a, b, g y n. dual band (2.4 y 5 GHz).

Ilustración 4 TP-LINK TL-WDR3600/4300/4310 Fuente: http://cdn3.pcadvisor.co.uk/cmsdata/features/3410962/tp-link-tl-wdr3600_thumb.jpg

6.2 HERRAMIENTAS Y SOFTWARE

6.2.1 PUTTY

PuTTY es un emulador gratuito de terminal que soporta SSH y muchos otros protocolos. La mayoría de usuarios, especialmente los que trabajan sobre sistemas operativos Windows, lo encuentran muy útil a la hora de conectar a un servidor Unix o Linux a través de SSH.

PuTTY ofrece una interfaz gráfica de configuración muy sencilla e integra múltiples opciones:

Guardar las preferencias de conexión para establecerla rápidamente en el futuro

- Respuestas de puertos
- Soporte Ipv6
- Soporte SCP y SFTP

6.2.2 INSSIDER

Dicha aplicación nos muestra datos sobre las redes que tenemos alrededor como puede ser su canal, su cifrado, intensidad y un largo, todo esto con una interfaz agradable para el usuario.

Entre las características más destacadas tenemos las siguientes:

- Muestra un gráfico de la intensidad que tienen las diferentes señales de red
- Obtiene datos de cada una de las redes: Dirección MAC, Nivel de seguridad, SSID, Canal, Tipo de red, Velocidad y la marca del dispositivo de red utilizado
- Permite ver gráficos del canal 5GHz y 2.4GHz
- Soporte para señales GPS

6.3 IMPLEMENTACIÓN DEL PROTOTIPO

6.3.1 ingreso a luci y configuración network

- Ingresamos por el navegador con la dirección por defecto 192.168.1.1 a la interfaz de acceso del router, e ingresamos las credenciales de usuario y contraseña por default, las cuales son root y root respectivamente.

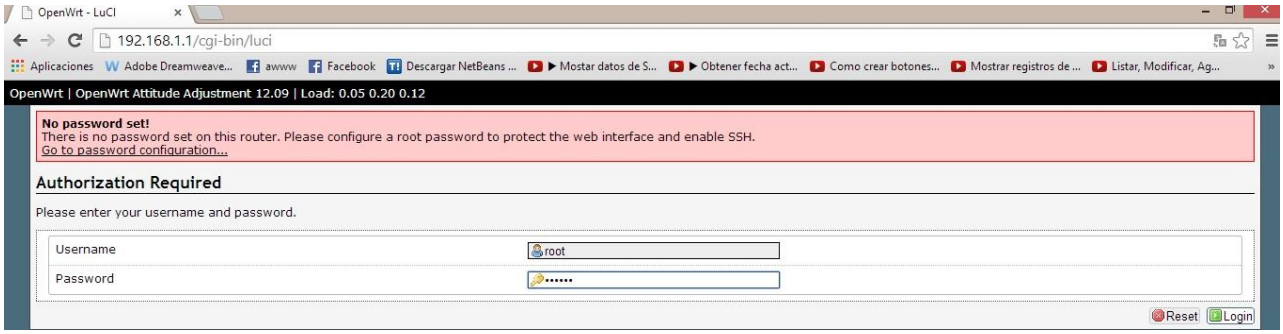

Ilustración 5- ingreso al sistema **Fuente: propia**

- Luego de autenticarnos, se muestra la interfaz gráfica para la configuración del router, además de todas que este presenta.

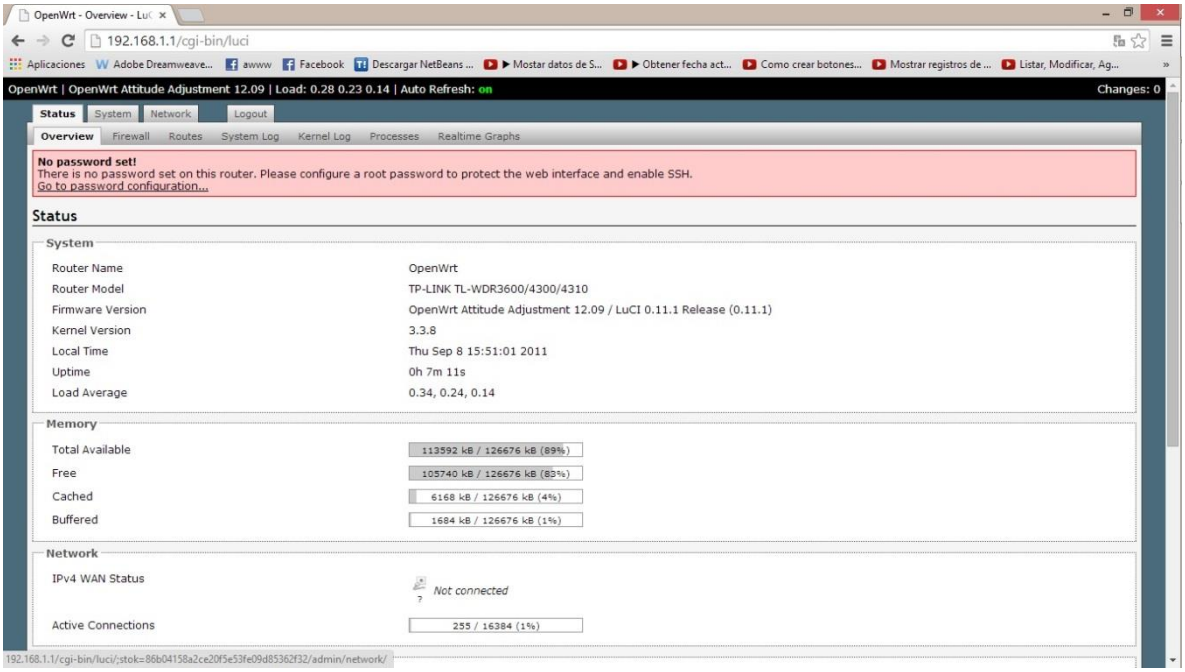

Ilustración 6 - Interfaz gráfica de luci **Fuente: propia**

- Es necesario conectarnos a un ISP o Ap que nos brinde el servicio de internet, para ello hacemos click sobre network, y seleccionaremos wifi en el menú que este despliega.

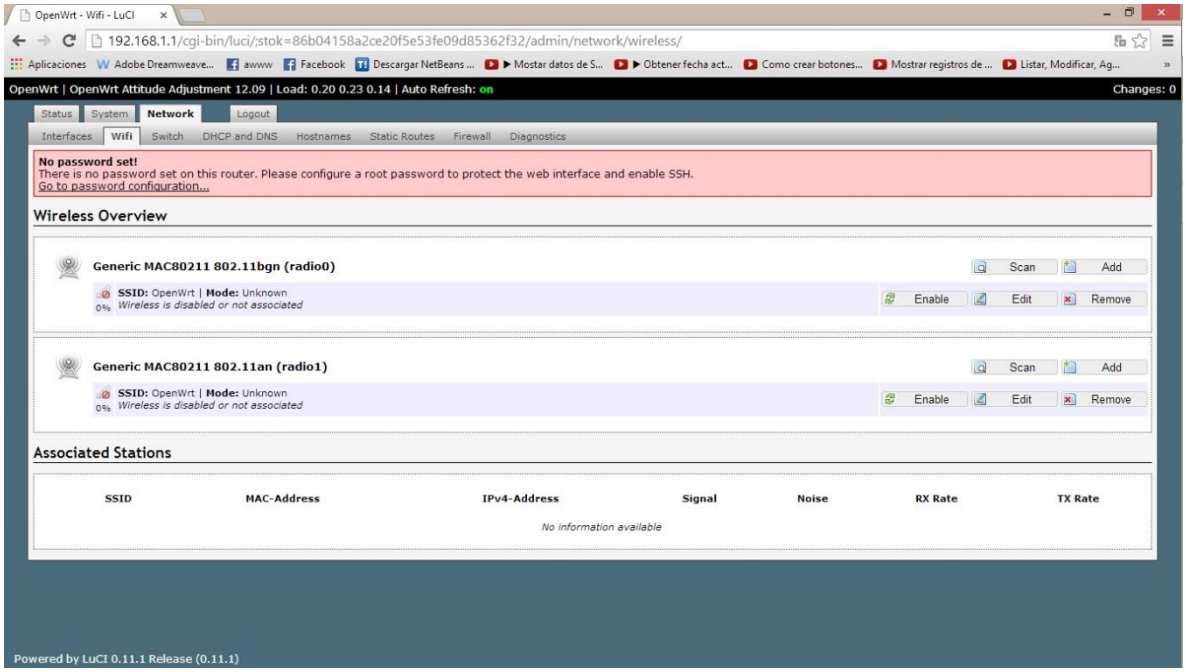

Ilustración 7 - Conexión a un proveedor de internet **Fuente: propia**

- En la pestaña System, se nos desplegara un menú, hacemos click en Administration para asignar la contraseña del router, de esta forma prevenimos que usuarios no autorizados cambien nuestra configuración.

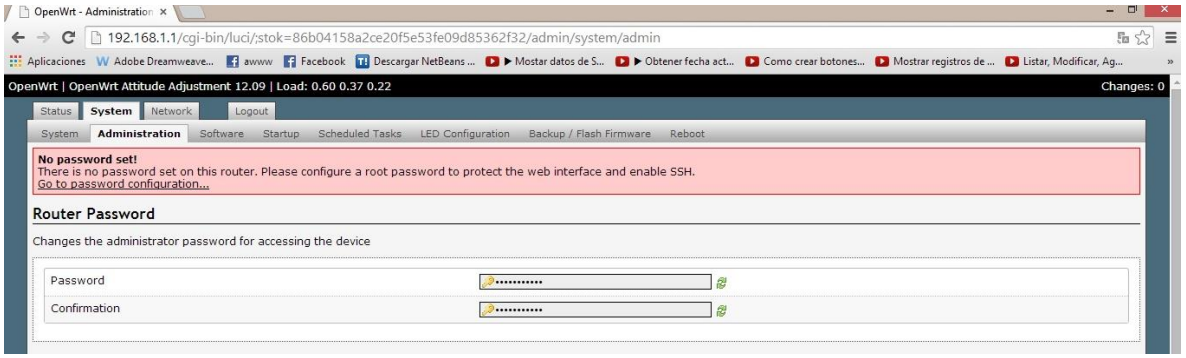

Ilustración 8 - Asignación de contraseña **Fuente: Propia**

6.3.2 instalación de server radius

- Descargamos e instalamos PUTTY, el cual es un emulador de terminal Linux a través de SSH, en hostname colocamos la dirección de nuestro router la cual es 192.168.1.1 y damos click en open para abrir la consola.

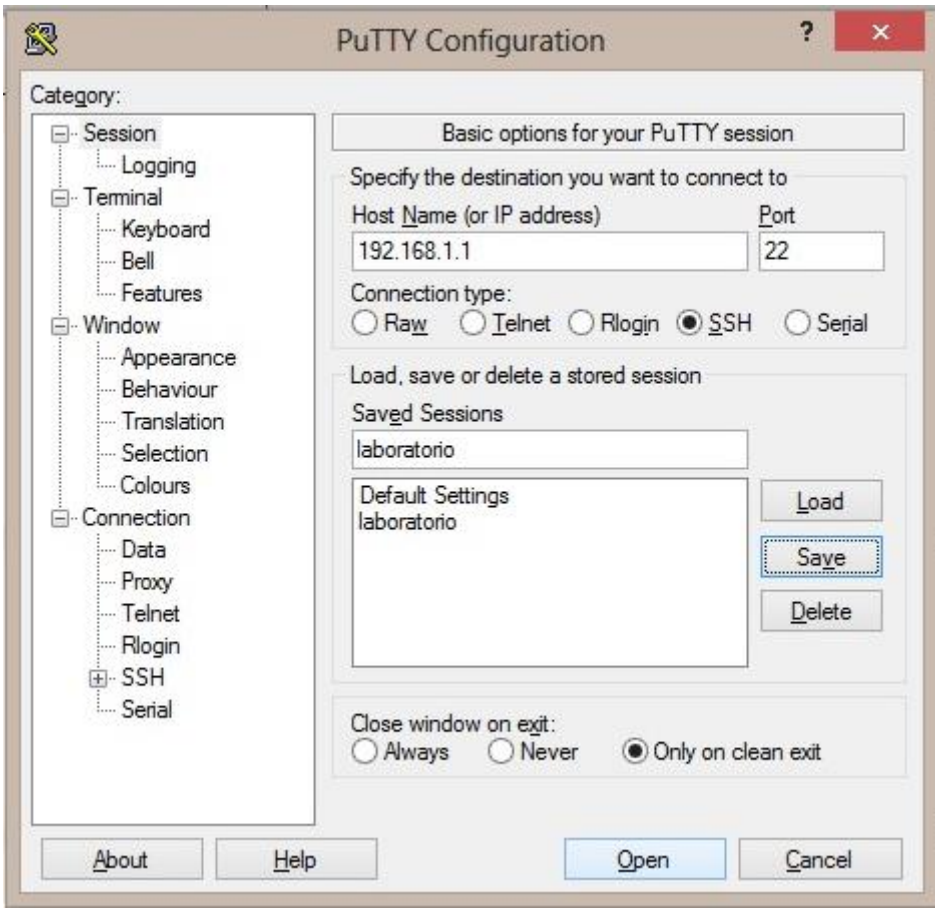

Ilustración 9 - Configuración PUTTY **Fuente: Propia**

- Proseguimos a autenticarnos con el usuario y contraseña del router para acceder a la configuración por consola.

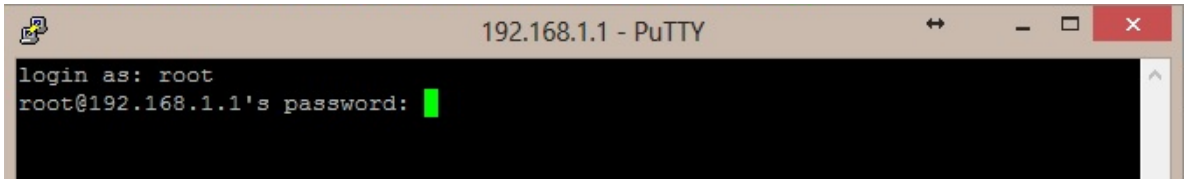

Ilustración 10 - Login PUTTY **Fuente: propia**

- Una vez ingresamos comprobaremos nuestra conexión a internet, realizando un ping a google.

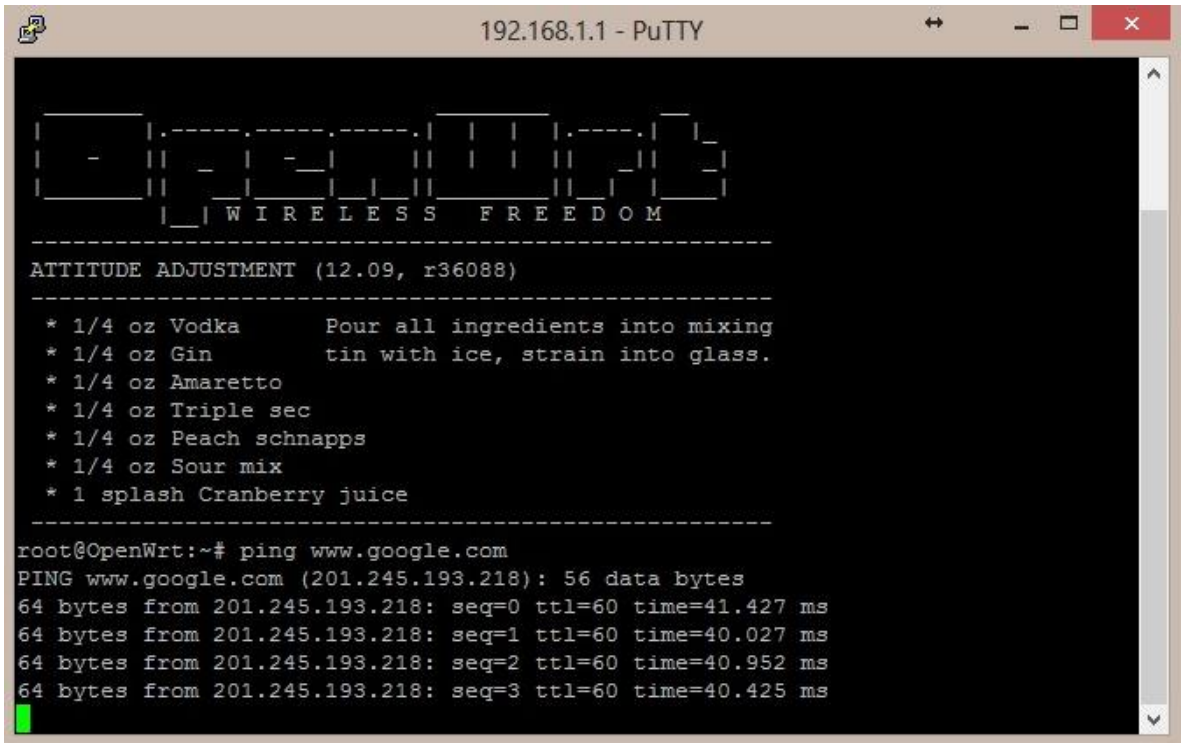

Ilustración 11 - Comprobar disponibilidad de conexión **Fuente: Propia**

- Una vez comprobado que si tenemos servicio de internet proseguimos a actualizar la lista de paquetes disponibles, como son el servidor radius, modulos mysql y repositorios de base de datos mediante el comando “opkg update”

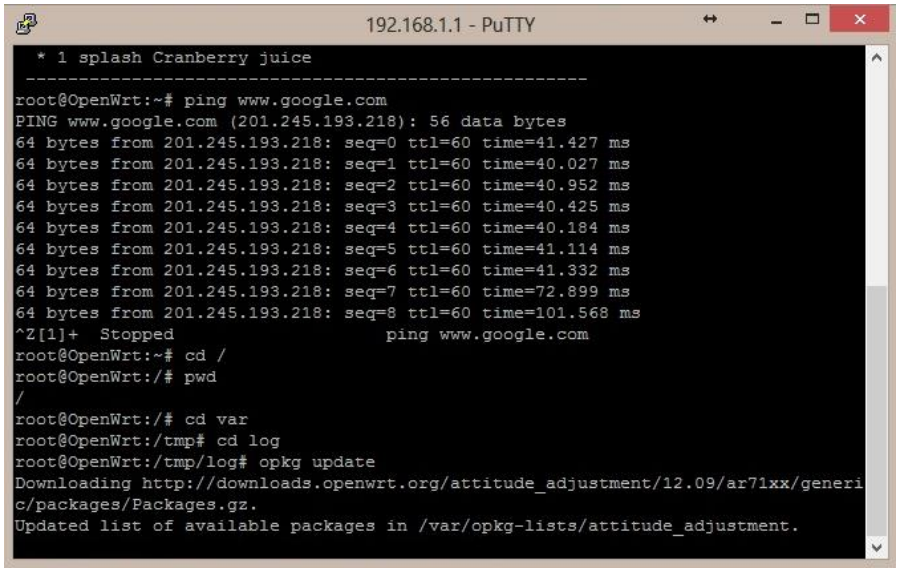

Ilustración 12 - Actualiza lista de paquetes **Fuente: Propia**

- Luego de actualizar los paquetes ingresamos el comando “opkg remove wpad-mini” el cual elimina el paquete de encriptación básico wpa antiguo.

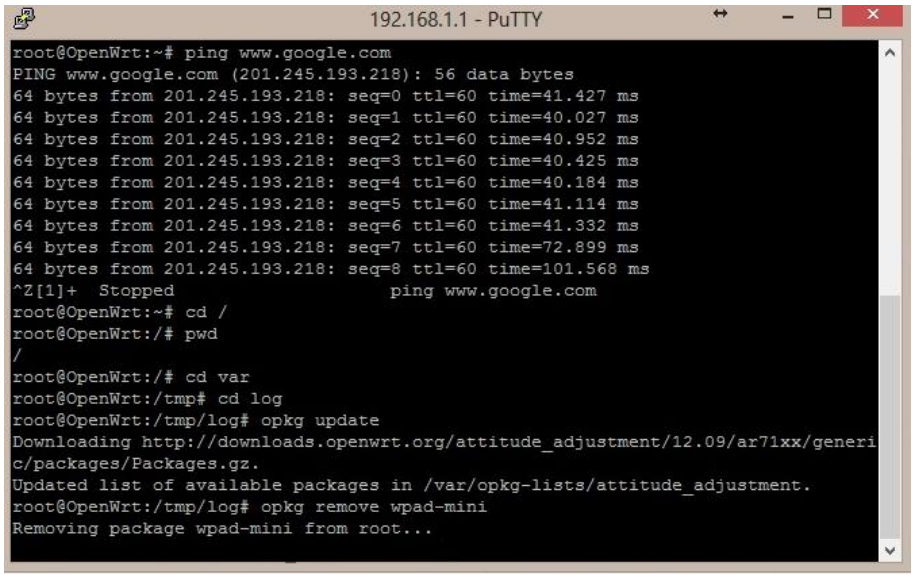

Ilustración 13 - Elimina el paquete wpa-mini **Fuente: Propia**

- Proseguimos remplazando el paquete eliminado, con el comando “opkg install wpad” el cual nos habilitara el modo WPA2 Enterprice Full compatible con los servidores radius.

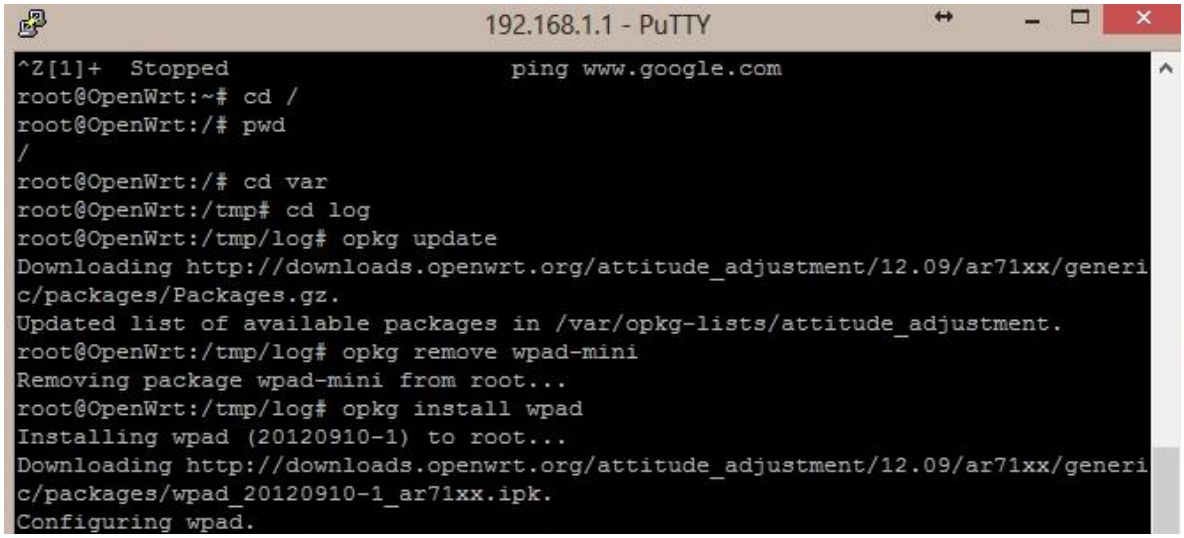

Ilustración 14 - instala todos los paquetes wpa **Fuente: Propia**

- Se instalan los paquetes de freeradius, módulos adicionales, librerías, servidores de datos, repositorios, módulos de encriptación, etc…

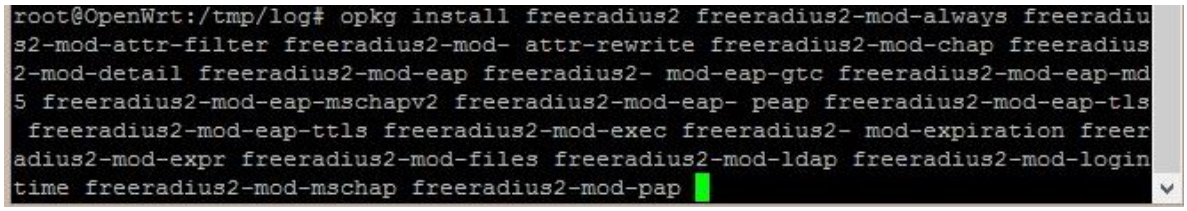

Ilustración 15 - instalación de paquetes adicionales 1 **Fuente: Propia**

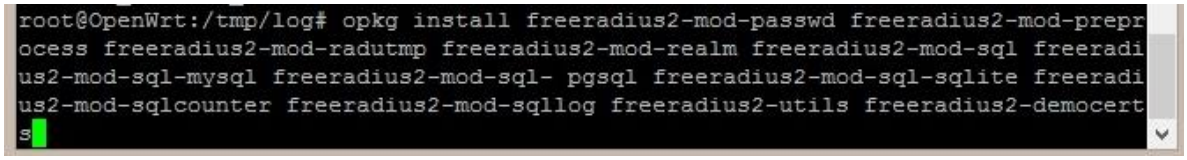

Ilustración 16 - instalación de paquetes adicionales 2 **Fuente: Propia**

6.3.3 configuración de server radius

Es necesario abrir los archivos de los paquetes instalados y editarlos en consola para realizar la respectiva configuración del servidos radius. Para editarlos utilizamos la opción Inserción que se activa oprimiendo la tecla (I) en la consola, una vez editados guardamos los respectivos cambios realizados digitando la expresión (:x!).

- Con la línea de código (#vi /etc/freeradius2/users) editaremos la línea 77 y aquí es donde crearemos las credenciales de usuarios que necesitamos para autenticar en nuestro servidor

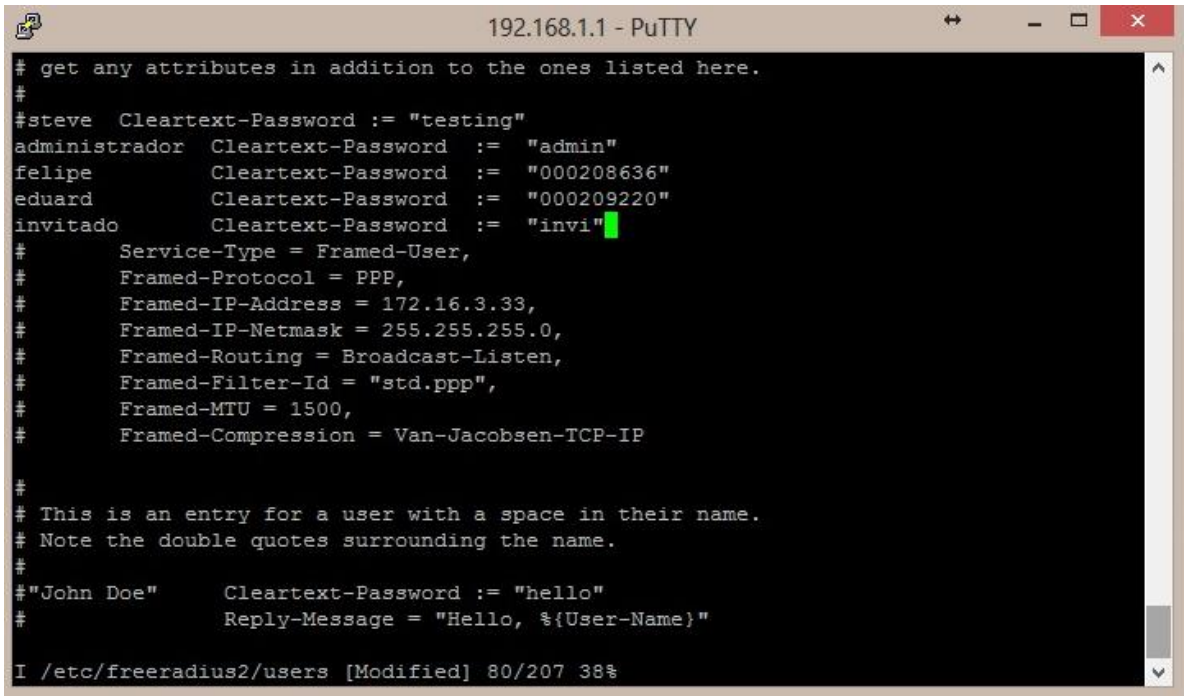

Ilustración 17 - Creación de credenciales **Fuente: Propia**

- Con la línea de código (#vi /etc/freeradius2/clients.conf) etidamos la línea 34, donde se encuentra la ip del local host por defecto, sustituyéndola por la de nuestro router 192.168.1.1 , y en la línea 101 cambiamos el password de validación del servidor radius a decisión del usuario.

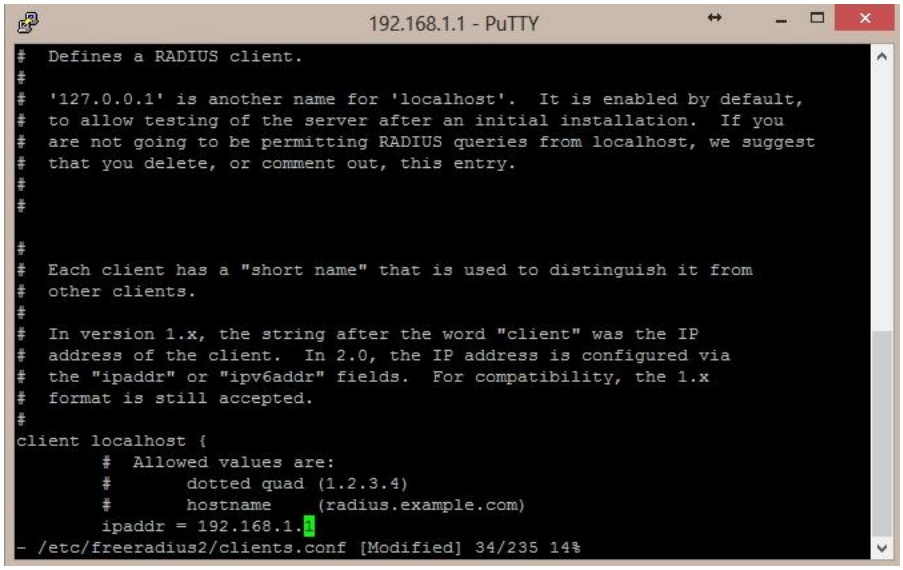

Ilustración 18 - cambio de ip **Fuente: Propia**

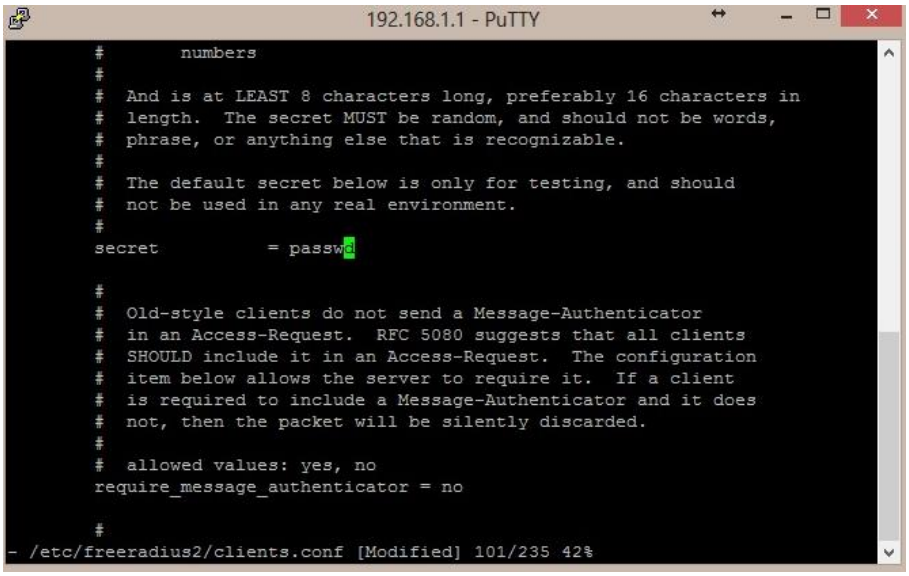

Ilustración 19 - Asignación del password server radius **Fuente: Propia**

- Abriremos el arhivo radiusd.conf, con la línea de código (#vi /etc/freeradius2/radiusd.conf) y haremos un comentario en la línea 293 y en la 443 cambiamos los valores de (auth=no) a (auth=yes)

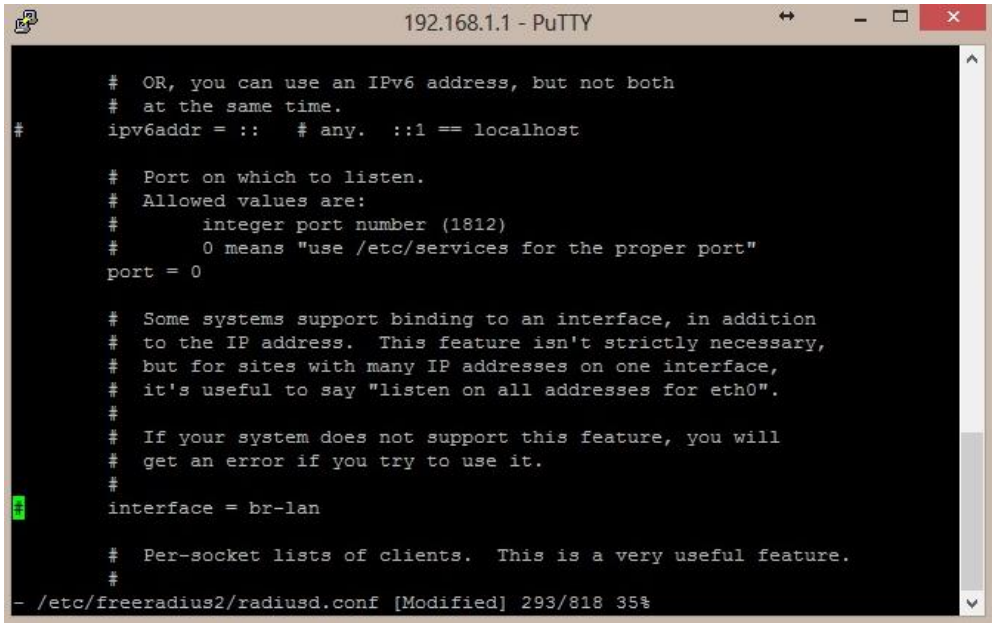

Ilustración 20- comentar la línea 293 **Fuente: Propia**

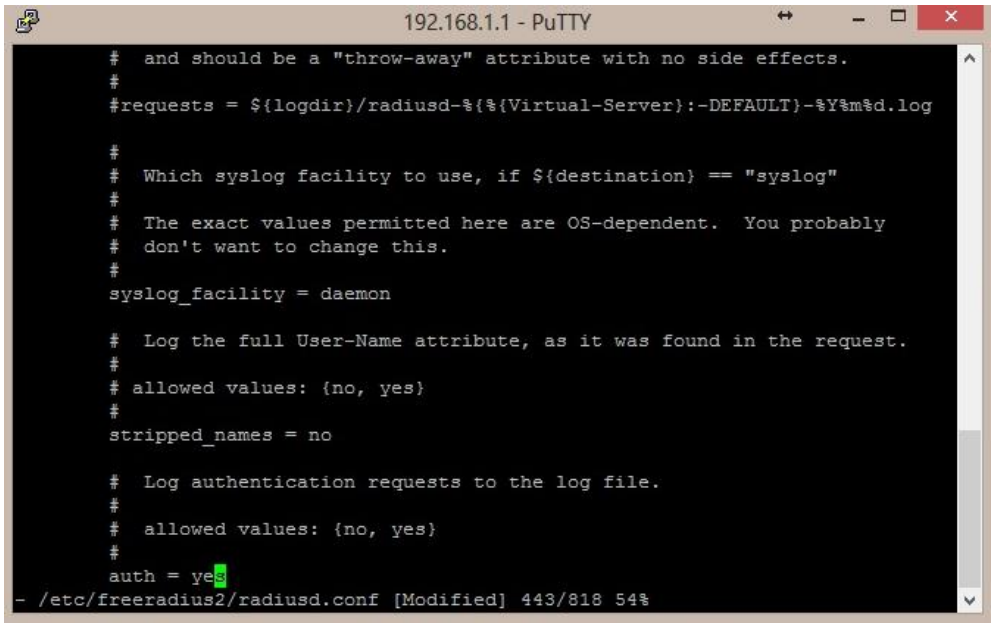

Ilustración 21 - cambio de valores **Fuente: Propia**

6.3.4 Instalación de OPEN-SSL

En esta parte instalaremos OPEN-SSL bajo openwrt, y crearemos los certificados de seguridad informática y algoritmos de cifrado.

- Con el comando (opkg install openssl-util) instalaremos OPEN-SSL en nuestro router

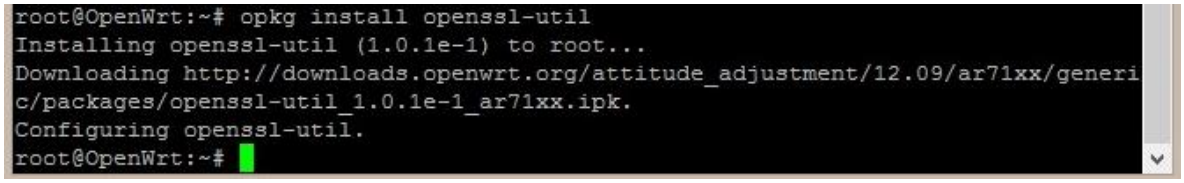

Ilustración 22 - Instalación OPEN-SSL **Fuente: Propia**

- Proseguimos a entrar al achivo certs, con el comando (#cd /etc/freeradius2/certs), y borramos los certificados que viene por default, los cuales son ca.pen y server.pem, para poder crear los nuevos certificados.

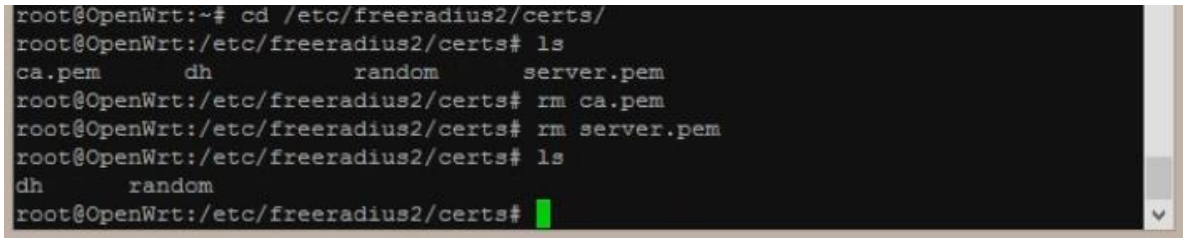

Ilustración 23 - eliminación de certificados anteriores **Fuente: Propia**

- Ahora bien, para generar nuestro primer certificado utilizamos el código (# openssl genrsa -des3 -out ca.key 2048), el cual le dira a OPEN-SSL que nos cree una llave de tipo rsa de 2048 bits, y que la guarde y cree el archivo ca.key

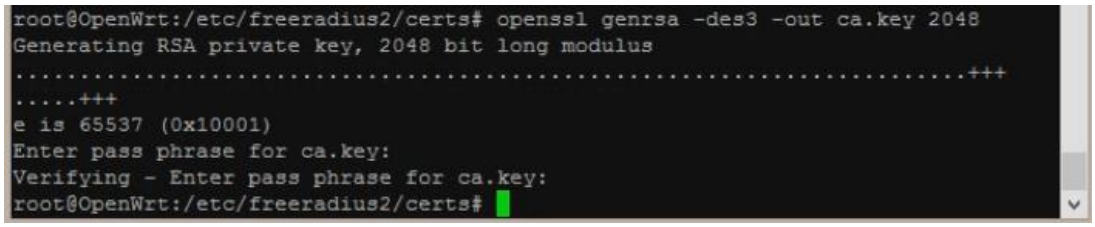

Ilustración 24 - Creación del certificado ca.key Fuente: Propia

- Con el comando (#openssl req -new -x509 -days 9999 -key ca.key -out ca.pem) le da 999 días de vigencia al certificado creado anteriormente y luego lo convierte en un ca.pem, el archivo ca.pem se debe ingresar unas pautas, las cuales son para determinar de qué lugar se emite el certificado.

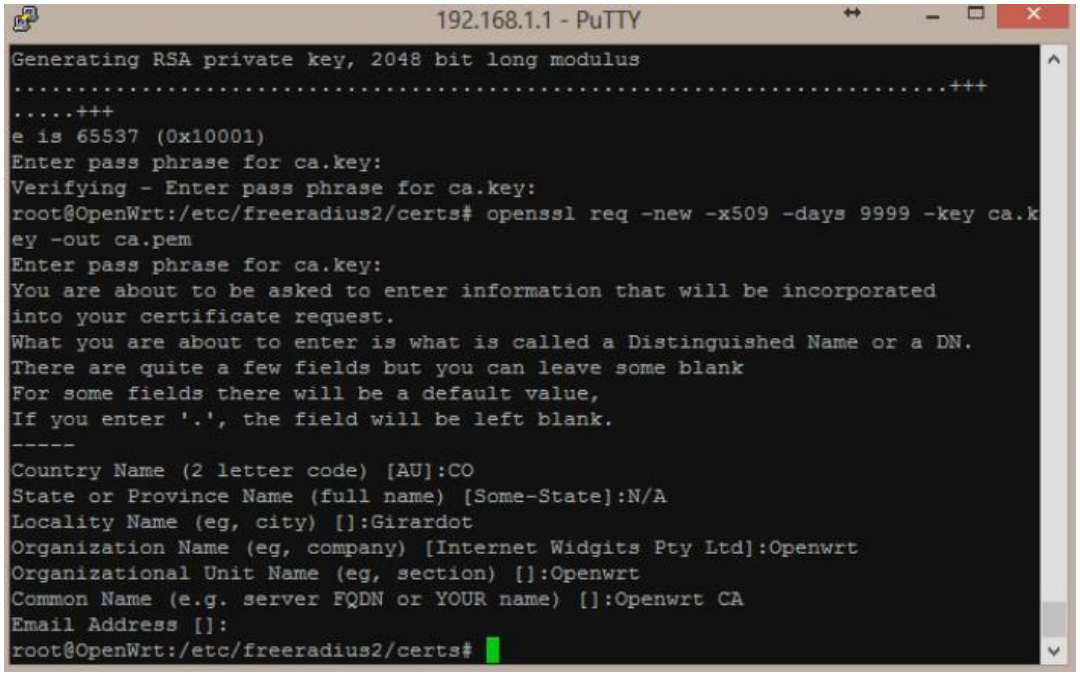

Ilustración 25 - Crear licencias Fuente: Propia

- Con el comando (#openssl genrsa -des3 -out server.key 2048) creamos un certificado para generar la llave rsa con algoritmo des3 creando el archivo server.key

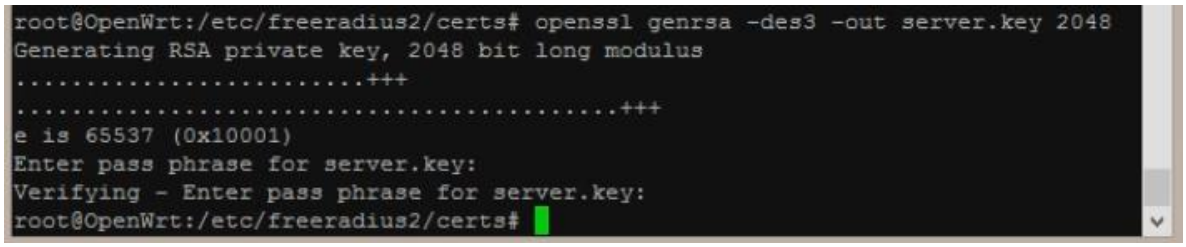

Ilustración 26 - Crea el archivo Server.key **Fuente: Propia**

- Una vez creamos la llave con el comando (#openssl req -new -key server.key -out server.csr) cramos el certificado del server, luego ingresamos el comando (# openssl x509 -req -days 9999 -in server.csr -CA ca.pem -CAkey ca.key -set_serial 01 -out server.pem) el cual nos dara la vigencia para el certificado anterior.

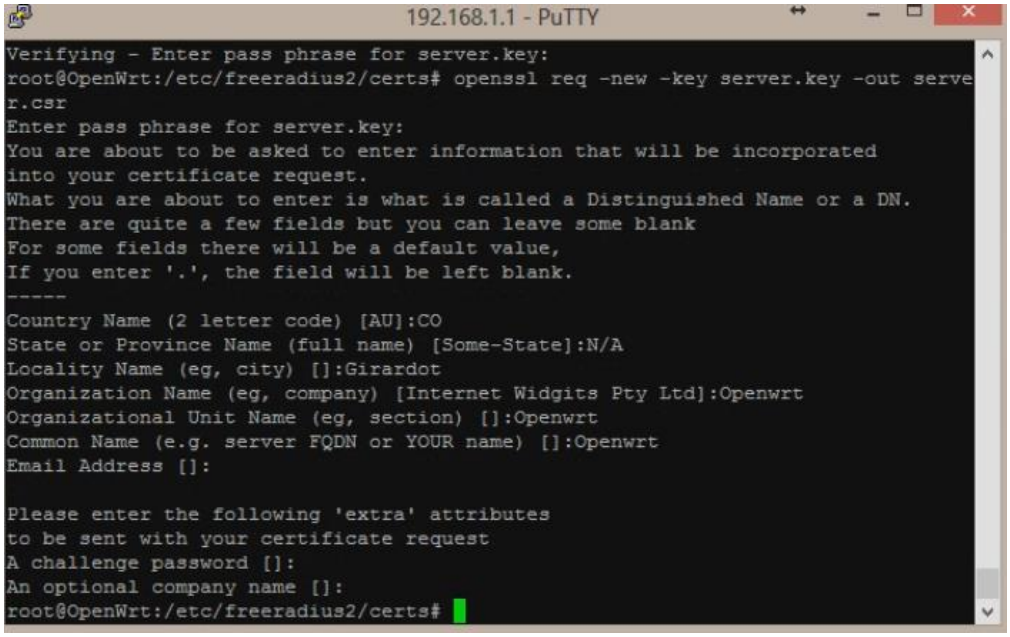

Ilustración 27 - Creación del archivo server.pem Fuente: Propia

- Por ultimo configuramos el protocolo EAP, con el comando (#vi /etc/freeradius2/eap.conf) en el cual editamos la línea (158 – 159) cambiando el password y el valor server.pem por server .key

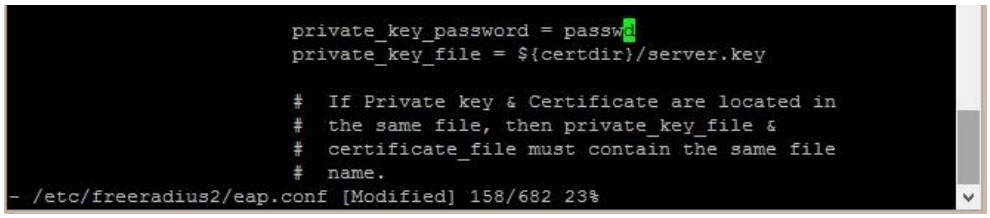

Ilustración 28 - Configuración del protocolo EAP **Fuente: Propia**

- Una vez terminada toda la instalación y configuración de los paquetes para nuestro servidor radius procedemos a habilitar el servidor radius, con la línea de código (# /etc/init.d/radiusd enable), luego de encenderlo procedemos a arrancar el servidos, para ello utilizamos la línea de código (# /etc/init.d/radiusd start) por ultimo con la línea de código (#reboot) reiniciamos el router.

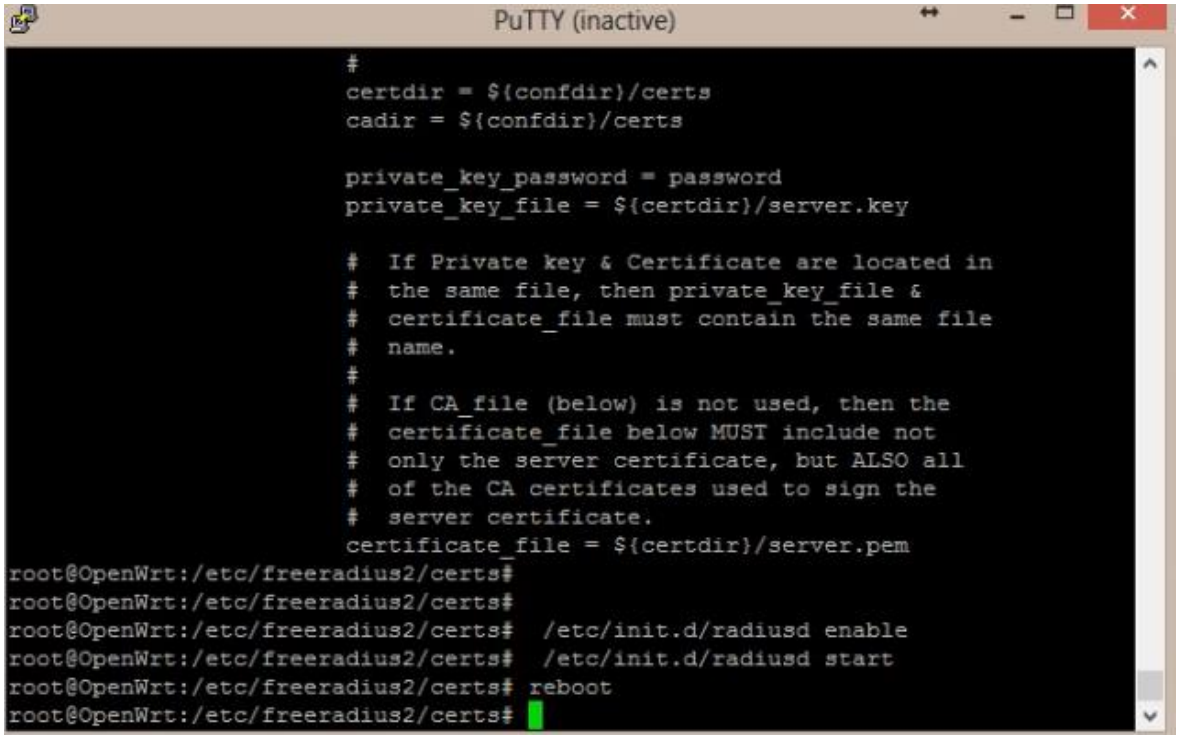

Ilustración 29 - Iniciar el server radius **Fuente: Propia**

.3.5 Configuración de la red inalámbrica con encriptación wpa2 eap

En esta fase crearemos una red inalámbrica de en modo master infraestructura la cual emitirá la señal de nuestro proveedor de internet redistribuyendo el espectro con un nuevo SSID y protocolos de seguridad inalámbrica distintos.

- Creamos una nueva red inalámbrica que emita otro SSID en este caso (EMPRESAX) y que tenga un protocolo de seguridad WP2 EAP Enterprice .

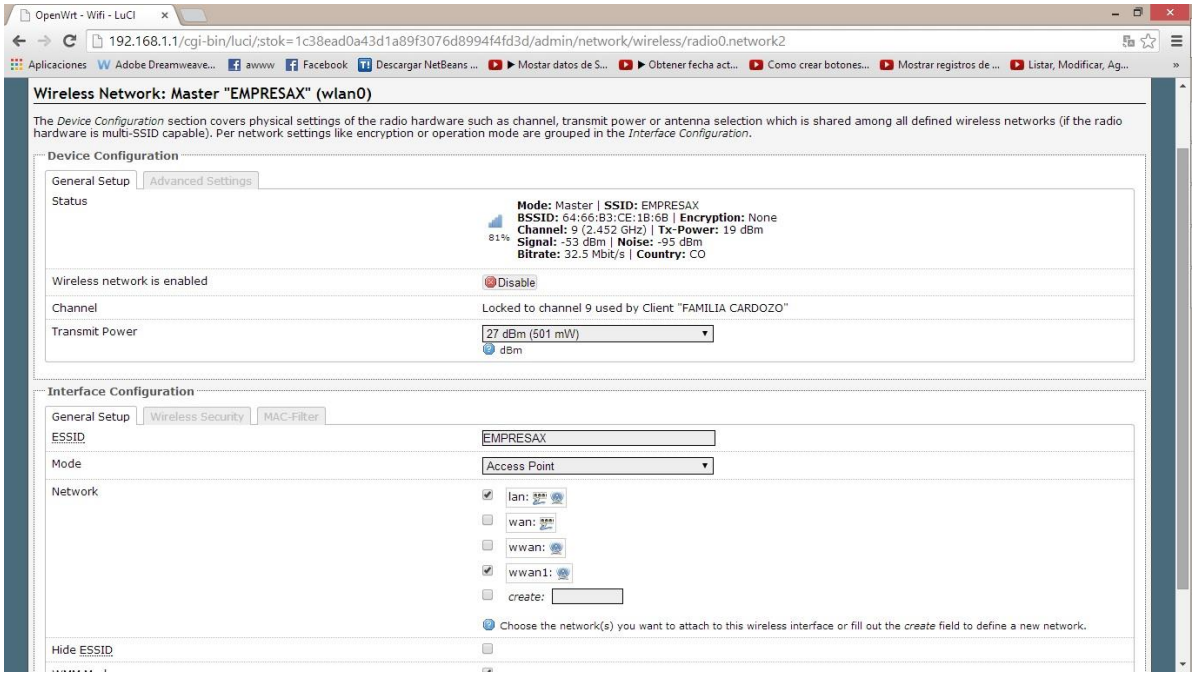

Ilustración 30 - Creación de una nueva red inalámbrica **Fuente: Propia**

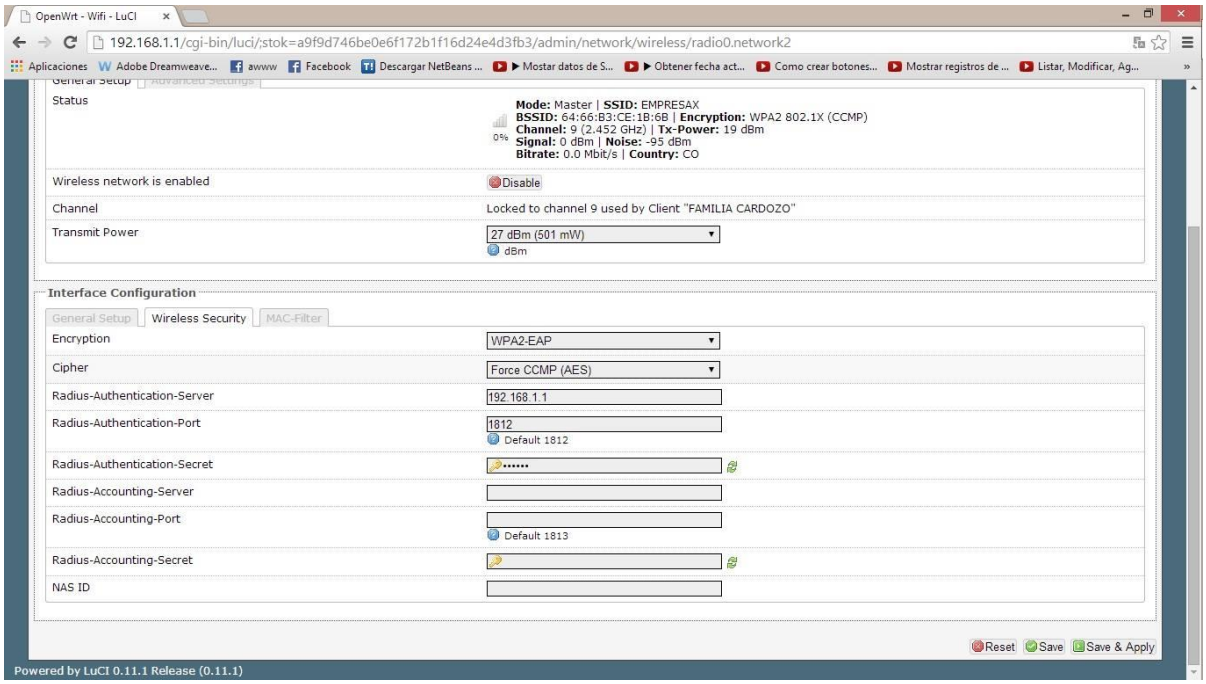

Ilustración 31 - Configuración de protocolo y encriptación Fuente: Propia

- Por último se crea un bridge ente nuestra red inalámbrica terminada y la interface LAN para volverlas una sola

  .

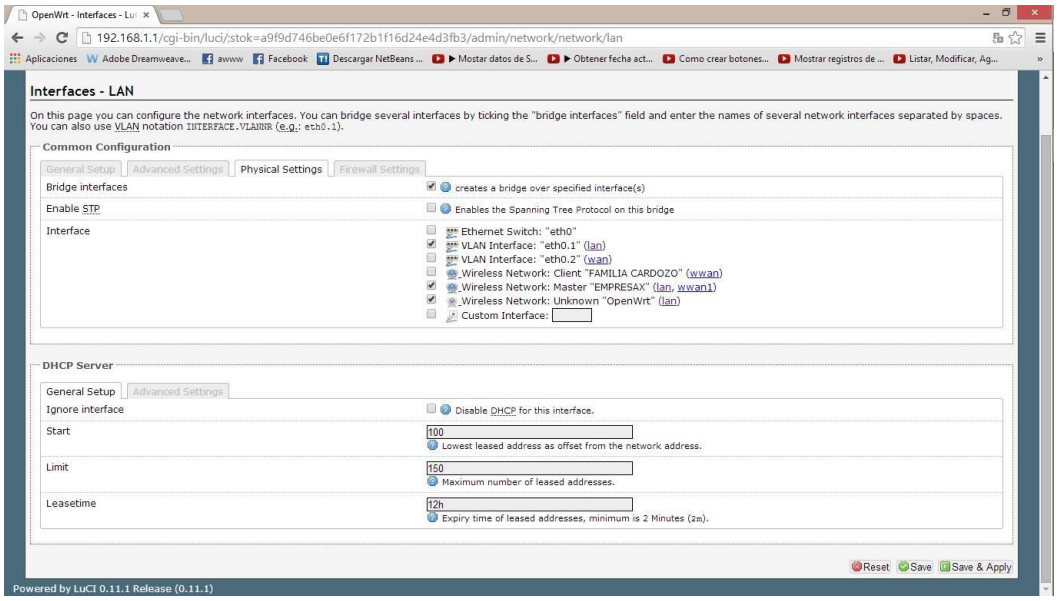

Ilustración 32 - Creación de bridge **Fuente: Propia**

De esta manera tendremos nuestro servidor radius funcionando, irradiando la señal de nuestro proveedor con un nuevo SSID, protocolos de seguridad distintos, validando las credenciales de los equipos asociados.

7. CONCLUSIONES

Al culminar este proyecto de investigación, podemos entender la importancia que tiene la seguridad para una red inalámbrica. Hoy en día para las empresas es idóneo poseer un una red inalámbrica robusta y segura para sus usuarios, ya que cuenta con factores como su movilidad, instalación, bajo costo, entre otros…

Es por estas razones que se escoge radius como servidor de autenticación, debido a que es el servidor más factible para la implementación en cualquier empresa que requiera tener un control sobre el acceso de los usuarios a los recursos de la red, y que al mismo tiempo brinde un mayor grado de seguridad. Ya que radius fue desarrollado para soportar un gran número de usuarios y varias transacciones simultaneas.

La implementación de este proyecto nos proporciona un sistema robusto, que posee los mejores protocolos de seguridad, haciéndolo la mejor opción de implementación en una empresa.

8. REFERENCIAS

- Cisco. Autenticación EAP con servidor radius. Recuperado el 10 de agosto de 2014 de: http://www.cisco.com/cisco/web/support/LA/7/76/76650_leapserver.html
- Cisco. Tecnología inalámbrica. Recuperado el 10 de agosto de 2014 de: http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html
- Criptografía, certificado digital y firma digital. Recuperado el 10 de agosto de 2014 de: http://portalae.sci.uma.es:8080/export/sites/default/uma/documentos/criptografia_certificado_digital_firma_digital.pdf
- Escuela superior politécnica de Chimborazo facultad de informática. Análisis comparativo de servidores de autentificación radius y ldap con el uso de certificados digitales para mejorar la seguridad en el control de acceso a redes wifi. Recuperado el 10 de agosto de 2014 de: http://dspace.espoch.edu.ec/bitstream/123456789/2422/1/98T00020.pdf
- Instalación y configuración de un servidor radius. Recuperado el 10 de agosto de 2014 de: http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf
- Microsoft. Protocolo de autenticación extensible. Recuperado el 10 de agosto de 2014 de: http://technet.microsoft.com/es-es/library/cc772110%28v=ws.10%29.aspx
- Que es Putty y para qué sirve. Recuperado el 10 de agosto de 2014 de: http://www.internetlab.es/post/891/que-es-putty-y-para-que-sirve/
- Servidor radius. Recuperado el 10 de agosto de 2014 de: http://jgdasir2.files.wordpress.com/2012/02/9-b-servidor-radius.pdf
- Universidad del Norte. Seguridad en desarrollo del software. Recuperado el 10 de agosto de 2014 de: http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Criptograf%C3%ADa%20I.pdf?sequence=1

- Universidad veracruzana. Mecanismos de seguridad en redes inalámbricas. Recuperado el 10 de agosto de 2014 de: http://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf

9. ANEXOS

9.1 Configuración equipo del usuario

Abrimos la configuración de redes inalámbricas, y agregamos una nueva red inalámbrica, donde colocaremos el SSID con los protocolos de autentificación configurados para radius.

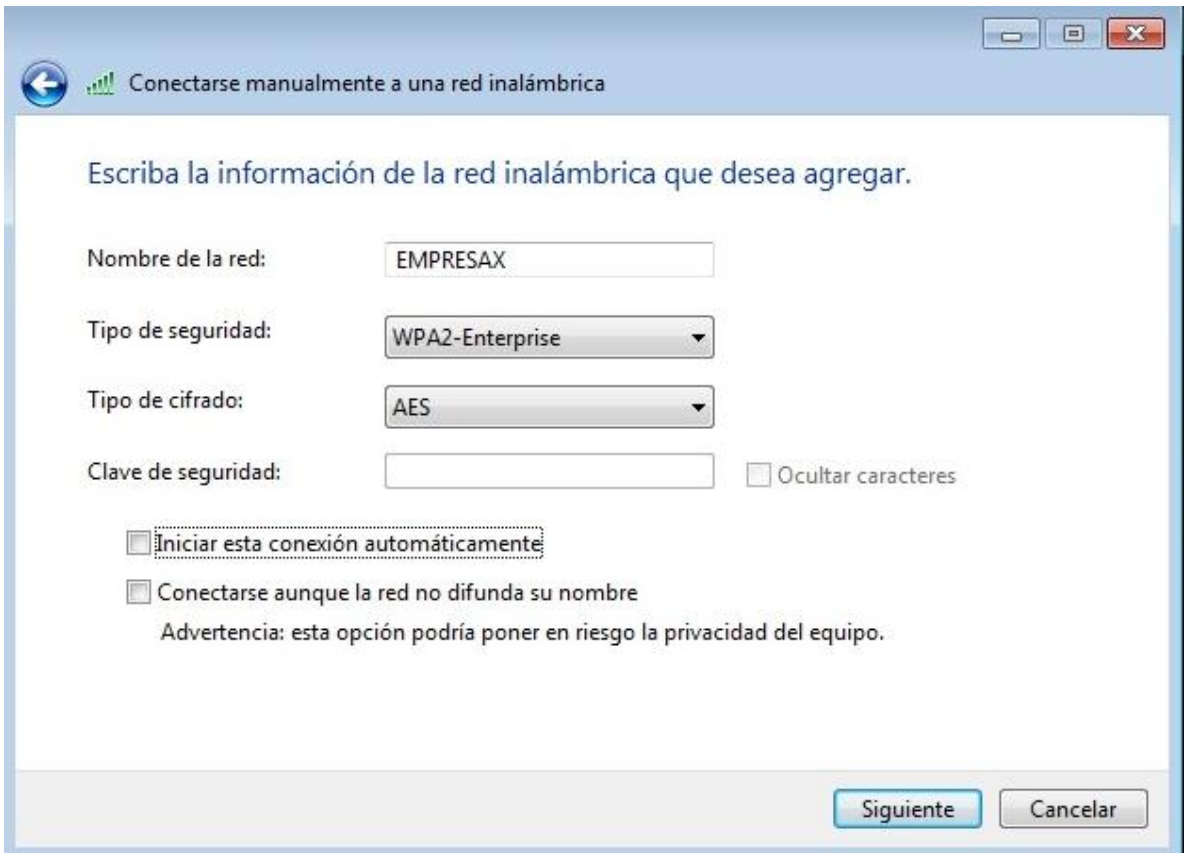

Ilustración 33 - Creación red usuario final **Fuente: Propia**

- Una vez creada proseguimos a realizar la confirmación de esta, deseleccionando recordar las credenciales, validar un certificado del servidor y usar automáticamente el inicio de sesión

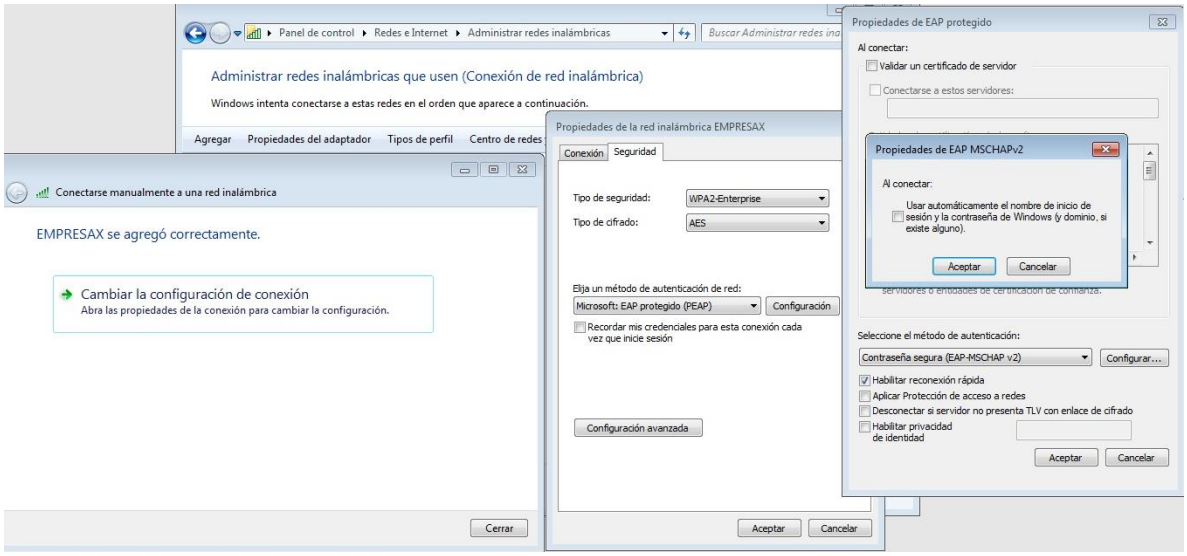

Ilustración 34 - Configuración red EMPRESAX **Fuente: Propia**

9.2 Verificación de ping al servidor radius

Realizamos un ping desde la maquina configurada para autenticarse, abriendo el CMD y escribiendo “ping 192.168.1.1”

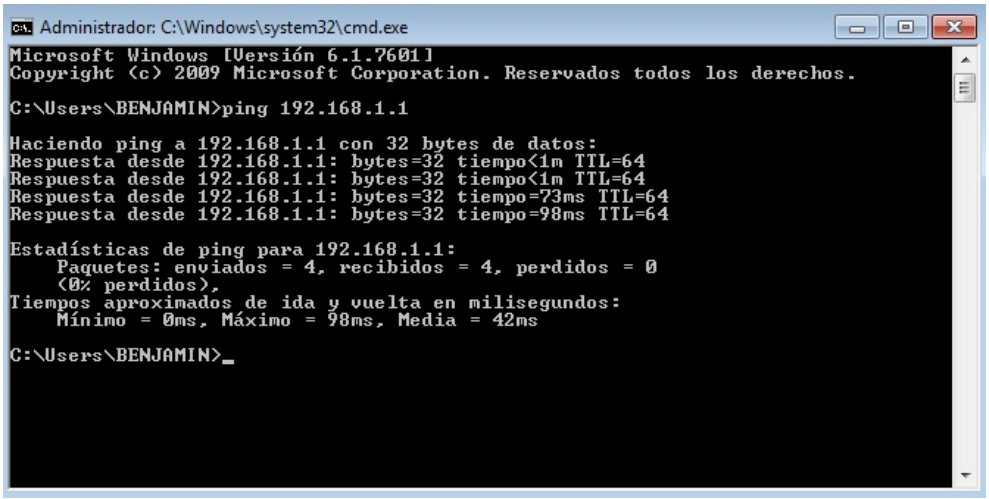

Ilustración 35 - Ping al servidor **Fuente Propia**

9.3 Ping del servidor radius a los equipos

Realizamos un ping desde consola a las respectivas direcciones de los equipos

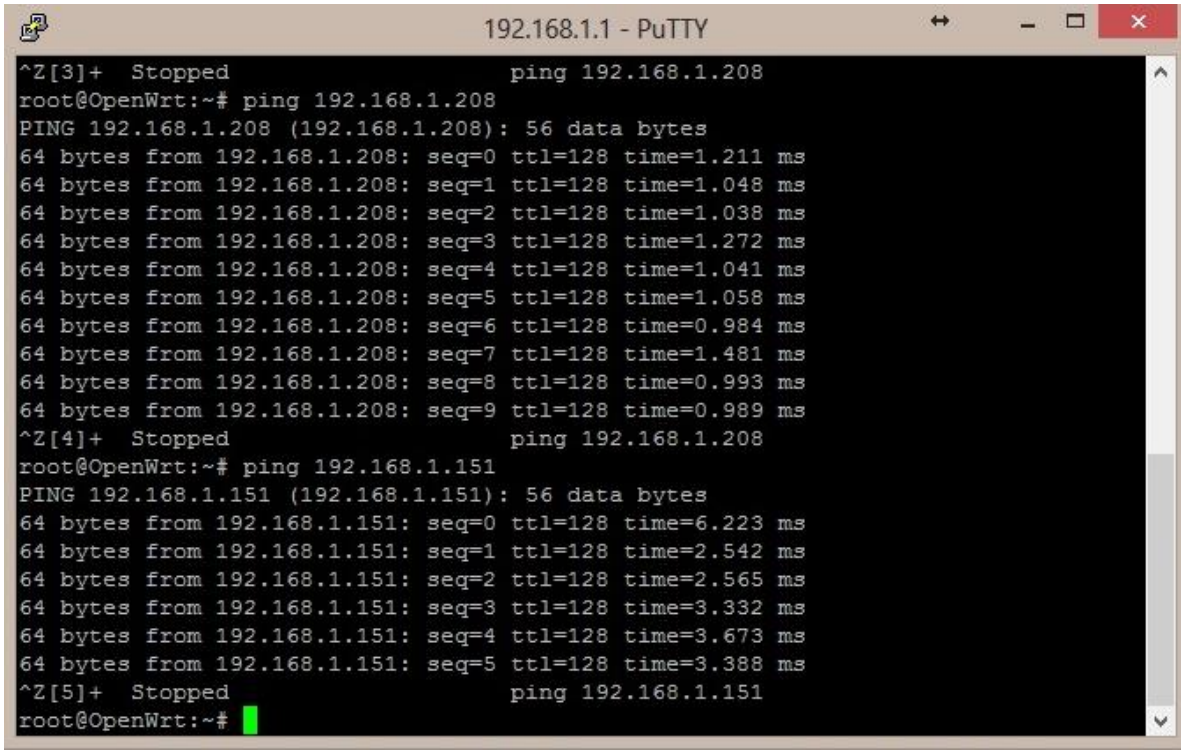

Ilustración 36 - Ping servidor a equipos Fuente: Propia

9.4 Log de conexiones al server radius

Con el comando (#cd /var/log/) entramos a log, donde utilizaremos el comando (#vi radiusd.log) para revisar nuestro log de conexiones al server

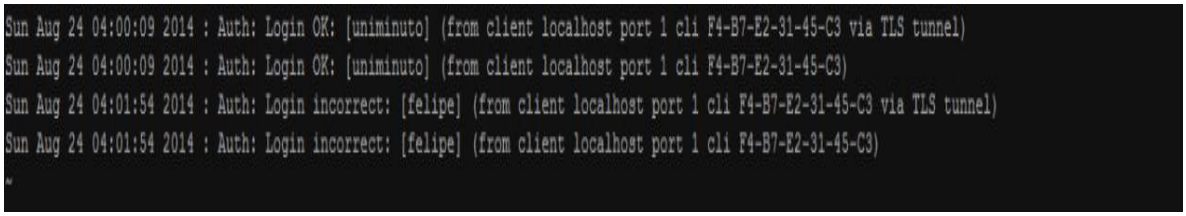

Ilustración 37 - Log de conexiones Fuente: Propia