UNIVERSIDAD TECNOLÓGICA ISRAEL

CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN SISTEMA INTEGRADO DE HERRAMIENTAS BASADAS EN SOFTWARE LIBRE PARA CREAR UN ENTORNO DE RED INTELIGENTE CON ASIGNACIÓN DINÁMICA DE VLANs, ADMINISTRACIÓN SIMPLIFICADA Y PROTOCOLOS DE CONTROL DE ACCESO A RED (NAC)

AUTOR:

SANTIAGO DAVID IZA CUMBAL

TUTOR:

MG. ARMANDO MENDEZ

Quito Ecuador.

Diciembre 2013.

DECLARACIÓN

Yo Santiago David Iza Cumbal, en calidad de estudiante de la Carrera de Ingeniería en Electrónica y Telecomunicaciones, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

Quito D.M., Diciembre 2013

Atentamente

_____

Santiago David Iza Cumbal

CERTIFICACIÓN

Certifico que el presente trabajo de titulación de grado **"IMPLEMENTACIÓN DE UN SISTEMA INTEGRADO DE HERRAMIENTAS BASADAS EN SOFTWARE LIBRE PARA CREAR UN ENTORNO DE RED INTELIGENTE CON ASIGNACIÓN DINÁMICA DE VLANs, ADMINISTRACIÓN SIMPLIFICADA Y PROTOCOLOS DE CONTROL DE ACCESO A RED (NAC)"** fue desarrollado por Santiago David Iza Cumbal, estudiante de la Carrera de Ingeniería en Electrónica y Telecomunicaciones, reúne los requisitos y meritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D.M., Diciembre 2013

_____

Mg. Armando Méndez

DIRECTOR DEL PROYECTO

APROBACION DEL TRIBUNAL DE GRADO

Los miembros del Tribunal de Grado, aprueban la tesis de graduación de acuerdo con las disposiciones reglamentarias emitidas por la Universidad Tecnológica Israel para títulos de pregrado.

Quito D.M., Diciembre del 2013

Para constancia firman:

TRIBUNAL DE GRADO

PRESIDENTE

MIEMBRO 1

MIEMBRO 2

AGRADECIMIENTOS

En primer lugar a mis Padres, familiares cercanos y amigos quienes siempre me han alentado a seguir adelante sin importar el resultado de las decisiones que haya tomado en mi vida, siempre he contado con su apoyo y sabio consejo.

Al Ing. Gerson Taipe, Supervisor de Telecomunicaciones y a mis compañeros de trabajo, quienes desde el primer día de trabajo me brindaron su apoyo y amistad para realizar este y todos los proyectos que hemos emprendido como equipo.

A la empresa ComWare S.A, por permitirme utilizar sus instalaciones y equipamiento sin los cuales no hubiese sido posible la realizar este proyecto.

A mis amigos y compañeros de Universidad más allegados (Xavier, Pamela, Cristian, Fernando, Diego, Las Dianas) con quienes compartí momentos de alegría, tristeza, satisfacción y decepción. Pero al final siempre supimos salir victoriosos como equipo y como amigos sobre todo.

Al Mg. Armando Méndez, Tutor de esta tesis, cuyos consejos oportunos y confianza puesta en mí, me permitieron realizar este proyecto a mi manera y en total libertad de acción.

Y al final pero no menos importante, agradezco de forma especial a Gabriela Montalván, por iluminar mi mundo, por su enorme amor que supera distancias y barreras, por ser mi piedra de apoyo y psicóloga personal en los momentos de dificultad.

DEDICATORIA

A mi Madre por su apoyo y amor durante todas las etapas de mi vida, no me alcanzarían mil años para agradecerle tan solo una parte de todo lo que ha hecho por mí. También dedico este trabajo a la memoria de mi querido Abuelo Tobías, un verdadero ejemplo de amor y devoción hacia su familia hasta el último instante de vida.

"Ver materializadas tus aspiraciones forjadas por tu propio esfuerzo, compensa todos los sacrificios."

Gendou Ikari – Neon Genesis Evangelion

RESUMEN

El presente proyecto consiste en la implementación de un sistema integrado de herramientas basadas en Software Libre para crear un entorno de red inteligente con asignación dinámica de VLANs, administración simplificada y protocolos de control de acceso a red (NAC), el cual pretende servir como guía de configuración y/o material de consulta para el personal de tecnologías de información que tenga la necesidad de implementar un sistema NAC económico y fácil de administrar dentro de sus instituciones. El sistema principalmente consta de un servidor FreeNAC el cual por medio de la tecnología VMPS asigna de forma dinámica las VLANs a los usuarios conectados a la red física y un servidor PacketFence que de forma similar controla el acceso de los usuarios conectados a la red inalámbrica

La implementación del sistema se realiza en un ambiente de laboratorio que fue diseñado tomando en cuenta e incluyendo las principales funciones de red que pueden ser encontradas en la mayoría de empresas de la actualidad como son: VLANs, Telefonía IP, redes Inalámbricas, servidores DHCP, entre otras. Simulando de esta manera una red real de producción con usuarios, equipos y servicios que deben ser configurados e incorporados al sistema de red de acceso inteligente para su correcto desempeño.

El laboratorio representa un modelo de red a escala reducida que posee limitaciones en cuanto al número de equipos de red y usuarios controlados simultáneamente, pero el diseño y la configuración de equipos que se detallan dentro de este proyecto no posee restricciones y son de carácter explicativo para que sean adaptados de manera sencilla a casi cualquier red de entidades públicas o privadas que cumplan con los requisitos de personal técnico capacitado, hardware y software mínimos necesarios para su implementación a mayor escala. Adicionalmente, el capitulo 5 detalla a través de ejemplos de funcionamiento los pasos necesarios para permitir o denegar el acceso a dispositivos según sea el caso dentro de los escenarios posibles que se pueden encontrar en un ambiente de red en producción con usuarios reales.

ABSTRACT

This project involves the implementation of an integrated system based on Free Software tools to create a smart grid environment with dynamic assignment of VLANs, simplified management and network access control protocols (NAC), which is intended as a guide configuration and / or reference materials for information technology personnel who have a need to implement an economical and easy to manage NAC system within their institutions. The system mainly consists of a FreeNAC server which through VMPS technology dynamically assigns VLANs to users connected to the physical network and a PacketFence server which similarly controls the access of users connected to the wireless network.

The system implementation is done in a laboratory environment that was designed taking into account and including the main network functions that can be found in most businesses today such as: VLANs, IP Telephony, Wireless Networks, DHCP servers, among others. Thus simulating an actual production network with users, equipment and services that have to be configured and incorporated into the smart access network system for their proper performance.

The laboratory network is a model of reduced scale that has limitations on the network equipment and number of users controlled simultaneously, but the design and configuration of network equipment listed within this project has no restrictions and its character is explanatory, so it can be easily adapted to almost any network of public and private entities that meet the requirements of skilled technical personnel, hardware and software needed to implement a larger scale. Additionally, Chapter 5 details through working examples steps to allow or deny access to devices as applicable within the possible scenarios that can be found in a production network with real users.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

CAPITULO I

1. INTRODUCCION

1.1. PROBLEMATIZACION

1.1.1. ANTECEDENTES

La situación actual de los administradores de redes de comunicación presenta varias problemáticas originadas por la necesidad de mejorar los procesos de administración, mantenimiento y control de acceso de equipos y/o usuarios a la red. La falta del control de acceso a la red deriva en situaciones que exponen la seguridad de los datos de las instituciones. A medida que la red incrementa su número de equipos y usuarios estos problemas se hacen más evidentes y caóticos imposibilitando los métodos de corrección manual utilizados por los administradores en la mayoría de los casos. Para contrarrestar estos problemas actualmente es posible utilizar herramientas especializadas de hardware o software que funcionan de forma automática minimizando el trabajo de los administradores, pero este tipo de soluciones representa una gran inversión de recursos económicos, humanos, tecnológicos que pocas empresas son capaces de afrontar. Por lo tanto se presenta la necesidad de adquirir soluciones de similares características a costos accesibles, utilizando estándares aprobados a nivel mundial, con tecnología robusta y actual.

1.1.2. DEFINICIÓN DEL PROBLEMA DE INVESTIGACIÓN

Las redes de datos son la parte vital de la comunicación de cualquier empresa o institución y la constante presencia de amenazas a la seguridad de la información genera nuevos retos para los administradores de red. Con el incremento actual de dispositivos móviles cada vez es más fácil que usuarios no autorizados ingresen a la red prácticamente desde cualquier ubicación. A menudo se desconoce qué y cuantos equipos están conectados a la red ya sea de forma física o inalámbrica y cuántos de ellos tienen la autorización para hacerlo. La presencia de redes inalámbricas (Wireless) en la mayoría de ambientes de red tanto empresariales como públicos obliga a que se tenga control sobre los usuarios que se conectan a

través de ella. Como medida ante esta problemática se han desarrollado nuevos protocolos y técnicas que benefician a la administración de la red pero en contraparte requieren mayores conocimientos técnicos, capacitación adecuada para su implementación y mantenimiento así como mayor inversión económica en adquisición de equipos e infraestructura tecnológica.

Una de las técnicas más conocidas en el medio es crear redes virtuales de acceso local conocidas como VLAN's, estas redes virtuales logran reunir a varios usuarios en grupos de trabajo lógicamente definidos. Con esto se logra controlar el acceso que tienen los usuarios a los recursos de red y además se los ubica en el segmento que les corresponde de acuerdo a sus funciones dentro de la empresa, limitando el intercambio de información con otros departamentos ya que esto representa riesgos a la seguridad de información y ocasiona incrementos innecesarios del tráfico de datos. Actualmente la configuración y asignación de VLANs en la mayoría de los casos se realiza de manera manual lo cual requiere tiempo y esfuerzo por parte del administrador cada vez que un usuario ingresa a la empresa, es reubicado o cuando necesita conectarse a la red con su computador o dispositivo móvil, lógicamente este problema se incrementa proporcionalmente al número usuarios existentes, equipos y expansión de la red, en ciertos casos la configuración de redes virtuales puede tardar varios días y la necesidad es inmediata.

Existen herramientas desarrolladas por empresas privadas que facilitan la opción de controlar la asignación de VLANs de manera automática o dinámica como se la denomina, pero el costo de adquisición de licencias, equipos, soporte técnico especializado hacen que pocas empresas que cuentan con el recurso económico suficiente opten por la implementación de estas alternativas, y las empresas que no disponen de presupuesto necesario se ven obligadas a buscar alternativas más económicas y eficientes o a continuar con el esquema actual de asignación manual.

1.1.3. PROBLEMA PRINCIPAL

No se dispone de un sistema especializado de herramientas de Software Libre dedicadas a controlar el acceso de equipos en un dominio de red de prueba, que sirva de modelo de referencia para administradores de red que deseen controlar de forma automática la asignación de redes virtuales, de operación sencilla, segura y sea económicamente viable para cualquier institución que cumpla con los requisitos técnicos mínimos necesarios del sistema.

1.1.4. PROBLEMAS SECUNDARIOS

- No existe un análisis de las alternativas dedicadas al control de acceso (NAC) propietarias versus las herramientas de Software Libre que comparen sus características, beneficios y funciones.
- No existe el diseño de un entorno de red de laboratorio que sirva para probar y validar las configuraciones de las herramientas de control de acceso.
- Es necesario configurar e implementar un laboratorio de red a escala reducida que contenga los principales servicios de red de una empresa e integrarlo con el sistema de herramientas de Software Libre para controlar el acceso de los usuarios a la red ya que actualmente no se dispone de uno.
- No existe un proceso de validación de integración y operación del sistema de Herramientas de control de acceso (NAC) de Software Libre dentro de un laboratorio de red de pruebas.

1.2.JUSTIFICACION

La finalidad de este proyecto es plantear una nueva alternativa para el diseño de redes y proporcionar nuevas técnicas para la administración automatizada de redes ya existentes, de esta manera se podrá entregar a los usuarios los servicios requeridos para el desarrollo de sus actividades laborales de manera rápida, eficiente y segura. Ofreciendo asignación simplificada de redes virtuales, control de acceso a redes (para todo tipo de dispositivos de red tales como Servidores,

Estaciones de trabajo, Impresoras, Teléfonos IP, Webcams, etc), inventario de dichos dispositivos de red en tiempo real, administración de redes virtuales de forma automática, acceso a la red para usuarios invitados limitando el acceso a recursos privados, generación de reportes que enlazan datos de red con usuario y dispositivo, mejora de la practicas de seguridad informática al aislar a dispositivos no autorizados que de una u otra estén conectados a la red.

Adicionalmente este proyecto pretende concientizar y brindar toda la información necesaria para que el usuario se sienta parte activa de él y lo pueda llevar inclusive a su vida cotidiana fuera de la empresa fomentando de esta manera la aplicación de entornos de software libre a varios niveles de interacción social.

1.3.OBJETIVOS

1.3.1. OBJETIVO PRINCIPAL

Implementar un sistema integrado de herramientas basadas en Software Libre dentro de un dominio de red de prueba a escala reducida que servirá de modelo de referencia para los administradores de red que deseen controlar el acceso de red a equipos, asignar redes virtuales de forma automática, y que funcione de manera eficiente, sencilla, económica y segura.

1.3.2. OBJETIVOS SECUNDARIOS

- Analizar las principales alternativas de herramientas dedicadas al control de acceso a red (NAC) Propietarias existentes en el mercado actual y compararlas con las herramientas de Software Libre, identificando características, beneficios y funciones para luego seleccionar las herramientas Software Libre que brinden mejores funcionalidades para que formen parte del sistema.
- Diseñar un entorno de red de laboratorio en donde se pueda probar y validar las configuraciones de las herramientas de Software Libre que conforman el sistema.

- Implementar un laboratorio de red a escala reducida que contenga los principales servicios de red utilizados por los usuarios que pueden encontrarse en cualquier empresa o institución, integrando las herramientas NAC de software libre para controlar la forma en que los usuarios acceden a la red y administrar los recursos que utilizan.
- Validar la integración y operación eficiente del sistema de herramientas NAC de Software Libre que serán utilizadas en el proyecto dentro de la red de datos del laboratorio de pruebas.

1.4.METODOLOGIA

El presente proyecto se desarrollo en cuatro etapas (Estudio, Diseño, Implementación y Validación) utilizando los siguientes métodos:

- **Inducción**

Estudio las alternativas comerciales actuales utilizadas para proporcionar acceso a la red a usuarios de forma automatizada, además de las herramientas existentes para esta gestión. La documentación es la principal fuente de información, el estudio de proyectos similares y guías ayudaron a determinar los requerimientos necesarios para la implementación.

- **Deducción**

Luego de realizar los estudios y análisis de información del mercado se pudo comparar con las alternativas de software libre que poseen similares características. Por lo tanto, al finalizar el proceso de implementación se obtuvo una solución eficiente que reúne principales las características de las aplicaciones comerciales pero dentro de un entorno de Software Libre y de forma gratuita.

- **Análisis**

El método analítico que se aplico en la la realización de este proyecto consistió en planificar actividades y separarlas por etapas (Estudio, Diseño, Implementacion y

Validación) cada una de estas etapas fue abarcada dentro de un capitulo en concreto. Los resultados obtenidos de cada etapa sirvieron como directrices para modificar las siguientes etapas de implementación.

- **Síntesis**

Las conclusiones obtenidas con este proyecto proceden del análisis de las necesidades existentes. El método experimental basado en pruebas y observación del funcionamiento del proyecto en cada etapa proporciona la facilidad de corregir errores, pulir detalles y obtener resultados reales a una vez cubiertas las necesidades.

1.5.MARCO TEORICO

1.6.REDES DE AREA LOCAL (LAN)[1]

1.6.1. INTRODUCCIÓN

Una red es básicamente el conjunto de todos los componentes (hardware y software) involucrados en la comunicación de computadores y aplicaciones a través de pequeñas y grandes distancias. Las redes son usadas para proveer acceso sencillo a la información, y de esta manera se incrementa la productividad de los usuarios.

A continuación se identifican los principales componentes involucrados en una red de datos y comunicaciones, así como los tipos básicos de topologías utilizados para conectar componentes de red. Los recursos que son comúnmente compartidos en la red incluyen datos y aplicaciones, impresoras, componentes de almacenamiento de red (discos de espacio compartido), y componentes de almacenamiento de respaldo.

1.6.2. CARACTERÍSTICAS DE LA RED

Las siguientes características deben ser consideradas en un diseño de red y en el mantenimiento de una red en producción.

[1] Deal, R. (2008) *Cisco Certified Network Associate Study Guide*. United States: McGraw-Hill. Copyright 2008 by The McGraw-Hill Companies

- **Costo:** incluye el costo de los componentes de la red, su instalación, y mantenimiento continuo.
- **Seguridad:** la seguridad incluye la protección de los componentes de la red y los datos que contienen y/o los datos transmitidos entre ellos.
- **Velocidad:** que tan rápidos son los datos transmitidos entre los terminales de red (velocidad de datos).
- **Topología:** Describe el diseño de cableado físico y la manera lógica en que los datos se mueven entre los componentes.
- **Escalabilidad:** Define que tan bien la red puede adaptarse a un nuevo crecimiento, incluyendo nuevos usuarios, aplicaciones y componentes de red.
- **Confiabilidad:** Define la fiabilidad de los componentes de la red y la conectividad entre ellos. El tiempo medio entre fallos (MTBF) es una medida comúnmente utilizada para indicar la probabilidad de que un componente que falle.
- **Disponibilidad:** Mide la probabilidad de que la red esté disponible para los usuarios, donde el tiempo de inactividad se produce cuando la red no está disponible debido a un corte de luz o por un mantenimiento programado. La disponibilidad se mide típicamente en un porcentaje basado en el número de minutos que existen en un año. Por lo tanto, el tiempo de actividad sería el número de minutos en que la red está disponible dividido por el número de minutos en un año.

1.6.3. COMPONENTES DE RED

- **Aplicaciones:** Permiten a los usuarios realizar varias tareas, constituyen un componente clave de las redes. Muchas aplicaciones son dependientes de red, lo que permite acceder y utilizar recursos que no se encuentran en el equipo local del usuario. Existe un alto rango en relación al número de aplicaciones de red que abarca inclusive los miles, algunos de las aplicaciones más comunes de redes incluyen aplicaciones de correo electrónico, Protocolos de Transferencia de Archivos (File Transfer Protocol - FTP) y aplicaciones web para proporcionar una representación gráfica de la información.

- **Protocolos:** Se utilizan para implementar aplicaciones. Algunos protocolos son estándares abiertos, lo que significa que muchos fabricantes pueden crear aplicaciones que pueden interoperar entre ellas, mientras que otros son propietarios, lo que significa que sólo funcionan con una determinada aplicación. Los protocolos comúnmente utilizados en Internet son Simple Mail Transfer Protocol (SMTP), Protocolo de acceso a mensajes de Internet versión 4 (IMAP4), y PostOffice Protocol 3 (POP3) que son utilizados en a aplicaciones de correo electrónico, como Microsoft Exchange; File Transfer Protocol (FTP) que es utilizado en programas de transferencia de archivos como FTP Explorer, CuteFTP y WSFTP; y el protocolo hipertext Transfer Protocol (HTTP) que se lo utiliza en aplicaciones web tales como los navegadores Internet Explorer y FireFox, servidores web como Apache, Microsoft IIS.

Las redes de hoy necesitan dar cabida a todos estos tipos diferentes de recursos y aplicaciones, incluyendo sus requisitos específicos, tales como ancho de banda para grandes transferencias o mínimas demoras y latencia para VoIP y video. Las características de calidad de servicio (QoS) se utilizan comúnmente para cumplir con estos requisitos.

Las redes de área local (LAN) se utilizan para conectar dispositivos de red que se encuentran en una zona geográfica cercana, tal como el piso de un edificio, el mismo edificio en sí, o dentro de un campus. En una Red LAN, se encontrarán PCs, servidores de archivos, hubs, switches, routers, equipos de telefonía, firewalls y otros dispositivos. Los tipos de medios utilizados en las LAN incluyen cableado de cobre y fibra óptica. Ethernet, Fast Ethernet (FE),Gigabit Ethernet (GE), Token Ring, y Fiber Distributed Data Interface (FDDI) son tipos de tramas utilizadas para la comunicación entre componentes de fibra y cobre.

1.6.4. TOPOLOGÍAS DE RED

Cuando se realiza el cableado de los componentes de la red, varios tipos de topologías pueden ser utilizadas. La topología define cómo los dispositivos están conectados. La Figura 1.1 muestra ejemplos de topologías que utilizan diferentes tipos de medios.

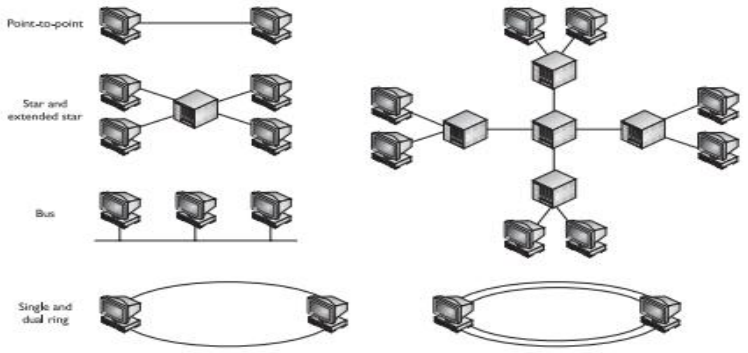

Figura 1.1: Topologías de red[2]

Una topología punto a punto consiste de una única conexión entre dos componentes. En esta topología, dos componentes se pueden comunicar directamente sin interferencia de otros. Este tipo de conexiones no son comunes cuando varios componentes necesitan estar conectados a la vez. Un ejemplo de una topología de punto a punto se da cuando dos routers están conectados a través de un circuito WAN dedicado en un enlace diseñado para la sucursal de una empresa.
En una topología estrella, un dispositivo central tiene muchas conexiones punto-a-punto hacia otros componentes. Las topologías en estrella se utilizan en entornos en los que muchos de los componentes deben estar conectados y disponibles a la vez.

El problema principal con una topología en estrella es que si el equipo central de la estrella falla, el resto de equipos no pueden comunicarse uno con el otro. Para resolver este problema, se puede utilizar una topología en estrella extendida. Una topología en estrella extendida es, básicamente, varias topologías en estrella interconectadas entre sí.

En una topología en bus, todos los componentes son conectados a un mismo cable el cual lo comparten. Típicamente, se utilizan conectores especiales o transceivers para conectar a los cables que proveen la topología en bus. Esta topología no es utilizada en la actualidad a excepción de las redes de cable coaxial 10base5.

[2] Figura 1.1: Topologías de red. De "Cisco Certified Network Associate Study Guide" por Deal, R. 2008, United States: McGraw-Hill. Copyright 2008 by The McGraw-Hill Companies.

En la topología en Anillo, el dispositivo uno se conecta con el dispositivo dos, el dispositivo dos se conecta con el tercero y así hasta el último dispositivo de la red el cual conecta de nuevo al primer equipo. La topología en Anillo puede ser implementada con un anillo único o con anillo doble, el anillo doble es utilizado típicamente cuando deseas redundancia. Por ejemplo, si uno de los dispositivos del anillo falla, la comunicación puede proseguir por el otro anillo.

Se debe distinguir los tipos de topología física y lógica. Una topología física describe como los componentes se encuentras conectados o cableados de forma física a la red. Una topología lógica describe como se comunican los componentes de la red a través de la topología física. La topología física y lógica son independientes entre sí. Por ejemplo, el protocolo Token Ring usa una topología en estrella para conectar a sus componentes similar a 10Base Ethernet, pero a nivel lógico los componentes Token ring usan topología en anillo para la comunicaciones entre dispositivos. Esto puede confundir cuando se trata de determinar cómo los componentes están conectados.

1.6.5. TOPOLOGÍAS DE MALLA COMPLETA Y MALLA PARCIAL

Las mallas generalmente describen como los componentes están conectados entre ellos. Se utilizan dos tipos de topología de malla: malla parcial y malla completa.

En un entorno de malla parcial, cada dispositivo no está conectado a todos los demás solo a una parte de ellos. En cambio en una topología de malla completa, cada uno de los dispositivos tiene una conexión física hacia todos los equipos de la red. La figura 1.2 muestra ejemplos de estas dos topologías.

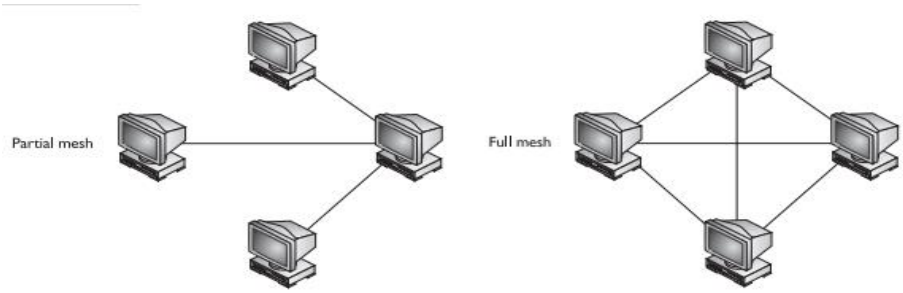

Figura 1.2: Topologías de malla completa y parcial[3]

1.7.REDES LAN VIRTUALES (VLANs)[4]

Una VLAN (red de área local virtual) es un método de crear redes lógicas e independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único switch o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

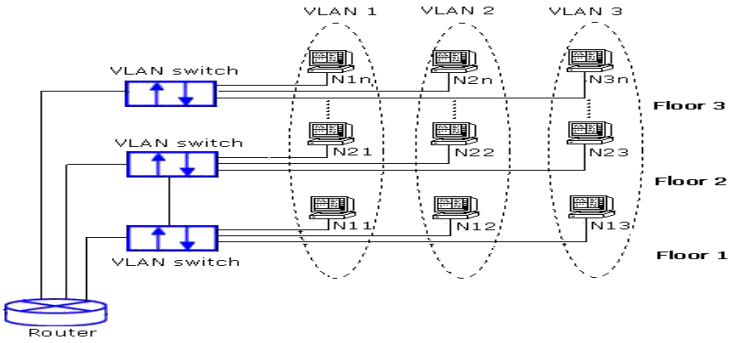

Figura 1.3: Red de área local virtual (VLAN)[5]

[3] Figura 1.2: Topologías de malla completa y parcial. De "Cisco Certified Network Associate Study Guide" por Deal, R. 2008, United States: McGraw-Hill. Copyright 2008 by The McGraw-Hill Companies.

[4] *Redes LAN Virtuales.* Recuperado de: http://es.wikipedia.org/wiki/VLAN

[5] Figura 1.3: Red de área local virtual (VLAN) Recuperado de: http://www.simulationexams.com/tutorials/netplus/network-implementation/images/vlan2.gif

1.7.1. ASIGNACIÓN DE PERTENENCIA A UNA VLAN[6]

Las dos aproximaciones más habituales para la asignación de miembros de una VLAN son las siguientes: VLAN estáticas y VLAN dinámicas.

- **VLANs estáticas:** También se denominan VLANs basadas en el puerto. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un switch o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el switch.

- **VLANs dinámicas:** la asignación se realiza mediante paquetes de software a través de VMPS (VLAN Management Policy Server o Servidor de Gestión de Directivas de la VLAN), el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo. En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN. Se puede consultar el software FreeNAC para ver un ejemplo de implementación de un servidor VMPS.

1.8.SEGURIDAD DE REDES

Entre el 60 y el 80% de las brechas de seguridad o ataques en la mayoría de las empresas son originadas al interior de la red, no por un atacante externo. Porque la mayoría de las compañías están conectadas al internet y porque también es fácil ingresar a la red interna la seguridad de la red cumple con un papel predominante en los diseños de red actual.

Una política de seguridad define los que las personas pueden o no pueden hacer con los componentes y recursos de la red. Una solución de seguridad deriva de la

[6] *Asignacion de pertenencia a una VLAN.* Recuperado de http://es.wikipedia.org/wiki/VLAN

política de seguridad. Una solución de seguridad que dificulta alcanzar las metas del negocio de la empresa es contraproducente. Por lo tanto, las compañías deben balancear los planes de seguridad y negocio. Esto puede ser difícil cuando se trata de una compañía de servicios como, comercio electrónico, que debe ser accedida por los clientes a través del internet.

Hoy en día, la mayoría de los ataques son automáticos y auto replicados los cuales requieren de poca configuración por parte del atacante. Herramientas como Metasploit y Core Impact hacen que los ataques sean literalmente tan simples como presionar un botón.

1.8.1. CLASES DE ATAQUES

Para proveer una defensa de seguridad efectiva, una compañía debe confrontar las siguientes tres cosas:

- **Adversarios:** un adversario es una persona o personas interesadas en atacar nuestra red. Los adversarios más comunes incluyen a empleados con resentimientos hacia la empresa, hackers novatos o experimentados, intrusos de otros países, terroristas, compañías rivales y otros.
- **Motivaciones:** el rango de las motivaciones de los adversarios van desde los desafíos (hackers), robar información (compañías rivales y criminales) hasta denegar el servicio (terroristas, otros países).
- **Clases de Ataques:** los adversarios pueden emplear cinco clases de ataques: pasivos, activos, distribuidos, infiltrados y cercanos.

Un ataque pasivo monitorea trafico encriptado y busca contraseñas en texto plano e información especifica que puede ser utilizada en otros tipos de ataques. Un ataque activo, trata de evitar o vulnerar al sistema de seguridad. Esto puede ser realizado a través de virus, gusanos, caballos de Troya o explotando vulnerabilidades de seguridad conocidas. Un ataque distribuido requiere que el adversario distribuya un código, como un caballo de Troya o un programa de puerta trasera a un componente o software “confiable” para que este luego se distribuya a muchos otros usuarios. La instalación de este componente o software se realiza sin el conocimiento del usuario

de la red. Un ataque infiltrado involucra alguna persona desde el interior como un empleado molesto que ataca a la red. Este es el tipo de ataque más común, donde el atacante infiltrado intenta copiar, capturar o dañar la información. Un ataque cercano involucra a alguien que trata de obtener acceso físico a los componentes de red, datos y sistemas con la finalidad de aprender más sobre la red. Esto puede llevar a que el atacante dañe los sistemas creando denegación de servicio (DoS).

1.8.2. AMENAZAS COMUNES Y MITIGACIÓN

Las principales categorías de amenazas comunes a las redes y sus componentes son:

- Ataques a instalaciones físicas
- Ataques de reconocimiento
- Ataques de acceso
- Ataques denegación de servicio (DoS).

En los párrafos siguientes se discuten cada una de estas cuatro amenazas y las técnicas aplicadas para impedir y / o derrotar estos ataques.

- **Ataques a Instalaciones Físicas:** Las instalaciones físicas incluyen cuatro tipos de amenazas: hardware, electricidad, medio ambiente, y mantenimiento. Las amenazas de hardware implican daño físico a los componentes de la red, tales como servidores, routers y switches. Para reducir la probabilidad de una amenaza de hardware, los componentes críticos de la red deben ser colocados en una habitación cerrada, donde sólo los administradores autorizados se les permitan el acceso. Para asegurarse de que nadie más pueda acceder a los componentes críticos de la red, la habitación no debe tener accesos como ventanas, rejillas de ventilación, cielos o pisos falsos. Para reducir aún más la probabilidad de que alguien tenga acceso no autorizado a la habitación segura, todas las entradas deben ser controlados, tanto en entrada y salida del personal, a través del control electrónico de acceso y vigilancia por vídeo.

Se debe recordar que la mayoría de amenazas a una red son INTERNAS; por lo tanto, se debe implementar un plan de seguridad para enfrentar las amenazas físicas. Las amenazas eléctricas incluyen fluctuaciones irregulares de voltaje, tales como caídas de tensión y picos o la pérdida completa de energía. Para mitigar estas amenazas, se deben instalar sistemas de alimentación ininterrumpida (UPS) y sistemas generadores de copias de seguridad para los componentes críticos de la red. Estos deben ser monitoreados continuamente y probados periódicamente. Además, para los componentes críticos de la red se deben comprar sistemas de alimentación redundante si estos son compatibles con los componentes de red.

Las amenazas ambientales incluyen temperaturas muy altas o bajas, humedad, descargas electrostáticas, y la interferencia magnética. Un sistema adecuado de temperatura y humedad debe ser utilizado para asegurar que los componentes de red están operando en un entorno especificado por sus fabricantes. Se debe utilizar un sistema de monitoreo para que el administrador pueda tomar medidas inmediatas si se producen anomalías en la temperatura o la humedad. No deben existir alfombras o materiales similares en una habitación con componentes críticos de la red, ya que pueden producir electricidad estática que puede dañar los componentes cuando se transfiere accidentalmente por descarga de una persona al momento de tocarlos. Del mismo modo, cualquier dispositivo que emite una gran cantidad de interferencia magnética debe ser colocado en un lugar separado para asegurar que no cause daños a los equipos de red, tales como las unidades de disco.

Las amenazas de mantenimiento incluyen no tener partes de respaldo para los componentes críticos de la red; no etiquetar a los equipos y cableado de forma correcta, causando problemas de identificación al realizar el mantenimiento, y no seguir los procedimientos de descarga electrostática antes de manipular los componentes de red.

Para mitigar estas amenazas, un administrador debe mantener a la mano las piezas para los componentes críticos de la red. Todos los cables deben estar claramente etiquetados para que sean correctamente identificados y el

seguimiento de los cables sea un asunto fácil. Antes de realizar cualquier mantenimiento de un elemento de red, los procedimientos de descarga electrostática deben seguirse para minimizar el riesgo que la electricidad estática del cuerpo dañe a los componentes críticos de la red.

- **Ataques de reconocimiento:** Un ataque de reconocimiento se produce cuando un adversario trata de obtener información acerca de nuestra red. Lo hará al tratar de descubrir vulnerabilidades de los componentes de red y recursos que existen en ellas. Los adversarios comúnmente utilizan varias herramientas en sus ataques: ingeniería social (que pretende ser una fuente de confianza para ganar acceso no autorizado a la información), herramientas de análisis, sniffers de paquetes, y otras herramientas. Para mitigar un ataque de ingeniería social, los usuarios tienen que ser capacitados sobre el tipo de información que se puede y no se puede compartir con otras personas dentro y fuera de la compañía. Para mitigar los ataques de escaneo y detección de paquetes, existen varios mecanismos de control de acceso, tales como firewalls e IDS / IPS.

- **Ataques de acceso:** Un ataque de acceso se produce cuando alguien trata de acceder sin autorización a un componente de red, para tratar de obtener acceso no autorizado a la información sobre un componente, o aumentar sus privilegios de utilización de un componente de red. Hay muchos tipos de ataques de acceso, pero la forma más común es un ataque de contraseña. En un ataque de contraseña, el adversario trata de adivinar una contraseña válida para una cuenta existente. El realiza este tipo de ataque mediante el uso de un programa de descifrado de contraseñas que usa combinaciones de palabras existentes en un diccionario para adivinar contraseñas comunes o utilizar un enfoque de fuerza bruta para generar palabras y adivinar números, letras y caracteres especiales. Un ataque de fuerza bruta puede tardar mucho tiempo en romper una contraseña, dependiendo de la longitud de la contraseña y la potencia de algoritmo utilizado para encriptar la contraseña. L0ptcrack y Caín & Abel son muy buenos programas de descifrado de contraseñas que apoyan el uso de la fuerza bruta. Los

adversarios utilizan la ingeniería social para engañar a un usuario para que este revele las contraseñas o pueden instalar caballos de Troya para capturar las pulsaciones de teclado de la PC de un usuario de esta manera también capturan las credenciales de inicio de sesión. Algunos adversarios incluso pueden utilizar analizadores de paquetes para examinar texto plano y conexiones como Telnet y FTP, para los nombres de usuario y contraseñas. Para mitigar este tipo de ataques de acceso, se deben efectuar estrictas funciones de control de acceso. El acceso debe estar restringido a componentes de la red e información mediante el uso de filtros de red, por ejemplo, sólo las personas de contabilidad deben tener acceso a los servidores de contabilidad y los datos sobre los servidores. Este tipo de característica puede ser aplicada por las listas de control de acceso (ACL) en los routers o cortafuegos. Para mitigar los ataques de caballo de Troya, se deben utilizar IDS / IPS y software anti-spyware. Para reducir la probabilidad de que una contraseña sea adivinada por un ataque de fuerza bruta, estas las contraseñas deben contener una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales.

- **Ataques de denegación de servicio (DoS):** Los ataques de denegación de servicio son realizados por un adversario con la finalidad de reducir el nivel de funcionamiento o servicio de la red, impidiendo el acceso o haciendo que la red o servicio estén totalmente deshabilitados. Los ataques de denegación de servicio inundan la red con millones de paquetes o códigos que son inyectados en una aplicación con la finalidad de desbordar el búfer (s) de memoria, provocando que la aplicación se bloquee .Se requieren mecanismos de control de acceso como firewalls con filtrado de paquetes para controlar el acceso a un sistema y mitigar ciertos tipos de ataques de DoS.

  La limitación de velocidad y otras herramientas deben utilizarse para asegurar que el sistema no se sienta abrumado por un ataque de inundación. La detección de intrusos y los sistemas de prevención (IDS/IPS) deben ser utilizados para prevenir ataques de vulnerabilidades conocidos que pueden causar accidentes en el sistema, como los ataques de desbordamiento de búfer.

1.9.CONTROL DE ACCESO A RED (NAC)[7]

Es una solución que utiliza un conjunto de protocolos para definir e implementar políticas que describen como los dispositivos obtienen acceso a la red de forma segura. NAC integra un proceso de mediación automática que permite a los equipos de infraestructura de red routers, switches y firewalls trabajar en conjunto con servidores y computadores de usuario para afirmar que el sistema informático está operando de forma segura antes de que la interoperabilidad sea permitida.

El control de acceso a red realiza exactamente lo que dice su nombre, controla el acceso a la red por medio de políticas, incluyendo pre admisión de dispositivos, revisiones de políticas de seguridad y controles post admisión sobre los privilegios de los usuarios y dispositivos dentro de la red.

1.9.1. OBJETIVOS DEL CONTROL DE ACCESO A RED

Los objetivos principales de este concepto se pueden resumir en:

- **Mitigar ataques de día cero:** El propósito clave de una solución NAC es la habilidad de prevenir en los equipos finales la falta de antivirus, parches, o software de prevención de intrusión de hosts y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de gusanos informáticos.

- **Refuerzo de políticas:** Las soluciones NAC permiten a los operadores de red definir políticas, tales como tipos de ordenadores o roles de usuarios con acceso permitido a ciertas áreas de la red, y forzarlos en switches y routers.

- **Administración de acceso e identidad:** Donde las redes IP convencionales refuerzan las políticas de acceso con base en direcciones IP, los dispositivos NAC lo realizan basándose en comparar identidades de usuarios

[7] *Control de Acceso a Red.* Recuperado de http://es.wikipedia.org/wiki/Control_de_acceso_a_red

autenticados, al menos para usuarios finales de equipos portátiles y sobremesa.

1.9.2. TECNOLOGÍAS UTILIZADOS PARA EL CONTROL DE ACCESO A RED

Las soluciones NAC son diferentes pero pueden ser clasificadas en dos grupos:

- **Clientless**: no necesita de ningún software instalado en los dispositivos
- **Client-based**: un componente de software es preinstalado en los dispositivos para poder asistir al proceso de NAC

Existe un numero de factores para decidir cual tipo de solución es la más adecuada dependiendo de cómo está formada la organización, NAC basado en cliente provee mas detalle del dispositivo pero también hay que tener en cuenta que requiere su instalación equipo por equipo.

1.10. SOFTWARE LIBRE[8]

Software Libre es la denominación del software que brinda libertad a los usuarios sobre su producto adquirido, y por tanto una vez obtenido puede ser usado, copiado, estudiado, modificado y redistribuido libremente. Gracias a estas características puede ser configurado, mejorado y utilizado sin tener que pagar derechos de autor por ello. Eso significa que por el código del programa no debemos pagar, aunque si se puede pagar por servicios derivados, como por ejemplo instalación, configuración, soporte, auditoría, formación, e incluso por mejorar la aplicación.

El Software Libre existe, y es muy utilizado dentro de las empresas y entidades públicas. En la mayoría de los casos ofrece la misma calidad y posibilidades que el software propietario. Incluso en determinados campos ganan la batalla al software propietario o software no libre, como en aplicaciones para Internet y comunicaciones.

[8] Junta de Comunidades de Castilla-La Mancha (2009). *Taller de Migración al Software Libre.* Centro de Excelencia de Software Libre (Versión 1.0) Castilla: La Mancha. Creative Commons by-Sa

1.10.1.VENTAJAS DEL SOFTWARE LIBRE

Algunas de las ventajas más importantes de este tipo de software son:

- Es más económico
- Software adaptable.
- Independencia del proveedor:
- Cultura de colaboración y modelo científico:
- Fomento de la industria local:
- Mejores prestaciones con el mismo hardware:
- Libertad de uso y redistribución:
- Aumento de la productividad:
- Formatos estándar:
- Mayor estabilidad y seguridad:
- Sistema en expansión:

1.10.2.LICENCIAS DE SOFTWARE LIBRE

Una licencia es aquella autorización formal con carácter contractual que el autor de un producto da a los usuarios de ese bien. Pueden existir tantas licencias como acuerdos concretos se den entre el autor y el licenciatario. Pero para que una licencia pueda ser considerada software libre ha de cumplir una serie de condiciones que vienen dadas en la definición de Software Libre realizada por el fundador del movimiento, Richard M. Stallman, y que son:

- Libertad para usar el programa con cualquier propósito
- Libertad para estudiar cómo funciona el programa
- Libertad para mejorar el programa
- Libertad para redistribuir las propias modificaciones

Las libertadas del software están garantizadas por una serie de condiciones que se plasman en una licencia. Una de las características del Software Libre es la libertad para hacer obras derivadas por parte de terceros, siendo éstas legalmente obras nuevas.

CAPITULO II

2. ANALISIS DE LAS PRINCIPALES SOLUCIONES NAC PROPIETARIAS Y DE SOFTWARE LIBRE DEDICADAS AL CONTROL DE ACCESO A RED

2.1. TIPOS DE NAC

- **NAC basado en hardware:** Esta opción necesita habitualmente de un equipo dedicado específicamente para esta tarea (conocido como appliance) que deberá ser instalado en casi cualquier ubicación donde sea preciso contar con NAC. Algunos de estos appliances han sustituido a los switches de acceso, mientras que otros operan entre la capa de acceso a red y la capa de red del modelo OSI.
- **NAC basado en agentes software:** Se basa en pequeños programas residentes en los ordenadores y dispositivos del usuario, instalándose estos agentes en cada uno de los sistemas que deban ser controlados por el NAC. Dichos agentes escanean y monitorizan el dispositivo, generalmente enviando los resultados a un servidor central. Los sistemas que no cumplen con los requisitos no tendrán autorización de acceso a la red, y a menudo se les envía algún tipo de medida correctora para que cumplan las directivas de seguridad.

- **NAC sin agentes software:** El NAC sin agentes es otra de las variantes, Con esta configuración, la idea es que un agente temporal (generalmente algún tipo de control ActiveX) escanee el cliente periódicamente en búsqueda de vulnerabilidades o incumplimientos en la política de seguridad. Los resultados del escaneo son enviados al servidor central de políticas, y se ejecuta una acción si es necesario en caso de que el sistema no cumpla con los requerimientos.

- **NAC dinámico:** El NAC dinámico, utiliza agentes sólo en un porcentaje determinado de equipos. También se conoce como NAS peer-to-peer, siendo una opción que no requiere cambios a nivel de red o software que deba ser instalado

en cada equipo. Los agentes, que en ocasiones pueden llegar a ser obligatorios, son instalados en sistemas seguros. A partir de aquí, sólo se necesita controlar el cumplimiento de una serie de normas y leyes en la red, para hacer que los usuarios de red cumplan las reglas.

Al momento de seleccionar cualquiera de estas opciones como son la de hardware, con agentes software, sin agentes o de NAC dinámico, se necesita evaluar los objetivos del despliegue NAC, tales como el nivel de seguridad frente a la facilidad de administración, u otras cuestiones que dependen del tamaño de la compañía o la red.

Para este proyecto se selecciono la alternativa de solución NAC sin agentes, ya que de esta manera el impacto es menor para el usuario al no depender de un agente instalado en su computador para autorizar su ingreso, el proceso de validación y autorización de acceso a la red se convierte en un proceso ejecutado en segundo plano que no se refleja en las operaciones del usuario a menos que el equipo no cumpla con las requisitos de autenticación y en dicho caso será relegado a una red virtual segura con acceso mínimo a los recursos como puede pasar con los equipos de personas invitadas o proveedores que solo requieren acceso temporal y navegación a internet.

2.2.CLAVES PARA ELEGIR LA MEJOR SOLUCIÓN NAC

Desde la perspectiva del usuario final, el establecimiento de un Control de Acceso a Redes (NAC) debe ser transparente, es decir, debe funcionar de forma autónoma. Cuando los usuarios se registran en la red, sus sistemas deben ser revisados, en segundo plano, para que los niveles de fiabilidad sean los adecuados según la política de seguridad interna de la red.

Entre los ejemplos de lo que un sistema NAC examinaría en un terminal están los parches del sistema operativo, la actualización de los antivirus y cortafuegos personales, verificación de direcciones MAC de los equipos, nombres de usuario y contraseña, entre otros. Sólo en los casos en los que se produce algo fuera de lo normal se informa a los usuarios de que sus sistemas no funcionan bien. En ese

caso, lo más normal es que sean guiados a un portal de la intranet donde el sistema recupera los niveles adecuados de seguridad.

Tanto para las pequeñas empresas como para las grandes, son muchas las ventajas de contar con un nivel de seguridad tan dinámico. Una red con NAC no sólo funciona de forma más segura, sino también más productivamente, ajustándose a la normativa establecida y generando menos llamadas al centro de asistencia técnica. Aunque los beneficios de una solución NAC son evidentes, la manera en la que las distintas soluciones hacen el trabajo dependiendo de si se basan en hardware, en línea, fuera de banda, con agente o sin agente las hacen ser algo más complejas.

2.3. ANÁLISIS DE SOLUCIONES NAC DE EMPRESAS PROPIETARIAS

Este tema se enfoca en comparar las diferentes soluciones NAC actualmente presentes en el mercado que son desarrolladas por diferentes fabricantes, al ser un mercado de competencia directa cada uno de ellos trata de diferenciar su producto agregando funciones o características adicionales que mejoran el sistema pero en la mayoría de casos estas opciones adiciones no se encuentran cubiertas dentro de la solución estándar, sino en versiones más avanzadas que requieren de licenciamiento y esto, claro está, representa mayor inversión económica al momento de la adquisición.

Existen varias empresas que ofrecen soluciones NAC a sus clientes, es un negocio rentable ya que estas soluciones pueden ser implementadas en casi cualquier institución sin importar el tamaño de la misma. Todas las empresas, grandes o pequeñas, tienen información que consideran importante para la estabilidad de su negocio y no quieren que esta se destruya o caiga en manos equivocadas; por lo tanto el mercado potencial para la venta de sus soluciones es bastante amplio.

De la gran cantidad de fabricantes, para este análisis se escogen a las marcas más conocidas en el mundo de las comunicaciones como son Cisco, Microsoft, Trusted Computing Group, Enterasys, Juniper ya que son las empresas dominantes del

mercado y se dispone de mayores fuentes de información y son las soluciones más implementadas dentro de nuestro país.

2.3.1. CISCO NAC FRAMEWORK Y APPLIANCE[9]

Iniciativa propietaria de Cisco basada en la implementación de una arquitectura completamente diseñada para aprovechar al máximo la red existente. Está basada en equipos Cisco, centralizando el control en un servidor de acceso dedicado (appliance) que permite una rápida implantación de políticas sin realizar cambios en switches y routers.

Cisco es la marca líder mundial en el mercado de las soluciones de control de acceso, ha desarrollado esta tecnología desde hace varios años atrás y cuenta con la mayor experiencia en este campo creando protocolos de comunicación propios de la marca y que pueden ser implementados solo en sus equipos. Aunque también posee mecanismos para interoperar con otros fabricantes.
La tecnología utilizada es CISCO NAC.

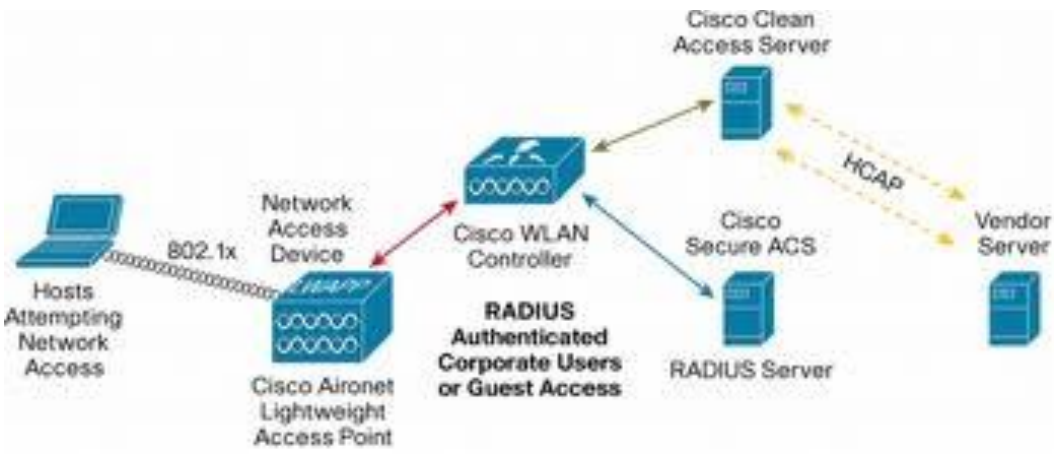

Figura 2.1: Arquitectura Cisco NAC Framework

[9] Network Admission Control (NAC) Framework. Recuperado de: http://www.cisco.com/en/US/netsol/ns617/index.html

2.3.2. CONSENTRY LANSHIELD[10]

Solución desarrollada por Consentry Networks, muy conocida en el mercado mundial asegura proveer de switches seguros habilitando el control de cada usuario y puerto de la LAN. Esta solución como base consta de dos equipos: un controlador y un swtich personalizados con buenas características de hardware para proveer de inspección de paquetes en altas velocidades de transmisión sin impactar al rendimiento y aplicación de políticas de seguridad.

El equipo LanShield Controller trabaja con la infraestructura de red LAN existente y con la base de datos de autenticación para proveer comunicación segura. Este equipo se ubica entre los switchs de acceso y los switchs de distribución o core, agregando enlaces hacia los datacenters y aplicando políticas de acceso a todo el tráfico que pasa a través de ellos. Este dispositivo no requiere cambios en el diseño de la red.

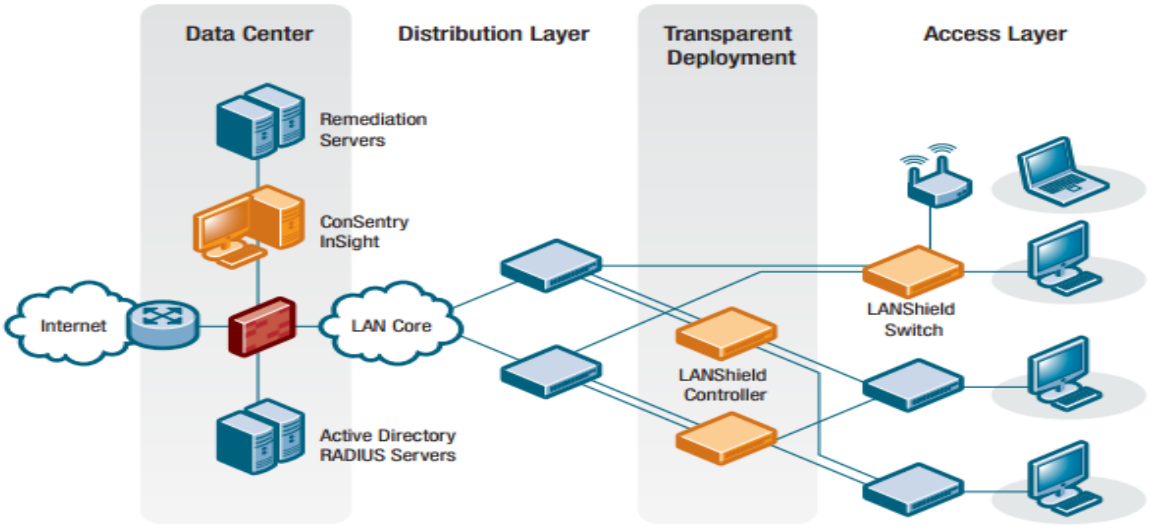

Figura 2.2: Arquitectura ConSentry LanShield

[10] Consentry LanShield. Recuperado de: *http://www.ruthvictor.com/pdf/NAC/Datasheet/ConSentry_LANShield_controller_DS_012608.pdf*

2.3.3. ELEMENTAL SECURITY PLATAFORM[11]

Los equipos Elemental ofrecen un enfoque para la gestión de acceso a la red que se centra específicamente en la prestación basada en políticas de control de acceso a los recursos críticos. La Plataforma de Seguridad Elemental (ESP) proporciona una solución basada en agentes de usuario que complementa la infraestructura de admisión a nivel de NAC. Esto permite a las organizaciones implementar un sistema de control de acceso que proporciona tanto la evaluación de las posturas de seguridad de los dispositivos necesarios para gestionar la admisión de red y un enfoque basado en políticas para administrar el acceso a los servidores de información críticos para el negocio y los sistemas.

Mediante la implementación de la ESP, las empresas pueden mejorar NAC y aplicarla en sus niveles de seguridad más amplios. El ESP no sólo evalúa herramientas de seguridad instaladas en los hosts (antivirus, anti-spyware, prevención de intrusiones) sino que se instalan y ejecutan según la operación que se requiera. También el ESP realizan un monitoreo continuo de la situación de seguridad de las máquinas a través de una amplia biblioteca de plantillas de políticas de seguridad y las reglas que permiten a las organizaciones fácilmente traducir sus objetivos de negocio a los requisitos de cumplimiento en los controles de seguridad exigidos. Esta evaluación en profundidad de la seguridad de los servidores y estaciones de trabajo permite a los administradores de red conceder el acceso sólo a aquellas máquinas que estén autorizados, y que demuestren un nivel aceptable de seguridad.

[11] Elemental Security Plataform. Recuperado de: *http://www.elementalsecurity.com/network-access-control/*

2.3.4. ENTERASYS SECURE NETWORKS[12]

La ventaja Enterasys NAC brinda a las empresas visibilidad, control sobre los usuarios y aplicaciones en infraestructuras de varios proveedores. NAC protege las inversiones existentes en infraestructura ya que no requiere implementación de nuevo hardware de comunicación (switches por ejemplo) o agentes que deben ser instalados en todos los usuarios finales. Enterasys NAC realiza métodos múltiples de autenticación para usuarios, evaluación de vulnerabilidades y remediación asistida. Ofrece la posibilidad de elegir si se desea o no restringir el acceso para invitados/contratistas a los servicios públicos de Internet y cómo se debe manejar a usuarios internos autenticados o dispositivos que no aprueben la evaluación de la seguridad. De esta manera las empresas tienen la flexibilidad de equilibrar la productividad del usuario y la seguridad en el acceso. La capacidad de evaluación de alertas de NAC advierte a los usuarios que tienen que actualizar su sistema operativo, pero puede permitir un período de gracia antes de que se ponga a su equipo en cuarentena.

Las políticas de Enterasys NAC permiten, deniegan, priorizan, limitan la velocidad, etiquetan, re direccionan y permiten auditoria del tráfico de red en función de la identidad del usuario, la hora y la ubicación, tipo de dispositivo y otras variables ambientales.

Enterasys NAC soporta la cuarentena RFC 3580 basada en puertos y Vlans para Enterasys y switches de otras marcas, además de políticas de aislamiento potentes (evitando que los equipos comprometidos lancen ataques durante el estado de cuarentena) en los switches Enterasys. Este tipo de NAC es adaptable a cualquier dispositivo que utilice RADIUS para autorización con atributos configurables como identificación LAT o filtro de ID. Las empresas pueden aplicar diferentes políticas dependiendo de la configuración de rechazo de RADIUS. Por ejemplo, se pueden aplicar una política para un usuario con contraseña caducada y otra diferente para un usuario que no tiene una cuenta. Esta solución ofrece una gran interoperabilidad

[12] Enterasys NAC. Recuperado de: *http://www.enterasys.com/company/literature/nac-ds.pdf*

entre marcas, ofrece el mayor número posible de opciones de autenticación, y soporta acceso de capa 2, capa 3 y tecnologías VPN.

Enterasys NAC permite la configuración homogénea de las políticas en switches y access points inalámbricos de múltiples proveedores. Esta característica reduce significativamente la gestión de la política y su ciclo de vida facilitando la implementación de NAC en infraestructuras heterogéneas formadas de redes cableadas e inalámbricas.

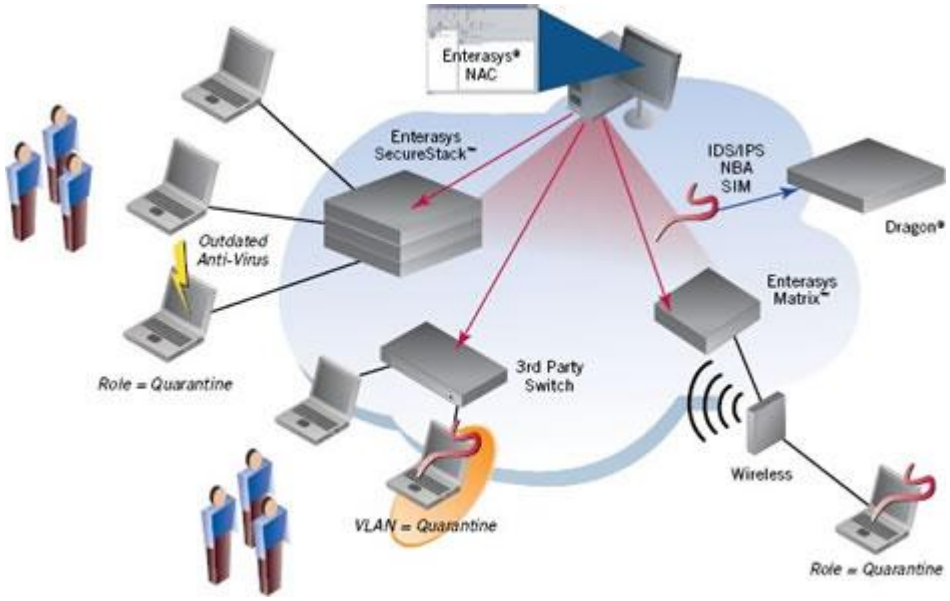

Figura 2.3: Enterasys Network Access Control[13]

[13] Figura 2.3: Enterasys Network Access Control. Recuperado de: *http://www.hoangco.com.vn/en/Solutions/Networking/tabid/153/articleType/ArticleView/articleId/24/Security-Networks-Enterasys.aspx*

2.3.5. CUADRO ANALÍTICO DE SOLUCIONES NAC DE EMPRESAS PROPIETARIAS

Fabricante	Control de Acceso	Control de Recursos	Evaluación de posturas	Cuarentena/Remediación	Evaluación de amenazas
Cisco	●	▮	✸	●	▮
ConSentry Networks	●	●	▮	▮	▮
Elemental	▮	▮	●	▮	▮
Enterasys Networks	●	▮	✸	▮	▮
Extreme Networks	○	○	✸	▮	▮
ForeScout	●	▮	▮	▮	▮
Hewlett Packard	●	▮	▮	▮	▮
InfoExpress	●	▮	▮	▮	▮
Juniper Networks	●	▮	✸	▮	▮
Lockdown Networks	●	▮	●	▮	▮
McAfee	▮	○	●	▮	▮
Microsoft	▮	▮	✸	✸	○
Mirage Networks	●	○	▮	▮	▮
Nevis Networks	●	●	○	○	▮
StillSecure	▮	▮	●	●	○
Symantec	▮	○	●	▮	▮
Vernier Networks	▮	▮	▮	▮	▮

● Alta, ▮ Media, ○ Baja, ✸ Alta dependiendo de la integración con otros fabricantes

Tabla 2.1: Cuadro Analítico de soluciones NAC de empresas Propietarias

2.3.6. CUADRO DE CARACTERÍSTICAS DE LAS SOLUCIONES PROPIETARIAS EXISTENTES[14]

Producto	Descripción de la solución	Tecnología
Cisco NAC Framework	Iniciativa propietaria de Cisco basada en la implantación de control de acceso dentro de la infraestructura de red	Cisco NAC
Cisco NAC Appliance	Equipos Cisco que permiten una rápida implantación de políticas de control de acceso a la red sin realizar cambios en *switches* y *routers*	Cisco NAC
ConSentry LANShield	Solución NAC de alto rendimiento pensada para ser desplegada de forma perimetral. Control de acceso basado en identidad, políticas y datos de usuario	Basada en dispositivos propios, *appliances* creados por ConSentry
Elemental Security Platform	Sistema diseñado para monitorizar dispositivos de red, configuraciones, actividad de los usuarios, implementando políticas de seguridad basadas en roles	Propietaria, basada en un modelo de servidores y software de agentes
ENDFORCE Enterprise	Solución basada en software, diseñada para redes heterogéneas, con la capacidad de extender las funcionalidades ofrecidas por las arquitecturas NAC, NAP y TNC	Basada en estándares, compatible con C-NAC, NAP y TNC
FireEye NAC Appliance	Basada en *appliances* que implanta el control de acceso basándose en la inspección del tráfico de los dispositivos de la red, y por tanto en la detección de tráfico peligroso o dañino	Propietaria, basada en dispositivos propios junto con la tecnología FACT
ForeScout CounterAct	Utiliza *appliances* propios, para realizar un despliegue transparente, no perjudicial para la red donde se realiza, combinando control de acceso que no utiliza clientes con prevención de intrusos para asegurar el correcto cumplimiento de la seguridad en los equipos	Propietaria, basada en dispositivos propios junto con la tecnología FastPass
InfoExpress CyberGatekeeper	La familia CyberGatekeeper ofrece tres productos, uno para implementar en entornos LAN, otro para sistemas remotos y el tercero que focaliza el control de acceso sobre el usuario final	Propietaria, basada en dispositivos servidores y software de agentes y servidores
Insightix NAC	Mantiene un inventario exhaustivo de todos los dispositivos conectados a la red, permitiendo, gracias a su tecnología de bloqueo y cuarentena única, implementar políticas de seguridad y control de acceso para cualquier dispositivo o tráfico	Propietaria
Juniper Networks Unified Access Control (UAC)	El Control de Acceso Unificado 2.0 incluye varios elementos: Infranet Controller, agente UAC y puntos de aplicación de la política de seguridad. Funciona en gran variedad de entornos, incluyendo aquellos con 802.1X	Compatible con la arquitectura TNC
Lockdown Enforcer	Se trata de *appliances* dinámicos de control de acceso a la red, que autentica de forma simultánea a usuarios y dispositivos y los analiza de forma periódica y también en caso de solicitud puntual, comprobando que cumplen las políticas de seguridad	Propietaria, basada en *appliances*
Microsoft NAP	Iniciativa propietaria de Microsoft	Microsoft NAC
Mirage Networks NAC	Familia de productos NAC, en la que las decisiones sobre qué política aplicar a los usuarios se toman en dispositivos diferentes a los que finalmente aplican la política, basada en escaneos de dispositivos y prevencion de intrusos	Propietaria, compatible con arquitecturas TNC y NAP
Nevis Networks LANenforcer	Esta solución se implementa sobre *switches* que son los que realizan el control de acceso de los usuarios, cada uno de los cuales se ubica en una DMZ personal donde se le protege de amenazas, y a la vez se protege a la red de las amenazas que pueda provocar dicho usuario	Propietaria, basada en el uso de dispositivos propios (*switches*)
Nortel Secure Network Access	Solución de control de acceso a redes basada en la implementación del control en los *switches* LAN, *routers* y *gateways* SSL VPN de Nortel	Propietaria
Senforce NAC & Endpoint Security Suite	Solución que integra la comprobación de que los usuarios finales están libres de amenazas, con la seguridad inalámbrica y el control de acceso a la red	Compatible con la arquitectura Cisco NAC
StillSecure SafeAccess	Solución muy flexible, que ofrece cinco opciones de aplicación de políticas en diferentes entornos, por lo que se adapta muy bien a redes complejas y heterogéneas	Compatible con la arquitectura Cisco NAC
Symantec Network Access Control	Ofrece una solución que permite aplicar control de acceso para dispositivos que se conecten a través de SSL VPNs, *switches* inalámbricos, aplicaciones basadas en Web, usando 802.1X, y casi cualquier infraestructura LAN o inalámbrica	Compatible con la arquitectura Cisco NAC
Vernier EdgeWall	*Appliances* NAC, que validan a los usuarios mediante una mezcla de política de confianza y chequeo de vulnerabilidades	Propietaria
Enterasys Secure Networks	Arquitectura basada en redes inteligentes, capaces de gestionar de forma individualizada cada usuario o dispositivo, permitiendo un control granular de usuarios, dispositivos y aplicaciones, ofreciendo una respuesta dinámica a intrusiones	Basada en estándares, no propietaria
HP Procurve Networking Adaptative EDGE	Arquitectura que permite construir redes con inteligencia perimetral, que pone la inteligencia en el punto de conexión del usuario, permitiendo realizar en ese punto funciones como la priorización de tráfico, autenticación, reserva de ancho de banda y aplicación de políticas	Arquitectura propietaria

Tabla 2.2: Cuadro de características de las Soluciones Propietarias Existentes

[14] Esmoris, D. *Control de Acceso a Redes* (Trabajo Investigativo). Facultad Informática de la Univ. de la Plata

2.4. ANÁLISIS DE SOLUCIONES NAC BASADAS EN SOFTWARE LIBRE

Las soluciones NAC comerciales pueden ser costosas y estos precios se incrementan si la solución requerida por la empresa necesita de funciones opcionales que no están incluidas con el paquete básico. Las empresas pymes a menudo no cuentan con el presupuesto necesario para la adquisición de estas soluciones, por lo cual una opción menos costosa es implementar una solución basada en Software Libre.

2.4.1. CONSIDERACIONES SOBRE LAS SOLUCIONES TECNOLÓGICAS DE SOFTWARE LIBRE

- Las soluciones de Software Libre son beneficiosas para el mercado. Los fabricantes conocen que hay soluciones gratuitas que se incrementan cada día y con el pasar del tiempo mejoran constantemente, lo que debe ser un factor influyente para que ellos comiencen a disminuir los costos de sus soluciones. Adicionalmente las tecnologías NAC de software libre empujan a todo el mercado del control de acceso a red a formar más normas y estándares abiertos fomentando la innovación.
- Las soluciones de Software libre permiten el acceso al código fuente. Tal vez exista una característica que una empresa busca pero no la encuentre en ninguna solución privada; con las soluciones NAC de Software Libre es posible adaptar el software al gusto y necesidad de cada persona.
- A través de los años, los productos de Software Libre han demostrado su confiabilidad y funcionalidad para empresas a un costo virtualmente inexistente. Por ejemplo el Sistema operativo Linux, el sistema de telefonía IP Asterix, Snort, Nmap, Nessus y otros. Todas estas son alternativas exitosas a productos comerciales.
- Las comunidades dedicadas al desarrollo de Software Libre dan soporte a los productos, los inconvenientes pueden ser identificados y resueltos con facilidad.

Esto ocurre mucho más rápido que el tiempo que le toma a los fabricantes hacerlo.

- El costo es sin duda una de las mayores razones por las que los administradores suelen acudir a los productos de Software Libre. Siempre será difícil de justificar un producto comercial con una etiqueta de precio grande en comparación con un producto de Software Libre con precios inferiores ofreciendo similares características.

Existen varias soluciones NAC desarrolladas en Software libre a continuación un breve listado de las más conocidas junto con una descripción breve de sus funciones.

Nombre	Descripción de la Solución
PacketFence	Es un dispositivo virtual que se ejecuta dentro de Windows o Linux. Revisa las políticas de seguridad cuando un dispositivo se conecta a la red. ZEN está basado en Linux Fedora, LAMP, Perl, y Snort. Es utilizado en universidades alrededor del mundo. Puede operar en cualquier entorno de red. Esta plataforma es gratuita
FreeNAC:	Es un software de código abierto, pero recientemente también ha sido ofrecido en una versión comercial con algunas características extra a la versión gratuita. FreeNAC trabaja con el protocolo 802.1X o si se tienen equipos Cisco puede utilizar VMPS. Además, FreeNAC ofrece administración de VLAN y puertos de switch, información de puntos de cableado, y descubrimiento de dispositivos.
Rings	Es una plataforma NAC creada en la Universidad de Kansas, adoptado por otras universidades y desarrollado con la meta de ser utilizado en un rango amplio de redes.
NetReg	Desarrollado en la Universidad Carnegie Mellon, esta plataforma está diseñada con un set de características principales y otras varias opcionales que pueden o no afectar la funcionalidad principal de NAC.
HUPnet	Es un proyecto de la Universidad de Helsinki diseñado para el control de acceso a las redes inalámbricas pero aplicables también a las redes cableadas.
Ungoliant	La Universidad de Indianapolis es la desarrolladora de esta plataforma, la cual tiene una versión privada llamada Shelob que es utilizada en su campus.

Tabla 2.3: Soluciones NAC desarrolladas en Software libre

Para la realización de este proyecto se opto por utilizar las plataformas ***PacketFence*** y ***FreeNAC*****,** ya que son las dos alternativas de Software Libre más conocidas e implementadas a nivel mundial. Ambas cuentan con basta documentación técnica,

foros de soporte, guías de instalación y versiones estables. De este modo facilitan su implementación en el ambiente de laboratorio.

2.4.2. DESCRIPCIÓN DE LA SOLUCIONES DE SOFTWARE LIBRE QUE INTEGRAN EL SISTEMA

2.4.3. PACKETFENCE[15]

Es una solución NAC de código abierto, confiable, gratuita y ampliamente soportada. Posee un impresionante conjunto de características entre las que se incluye portal cautivo para registro y remediación, administración centralizada para redes cableadas e inalámbricas, soporte 802.1X, aislamiento de capa 2 para equipos que causen problemas, integración con Snort IDS y con el scanner de vulnerabilidades Nessus. PacketFence puede ser utilizado para asegurar redes de forma efectiva, desde pequeñas a grandes.

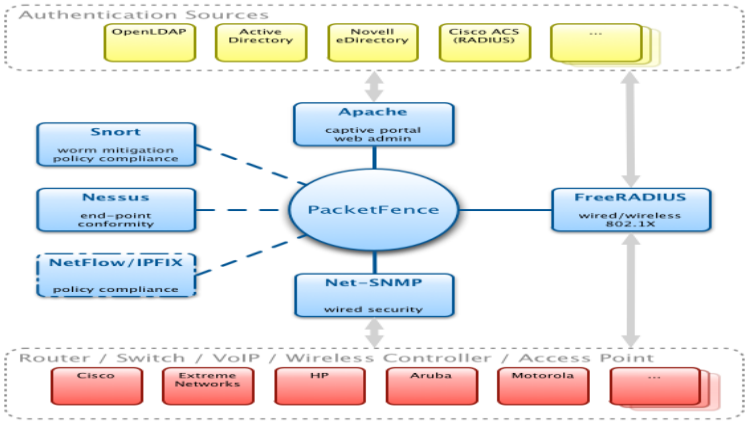

Figura 2.4: Arquitectura PacketFence[16]

2.4.4. AUTENTICACIÓN Y REGISTRO

- **Soporte 802.1X:** 802.1X es soportado para redes cableadas como inalámbricas a través del modulo FreeRadius que está incluido en PacketFence
- **Soporte Voz sobre IP (VoIP):** También llamada telefonía IP (IPT), VoIP es totalmente soportado (aun en ambientes heterogéneos) para switches de múltiples fabricantes como Cisco, HP, Enterasys, LinkSys, Nortel, entre otros.

[15] PacketFence . Recuperado de: *http://www.packetfence.org/about/overview.html*
[16] Figura 2.4: PacketFence. Recuperado de: *http://www.packetfence.org/fileadmin/images/pf/components.png*

- **Integración Wireless:** Se integra de forma perfecta a las redes inalámbricas a través del modulo FreeRadius. Esto permite asegurar las redes cableadas e inalámbricas de la misma manera usando la misma base de datos de usuarios y el mismo portal cautivo, proveyendo de una experiencia consistente para los usuarios. Access points de varios fabricantes así como controladoras inalámbricas son soportadas.
- **Registro de Dispositivos:** Soporta un mecanismo de registro opcional similar a la solución de portal cautivo. Contrario a la mayoría de soluciones de portal cautivo, PacketFence recuerda a los usuarios previamente registrados y automáticamente les dará acceso sin otro tipo de autenticación necesaria. Un aceptable uso de políticas de seguridad puede ser especificado como: los usuarios no podrán acceder a la red sin antes haber sido autenticados.

2.4.5. DETECCIÓN DE ACTIVIDADES ANORMALES DE RED

Las actividades de red anormales (Virus de computadoras, gusanos, spyware, denegación de tráfico, etc.) pueden ser detectadas usando sensores Snort locales y remotos.

Más allá de una simple detección, las capas de PacketFence tienen su propio mecanismo de alerta y supresión para cada tipo de alertas. Un conjunto de acciones configurables para cada violación está disponible para los administradores.

2.4.6. DECLARACIONES DE SALUD

Mientras se realiza la autenticación 802.1X, PacketFence puede ejecutar tareas sobre los usuarios conectados utilizando el protocolo de declaraciones de salud TNC. Por ejemplo, puede verificar si un antivirus está instalado y actualizado, si se han instalado parches al sistema operativo y muchas más. Todo esto sin la necesidad de instalar ningún agente en los equipos del usuario.

2.4.7. ESCÁNER DE VULNERABILIDADES PROACTIVO

PacketFence correlaciona las identificaciones de vulnerabilidades Nessus/OpenVAS de cada escaneo a la configuración de violaciones, entregando páginas web con contenido especifico acerca de la vulnerabilidad que el host puede tener.

2.4.8. SOLUCIONES A TRAVÉS DE PORTAL CAUTIVO

Una vez atrapado, todo el tráfico de la red es bloqueado por el sistema PacketFence. Basado en el estado actual de los nodos (sin registrar, violación abierta, etc.) el usuario es re direccionado al URL apropiado. En el caso de violación, al usuario se le mostrara las instrucciones para el caso. De esta manera se reduce la intervención del departamento Help desk.

2.4.8.1. Aislamiento de equipos con problemas

Soporta varias técnicas de aislamiento, incluyendo aislamiento de VLANs con soporte VoIP (aun en ambientes heterogéneos) para múltiples fabricantes de switches.

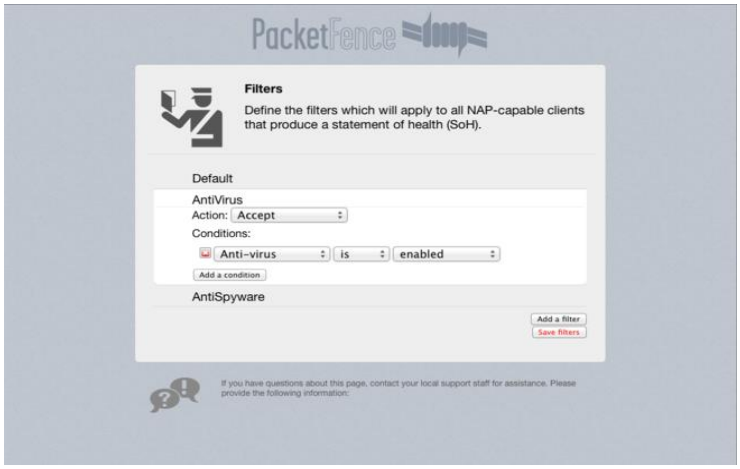

Figura 2.5: Filtros PacketFence[17]

2.4.8.2. Administración Web y línea de comandos

Posee interface web y línea de comandos para todas las tareas de administración. La administración web soporta varios niveles de permisos y autenticación de usuarios con LDAP o Microsoft Active Directory.

[17] Filtros PacketFence. Recuperado de: *http://www.packetfence.org/about/overview.html*

2.4.8.3. Administración de VLANS y control de accesos basado en Roles

La asignación de VLANS se realiza normalmente usando varias técnicas diferentes. Estas técnicas son compatibles entre ellas. Esto significa que se puede utilizar las técnicas más seguras y modernas para sus nuevos switches y otras técnicas para switches antiguos que no son compatibles con las últimas técnicas.

La solución se basa en el concepto de aislamiento de la red a través de la asignación de VLAN. La topología de VLANS no es alterada y sólo dos nuevas VLANS son añadidas a través de la red: la VLAN de registro y la VLAN aislada. Por otra parte, también se pueden hacer uso de los roles de apoyo de varios proveedores.

2.4.8.4. Acceso de invitados - Traiga su propio dispositivo (BYOD)

Hoy en día, la mayoría de las empresas cuentan con un montón de asesores de diversas compañías externas que requieren acceso a Internet para sus trabajos. En la mayoría de los casos, un acceso a la red corporativa se da con poca o ninguna auditoría de la persona o dispositivo. Además, rara vez se requiere que ellos tengan acceso a la infraestructura corporativa interna.

PacketFence Soporta una VLAN de invitados especial. Si se utiliza esta VLAN de invitados se configura la red para que esta VLAN solo tenga salida a internet, el portal cautivo se utiliza para explicarle al invitado como debe registrarse para obtener acceso y como funciona. Varias formas de registro de usuario son soportadas.

- Registro manual del invitado
- contraseña del día
- Auto registro (con o sin credenciales)
- Acceso de invitados patrocinados (un empleado de la empresa confía en el invitado)
- Acceso de invitados activado por confirmación de email
- Acceso de invitados activado por teléfono (SMS de confirmación)

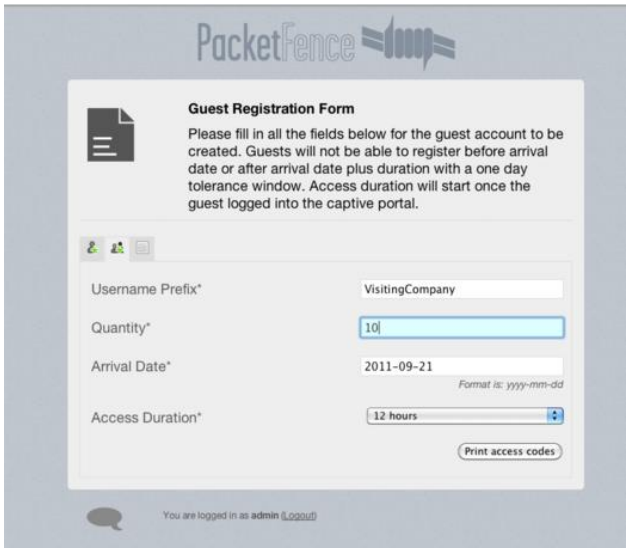

Figura 2.6: Registro de invitados[18]

2.4.8.5. Vencimiento

La duración del acceso a la red puede ser controlada con parámetros configurables como una fecha específica (ejem: “martes, 20 enero 2011 hasta las 20h00”) o una ventana (ejem:”cuatro semanas desde el primer acceso a la red”). Luego de cumplirse el periodo de vencimiento los dispositivos registrados vuelven al estado de no registrados.

2.4.8.6. Auditoria de Ancho de Banda

PacketFence puede rastrear automáticamente la cantidad de ancho de banda que los dispositivos consumen en la red. Con el soporte de violaciones incorporado se puede agregar a los equipos en cuarentena o cambiar su nivel de acceso si están consumiendo demasiado ancho de banda durante una ventana de tiempo en particular. También es posible generar reportes del consumo de ancho de banda.

2.4.8.7. Autenticación Flexible

Es posible autenticar a los usuarios utilizando varios protocolos o estándares. Esto permite integrar PacketFence a cualquier ambiente sin requerir a los usuarios recordar otros nombres de usuario y contraseña. Algunas fuentes de autenticación pueden ser:

[18] Figura 2.6: Registro de invitados. Recuperado de: *http://www.packetfence.org/about/advanced_features.html*

- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP
- Cisco ACS
- Radius (FreeRADIUS, Radiator,etc.)
- Archivos del usuarios locales

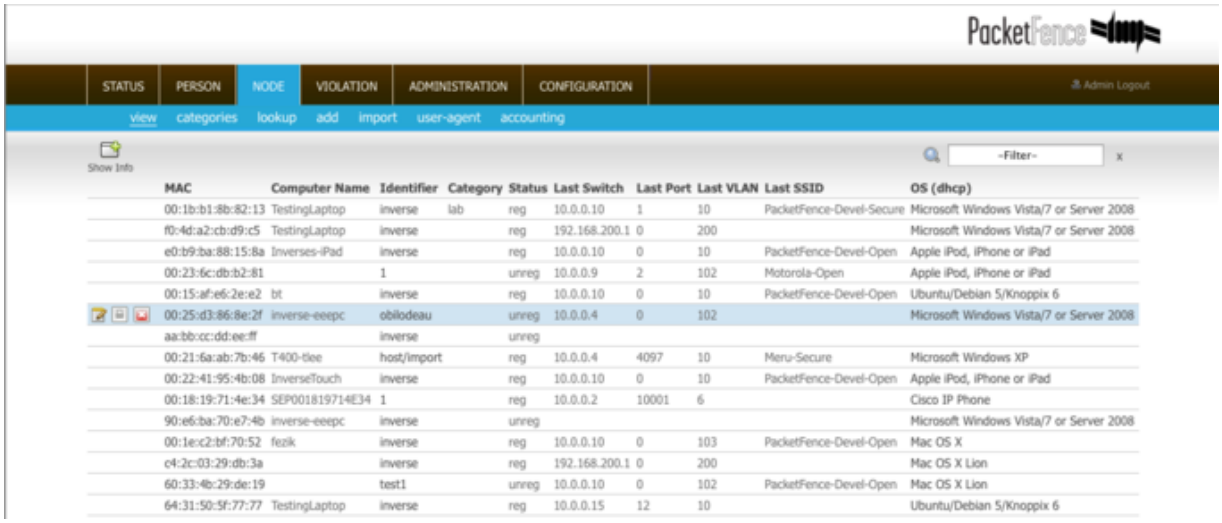

Figura 2.7: Autenticación flexible[19]

2.4.8.8. Alta Disponibilidad

Esta desarrollado con la opción de alta disponibilidad en mente. Todas las implementaciones son hechas usando alta disponibilidad del tipo activo-pasivo.

2.4.9. FreeNAC[20]

FreeNAC puede ser una solución para control de acceso a redes, administración de switches, inventario automatizado de dispositivos de red, administración de redes virtuales y para proporcionar acceso a la red para usuarios invitados.

Puede ayudar a:

[19] Figura 2.7: Autenticación flexible. Recuperado de: *http://www.packetfence.org/about/overview.html*

[20] FreeNAC. Recuperado de: *http://freenac.net/es*

- Limitar el acceso a los recursos de red.
- Rastrear qué equipos estuvieron en la red, dónde, cuándo.
- Proporcionar un inventario en tiempo real de los dispositivos de red, y enlazarlo a un inventario estático.
- Ofrecer reportes que enlacen los datos de red, usuario e información sobre el dispositivo.

2.4.9.1. Funcionamiento

El switch detecta un nuevo equipo y solicita autorización del servidor FreeNAC, el cual verifica los derechos en la base de datos, y rechaza o permite el acceso asignando la red virtual apropiada para el equipo en cuestión.

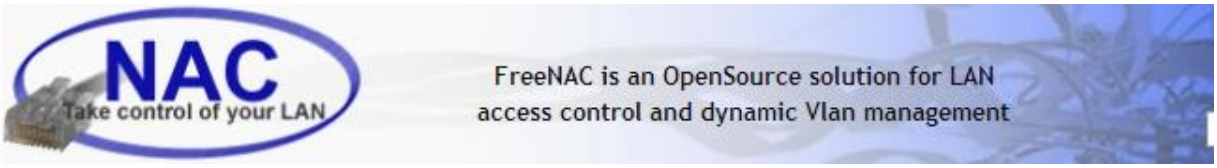

Figura 2.8: FreeNAC logo[21]

2.4.9.2. Autenticación

- **Modo VMPS:** Los equipos se identifican por su dirección MAC. Los usuarios no son autentificados en este modo.
- **Modo 802.1x:** Los equipos se pueden autentificar por medio de certificados. Los usuarios pueden ser autentificados por medio de su cuenta en un dominio Windows.

La asignación de una red virtual se basa en la dirección MAC del dispositivo. En el modo VMPS, la autentificación/asignación toman lugar en una sola etapa. En el modo 802.1x, la autentificación de los usuarios (en el dominio Windows) o de los equipos (por medio de un certificado) se desarrolla primero, y solamente cuando

[21] Figura 2.8: FreeNAC logo. Recuperado de: *http://freenac.net/es*

estas credenciales han sido validadas, se utiliza la dirección MAC para asignar una red virtual.

FreeNAC está diseñado para funcionar sin software en los equipos. Por lo tanto, la verificación de seguridad de los dispositivos de red puede ser solamente hecho por medio de un chequeo o evaluando la seguridad del dispositivo en el lado del servidor. Esto significa que si se utilizan los servicios McAfee EPO or MS-WSUS, por ejemplo, puede ser posible verificar la seguridad del dispositivo antes de permitir el acceso.

Es usualmente instalado en redes heterogéneas que no solamente tienen Windows, sino también muchos otros clientes, y así, la información EPO/WSUS es usada como una indicación/ayuda para el administrador de seguridad, pero no usada para excluir dispositivos de la red.

2.4.9.3. Administración de redes virtuales (VLANs)

Una red virtual es especificada por cada dispositivo, y esta red virtual será siempre utilizada por este dispositivo, sin importar su posición geográfica dentro de sus instalaciones. Si se presentan reorganizaciones, no se necesita adaptar la configuración de los switches, ya que la red se adaptará a su nueva organización (todos los puertos son 'dinámicos').

Cambiar las asociaciones de redes virtuales es sólo cosa de seleccionar la VLAN a usar de una lista y eso es todo, disminuyendo así la cantidad de trabajo para el administrador de red cuando se trata de crear membrecías de redes virtuales para proyectos específicos.

Se puede atribuir una red virtual por defecto para puertos específicos. Por ejemplo, la política por defecto puede ser negar acceso a dispositivos desconocidos, excepto en salas de conferencias donde visitantes (equipos desconocidos) son automáticamente admitidos a una red virtual específica para invitados.

2.4.9.4. Acceso a la red de invitados

La política de acceso para invitados (equipos desconocidos sobre la red) puede ser especificada globalmente, o bien, de forma individual para ciertos puertos. La política específica una VLAN para ser atribuida a los dispositivos visitantes.

- La política por defecto podría, por ejemplo, ser negar el acceso a los usuarios desconocidos y generar una alerta.
- bien, la política por defecto podría, por ejemplo, ser negar el acceso a los usuarios desconocidos, excepto en salas de reuniones o los invitados pueden automáticamente acceder a una VLAN dedicada a los visitantes.

2.4.9.5. Administración de visitantes

Los visitantes (dispositivos desconocidos), pueden opcionalmente tener acceso a una zona de redes virtuales por defecto o para invitados. Esto puede ser útil, por ejemplo, para organizaciones que desean permitir a sus visitantes acceso Web/VPN a Internet, pero restringir el acceso a las redes internas.

Tan pronto como un nuevo dispositivo es conectado al puerto del switch, su dirección MAC se pasa al servidor, donde será almacenada y comprobada para determinar si este dispositivo tiene acceso a la red. Si el dispositivo está autorizado a tener acceso, el servidor le regresará al switch la red virtual a la que este dispositivo pertenece. Si este dispositivo todavía no está registrado, su acceso es bloqueado o se coloca en una red virtual limitada, dependiendo en la política como se puede ver en la siguiente figura

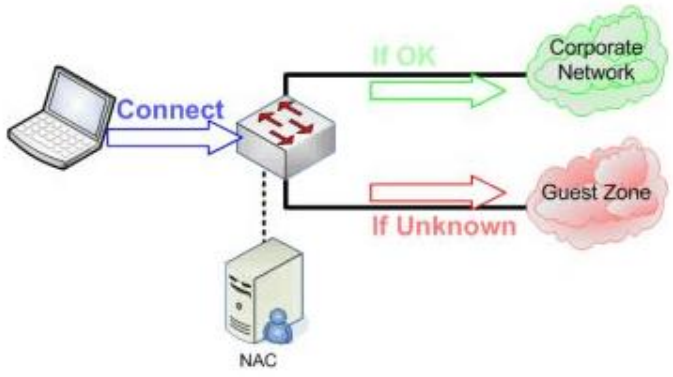

Figura 2.9: FreeNAC Administración de visitantes[22]

[22] Figura 2.9: FreeNAC Administración de visitantes. Recuperado de: *http://freenac.net/es/products/solution*

2.4.9.6. Modos de Operación

FreeNAC tiene dos modos de operación:

- **VMPS (VLAN Management Policy Server):** es un método para asignar puertos de un switch a redes virtuales específicas de acuerdo a la dirección MAC del dispositivo que busca acceso a la red. En modo VMPS, un switch compatible con VMPS detecta una nueva PC y crea una petición VMPS pidiendo autorización de FreeNAC, el cual revisa en su base de datos y permite o niega el acceso a la red basándose en la dirección MAC. El switch se encarga de respaldar la decisión tomada por FreeNAC y niega acceso o en caso contrario, coloca el dispositivo de manera dinámica en su red virtual por defecto.

- **802.1X**: es un estándar creado por la IEEE para el control de acceso a redes basándose en el puerto del switch. Proporciona autentificación a dispositivos conectados a un puerto de la red, estableciendo una conexión punto a punto o restringiendo el acceso en caso de que la autentificación falle. 802.1x está disponible en algunos modelos recientes de switches y puede ser configurado para autentificar equipos los cuales cuenten con un software suplicante, no permitiendo accesos no autorizados a la red en la capa de enlace.

  En modo 802.1x, FreeNAC verifica las credenciales de los usuarios (a través del uso de un servidor de autentificación externo) y usa la dirección MAC del dispositivo que se conecta para asignarlo a una red virtual. Esto crea un par nombre de usuario/dispositivo que es único para cada cliente que se conecta.

2.4.9.7. Características

FreeNAC contiene numerosas funciones para ayudar al administrador con el manejo y puesta en marcha de redes virtuales, al mismo tiempo que proporciona control de acceso a redes.

Las características principales son:

- Asignación dinámica de redes virtuales
- Control de acceso a redes

- Flexibilidad en mecanismos de autentificación para redes: 802.1x, VMPS
- Altamente automatizado
- Redundancia y repartición de carga de red para una mejor disponibilidad
- Inventario en tiempo real de los aparatos conectados a la red
- Documentación del cableado de la red
- Reportes flexibles

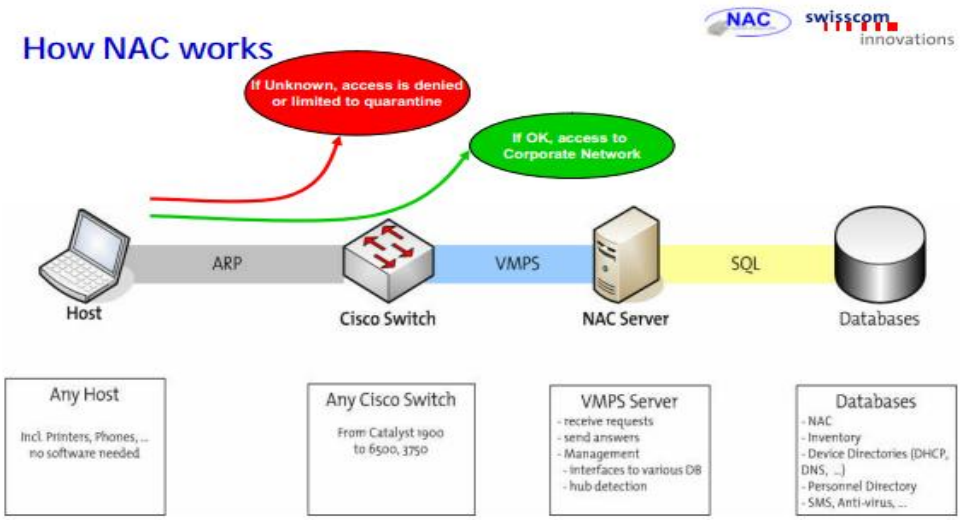

Figura 2.10: Funcionamiento FreeNAC[23]

2.4.9.8. Beneficios

Principales beneficios

- Una red dinámica permite un mejor uso de los puertos de switches disponibles, lo cual reduce costos y aumenta la eficiencia, facilita la configuración de los switches y hace posible tener menos cambios en el cableado durante reorganizaciones.
- FreeNAC no requiere software instalado en los dispositivos en modo VMPS. En modo 802.1x, un software suplicante necesita ser instalado. Clientes que ya usan acceso manual basado en puerto ahorrarán tiempo y ganarán efectividad.
- FreeNAC también funciona con antiguos switches Cisco, no es necesario adquirir nuevo hardware Cisco.

[23] Figura 2.10: funcionamiento FreeNAC. Recuperado de: http://freenac.net/files/presentations/NAC-TakeControlofyourLAN.pdf

Beneficios adicionales

- Permite que el cableado de red sea más dinámico y eficiente.
- Altamente automatizado y fácil de usar, lo que reduce costos por soporte.
- Extensible: es posible agregar módulos o interfaces personalizados para integrar NAC mejor en los procesos ya que está basado en estándares abiertos (open source).
- FreeNAC corre sobre hardware y sistemas operativos estándar (Linux/Unix).
- Tecnología comprobada: en producción desde 2004.
- Más eficiente que acceso manual basado en puertos.

CAPITULO III

3. DISEÑO DEL ENTORNO DE RED DE LABORATORIO PARA VALIDACIÓN DEL SISTEMA

3.1.INTRODUCCIÓN Y PREMISAS DE DISEÑO

Para la implementación del sistema integrado de acceso inteligente, se necesita de un escenario de red que simule los principales servicios que están presentes en la mayoría de empresas PYMES, instituciones educativas y similares. Por lo tanto las funciones y configuraciones de los equipos deben cumplir con estas premisas, y es por este motivo que el diseño del laboratorio de pruebas debe a más de brindar los servicios requeridos por cualquier empresa actual también ofrecer estabilidad y robustez tanto en sus equipos como en su funcionamiento. Para pequeñas y medianas empresas, la comunicación digital con datos, voz y video es esencial para la supervivencia. En consecuencia, una red LAN con un diseño apropiado es un requisito fundamental para la estabilidad de las empresas.

La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico. En comparación con otros diseños de redes, una red jerárquica se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez.

El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo. En este proyecto se separo la red en las capas de acceso y núcleo debido a la baja cantidad de equipos conectados en el ambiente de pruebas el switch núcleo, también conocido como CORE cumple con las funciones de distribución y núcleo sin inconvenientes.

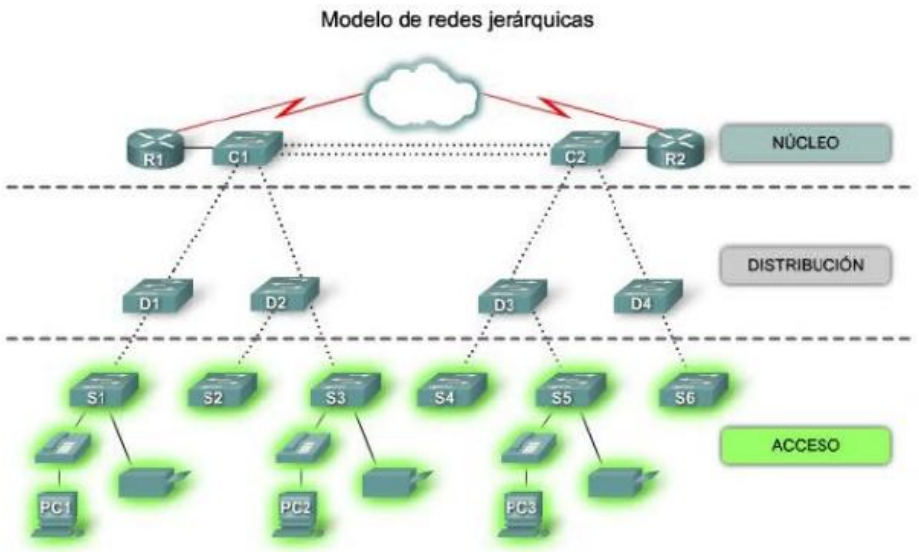

Figura 3.1: Modelo de redes jerárquicas[24]

3.2.EQUIPOS UTILIZADOS EN LA INFRAESTRUCTURA DE RED

A continuación se describe de forma breve los principales equipos que conforman la infraestructura de red del laboratorio además de sus principales características técnicas

3.2.1. SWITCH DE NÚCLEO (CORE):

Es el switch central de la red, posee las mejores características para manejo de los paquetes que circulan por ella, a este equipo se conectan el resto de switches, routers y servidores que brindan acceso y proveen servicios a los usuarios. La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de acceso, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. Por lo general se lo posiciona como puerta de enlace entre la red interna y la red pública que puede ser WAN o internet.

[24] Figura 3.1: Modelo de redes jerárquicas. Recuperado de: https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcTNRBKufm6aTSnkoI7JAfheTQQDpsm4LXCxzO9_ExGAJyI2LdFK7g

3.2.1.1. Cisco Catalyst WS-C3560G-24TS[25]

Es un equipo diseñado para el ámbito empresarial incluye la funcionalidad IEEE 802.3af Power over Ethernet (PoE) que provee voltaje de alimentación para el encendido de los equipos que se conecten a los puertos de red y que soporten esta tecnología. Maximiza la productividad y protección de la inversión al tiempo que permite el despliegue de nuevas aplicaciones como la telefonía IP, acceso inalámbrico, vigilancia por video. Los clientes pueden desplegar servicios inteligentes a lo largo de la red como la calidad de servicio avanzada (QoS), limitación de velocidad, las listas de control de acceso (ACL), la gestión de multidifusión IP y de alto rendimiento de enrutamiento mientras se mantiene la simplicidad de la conmutación LAN tradicional.

- **Características Técnicas:**
  - 24 puertos fastethernet 10/100/1000 y 4 puertos SFP Gigabit Ethernet para conexión de fibra óptica
  - Negociación automática en todos los puertos selecciona automáticamente el modo de transmisión full o half duplex para optimizar el ancho de banda.
  - Soporte IEEE 802.1d Spanning Tree Protocol para conexiones troncales redundantes y redes sin lazos simplifica la configuración de la red y mejora la tolerancia a fallos.
  - Enrutamiento IP entre VLANs que permite enrutamiento completo de Capa 3 entre dos o más VLAN.
  - IEEE 802.1x con VLAN de voz permite a un teléfono IP para acceder a la VLAN de voz, independientemente del estado autorizado o no autorizado del puerto.

[25] Cisco Catalyst WS-C3560G.24TS. Recuperado de: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.html

3.2.2. SWITCH DE ACCESO:

La capa de acceso interactúa con dispositivos finales de los usuarios, como PCs, impresoras, teléfonos IP, puntos de acceso inalámbricos (AP) para proporcionar acceso al resto de la red. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.

3.2.2.1. Cisco Catalyst WS-C3560G-8PC[26]

Comparte similares características técnicas que el switch de núcleo ya que pertenecen a la misma familia de producción y son perfectamente compatibles en funcionalidad al 100%, es decir, si en el equipo Core se configura algún servicio este será admitido por el equipo de acceso y ofrecido a los equipos que a él se conecten. Este equipo es el menor de la familia 3500 y las principales diferencias que tiene este modelo a comparación del equipo Core es la cantidad de puertos que dispone (8 en este caso) y la velocidad de procesamiento de paquetes y tramas que es menor por obvias razones

Como se detallo con anterioridad la función de este equipo es otorgar acceso a los equipos de usuario como PCs, teléfonos, APs entre otros.

3.2.3. CENTRAL DE TELEFONÍA IP: CISCO UNIFIED COMMUNICATION MANAGER EXPRESS

Las empresas pequeñas y medianas adoptan la idea de ejecutar servicios de voz y video en sus redes de datos y esto afecta a las redes jerárquicas si no son diseñadas para soportar estos servicios. Este proceso de lograr comunicaciones unificadas por

[26] Cisco Catalyst WS-C3560G-8PC. Recuperado de: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.html

medio de una misma red de datos se denomina convergencia. La convergencia es el proceso de combinación de las comunicaciones con voz y video en una red de datos. Las redes convergentes han existido durante algún tiempo, pero sólo fueron factibles en grandes organizaciones empresariales debido a los requisitos de infraestructura de la red y a la compleja administración necesaria para hacer que dichas redes funcionen en forma continua. Los costos de red asociados con la convergencia eran altos porque se necesitaba un hardware de switchs más costoso para admitir los requisitos adicionales de ancho de banda.

La convergencia de redes de voz, video y datos se ha vuelto muy popular recientemente en el mercado empresarial pequeño y mediano debido a los avances en la tecnología. En el presente resulta más fácil implementar y administrar la convergencia y su adquisición es menos costosa.

Un beneficio es el menor costo de implementación y administración. Es menos costoso implementar una infraestructura de red única que tres infraestructuras de redes distintas. La administración de una red única es también menos costosa.

Cisco Unified Communications Manager Express brinda procesamiento de llamadas para teléfonos IP de Cisco Unified para entornos de sucursales u oficinas pequeñas. Integra la amplia cartera de enrutadores de servicios integrados Cisco para ofrecer las funciones de comunicaciones unificadas que utilizan habitualmente los usuarios comerciales para satisfacer los requisitos de comunicaciones de voz y video de las oficinas pequeñas y medianas. Permite la implementación de un sistema de comunicaciones rentable y altamente confiable a través de un dispositivo único con software Cisco IOS.

3.2.3.1. Cisco 2911 Integrated Services Router [27]

Este equipo ofrece tiene la capacidad de de soportar comunicaciones unificadas de telefonía y video. Para este proyecto este equipo es configurado como la central de telefonía IP encargada de comunicar a los usuarios al interior de la red por medio de telefonía IP dentro de la misma infraestructura de datos ya que este entorno es común en la mayoría de empresas de la actualidad. En adición estas plataformas soportan un amplio rango de opciones de conectividad cableada como inalámbrica como puertos T1/E1, T3/E3, xDSL, Cobre y fibra óptica.

- **Características Técnicas**
  - Máximo 450 teléfonos por cada sistema
  - Hasta 34 líneas de llamada por teléfono
  - Funciones de la consola de operadora mediante módulos de expansión Cisco Teléfono IP Unificado de 7915 y 7916
  - Timbre distintivo por línea y opciones de llamada silenciosa
  - Selección automática de línea para llamadas salientes
  - Desvío de llamadas en ocupado, sin respuesta, y todos (interno o externo) No molestar (DND)
  - Identificador de llamadas: nombre y número.
  - Soporte para troncales digitales E1/T1.\

[27] Cisco 2911 Integrated Services Router. Recuperado de: http://www.cisco.com/en/US/prod/collateral/routers/ps10537/data_sheet_c78_553896.html

3.2.4. ACCESS POINT INALÁMBRICO

3.2.4.1. Cisco AIR AP1142N[28]

Este access point está diseñado para ser utilizado en interiores, de simple implementación y energía eficiente. Este modelo funciona en modo autónomo, es decir, no requiere de un equipo centralizado de administración (controladora) y puede trabajar de forma independiente en cualquier entorno de red, es ideal para empresas de mediana escala o implementaciones distribuidas.

- **Características técnicas:**
  - Soporte para tecnologías wifi: 802.11 a/b/g/n
  - Fácil instalación y manejo eficiente de energía
  - Soporta detección de access points amenazantes y ataques de denegación de servicio.
  - Bandas de frecuencia de 2.4 – 5 Ghz y canales operativos de 20Mhz
  - Estándares de seguridad 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA, 802.1x, AES,TKIP
  - Métodos de autenticación: EAP-TLS, TTLS, MSCHAPv2, PEAP, EAP-MSCHAPv2, EAP-FAST. PEAPv1
  - Antenas de radiación incorporadas al interior del equipo
  - Radiación de Múltiples SSIDs

[28] Cisco AIR AP1142N. Recuperado de: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/datasheet_c78-502797.html

3.2.5. TELÉFONOS IP

3.2.5.1. Cisco Unified IP Phone 7945G[29]

Este modelo de teléfono cuenta con los últimos avances de la tecnología VoIP, incluyendo amplio soporte para audio, pantalla a color retro iluminada, y un puerto integrado gigabit Ethernet. Puede encargarse de las necesidades telefonía con tráfico significativo para los usuarios que utilizan aplicaciones con gran consumo de ancho de banda de sus PCs. Este teléfono cuenta con una pantalla grande, fácil de leer para facilitar el acceso a la información de comunicación, y aplicativos como fecha y hora, identificación de llamadas, dígitos marcados, e información de presencia. El teléfono provee acceso a dos líneas telefónicas y un amplio soporte para codecs así como servicios de mensajería.

[29] Cisco Unified IP Phone 7945G. Recuperado de: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps8534/product_data_sheet0900aecd8069bb80.html

3.2.5.2. Cisco Unified IP Phone 9971[30]

Es un teléfono de clase ejecutiva que provee telefonía, video, aplicaciones y accesorios. Incluye un puerto gigabit Ethernet para conexión de la pc del usuario, pantalla touchscreen, conectividad WiFi, entre otras. Ofrece la posibilidad de manejar muchos números puede soportar hasta 200 llamadas por dispositivo. Interoperabilidad con el protocolo SIP proporciona control de llamadas y una solida solución de comunicaciones unificadas.

3.3. SERVICIOS DE RED

3.3.1. SERVIDOR DHCP

DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

El servidor DHCP puede ser instalado en varios tipos de equipos como PCs, Routers, switchs. Para este proyecto los equipos designados como *servidores DHCP son el router Cisco 2911* debido a que este equipo es el encargado de proveer de

[30] Cisco Unified IP Phone 9971. Recuperado de: http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10453/ps10512/data_sheet_c78-565717.html

direcciones IP a los teléfonos de la red de esta manera aprovechando la activación de este servicio también se brinda de direcciones IP a equipos de los usuarios que se conecten a la red. Y el *servidor PacketFence* que se encargara de brindar direccionamiento IP a los equipos invitados y no identificados en el entorno inalámbrico

3.3.2. SERVIDOR NTP

NTP (Network Time Protocol) es un protocolo de Internet ampliamente utilizado para transferir el tiempo a través de una red. NTP es normalmente utilizado para sincronizar el tiempo en clientes de red a una hora precisa. El protocolo tiene una estructura jerárquica. Un servidor Stratum 1, es el servidor primario de referencia y se asienta en el más alto nivel de la jerarquía. Este servidor primario está seguido de servidores secundarios de referencia y clientes. Un servidor NTP primario generalmente se sincroniza mediante una referencia externa de reloj, como puede ser un reloj de radio o GPS.

El equipo configurado como ***servidor NTP del laboratorio es el switch de Core*****,** ya que este equipo tiene accesibilidad a todos los equipos de red.

3.3.3. SERVIDOR DE MAQUINAS VIRTUALES

3.3.3.1. VMWare Player[31]

VMware Player es un programa que nos permite de forma sencilla ejecutar varios sistemas operativos a la vez en una sola PC. Este software es gratuito para uso personal. Aprovecha el hardware más nuevo para crear máquinas virtuales hasta con 4 procesadores virtuales, discos virtuales de 2 TB y hasta 64 GB de memoria por máquina virtual. El laboratorio de pruebas utiliza VMWare Player para ejecutar el *servidor FreeNAC* ya que el desarrollador de este producto lo puso a disposición en formato de maquina virtual que debe ejecutarse dentro de computadores con las características necesarias para su funcionamiento.

[31] VMWare Player. Recuperado de:
http://www.vmware.com/latam/products/desktop_virtualization/player/overview.html

3.4. CARACTERÍSTICAS TÉCNICAS DE EQUIPOS

La siguiente tabla muestra la cantidad de equipos utilizados en el laboratorio de la Red del laboratorio de pruebas así como su distribución e identificación dentro del entorno. Los equipos de red como routers y switches fueron montados dentro de un mismo Rack de 2,20 metros anclado al piso por facilidad de conexión. El detalle de la conexión fisca del rack se describe en el siguiente capítulo que trata sobre la implementación del la infraestructura e instalación física de equipos

MARCA	MODELO	CANTIDAD	MNEMONICO	FUNCION
CISCO	WS-C3560G-24TS	1	LAB_SWITCH_CORE	SWITCH CORE
CISCO	WS-C3560G-8PC	1	LAB_SWITCH_5	SWITCH ACCESO
CISCO	WS-C3560G-8PC	1	SW_PRUEBAS	SWITCH ACCESO
CISCO	ROUTER 2911 ISR	1	CME_CW_UIO	Central Telefónica Servidor DHCP
CISCO	IP Phone 7945G	1	N/A	Teléfono Ip del Usuario 1
CISCO	IP Phone 9971	1	N/A	Teléfono Ip del usuario 2
CISCO	AP-1142N	1	AP_LAB	Punto de Acceso Inalambrico
DELL	Latitude E5520	1	FreeNAC_SVR	Servidor NAC FreeNAC
HP	Pavilion DV4-2145DX	1	Server-PF	Servidor NAC Packet Fence
DELL	Optiplex 740	1	Desktop	Usuario1, MAC: 0022.1906.879D
MOTOROLA	Atrix 4 g	1	Celular	Usuario2, MAC: 40FC.8933.899A
SAMSUNG	Galaxy Tab 2	1	Tablet	Usuario3, MAC: F05A.0934.A0B2

Tabla 3.1: Equipos de Laboratorio

MARCA	MODELO	MNEMONICO	FIRMWARE
CISCO	WS-C3560G-24TS	LAB_SWITCH_CORE	c3560-ipservicesk9-mz.122-53.SE1.bin
CISCO	WS-C3560G-8PC	LAB_SWITCH_5	c3560-ipbase-mz.122-50.SE5.bin
CISCO	ROUTER 2911 ISR	CME_CW_UIO	c2900-universalk9-mz.SPA.151-4.M2.bin
CISCO	AP 1142N	AP_LAB	c1140-k9w7-mx.124-21a.JA1/c1140-k9w7-mx.124-21a.JA1
DELL	Latitude E5520	FreeNAC_SVR	Microsft Windows 7 64 bits, Ubuntu LTS 8 320 bits(Virtualizado)
HP	Pavilion DV4-2145DX	Server-PF	Ubuntu LTS 12.04 64 bits

Tabla 3.2: Firmware o Sistema Operativo de equipos de red

3.5. DIRECCIONAMIENTO IP Y ASIGNACIÓN DE VLANs

Todos los equipos que forman parte de la red poseen un número de identificación que sirve para que puedan ser localizados dentro de ella. Para esto se asigna a cada uno de los equipos una dirección IP única y irrepetible dentro del mismo entorno de red, de esta manera el router envía los paquetes de una red origen a una red destino utilizando el protocolo IP.

La gran mayoría de redes actuales agrupa a sus miembros de acuerdo al departamento que pertenecen, de esta manera se limita la comunicación y el acceso que pueden obtener al conectarse a la red. Para lograr este objetivo se necesita crear redes LAN virtuales denominadas VLANs, que no son más que redes de datos más pequeñas que agrupan a miembros en común, por ejemplo, de un mismo departamento, dentro de una misma red física.

Para nuestro proyecto se crearon 9 VLANs las cuales se encuentran detalladas en la siguiente tabla. Con la creación de estas redes virtuales se pretende simular la comunicación de los diferentes departamentos que posee una empresa.

VLAN ID	DEPARTAMENTO O FUNCION DENTRO DE LA RED
6	GESTION DE EQUIPOS
10	SERVIDORES
20	TELEFONIA
30	ADMINISTRATIVO
40	FINACIERO
50	VENTAS
60	SOPORTE
70	RESTRINGIDOS
80	AISLADOS

Tabla 3.3: Asignación de VLANs y su función dentro de la red

Teniendo en cuenta el esquema de VLANs detallado anteriormente asigna a cada una de ellas un segmento de direcciones IP únicas e independientes para cada departamento o función que realizan en la red. Estos segmentos de direcciones de

red originalmente solo pueden comunicarse con equipos que estén dentro de su mismo segmento, es decir, solo existe la comunicación con los miembros de su propio departamento, pero si se requiere de comunicación con otro segmento de red es necesario que un equipo capa tres actué como intermediario entre las dos equipos que desean comunicarse por medio protocolos de enrutamiento. Todas las VLANs tendrán comunicación entre ellas a excepción de las VLANs 70 y 80 que están asignadas a los usuarios invitados que tendrán una permanecía corta en las instalaciones y se les otorga conectividad únicamente a internet luego de haber sido autenticados dentro de los servidores FreeNAC o PacketFence de acuerdo al medio que escojan para su conexión el cual puede ser físico o inalámbrico respectivamente.

El segmento de Red principal que utiliza nuestro laboratorio es:

10.0.0.0/8

Este segmento con máscara de red /8 nos permite tener la posibilidad de tener 2^{24} – 2 usuarios en nuestra red, y 2^{8} – 2 cantidad de redes en los que podemos colocar a estos usuarios. Las subredes designadas a cada VLAN se detallan a continuación, cabe destacar que cada subred posee una máscara de red clase C (/24 = 255.255.255.0) que posibilita que cada una de ellas cuente con 254 direcciones IP libres para usuarios o equipos de red.

VLAN ID	NOMBRE	DIRECCIONAMIENTO IP
6	GESTION DE EQUIPOS	10.6.0.0/24
10	SERVIDORES	10.10.10.0/24
20	TELEFONIA	10.10.20.0/24
30	ADMINISTRATIVO	10.10.30.0/24
40	FINACIERO	10.10.40.0/24
50	VENTAS	10.10.50.0/24
60	SOPORTE TECNICO	10.10.60.0/24
70	RESTRINGIDOS	10.10.70.0/24
80	AISLADOS	10.10.80.0/24

Tabla 3.4: Asignación de segmentos de red por VLAN

La comunicación entre los equipos de la diferentes VLANs y su enrutamiento es responsabilidad del *SWITCH CORE* el cual será el único equipo encargado de esta labor. Dentro de la configuración del CORE se crea una interface virtual por cada VLAN existente en la red, a esta interface se la asigna una dirección IP que por lo general está ubicada entre las primeras o las ultimas de todo el rango y es esta dirección IP la que actúa como puerta de enlace (GATEWAY) para los equipos conectados en su respectiva VLAN, es decir, cada equipo de la VLAN de Ventas por ejemplo, debe tener configurado como Gateway la dirección IP de la interface virtual de la VLAN de ventas creada en el CORE de esta manera podrá comunicarse con otras redes y navegar por internet. Si un equipo no posee Gateway solo podrá comunicarse con equipos dentro de su mismo segmento de red. Las VLANs 70 y 80 poseen como Gateway las direcciones IP del servidor PacketFence ya que este equipo es quien aísla la comunicación de los invitados y equipos desconocidos dentro del entorno de red inalámbrico.

La siguiente tabla detalla las direcciones de IP de cada interface virtual que servirán de Gateways para cada VLAN.

VLAN ID	NOMBRE	GATEWAY
6	GESTION DE EQUIPOS	10.6.0.1
10	SERVIDORES	10.10.10.2
20	TELEFONIA	10.10.20.2
30	ADMINISTRATIVO	10.10.30.1
40	FINACIERO	10.10.40.1
50	VENTAS	10.10.50.1
60	SOPORTE TECNICO	10.10.60.1
70	RESTRINGIDO	10.10.70.10
80	ASILADOS	10.10.80.10

Tabla 3.5: Puertas de Enlace por VLAN en Switch Core

3.5.1. GESTIÓN DE EQUIPOS

Para poder administrar a cada uno de los equipos de networking se designa una VLAN en específico dedicada a esta labor, en nuestro laboratorio designamos a la VLAN 6 (Gestión de Equipos), por lo tanto debemos asignar una dirección IP a cada equipo que pertenece a esta VLAN de esta manera los administradores de red podrán comunicarse a los equipos de forma remota a través de protocolo SSH v2 para mantenimiento y gestión por medio de una red independiente al tráfico de datos y voz presente en la red. Este esquema de gestión no se aplica a los servidores ya que estos equipos pueden pertenecer a una sola VLAN que en este caso es la VLAN 10 (SERVIDORES)

El detalle de las direcciones IP designadas a cada equipo dentro de la VLAN de gestión se describe a continuación.

MARCA	MODELO	MNEMONICO	DIRECCION IP DE ADMISNITRACION
CISCO	WS-C3560G-24TS	LAB_SWITCH_CORE	10.6.0.10
CISCO	WS-C3560G-8PC	LAB_SWITCH_5	10.6.0.25
CISCO	ROUTER 2911 ISR	CME_CW_UIO	10.6.0.51
CISCO	AP_LAB	ACESS POINT	10.10.10.8
CISCO	WS-C3560G-8PC	SWITCH_PRUEBAS	10.6.0.24

Tabla 3.6: Direcciones IP para la Administración de Equipos

3.5.2. RED DE SERVIDORES

Los equipos de red y servidores tienen una VLAN dedicada a la comunicación entre ellos de forma exclusiva (VLAN 10) al realizarlo de esta manera los paquetes de sincronización de red, SNMP, NTP y demás protocolo pueden circular de forma libre sin que sean interferidos por otro tipo de tráfico y sin que los usuarios pueden acceder a ellos, esto se lo realiza por motivos de seguridad. Los únicos usuarios con acceso a la red de servidores son los ubicados en la VLAN 60 (SOPORTE TECNICO) por obvias razones, se restringe el ingreso de otros usuarios por medio de listas de control de acceso.

A diferencia de los equipos de red los servidores realizan su comunicación y administración por una misma interface que en este caso es la VLAN 10.
Se recomienda que los equipos que conforma esta VLAN utilicen asignamiento estático para sus direcciones IP, al hacerlo por medio de un servidor DHCP estas direcciones pueden cambiar cada vez que los equipos reinicien y pueden perder comunicación con los usuarios que tienen aprendida una ruta a una dirección IP única.

La siguiente figura detalla el direccionamiento IP de los equipos dentro de la VLAN SERVIDORES.

MARCA	MODELO	MNEMONICO	DIRECCION IP DE ADMISNITRACION
CISCO	WS-C3560G-24TS	LAB_SWITCH_CORE	10.10.10.2
CISCO	WS-C3560G-8PC	LAB_SWITCH_5	10.10.10.3
CISCO	ROUTER 2911 ISR	CME_CW_UIO	10.10.10.1
CISCO	AIR AP1142N	AP_LAB	10.10.10.8
CISCO	WS-C3560G-8PC	SWITCH_PRUEBAS	10.10.10.9
DELL	Latitude E5520	FreeNAC-SERVER	10.10.10.20
HP	Pavilion DV4-2145DX	Server-PF	10.10.10.10

Tabla 3.7: Direcciones IP para equipos y servidores dentro de la VLAN 10

3.6. DIAGRAMA DE RED

La siguiente figura describe el esquema de conexión de los equipos de red que forman parte del laboratorio de pruebas. Se detalla la función de cada equipo así como su mnemónico, interface física a la que están conectadas para su mejor identificación.

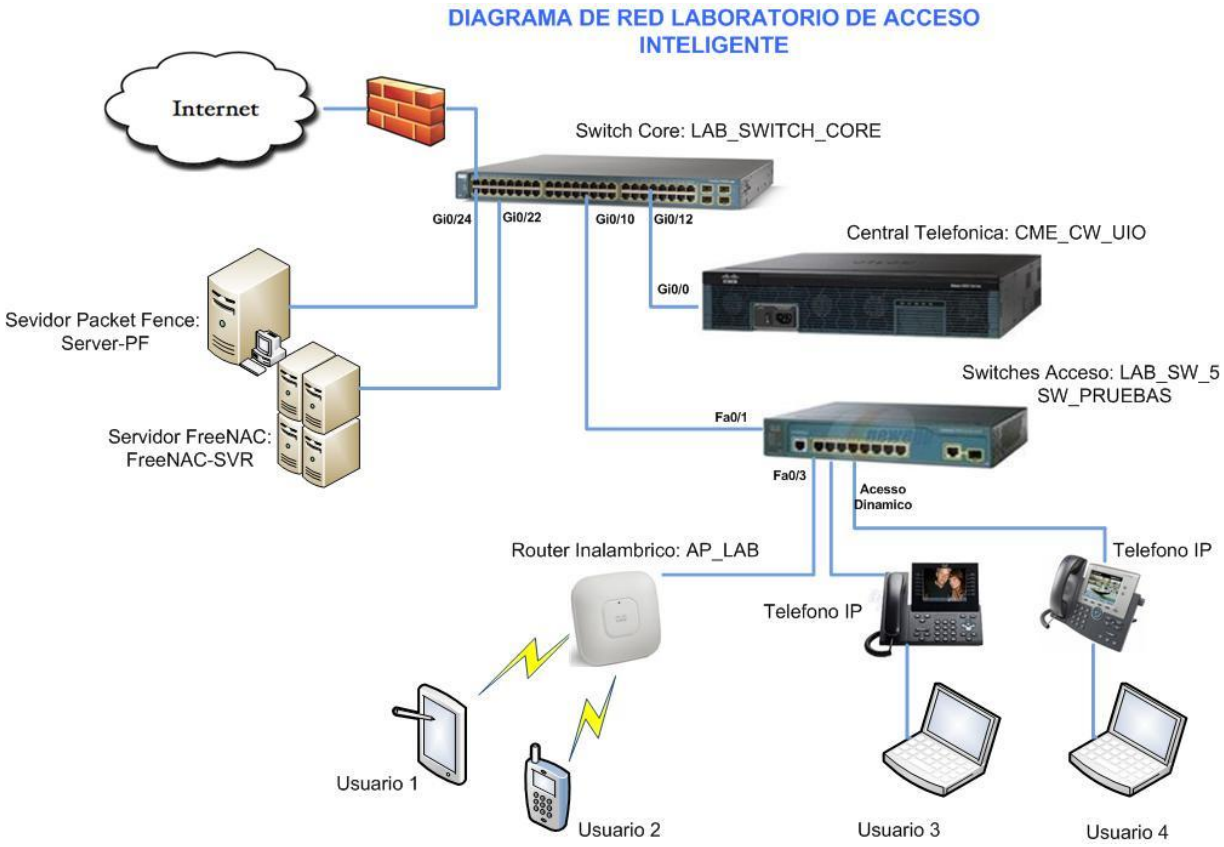

Figura 3.2: Diagrama de Red del Laboratorio de Pruebas

3.7. DISEÑO DE RED FÍSICA

Las pautas seguidas en el diseño de este proyecto fueron detalladas anteriormente en la introducción de este capítulo. Para dar cumplimiento de esas pautas se dispone de los equipos de red que pueden cumplir de forma eficiente los requerimientos de comunicación de cualquier red de pequeña y mediana empresa (PYMES) en donde se desee implementar este sistema de acceso inteligente.

Los equipos utilizados en la plataforma de red son exclusivos de la marca CISCO ya que la empresa COMWARE S.A, en cuyas instalaciones se encuentra instalado el

laboratorio de pruebas, es distribuidor autorizado de esta marca a nivel nacional y autorizó el uso de ellos dentro del ambiente de laboratorio que se encuentra aislado de su estructura de red y pueden ser modificados a voluntad.

Uno de los objetivos de este proyecto es integrar dentro de un entorno de laboratorio los principales equipos y servicios que podemos encontrar en un entorno de red normal, es por este motivo que se integraron servidores DHCP, DNS, servicios de telefonía, acceso a internet, asignación de redes virtuales (VLANs) entre otros como parte operativa del proyecto.

El método de acceso para los equipos y servidores de red se lo realiza de forma estática (asignación manual de dirección IP y VLAN en el switch) de esta manera aseguramos que los equipos tengan la misma dirección IP todo el tiempo a diferencia de los equipos de usuarios que poseen asignación dinámica de dirección IP (Servidor DHCP) y VLAN (protocolo VMPS controlado por FreeNAC) de esta manera los usuarios pueden conectar sus equipos en cualquier lugar de la red y serán dirigidos de forma automática a la VLAN que correspondan. Es de gran importancia destacar que, antes de instalar el servidor FreeNAC, los equipos de red deben contar con soporte del protocolo VMPS. Los equipos CISCO que forman parte de este proyecto cuentan con el soporte de esta función por defecto de acuerdo al firmware instalado en cada uno de ellos, se recomienda leer los datasheets de los equipos para validar el soporte VMPS, si los equipo no soportan este protocolo FreeNAC no puede ser implementado. Si este es el caso se recomienda que PacketFence sea la plataforma que controle el acceso a usuarios inalámbricos y físicos.

3.8. DISEÑO DE RED INALÁMBRICA

Debido a la proliferación de las redes inalámbricas dentro de entornos de red de empresas y hogares dentro de los últimos años es indispensable considerar este escenario dentro del presente proyecto. Las redes inalámbricas brindan grandes facilidades para que los usuarios puedan desarrollar sus actividades casi desde cualquier lugar en cualquier momento e inclusive por medio de sus propios

dispositivos electrónicos no solo de los recursos otorgados por la empresa. Esta gran facilidad también conlleva inherente un gran riesgo y es perder el control de que dispositivos tienen acceso a la red inalámbrica. Las mejores prácticas de seguridad de redes incentivan al usuario a instalar herramientas para monitoreo y control de acceso a los usuarios pero estas herramientas por lo general representan invertir grandes cantidades de dinero y recursos técnicos especializados. Este proyecto se presenta como una alternativa de fácil implementación y económicamente sostenible para cualquier entidad por medio de la utilización de herramientas de software libre de distribución gratuita.

El laboratorio cuenta con dos tipos de redes inalámbricas las cuales cumplen funciones diferentes para la administración de usuarios. En primer lugar se diseña una red inalámbrica dedicada únicamente a albergar usuarios invitados en la red los cuales por lo general no permanecen mucho tiempo en las instalaciones y requieren acceso a internet en su mayoría, ejemplos de estos usuarios invitados pueden ser: asistentes a juntas o reuniones, salas de espera y distracción, proveedores y personal externo que debe realizar trabajos en las entidades por cortos periodos de tiempo, estudiantes, entre otros. Esta red de invitados llevara el nombre de LAB_GUEST y para su acceso el usuario deberá contar con la contraseña entregada por el personal de tecnología. Una vez que el usuario ingresa a esa red, el servidor PacketFence entra en funcionamiento, identificando la dirección MAC del equipo y registrándolo para monitorear sus actividades. Luego que el usuario es registrado será asignado a la VLAN 70 (RESTRINGIDO) al igual que lo realiza FreeNAC con los equipos detectados en la red física, limitando su conexión a esta única red aislando cualquier posibilidad de conexión a otros equipos de red de las diferentes VLANs.

El segundo modelo de red inalámbrica con la que cuenta el laboratorio es la red de usuarios autorizados, la cual ubica al equipo conectada a ella a la VLAN que pertenece luego que el usuario ingrese la contraseña otorgada por el administrador de igual manera que los usuarios invitados. Packetfence detectara que equipos están conectados en la red inalámbrica y si resulta que un usuario no autorizado de

alguna forma consiguió la clave de acceso este será identificado por medio de su dirección MAC y el administrador del sistema puede desconectar al equipo amenazante evitando de esta manera posibles ataques de equipos no autorizados.
Cada una de la VLANs configuradas dentro del ambiente de red puede tener su propia red inalámbrica, para esto es de gran importancia que los equipos de acceso inalámbrico (Access Points) cuenten con la función de radiar diferentes redes desde un mismo equipo característica conocida como múltiple SSID, si el equipo no puede radiar varias redes es recomendable que se configure únicamente la red de invitados y el acceso de usuarios autorizados solo pueda ser controlado de forma física. Por motivos demostrativos se configura la red inalámbrica LAB_SOPORTE la cual está ligada a la VLAN 60 (SOPORTE TECNICO) y brinda acceso a los usuarios autorizados dentro de esta red, de esta manera los usuarios de esta VLAN cuentan con los mismos recursos de red sin importar si el acceso lo realizan de modo físico o inalámbrico.

3.9. SERVIDORES DE CONTROL DE ACCESO A RED (NAC)

Los servidores encargados de esta función dentro de la sistema diseñado en este proyecto son: FreeNAC y PacketFence. A continuación se describe de manera breve las funciones de cada uno de ellos. Una descripción más detallada de sus funciones puede ser encontrada en el Capitulo 4 dentro de la introducción a la instalación de cada plataforma.

FreeNAC es la plataforma encargada de controlar el acceso de todos los usuarios a la red cableada o física y de asignarlos de forma automática a la VLAN que pertenecen sin importar a que switch se conecten a o que puerto, esto se conoce como método de acceso dinámico acción que es realizada por el protocolo VMPS en los equipos Cisco. Para esto FreeNAC posee una base de datos propia que debe ser llenada con las direcciones MAC de los dispositivos de los usuarios autorizados, es decir, de los miembros de la empresa. Estas direcciones de MAC de computadores, teléfonos, cámaras, etc. son relacionadas con una VLAN de acuerdo al lugar en donde ejerzan sus funciones y es asignada al puerto del switch en donde FreeNAC

identifique que el usuario conectó sus equipos facilitando de gran manera la gestión del personal de tecnología y la movilidad para que los usuarios pueden realizar sus actividades en cualquier lugar con conexión física de la empresa.

En el caso que se detecten dispositivos desconocidos conectados a la red física, es decir, equipos de los cuales FreeNAC no posea registros en su base de datos, serán asignados de forma automática a la red de acceso restringido dentro de la VLAN 80 (AISLADOS) limitando el acceso de estos equipos a los recurso de red. Luego cuando el administrador de FreeNAC identifique la dirección MAC del equipo puede otorgarle acceso al puerto a la VLAN correspondiente

PACKETFENCE cumple similares funciones que FreeNAC, pero la diferencia es que esta plataforma administra el acceso de los usuarios conectados a la ***red inalámbrica***. Como se describió anteriormente el laboratorio cuenta con dos tipos de redes inalámbricas: LAB_SOPORTE destinada a brindar conexión a los usuarios que pertenecen a la VLAN 60 (SOPORTE) ingresando la contraseña de acceso y la red LAB_GUEST que se encarga de albergar a los usuarios invitados en la red limitando a través de PacketFence la conexión a internet y monitoreando sus acciones para prevenir posibles ataques. Antes que los invitados tengan acceso a la red, el administrador de PacketFence debe identificar la dirección MAC del equipo y registrarlo en la red, luego de esto el equipo será autorizado para su conexión a la VLAN 70 con acceso restringido.

La configuración detallada de los dos servidores se encuentra dentro del capítulo 4 y su ejemplo de funcionamiento se lo puede encontrar en el capítulo 5 que están desarrollados con bajo estas premisas específicamente.

CAPITULO IV

4. IMPLEMENTACION DEL LABORATORIO DE RED DE PRUEBAS E INTEGRACION DEL SISTEMA DE HERRAMIENTAS NAC DE SOFTWARE LIBRE

4.1. IMPLEMENTACION DE LA RED DE LABORATORIO

4.1.1. INSTALACIÓN FÍSICA DE LOS EQUIPOS

Los equipos de networking (switches, routers) se encuentran instalados dentro de un rack de piso de 2.2 m de altura dentro del data center de la Empresa ComWare S.A el cual provee la alimentación eléctrica y protección de descargas a los equipos. Adicionalmente los equipos de red se interconectan entre sí mediante cableado estructurado de categoría 5e con velocidades de conexión de 100 Mbps a 1 Gbps de acuerdo a las velocidades de transmisión soportadas por los puertos.

La siguiente figura muestra la instalación de los equipos en el rack del laboratorio.

Figura 4.1: Equipos de networking montados en rack

Las conexiones de los equipos de red al switch de Core que se denomina ***Backbone,*** y es la conexión principal por donde viajan los datos que circulan por la red tanto de los usuarios como de los equipos que utilizan protocolos de

comunicación para garantizar la estabilización de la red y su optimo funcionamiento. Estos puertos deben ser configurados en modo troncal para permitir el paso de información de todas la VLANs creadas dentro de la red. La tabla 4.1 detalla los puertos de conexión de backbone.

MNEMONICO	FUNCION	PUERTO DE BACKBONE	PUERTO DE CONEXIÓN EN SW CORE
LAB_SWITCH_5	SWITCH ACCESO	Fa 0/1	Gi 0/10
CME_CW_UIO	Central Telefónica Servidor DHCP	Gi 0/0	Gi 0/12
AP_LAB	Punto de Acceso Inalámbrico	Gi0/0	Fa0/3
Server-PF	Servidor NAC PacketFence	Eth0	Gi0/24
FreeNAC_SVR	Servidor NAC FreeNAC	Eth6	Gi0/22

Tabla 4.1: Puertos de conexión de backbone

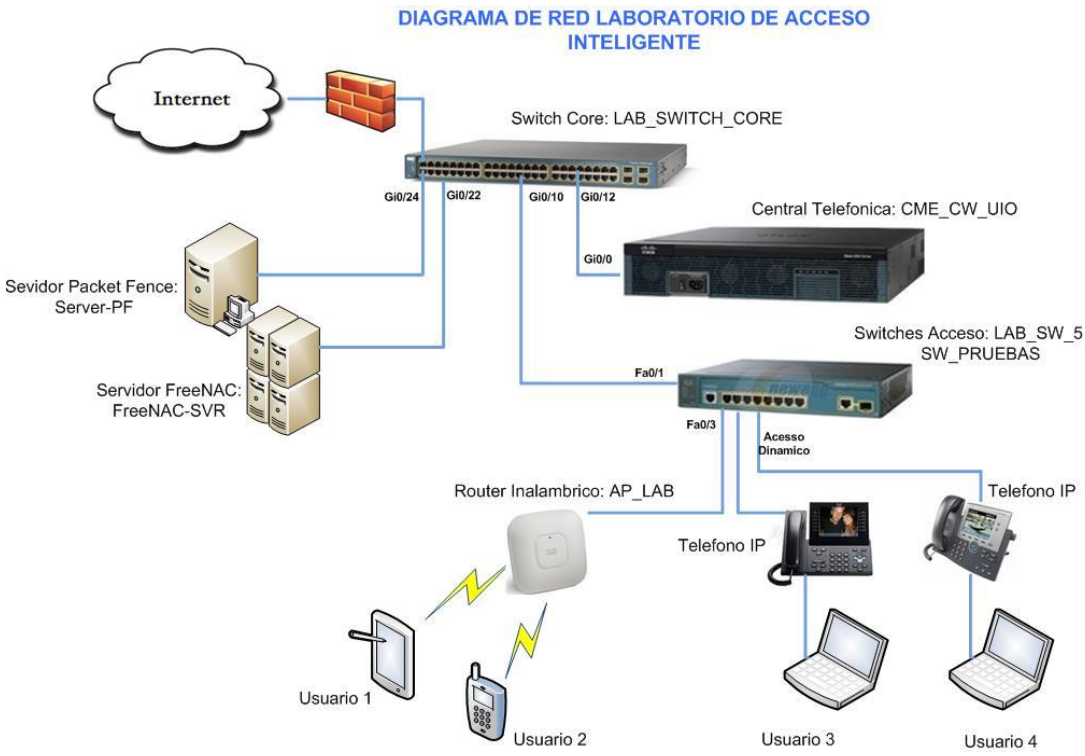

Figura 4.2: Diagrama de red

4.1.2. INGRESO A MODO DE CONFIGURACIÓN DE LOS EQUIPOS CISCO

El modo de configuración de los equipos Cisco es el mismo para los diferentes modelos de equipos presentes en el laboratorio sean estos routers, switches, access points. Facilitando de esta manera la configuración de cada uno de ellos.

Para ingresar al modo de configuración se necesita de un programa cliente de conexiones SSH como Putty, HyperTerminal, SecureCRT, apuntar a la dirección IP de gestión de cada uno de ellos y ejecutar los comandos detallados en las siguientes seccione, el detalle del direccionamiento IP de cada equipos se lo puede encontrar dentro del capítulo 3.

Se recomienda que el personal encargado de configurar los equipos de red tenga experiencia en administrar equipos de tecnología Cisco, aunque este proyecto detalla de gran manera los comandos de configuración y protocolos utilizados en los equipos, no se enfoca en enseñar a operar los equipos de red, este proyecto implica el diseño e implementación de sistemas mixtos de red que se desarrollan con cierto grado de complejidad y deben ser realizados por personal con conocimientos básicos de la materia.

Si la conexión SSH hacia la dirección de gestión de cada equipo es exitosa se mostrara una pantalla con solicitando el ingreso de usuario y contraseña como se muestra en la figura, el detalle de usuarios y contraseñas creados se encuentra más adelante dentro de este mismo capítulo.

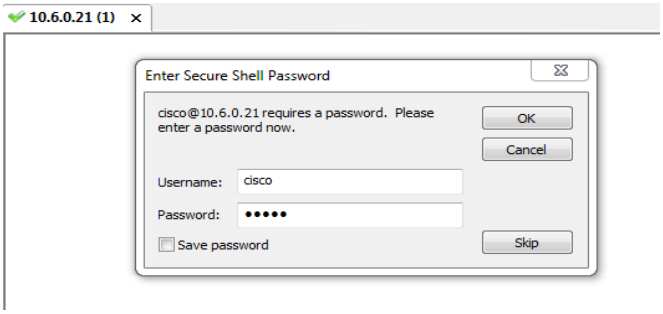

Figura 4.3: Pantalla de ingreso a administración de equipos cisco

Una vez autorizado el ingreso al equipo se deben digitar los siguientes comandos para ingresar en el modo global de configuración el cual puede ser reconocido por que junto al mnemónico presenta los símbolos *(config)* como se aprecia en la siguiente figura.

LAB_SWITCH_5>enable
LAB_SWITCH_5#configure terminal

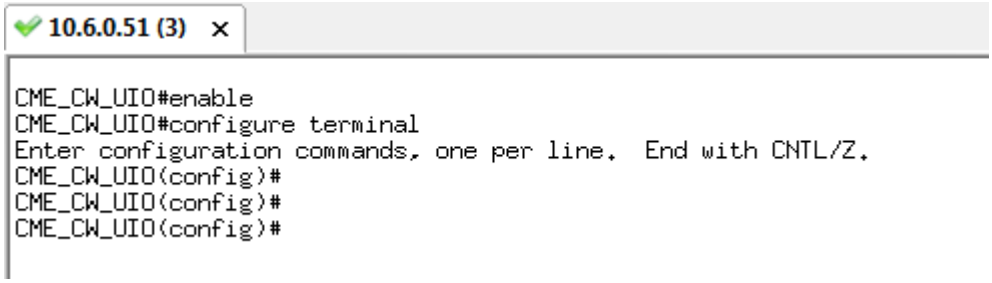

Figura 4.4: Ingreso a modo de configuración Global

4.1.3. CONFIGURACIÓN DE USUARIOS PARA ACCESO REMOTO VÍA SSH, Y CONSOLA

Para la administración remota de los equipos se configura el protocolo SSH en todos los ellos, se deshabilita el acceso vía telnet ya que este es un protocolo inseguro que envía la información del los equipo sin codificar y en texto plano la cual puede ser interceptada por usuarios externos a los administradores. El protocolo SSH corrige estas faltas de seguridad y actualmente es el protocolo más utilizado para conexiones remotas a equipos de red.

Al ser todos equipos del mismo fabricante en este caso CISCO, con versiones de firmware recientes utilizan los mismos comandos de configuración, por este motivo se explica la configuración de modo global aplicable a todos los equipos de red.

4.1.4. CONFIGURACIÓN PROTOCOLO SSH

Para la activación de SSH en los equipos se necesita configurar un dominio de red junto con las llaves de encripcion para autenticación de usuarios. Esto se realiza con los comandos:

CME_CW_UIO(config)#ip domain-name LAB_CW_CISCO
CME_CW_UIO(config)# crypto key generate rsa
CME_CW_UIO(config)#ip ssh authentication-retries 3
CME_CW_UIO(config)#ip ssh time-out 120
CME_CW_UIO(config)#line vty 0 4
CME_CW_UIO(config-line)#transport input ssh

4.1.5. CREACIÓN DE USUARIOS

Por motivos de seguridad se crean cuentas de usuario con nombre y contraseña de esta manera solo estas cuentas pueden realizar cambios en la configuración de los equipos.

Los usuarios creados son los siguientes:

Username	Password
cisco	cisco
comware	comware2013

Tabla 4.2: Nombres de usuarios y contraseñas

Para su creación dentro del modo global de los equipos se ingresa el siguiente comando

LAB_SWITCH_4(config)#username comware privilege 15 password comware2013

4.1.6. CONFIGURACIÓN DE SERVIDOR NTP

El servidor NTP se lo configura para que los eventos sucedidos en los equipos tengan un tiempo específico, es decir, hora y fechas adecuadas que permita al administrador de la red poder identificarlos con mayor facilidad. En el laboratorio, se configura un servidor NTP maestro como reloj de referencia para el resto de equipos, cualquier cambio realizado en este equipo maestro se reflejara de forma inmediata en el resto de equipos.

CME_CW_UIO#conf ter
CME_CW_UIO(config)#clock timezone ec -5
CME_CW_UIO(config)#ntp master

Para verificar la configuración se utilizan los comandos:

CME_CW_UIO#sh clock
CME_CW_UIO#sh ntp status

4.1.7. CONFIGURACIÓN DE VLANs

Los equipos Cisco utilizados en el laboratorio pueden soportar la creación de hasta 1000 VLANs por su versión de sistema operativo, en el laboratorio se configuraron 9 VLANS cuyas funciones fueron detalladas en el capitulo anterior. Los comando de configuración y verificación son los siguientes:

```
LAB_SWITCH_4(config)#vlan 50
LAB_SWITCH_4(config-vlan)#name VENTAS
LAB_SWITCH_4(config-vlan)#
LAB_SWITCH_4(config-vlan)#vlan 60
LAB_SWITCH_4(config-vlan)#name SOPORTE
LAB_SWITCH_4(config-vlan)#
LAB_SWITCH_4(config-vlan)#vlan 70
LAB_SWITCH_4(config-vlan)#name RESTRINGIDOS
LAB_SWITCH_4(config-vlan)#
```

Verificación

```
LAB_SWITCH_4#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/1
6    GESTION                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7
10   SERVIDORES                        active    Fa0/8
20   TELEFONIA                         active
30   ADMINISTRATIVO                    active
40   FINANCIERO                        active
50   VENTAS                            active
60   SOPORTE                           active
70   RESTRINGIDOS                      active
80   AISLADOS                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
LAB_SWITCH_4#
```

4.1.8. CONFIGURACIÓN DE PROTOCOLO SNMP

Este protocolo proviene de las siglas Simple Network Management Protocol (protocolo de administración simple de red) y como su nombre lo indica es el responsable de administrar de forma automática a los equipos que pertenecen a una misma comunidad.

Este protocolo es utilizado por los servidores FreeNAC y PacketFence para enviar comandos de configuración a los switches ya sean para asignar VLANs a los puertos, bloquearlos o activarlos. Los equipos de red también envían peticiones o mensajes de estado a los servidores a través de este protocolo por eso es fundamental que las configuraciones sean las mismas dentro de los equipos de red y servidores sobretodo los nombres de las comunidades de lectura y escritura.

Los siguientes comandos son utilizados para configurar el protocolo SNMP versión 2c en los equipos de red.

```
snmp-server community public RO
snmp-server community private RW
```

Como se puede apreciar en los comandos de configuración los nombres de las comunidades de lectura y escritura son *public y prívate* respectivamente, estos nombres de comunidades deben ser ingresados en los servidores FreeNAC y PacketFence para que puedan administrar a los equipos de red.

4.1.9. CONFIGURACIÓN DE PUERTOS TRONCALES

Son los puertos utilizados por el backbone de la red para conectar a los equipos de red hacia el Core, por estos puertos pueden circular varias VLANs a la vez las cuales deben ser etiquetadas para que el otro extremo puede reconocer desde que VLAN fue originado el paquete. Además de los puertos de conexión de switches, routers y Access point, el servidor PacketFence también necesita una configuración de puerto troncal para su interface de red ya que este servidor debe enviar información de varias VLANs a la vez.

La configuración de puertos troncales se realiza con los comandos:

```
interface FastEthernet0/1
 description TO_PACKETFENCE_SERVER
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

4.1.10.CONFIGURACIÓN DE PUERTOS PARA TELEFONÍA

Los teléfonos IP utilizados en el laboratorio a más de brindar los servicios de telefonía también proveen de un puerto de conexión para los equipos de los usuarios ya sean PCs o Laptops, estos equipos deben conectarse al teléfono y a través de este pueden acceder a la red. Por este motivo el puerto del switch al que se conecta el teléfono debe ser configurado de forma especial para que soporte dos tipos de tráfico: Datos de usuarios y datos de telefonía. Como son datos diferentes y no es conveniente que se mezclen entre ellos, por eso se los debe configurar en dos VLANs diferentes, los datos de telefonía viajan en la VLAN 20 y los datos de usuario viajan en la VLAN que corresponda según su funcion en la empresa

Para diferenciar la VLAN de telefonía de las otras VLANs dentro del puerto al que se va a conectar el teléfono se la agrega el comando:

switchport voice vlan 20

4.1.11.CONFIGURACIÓN DE PUERTO DE ACCESO Y ASIGNACIÓN DINÁMICA DE VLANS

Con la creación de VLANs los usuarios pueden mover sus equipos a cualquier ubicación física de la red y seguir trabajando dentro de la VLAN a la que pertenecen sin ningún problema, pero para lograr que los usuarios sigan perteneciendo a la VLAN que el administrador les asigno es necesario cambiar la configuración de los puertos de los switches de acceso. Esta tarea se realiza de forma manual mediante la técnica de asignación estática de VLANs, basada en puertos, lo cual requiere de tiempo y esfuerzo por parte del administrador cada vez que un usuario es reubicado o cuando un usuario necesita conectarse a la red con su computador portátil desde otra ubicación.

Como solución a esta problemática, se desarrollo una nueva técnica de asignación de VLANs que trabaja de forma automática asignando VLANs a los puertos basándose en la direcciones MAC aprendidas por los switches por medio del protocolo VMPS.

Para el funcionamiento de VLANs dinámicas es necesario configurar a los switchs de acceso y al switch de Core para habilitar las opciones del servidor VMPS. La configuración del servidor VMPS se detalla más adelante en la configuración del servidor FreeNAC.

La mayoría de los puertos del switch de acceso poseen la siguiente configuración, la cual garantiza el acceso de los equipos de telefonía y datos a un mismo puerto.

Donde el comando: *switchport access vlan dynamic,* asegura la asignación dinámica de VLAN por medio del protocolo VMPS.

```
interface FastEthernet0/8
 switchport access vlan dynamic
 switchport mode access
          no switchport nonegotiate
 switchport voice vlan 20
 spanning-tree portfast
```

4.1.12.CONFIGURACIÓN DE SERVIDOR DHCP

Existen dos equipos encargados de brindar el servicio DHCP dentro del laboratorio, uno es el router de telefonía que otorga el servicio DHCP para los equipos con acceso autorizado en la red y el servidor PacketFence otorga direccionamiento IP a los invitados y equipos con acceso restringido. Por lo tanto en la configuración del router de telefonía no se incluye un pool para las VLANs 70 y 80 administradas por PacketFence

Los comandos *excluded-address* son utilizados para seleccionar un rango de direcciones que IP que no pueden ser asignadas a los clientes, este rango de direcciones IP están destinadas a servidores y equipos de red.

Los comandos se repiten para cada red nombrando un pool de acuerdo a la VLAN a la que pertenezca. Los siguientes comandos muestran la configuración para las VLANs de SOPORTE, SERVIDORES y FINANCIERO. Para mayor información, la configuración completa del router está disponible en la sección Anexos.

```
ip dhcp excluded-address 10.10.10.1 10.10.10.25
ip dhcp excluded-address 10.10.20.1 10.10.20.10
ip dhcp excluded-address 10.10.30.1 10.10.30.10
ip dhcp excluded-address 10.10.40.1 10.10.40.10
ip dhcp excluded-address 10.10.50.1 10.10.50.10
ip dhcp excluded-address 10.10.60.1 10.10.60.10
ip dhcp excluded-address 10.10.70.1 10.10.70.10
ip dhcp pool SOPORTE
   network 10.10.60.0 255.255.255.0
   dns-server 10.6.0.1
   default-router 10.10.60.1
ip dhcp pool SERVERS
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.2
   dns-server 10.6.0.1
ip dhcp pool FINANCIERO
   network 10.10.40.0 255.255.255.0
   default-router 10.10.40.1
   dns-server 10.6.0.1
```

4.1.13.CONFIGURACIÓN DE ACCESS POINT PARA RED INALÁMBRICA

El access point de red inalámbrica del laboratorio provee acceso para los equipos móviles (celulares, tabletas, laptops) de los usuarios los cuales deben ser autenticados antes de permitir su acceso a la red. Como se detallo en el capitulo anterior el entorno de laboratorio cuenta con dos tipos de red inalámbrica una denominada LAB_GUEST destinada a brindar conectividad a los invitados y la otra LAB_SOPORTE que es una red modelo que brinda acceso a los usuarios de la VLAN 60 (soporte). La configuración realizada en la red LAB_SOPORTE puede ser replicada para cualquier VLAN que necesite otorgar acceso inalámbrico a sus usuarios. Para acceder a la red inalámbrica el usuario debe conocer la contraseña de acceso, las cuales que se muestran en la siguiente tabla.

NOMBRE (SSID)	VLAN ASIGNADA	CONTRASEÑA
LAB_SOPORTE	60 (SOPORTE)	SOPORTE2013
LAB_GUEST	70 (RESTRINGIDOS)	PUBLICO2013

Tabla 4.3: SSID de red inalámbrica y contraseñas

Nota: La radiación de varias redes inalámbricas desde un mismo access point es una característica propia del modelo de equipo instalado, se recomienda verificar si el modelo de access point seleccionado cumple con esta característica ya que la mayoría de equipos para interiores pueden radiar una sola red a la vez.

El proceso de ingreso al access point es el mismo utilizado en los swiches y los comandos deben ser ingresados en modo de configuración global.

```
dot11 vlan-name RESTRINGIDO vlan 70[32]
dot11 vlan-name SOPORTE vlan 60

dot11 ssid LAB_GUEST[33]
  vlan 70
  authentication open
  authentication key-management wpa
  mbssid guest-mode
  wpa-psk ascii 0 PUBLICO201334[34]
```

[32] Identificacion de Vlans en el AP
[33] Creacion de la red inalámbrica LAB_GUEST
[34] Creacion de la contraseña de acceso para esta red

```
dot11 ssid LAB_SOPORTE
   vlan 60
   authentication open
   authentication key-management wpa
   mbssid guest-mode
   wpa-psk ascii 0 SOPORTE2013

interface Dot11Radio1
 no ip address
 no ip route-cache

 encryption mode ciphers aes-ccm tkip
encryption vlan 60 mode ciphers aes-ccm tkip
 encryption vlan 70 mode ciphers aes-ccm tkip

 ssid LAB_GUEST[35]
 ssid LAB_SOPORTE

interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled

interface Dot11Radio1.60[36]
 encapsulation dot1Q 60
 no ip route-cache
 bridge-group 60
 bridge-group 60 subscriber-loop-control
 bridge-group 60 block-unknown-source
 no bridge-group 60 source-learning
 no bridge-group 60 unicast-flooding
 bridge-group 60 spanning-disabled

interface Dot11Radio1.70
 encapsulation dot1Q 70
 no ip route-cache
 bridge-group 70
 bridge-group 70 subscriber-loop-control
 bridge-group 70 block-unknown-source
 no bridge-group 70 source-learning
 no bridge-group 70 unicast-flooding
 bridge-group 70 spanning-disabled
```

[35] SSID son los nombres de la red que aparecerán en los dispositivos de usuario

[36] Creación de la interface radio para la red de la VLAN 60

```
interface GigabitEthernet0.10[37]
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled

interface GigabitEthernet0.60
 encapsulation dot1Q 60
 no ip route-cache
 bridge-group 60
 no bridge-group 60 source-learning
 bridge-group 60 spanning-disabled
interface GigabitEthernet0.70
 encapsulation dot1Q 70
 no ip route-cache
 bridge-group 70
 no bridge-group 70 source-learning
 bridge-group 70 spanning-disabled

interface BVI1
 ip address 10.10.10.8 255.255.255.0[38]
 no ip route-cache
```

4.2.INSTALACION DE SERVIDOR FreeNAC

4.2.1. INTRODUCCIÓN

La función de FreeNAC dentro de este proyecto es proporcionar acceso automático a los usuarios que se conecten de forma física a la red sin importar en que puerto se conecten o en que switch, el servidor es capaz de reconocer la dirección MAC del computador del usuario y ubicarlo en la VLAN a la que pertenezca y en el caso de no identificar la dirección MAC del equipo, el servidor bloqueara el puerto para que no se produzcan posibles ataques desde dispositivos desconocidos.

Para esto el FreeNAC cuenta con aplicaciones que se encargan de reconocer las direcciones MAC de los equipos conectados en los puertos de los switches a través del protocolo VMPS y de acuerdo a los datos almacenados en su base de datos esta aplicación permite o niega el acceso del equipo a la red de forma automática evitando que el administrador de la red configure el puerto del switch de forma manual cada vez que se conecte un equipo a ellos.

[37] Creación de subinterfaces para el envío de paquetes etiquetados al resto de equipos de red
[38] Dirección IP de administración del access point

El software FreeNAC puede ser instalado de dos maneras: En modo de paquetes disponibles para los sistemas operativos Ubuntu, Debian, SUSE o en modo de maquina virtual que contiene todo el sistema operativo Ubuntu y los paquetes necesarios para ejecutar Freenac sin necesidad de instalar componentes adicionales. Para este proyecto se selecciono como alternativa la instalación el modo maquina virtual. Para su ejecución y funcionamiento se utiliza el software ***VMWare Player*** [39] instalado dentro de un equipo portátil Dell con sistema Operativo Windows 7 64 bits.

A continuación se describen los pasos realizados para la instalación y configuración del software Freenac dentro del modelo de red del laboratorio.

Es de gran importancia destacar que antes de instalar este servidor se debe verificar que los equipos de red soporten el protocolo VMPS para asignar VLANs a puertos del switch de forma automática, ciertas marcas de equipos no soportan esta función.

4.2.2. REQUERIMIENTOS DE HARDWARE:

Para instalar FreeNAC en un entorno de red se necesita al menos los siguientes componentes de Hardware.

- Un servidor Linux o Maquina virtual con FreeNAC instalado que cumpla con las siguientes características:
  - Disco duro con al menos 20G de espacio
  - CPU 2 Ghz
  - Memoria ram de 1GB o superior
- Al menos un switch Cisco, en el cual se conectaran los usuarios. Si no se dispone de equipos cisco se deben instalar equipos que soporten el protocolo ***VMPS*** para asignación dinámica de VLANS
- Un computador instalado con sistema operativo Windows que será el encargado de editar la base de datos instalada en el servidor Linux

[39] WMWare Player: Software de distribución gratuita utilizado para la reproducción de maquinas virtuales, puede ser descargado desde la pagina web del fabricante: http://www.vmware.com/products/player/

4.2.3. INSTALACIÓN DE FreeNAC COMO MAQUINA VIRTUAL (MV)

La versión de FreeNAC Maquina virtual puede ser descargada desde la página Web: http://freenac.net/en/community/downloads

Esta máquina virtual incluye dos bases de datos, una denominada “nacdemo” que contiene una implementación de ejemplo que puede ser usada para motivos demostrativos de la aplicación y la una base de datos vacía denominada “opennac” que esta lista para ser puesta en producción aquí se almacena la información de los usuarios, direcciones MAC, equipos de red, y todos los datos necesarios para el funcionamiento de la aplicación.

- **Pasos de Instalación:**

  1. Instalar el software adecuado para manejar entornos de virtualización de computadores. Por ejemplo: VMWare Workstation, WMWare Player que son las herramientas recomendadas por el fabricante. Para nuestro proyecto se selecciona VMWare Player versión 5.0.2 como alternativa ya que es una aplicación gratuita que no requiere licenciamiento, la parte negativa de la versión gratuita es que no permite editar las características de los equipos virtuales y en ocasiones esto es necesario para adaptar a la maquina virtual a las condiciones de hardware y software del equipo real o anfitrión, por lo que se recomienda utilizar la versión Workstation.

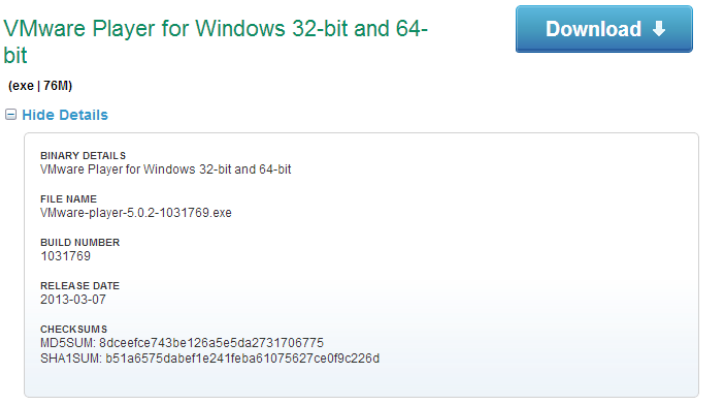

Figura 4.5: VMWare Player versión 5.0.240[40]

[40] Figura : VMWare Player versión 5.0.2. Recuperado de: https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/5_0|PLAYER-502|product_downloads

2. Descargar el archivo FreeNAC VM from SourceForge (aprox. 3Gb) desde la pagina web del desarrolador: http://freenac.net/en/installguide/vminstall
3. Descomprimir el archivo descargado y guardarlo en una carpeta en donde se encuentren las maquinas virtuales utilizadas por VMWare Player.
4. La interface de red de VMWare Player debe ser configurada en modo Bridge con lo cual el equipo virtual tendrá una conexión directa a la red de datos y podrá recibir una dirección IP única en el segmento de servidores y los demás equipos podrán comunicarse con ella de forma directa.

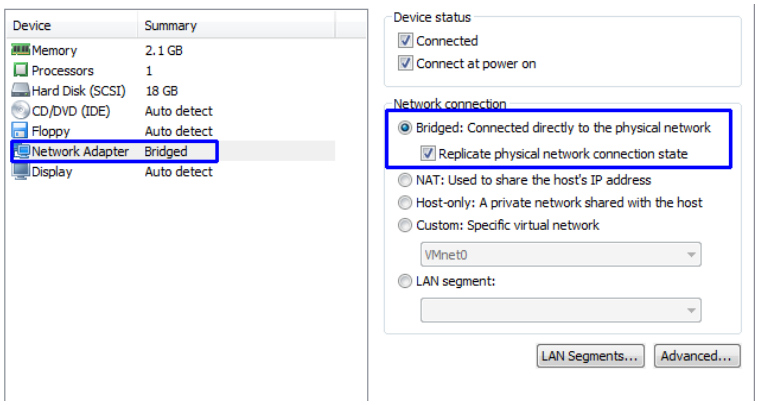

Figura 4.6: Configuración de interface de red MV en modo Bridge

5. En VMWare Player se debe agregar la maquina desde la carpeta en donde fue guardada e iniciarla ignorando los errores. Los nombres de usuario incluidos por defecto son:

Usuario login : freenac Contraseña: freenac

Usuario root: root Contraseña: freenac

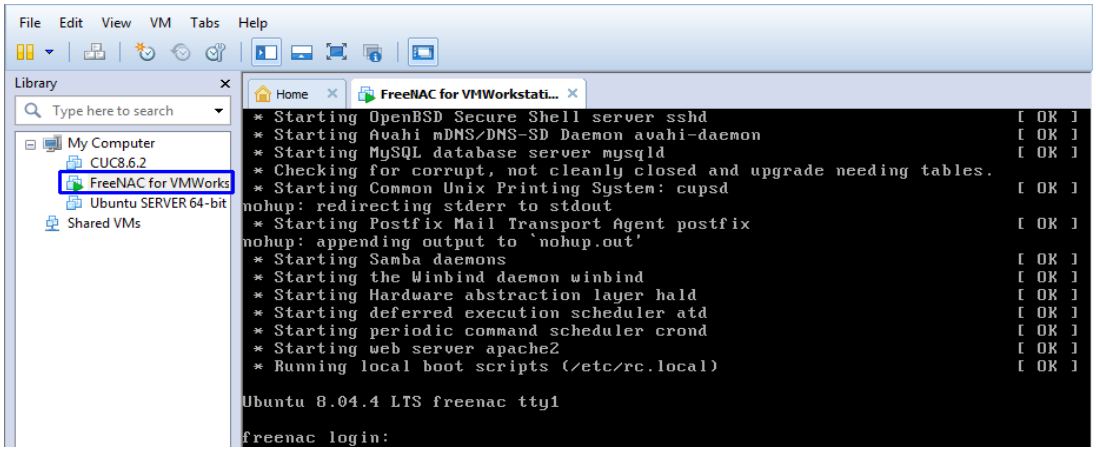

Figura 4.7: Inicio FreeNAC MV dentro de VMWare Player

6. La MV tratara de obtener una dirección IP por medio de DHCP, esto no es recomendable ya que asignación de direcciones IP por medio de este protocolo es variable, es decir, la dirección asignada al servidor FreeNAC puede variar cada vez que el equipo reinicie y los equipos de red necesitan apuntar las solicitudes de asignación de VLANS a una misma dirección cada vez. Por lo que se necesita asignar una dirección estática al servidor. Para realizar esta tarea debemos revisar las interfaces de red que están activadas dentro de la MV y luego editarlas. Para la verificación de las interfaces ingresamos el comando: ***ifconfig –a***

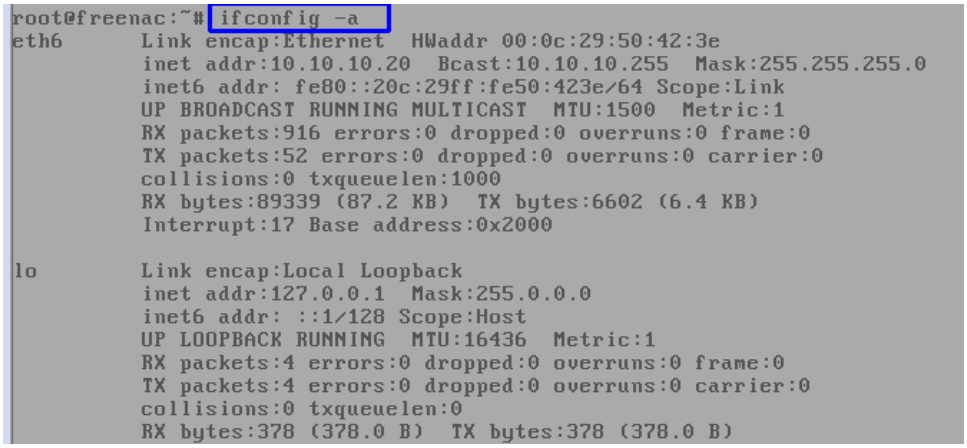

Figura 4.8: verificación de interfaces de FreeNAC

El equipo presenta dos interfaces activas: eth6 y lo. Interface lo (loopback) es una interface virtual activada por defecto por el sistema operativo para resolver procesos internos por lo que no puede ser modificada, por lo tanto las modificaciones de direccionamiento deben ser realizadas dentro de la interface eth6. La edición de la interface de red se realiza al editar el archivo INTERFACES que se encuentra dentro del directorio /etc/network esto se lo realiza con el editor de texto NANO que viene instalado por defecto en Ubuntu.

Nota: antes de realizar ediciones a cualquier archivo se recomienda realizar una copia de respaldo del mismo para evitar posibles problemas de mala configuración.

Para la edición de cualquier archivo de configuración de sistema operativo Linux, el servidor nos solicitara ingresar como super usuario y es aquí donde utilizamos el usuario root con contraseña freenac descrito anteriormente. Para esto ingresamos el comando

sudo bash

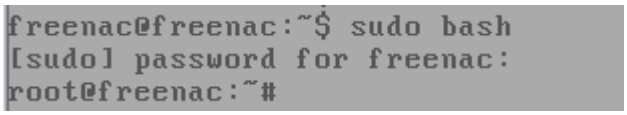

Figura 4.9: Ingreso super usuario

Si el ingreso de la contraseña es correcto el prompt debe cambiar a root@freenac como se muestra en la figura anterior.

La edición de las interfaces de red se realiza con siguiente comando.

nano /etc/network/interfaces

En la línea correspondiente a la interface eth6 se debe reemplazar el modo dynamic por el modo estático (static) y agregar la información IP que se desea configurar para el servidor. Al finalizar se presiona la secuencia de teclas Ctrl+O para guardar los cambios y se reinicia al equipo.

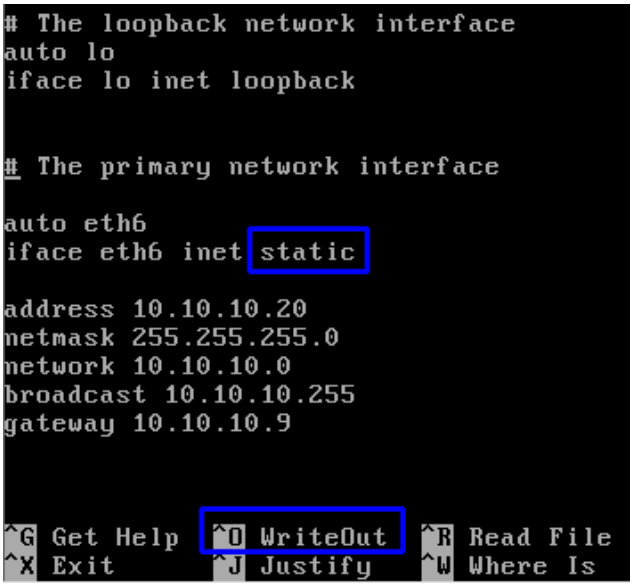

Figura 4.10: edición de interfaces de red

4.2.4. CONFIGURACIÓN DE MYSQL

Mysql viene incorporado dentro de la MV FreeNAC, para asegurarnos que inicie de forma automática al encender el servidor se ingresa el siguiente comando dentro del servidor.

Update-rc.d mysql

Luego se debe agregar una ruta corta hacia la aplicación:

ln –s /var/lib/mysql /mysqldata

Es necesario comparar el archivo **my.cnf** ubicado en **/etc/my.cnf** con el archivo **/opt/nac/contrib/etc/my.cnf**, los cuales deben coincidir en los principales parámetros de funcionamiento que son los siguientes:

Log-bin y report-host, estos archivos deben tener configurado el nombre del servidor que es este caso es **vmps1-bin**

```
log-bin = vmps1-bin
log-warnings
report-host = vmps1
server-id       = 10                    [10 for master, 20 for slave1,
relay-log=vmps1-relay-bin
replicate-do-db= opennac
replicate-wild-ignore-table= opennac.vmpsauth%
```

Figura 4.11: revisión de archivos my.cnf

Se recomienda incrementar los tiempos de conexión para evitar desconexiones por congestion y exceso de tráfico en la red. Para lo cual se agregan las siguientes líneas:

```
interactive_timeout = 604800
wait_timeout = 604800
```

Mysql necesita escuchar las peticiones de la red por el puerto 3306, pero por defecto este está ligado a la interface local de loopback por lo que debemos comentar siguiente línea anteponiendo el signo numeral a ella.

```
#bind-address = 127.0.0.1
```

El usuario mysql debe poder escribir dentro de la base de datos y debemos autorizar esta acción por medio del comando.

```
chown -R mysql /mysqldata /var/lib/mysql
```

Una vez finalizada esta configuración es necesario reiniciar el servicio para que los cambios entren en ejecución.

/etc/init.d/mysql restart

Para verificar que los servicios están iniciando de forma correcta, corremos la aplicación netstat con el comando: ***netstat –anp|grep mysql*** de este modo se puede

visualizar que mysql está escuchando peticiones de cualquier dirección IP (0.0.0.0) en el puerto 3306 y no en la interface loopback (127.0.01)

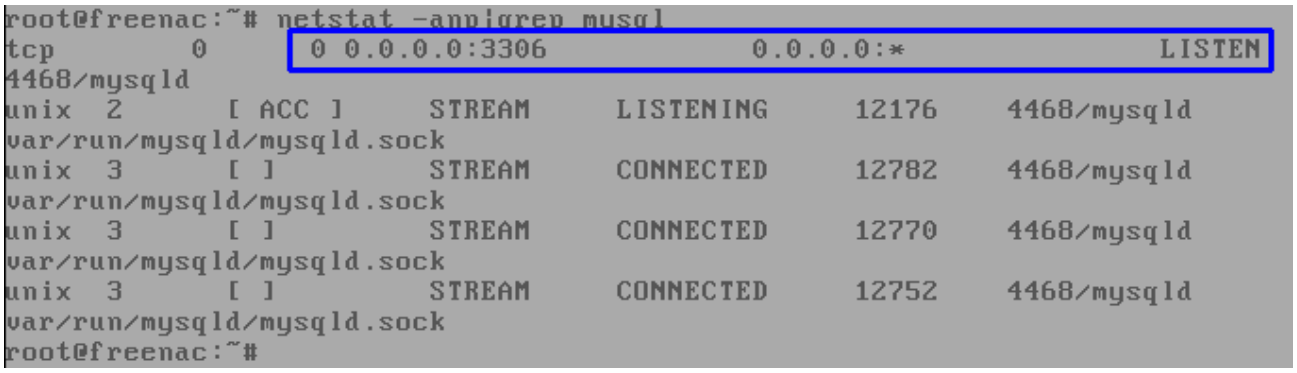

Figura 4.12: verificación de servicios mysql

4.2.5. CONFIGURACIÓN DE DATOS INICIALES DE FreeNAC

A continuación se detallan los pasos seguidos con el propósito de configurar la aplicación FreeNAC e integrarla con Mysql.

- **Extracción de scripts SQL**

```
cd /mysqldata
cp /opt/nac/contrib/opennac_db.tar.gz .
tar xvzf opennac_db.tar.gz
```

- **Creación de Base de Datos inicial (opennac)**

Este en un paso obligatorio en cada instalación nueva de un servidor FreeNAC y consiste en instalar un set inicial de tablas dentro de la base de datos “opennac” que viene vacía por defecto. Se recomienda que los comandos detallados a continuación sean realzados con el usuario root o anteponiendo el prefijo sudo a cada uno de ellos para contar con los permisos de acceso.

cd /mysqldata

cp –R opennac opennac.$$

mysql –u root –p –e “create database opennac”;

mysql –u root –p opennac < tables.sql

mysql –u root –p opennac < values.sql

- **configuración de permisos de base de datos**

La configuración de permisos se realiza dentro de mysql para lo cual debemos ingresar utilizando las credenciales por defectos que son ***User: root password: root***

Se para agregar al usuario "inventwrite" dentro de la plaforma mysql se agregan la siguientes líneas de comando:

```
SET PASSWORD FOR inventwrite@localhost=PASSWORD('NEW_PASSWORD2');
SET PASSWORD FOR inventwrite@'%'=PASSWORD('NEW_PASSWORD1');
```

Nota: El ingreso a la base de datos opennac dentro de mysql es muy frecuente durante instalación y configuración del servidor por lo que se recomienda tener a mano las credenciales de acceso así como los comandos de ingreso. Para este proyecto las credenciales son las siguientes:

Mysql username: ***inventwrite*** *contraseña:* ***NEW_PASSWORD2***

Comando de ingreso a mysql: ***mysql – u inventwrite –p mysql***

- **Configuraciones de mantenimiento**

El mantenimiento de los parámetros de configuración debe ser realizado de forma constante por medio de ejecución de ciertos comandos que mantienen las bases de datos actualizadas. Para esto utilizamos la herramienta *CRON* que se encarga de ejecutar las secuencias de comandos en un determinado tiempo configurado por el usuario.

Los comandos de manteniendo de bases que se ejecutan con CRON y su sintaxis son los siguientes:

```
0 1 * * 1               /opt/nac/bin/purge_unknowns.php
0 6 30  * 1     /usr/bin/mysql -uroot -e "PURGE MASTER LOGS BEFORE DATE_SUB( NOW( ), INTERVAL 30 DAY);"
0   3    * * 1-5 /opt/nac/bin/dump_ports.php
0   3    * * 1   /usr/bin/mysqlhotcopy --allowold --keepold --regexp=".+" /disk2/backups/mysql 2>&1 | logger
```

4.2.6. DEMONIOS FreeNAC

Los demonios son procesos que se ejecutan en segundo plano y sirven para mantener activa una aplicación. FreeNAC, al ser una aplicación que depende de un conjunto de subaplicaciones como por ejemplo: mysql, openvmps, cron, etc necesita

de varios demonios que se ejecuten a la vez y desde el arranque del sistema operativo. Para configurar los demonios de FreeNAC es necesario cumplir con los siguientes pasos:

- **Crear grupo y usuario**

Es necesario crear un usuario de FreeNAC y un grupo al que pertenezca para que el archivo de configuración sea de fácil acceso para demonios de otras sub aplicaciones como Apache, Radius, etc.

```
groupadd freenac && useradd freenac -r -g freenac
```

- **Archivo config.inc**

En los servidores se debe crear un archivo config.inc desde una plantilla y agregar los parámetros de conexión a la base de datos de mysql.

```
  cp /opt/nac/etc/config.inc.template /opt/nac/etc/config.inc
vi /opt/nac/etc/config.inc
```

Luego de esto se debe cambiar el grupo del archivo config.inc y el directorio *lib* a si como sus permisos.

```
chgrp freenac /opt/nac/etc/config.inc
chgrp freenac /opt/nac/lib
chmod 640 /opt/nac/etc/config.inc
chmod -R 640 /opt/nac/lib
```

- **Políticas**

El uso de políticas de conexión provee de gran flexibilidad y encapsulación de decisiones individuales según sea el caso del acceso a la red que se desee. Se debe especificar una política de uso que deben seguir los usuarios, para este proyecto se elige el uso de la política 5 la cual es útil para la mayoría de sitios en donde puede ser implementado este sistema.

```
cd /opt/nac/etc
ln -s policy5.php policy.inc.php
```

- **Inicio del demonio vmps**

Se crea un archivo de arranque y se inicia el servicio

cp /opt/nac/contrib/startup_init.d/vmps /etc/init.d/vmps

chmod 750 /etc/init.d/vmps

update-rc.d vmps defaults

/etc/init.d/vmps start

Monitoreo de eventos:

ps -ef | grep vmps

tail -f /var/log/messages

- **Inicio del demonios postconect**

cp /opt/nac/contrib/startup_init.d/postconnect /etc/init.d/postconnect

chmod 750 /etc/init.d/postconnect

- **Activación para que inicie de forma automática al iniciar el servidor**

update-rc.d postconnect defaults

ejecución y monitoreo de eventos

/etc/init.d/postconnect start

tail -f /var/log/messages

4.2.7. INSTALACIÓN DE LA INTERFACE DE VISUALIZACIÓN GRAFICA DE WINDOWS (WINDOWS GUI)

La interface de visualización grafica de Windows (GUI) es el método principal y recomendado de administración de FreeNAC ya que realiza cambios directamente a la base de datos por medio del usuario administrador

Los archivos que forman parte del GUI pueden ser descargados desde la pagina web del fabricante: http://freenac.net/en/installguide/wingui

- Descargar los archivos Windows GUI que son denominados (vmps.exe y vmps.xml) y guardarlos en una carpeta de fácil acceso.

Figura 4.13: archivos de interface Windows GUI

- El archivo de configuración (vmps.xml) se lo puede modificar por medio de cualquier editor de texto y sus cambios se verán reflejados en el archivo ejecutable (vmps.exe)
- En el archivo vmps.xml se debe ingresar en el campo “mysql server” la dirección ip del servidor FreeNAC. Por defecto la interface GUI espera

conectarse a la base de datos “opennac” la cual inicialmente se encuentra vacía. Esta base será utilizada por FreeNAC para almacenar la información de los usuarios, switches de la red.

- configurar los derechos de usuario GUI: existen dos niveles de autorización/autenticación que deben ser configurados en la interface GUI.
    - Autorización y autenticación MYSQL: la interface GUI utiliza un usuario y contraseñas especificas para conectarse a la base de datos, este usuario es identificado como “mysql user”
    - Identificación y autorización de Windows GUI: la interface GUI toma el usuario de Windows de la computadora en la que se está ejecutando la aplicación a manera de identificativo y utiliza el valor del campo nac_rights para este usuario, este usuario es identificado como “NAC user”

Estos usuarios tienen roles diferentes dentro de la interface por lo que es importante resaltar sus funciones dentro de la plataforma

4.2.8. USUARIO MYSQL (mysql user)

Este usuario es creado como parte de la configuración de MYSQL incluida en la MV y tiene derechos para acceder a varias tablas de forma remota. Por defecto este usuario utiliza el nombre de “inventwrite”. El password de este usuario necesita ser encriptado y almacenado dentro del archivo vmps.xml para que permita el acceso al GUI.

Para guardar los datos de usuario inventwrite y su contraseña se necesita ingresarlos en el campo “auth” del archivo vmps.xml para esto se realizan los siguientes pasos:

- Ejecutar el archivo vmps.exe
- Seleccionar Admin> Encryp User
- Llenar los datos con el nombre de usuario y contraseña, dar click en *generate*. En el caso de este proyecto se utilizan las credenciales:

username: inventwrite y password: NEW_PASSWORD2

- Copiar el valor que aparece en el campo Generated Key y pegarlo en el campo “auth” del archivo vmps.exe
- Salir del GUI (wmps.exe)

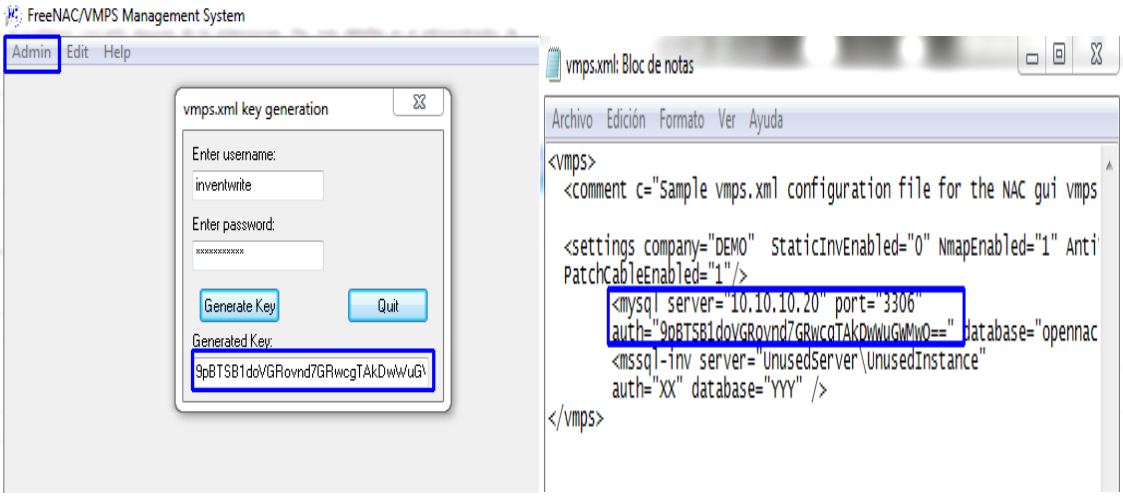

Figura 4.14: Edición de mysql server y msql user para GUI

4.2.9. USUARIO NAC (NAC user)

La interface GUI toma el usuario de la computadora de Windows desde la cual se está ejecutando el archivo vmps.exe y lo utiliza a manera de identificación en el servidor. Dependiendo de los derechos de este nombre de inicio dentro de la tabla “usuarios”, la interface GUI otorgara los derechos de edición de la base de datos.

Por lo tanto el usuario de Windows también debe de existir dentro de la tabla de usuarios de NAC, además este usuario debe tener un nivel de permiso asignado a él. Este nivel de permiso se encuentra dentro del campo “nac_rights” y puede tener tres posibles valores: (1= solo lectura, 2=escritura, 99=administrador).

Si el campo “DemoMode” es 1, y el nombre de la compañía esta identificada como DEMO dentro del archivo vmps.xml (como se puede ver en la imagen anterior) todos los usuarios de Windows serán otorgados derechos de administrador lo cual es optimo para una instalación inicial pero debe ser cambiado este valor de DemoMode a 0 por motivos de seguridad.

Para agregar este usuario se debe ingresar al servidor y dentro mysql digitar el siguiente comando:

mysql>UPDATE users SET nac_rights=1 WHERE username='NombreUsuarioWindows';

4.2.10.UTILIZACIÓN DE LA INTERFACE WINDOWS GUI

Iniciar el archivo GUI (vmps.exe) y presionar conectar. Si los parámetros fueron configurados de forma correcta la interface grafica nos presentara el contenido de la base de datos *opennac* y nos permitirá modificar su contenido además de los parámetros de configuración de FreeNAC.

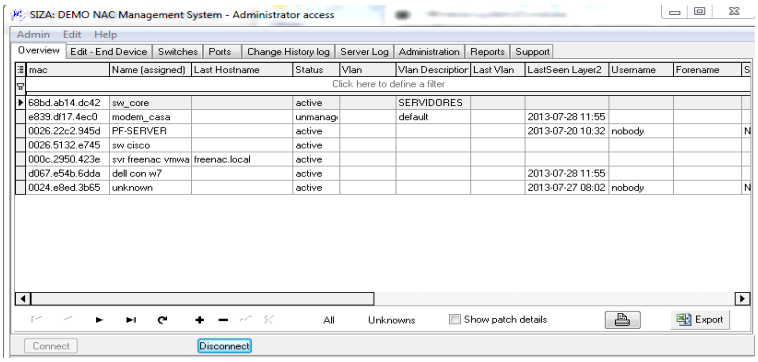

Figura 4.15: Interface grafica de usuario de Windows

Antes de utilizar la interface grafica en su totalidad en necesario agregar los equipos de red como switches y routers en la base de datos.

4.2.11.CONFIGURACIÓN SNMP EN FreeNAC

Los equipos de red deben enviar sus datos al servidor por medio de un protocolo que sea común para los dos equipos este es el caso del protocolo SNMP el cual es utilizado tanto para la transferencia de datos como para realizar modificaciones en la configuración de los equipos de red.

Las comunidades configuradas anteriormente en los switches deben coincidir con las configuradas dentro del archivo config.inc del servidor FreeNAC. El archivo config.inc se encuentra en el directorio /opt/nac/etc y se lo edita con el siguiente comando.

nano /opt/nac/etc/config.inc

```
## SNMP communities
 # $snmp_ro="PASSWORD2";
  $snmp_ro="private";
  $snmp_rw="private";
  $router_ro="private";
```

Figura 4.16: configuración de comunidades SNMP de FreeNAC

4.2.12.INTEGRACIÓN DE SWITCHES

FreeNAC incluye la herramienta *snmp_scan.php* la cual realiza la recolección de información desde los switchs y los guarda en la base de datos *opennac*. La información recolectada de los switches es la siguiente:

- Hardware y versión de software
- Nuevos puertos descubiertos
- Actualización de nombres de puertos, status, perfil de autenticación (VLAN estática, dinámica/vmps o troncal)
- Actualización de la ultima VLAN asignada en el puerto, para puertos estáticos
- Por cada dirección MAC descubierta en los puertos de los switches una nueva entrada se crea en la base de datos y la identifica con el nombre "unknown" (desconocido).

La herramienta solo realiza un escaneo de los switches que poseen el parámetro scan=1 dentro de la tabla *switch* y tener la opción *snmp_dryun* con valor 0.

Para agregar a los switches miembros de la red por primera vez se necesita ingresarlos de forma manual dentro de la tabla *"switch"* de la base de datos "*opennac*" para esto ingresamos a la aplicación Mysql y los ingresamos con los comandos INSERT y UPDATE.

mysql -u invetwrite -p mysql
mysql> use opennac;
mysql< INSERT INTO switch SET ip='10.10.10.2', name='SW_Core', location='1';
mysql> UPDATE switch SET scan='1' WHERE ip='10.10.10.2';

Se repite este procedimiento por cada equipo en la red.

Luego de ingresar los equipos a la base de datos se necesita iniciar la herramienta de escaneo de equipos para actualizar la información proveniente de los equipos. Para esto realizamos los siguientes comandos:

cd /opt/nac/bin
./snmp_scan.php

Nota: realizar este escaneo cada vez que se agregue un nuevo equipo a la red.

El tiempo que tarda esta aplicación en censar los equipos de red a través del protocolo SNMP depende de la cantidad de equipos de networking existentes en la misma. Si la aplicación tarda demasiado o presenta errores quiere decir que hay errores en las comunidades SNMP configuradas en ambos equipos por lo que deben ser revisadas nuevamente.

Para que este monitoreo se ejecute con regularidad utilizamos la herramienta CRON y ejecutamos un comando para que el monitoreo SNMP se realice cada dia a la 11:15 am por ejemplo.

3 11 * * 1-5 /opt/nac/bin/snmp_scan.php | logger

Luego de agregados los switches a la base de datos y si no hay problema con las comunidades SNMP estos podrán ser visualizados en la interface GUI de Windows como se ve en la siguiente figura y aquí podrán ser administrados directamente a través de esta misma interface. El proyecto cuenta con tres switches según lo detallado en el diagrama de red del capítulo 3 y estos pueden ser visualizados dentro del GUI Windows de FreeNAC.

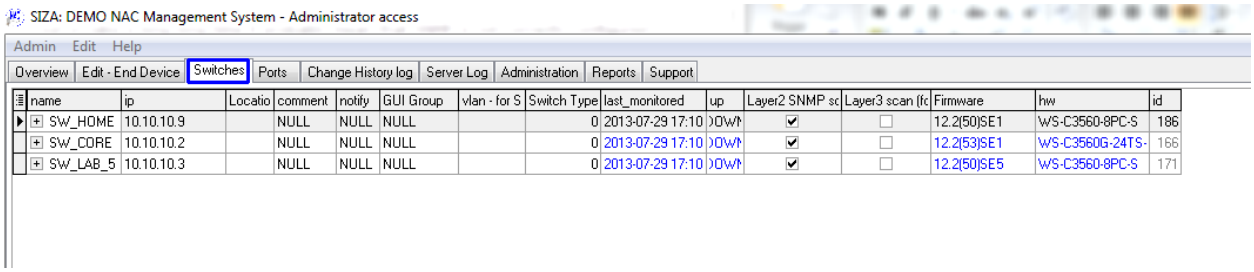

Figura 4.17: integración de Switches dentro GUI

4.2.13.FUNCIONES DE LOS SWITCHES DENTRO DEL SISTEMA DE RED INTELIGENTE

Una vez ingresados los switches de forma exitosa a FreeNAC ya es posible administrarlos. Las tareas más importantes que los switches deben cumplir dentro del sistema de red inteligente son las siguientes:

- **Control de puertos**

FreeNAC debe ser capaz de controlar a los switches de forma remota y tomar acciones correctivas de ser el caso si identifica usuarios desconocidos conectados

en sus puertos. Por este motivo es primordial que las comunidades y versiones del protocolo SNMP coincidan tanto en switches como en el archivo config.inc (nano /opt/nac/etc/config.inc) ya que por medio de la comunidad de escritura SNMP ($snmp_rw) el servidor enviara los comandos al switch para que este permita, bloquee o apague los puertos ante la identificación de amenazas o en su defecto asigne al puerto en la VLAN correspondiente si identifica a un usuario registrado y autorizado en la base de datos.

Las acciones que puede ejercer el servidor sobre los puertos del switch son las siguientes:

Restart: reinicio de puerto

Clear_mac: borrado de direcciones mac registradas en el puerto para poder aprender nuevas

Shutdown: apagado del puerto

Asignacion: dinámica o estática de VLANs

Estas acciones son realizadas por medio del proceso ***cron_restart_port.php*** por lo por lo que se recomienda que se realice con frecuencia utilizando una vez más la herramienta CRON y el siguiente comando para ejecutarlo cada minuto

**** * * * * /opt/nac/bin/cron_restart_port.php***

- **Requerimientos VMPS**

La función principal de FreeNAC es contestar los requerimientos VMPS con tramas de permitir (ALLOW) o denegar (DENY) a los equipos que se conecten a los switches y ubicarlos en la VLAN que corresponda según su autorización en la base de datos. Estas respuestas se realizan por medio del demonio ***vmpsd_external*** en concordancia con la política establecida para la red.

Dentro de los switches de red se deben configurar ciertos parámetros de forma manual vía telnet o ssh para que los requerimientos VMPS que originan sean enviados de forma correcta al servidor FreeNAC.

A continuación de detalla la configuración realiza en los switches de red para que soporten el protocolo VMPS.

4.2.14.CONFIGURACIÓN DE LOS SWITCHES PARA ACTIVAR EL PROTOCOLO VMPS

Esta sección pretende explicar cómo configurar los switches para que trabajen con el protocolo VMPS en los puertos de conexión de usuarios.

La configuración completa de los switches del laboratorio se adjunta en la sección de Anexos y puede ser analizada con mayor detalle. En esta sección solo se hará énfasis en el protocolo VMPS y los parámetros que influyen en su funcionamiento.

4.2.15.PARÁMETROS VMPS

- **VLANs**

Los nombres y números de VLANs deben ser configurados en los switches de forma **exacta** a ingresados en la tabla "*VLAN*" en FreeNAC. Este es uno de los pasos primordiales de la integración y debe ser realizado de forma **manual** en ambos equipos. FreeNAC no puede leer ni escribir VLANs en los switches.

En la siguiente figura se puede visualizar el detalle de las VLANS configuradas en los Switches y en la tabla *VLAN* de FreeNAC.

```
SW_PRUEBAS#
SW_PRUEBAS#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Gi0/1
6    GESTION                          active
10   SERVIDORES                       active    Fa0/8
20   TELEFONIA                        active
30   ADMINISTRATIVO                   active
40   FINANCIERO                       active
50   VENTAS                           active
60   SOPORTE                          active
70   RESTRINGIDO                      active
80   AISLADOS                         active
```

Figura 4.18: Nombres y números de VLANs configuradas dentro del switch

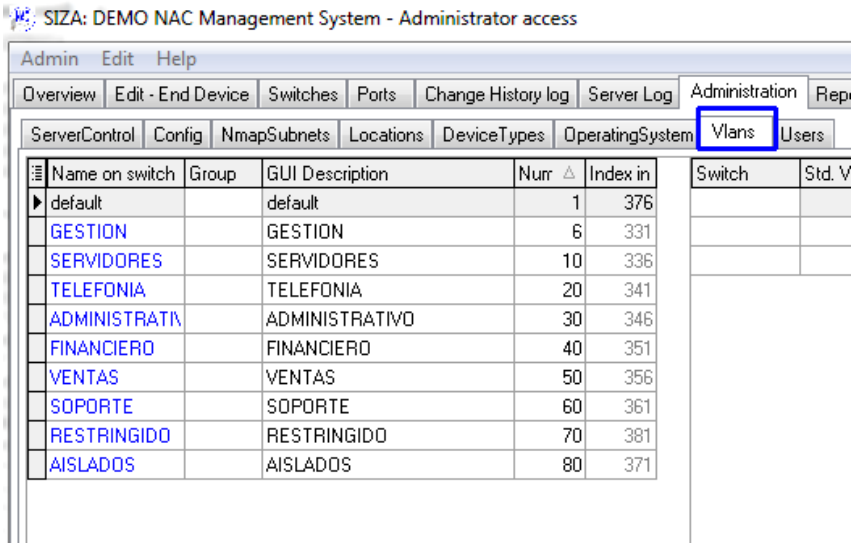

Figura 4.19: Nombres y números de VLANs configuradas dentro de FreeNAC

Nota: Si por equivocación los nombres o números de VLANS no concuerdan entre equipos al momento que FreeNAC envíe los paquetes de respuesta con la VLAN que pertenece la dirección MAC del cliente, el switch no sabrá en que VLAN ubicarlo y el puerto permanecerá en estado bloqueado.

- **Configuración de Servidor VMPS en switch**

Los siguientes comandos deber ser ingresados de forma manual en el switch en orden que switch apunte las solicitudes VMPS a la dirección IP del servidor FreeNAC que para nuestro caso es 10.10.10.20, el detalle de direcciones IP y equipos de red puede ser revisado en el capítulo 3.

Dentro del switch agregamos los siguientes comandos:

```
SW_PRUEBAS#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SW_PRUEBAS(config)#vmps reconfirm 120
SW_PRUEBAS(config)#vmps retry 5
SW_PRUEBAS(config)#vmps server 10.10.10.20 primary
SW_PRUEBAS(config)#
```

Figura 4.20: configuración de servidor VMPS en Switch Cisco

Vmps reconfirm 120: el switch re autenticara la conexión con el servidor cada 120 minutos

Vmps retry 5: número de veces que el switch intente contactar al servidor FreeNAC antes de presentar un mensaje de error de conexión.

Vmps server 10.10.10.20 primary: dirección IP del servidor FreeNAC

Verificación de configuración: ***show vmps***

```
SW_PRUEBAS#sh vmps
VQP Client Status:
-------------------
VMPS VQP Version:   1
Reconfirm Interval: 120 min
Server Retry Count: 5
VMPS domain server: 10.10.10.20 (primary, current)

Reconfirmation status
---------------------
VMPS Action:         No Dynamic Port
SW_PRUEBAS#
```

Figura 4.21: confirmación de configuración VMPS en Switch

Una vez verificada la configuración del protocolo VMPS en el switch se debe re autenticar las conexiones actuales y vaciar la tabla de direcciones MAC para esto dentro del switch se ingresan los siguientes comandos la primera vez se realiza esta configuración luego no se los requiere porque FreeNAC se encarga de realizarlos de forma periódica.

```
SW_PRUEBAS#
SW_PRUEBAS#vmps reconfirm
SW_PRUEBAS#clear mac-address-table dynamic
```

Figura 4.22: re autenticación de conexiones y borrado de tablas MAC en switches

- **Habilitación de VMPS en puertos de Usuario**

Esta configuración debe ser repetida en cada puerto del switch que sea destinado para conexión de usuarios finales. La siguiente figura muestra la configuración del puerto fa0/5 del switch “PRUEBAS” la cual está destinada a la conexión de un usuario en modo de acceso de VLAN dinámico.

```
SW_PRUEBAS(config)#
SW_PRUEBAS(config)#interface FastEthernet0/5
SW_PRUEBAS(config-if)# switchport access vlan dynamic
SW_PRUEBAS(config-if)# switchport mode access
SW_PRUEBAS(config-if)# spanning-tree portfast
SW_PRUEBAS(config-if)#
```

Figura 4.23: configuración de puerto de switch para acceso dinámico de usuario.

spanning-tree portfast: es un comando opcional configurado en los puertos destinados a computadores para mejorar el tiempo de inicio de transferencia de datos en la red al activar el puerto.

Nota: esta configuración debe ser aplicada ***UNICAMENTE*** en los puertos de conexión de computadores o teléfonos de usuarios finales, no en puertos que conecten otros dispositivos de red como routers, servidores, access points, impresoras, etc. En estos puertos se recomienda una configuración estática realizada de forma manual por parte del administrador como se aprecia en la siguiente figura.

En este caso la interface 0/8 está conectada al servidor FREENAC y se asume que este equipo no será desconectado de la red por lo cual no es necesario otorgar acceso de forma dinámica, por lo tanto, se reemplazo el comando ***switchport Access vlan dynamic*** por una configuración estática en la vlan 10 (SERVIDORES) que no cambiara independientemente de que equipo se conecte en este puerto.

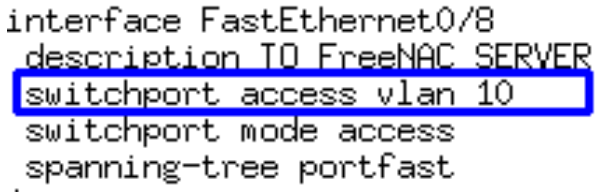

Figura 4.24: configuración de puerto de switch para acceso estático de servidor.

Un ejemplo de funcionamiento y verificación de la asignación dinámica de puertos del switch por parte de FreeNAC se puede observar en capitulo 5 que está dedicado a probar el sistema, monitorearlo y brindar pautas para la solución de problemas.

4.3.INSTALACION PACKETFENCE[41]

4.3.1. INTRODUCCIÓN

PacketFence es una herramienta Open Source de distribución gratuita que ofrece funciones de control de acceso a red (NAC) similares a FreeNAC con la ventaja que puede llevar control de los dispositivos inalámbricos que intentan acceder a la red y siendo esta la función que va a realizar PacketFence dentro de este proyecto.

[41] PacketFence – Overview. Recuperado de http://www.packetfence.org/about/overview.html

PacketFence provee gran cantidad de funciones para controlar el acceso de usuarios y controlar la actividad de la red generando reportes, alertas, políticas, detección de anomalías y más. Por lo tanto su implementación completa dentro de cualquier entorno de red representa un nuevo proyecto independiente. Para el laboratorio limitamos la funcionalidad de PacketFence exclusivamente a la administración del entorno inalámbrico (RED WIRELESS) ya que el entorno físico lo administra FreeNAC, por este motivo no todas las opciones de PacketFence estarán configuradas a excepción de las que tengan relación con el entorno inalámbrico.

Una vez explicada la funcionalidad y alcance de PacketFence dentro del sistema de red inteligente, las siguientes secciones detallan los pasos empleados para su instalación y configuración inicial.

La demostración de funcionamiento de PacketFence así como pautas para solventar problemas de configuración y funcionamiento puede encontrase en el capítulo 5.

4.3.2. REQUERIMIENTOS DE HARDWARE

Los requerimientos mínimos de hardware que requiere PacketFence para su implementación son los siguientes:

- Cpu Intel o AMD de 3Ghz
- 4 Gb de memoria RAM
- 100 GB de espacio de disco
- 1 interface de red

4.3.3. REQUERIMIENTOS DE SOFTWARE

El servidor packet fence soporta los siguientes sistemas operativos en arquitecturas de 32 o 64 bits.

- Red Hat Enterprise Linux 6.X server
- Community Enterprise Operating System (CentOS) 6.x
- Debian 7.0 (wheezy)
- Ubuntu 12.04LTS Desktop

Aunque PacketFence (PF) puede ser descargado en formato de maquina virtual con todos los servicios incorporados para ser ejecutado en VMWare player al igual que

FreeNAC, esta opción no es la más recomendada ya que PF utiliza configuraciones de interface de red en modo troncal y esta función tiene limitaciones en VMWare Player.

En este proyecto PacketFence es instalado en un servidor que cumple con las características de hardware y software solicitadas y detalladas a continuación:

Marca: HP

Modelo: Pavillion DV4-2145

Procesador AMD 2.4 Ghz CPU dual core (4.8 Ghz en total)

Memoria RAM 4GB

Disco Duro de 320GB

Sistema Operativo: Ubuntu 12.04 LTS Desktop de 64 bits.

Una vez instalado el sistema operativo Ubuntu y antes de instalar PacketFence se recomienda actualizar las librerías y programas instalados para esto ingresamos a través de terminal iniciando sesión de usuario root y ejecutamos los siguientes comandos:

sudo bash
Password: admin
apt-get update $$ apt-get upgrade

Además se recomienda instalar los siguientes repositorios y herramientas de red:

sudo apt-get install ubuntu-restricted-extras
sudo -E wget --output-document=/etc/apt/sources.list.d/medibuntu.list http://www.medibuntu.org/sources.list.d/$(lsb_release -cs).list && sudo apt-get --quiet update && sudo apt-get --yes --quiet --allow-unauthenticated install medibuntu-keyring && sudo apt-get --quiet update
sudo apt-get install app-install-data-medibuntu apport-hooks-medibuntu

sudo apt-get install vlan: Aplicación que permite al servidor Ubuntu soportar configuraciones de interface de red en modo troncal

sudo apt-get install nmap: Herramienta utilizada para visualizar los puertos abiertos de un servicio

4.3.4. INSTALACIÓN DE PAQUETES PACKETFENCE EN UBUNTU

Luego de actualizar el sistema operativo, para utilizar el repositorio de descarga se debe agregarlo a la lista de repositorios que utiliza Ubuntu. Se debe editar el archivo de repositorios con el siguiente comando:

nano /etc/apt/sources.list

y agregamos la línea:

deb http://inverse.ca/downloads/PacketFence/ubuntu precise precise

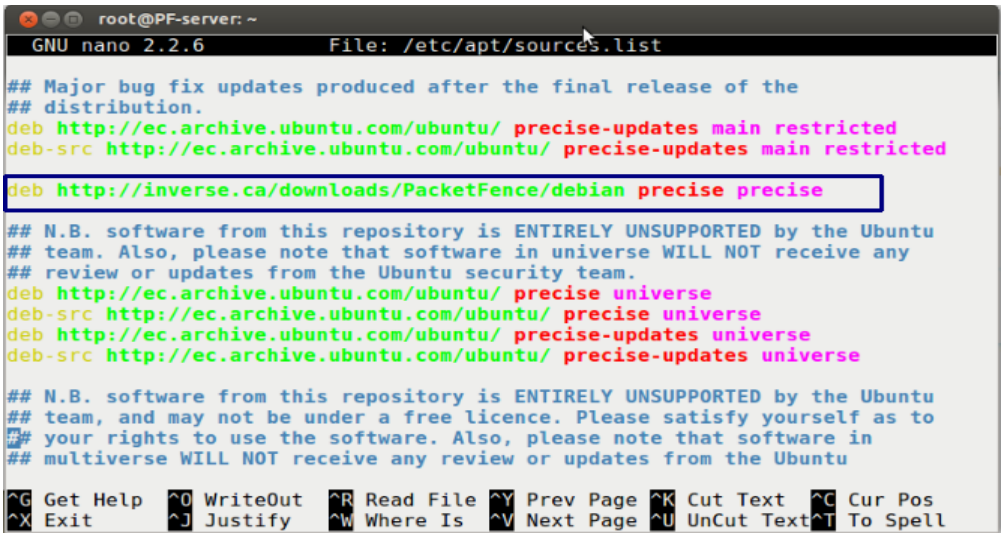

Figura 4.25: modificación de repositorios de Ubuntu

De esta manera Ubuntu ya conoce un camino para poder buscar el software de PacketFence.

A continuación se descarga e instala Packetfence con todas sus dependencias y servicios requeridos (Servidor DNS, servidor Mysql, servidor DHCP, servidor Radius) digitando en terminal:

sudo apt-key adv --keyserver keys.gnupg.net --recv-key 0x810273C4
sudo apt-get update
sudo apt-get install packetfence

4.3.5. CONFIGURACIÓN INICIAL

Es la configuración realizada para que PacketFence pueda iniciar sus servicios dentro de la Red. Los servicios utilizados por PacketFence son Mysql, Apache, DHCP, FreeRadius que fueron instalados por defecto desde el repositorio.

Como se menciono en la introducción de esta sección PacketFence necesita de interfaces de red configuradas en modo troncal que soporten el envío de paquetes etiquetados con varias VLANs a la vez. Por este motivo la configuración del sistema operativo debe soportar la creación de VLANs y editar las características de la interface de red gracias a la herramienta *vlan* instalada con anterioridad solo se debe editar el archivo de interfaces de la siguiente manera:

nano /etc/network/interfaces

Se agrega los parámetros de red con los que vamos a trabajar en el servidor:

IP del Servidor PacketFence: 10.10.10.10/24 en la VLAN 10

IP Gateway de invitados wireless: 10.10.70.10 en la VLAN 70

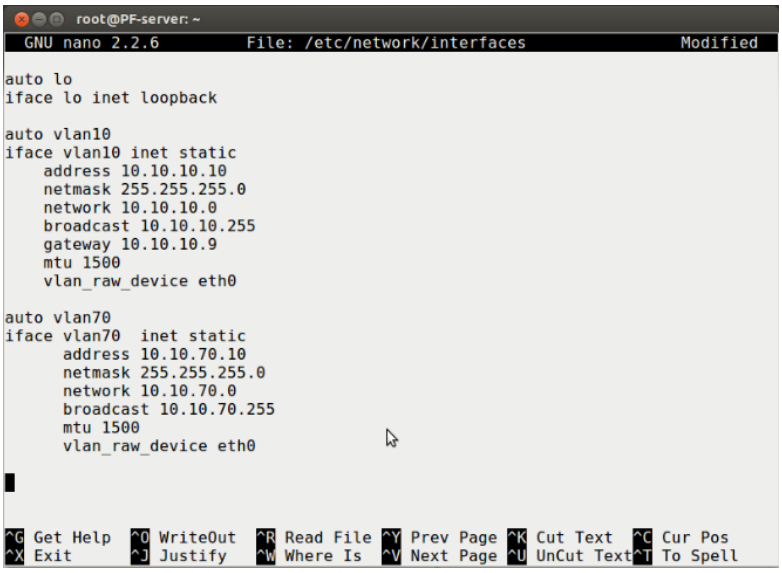

Figura 4.26: configuración de interface de red en modo troncal

Para que los cambios surtan efecto se recomienda reiniciar el servicio con el comando:

nano /etc/init.d/networking restart o reiniciar el servidor en su defecto. Para verificar que los cambios fueron implementados con éxitos se ejecuta el comando: ***ifconfig*** y se debe visualizar las interfaces VLAN con las IP creadas.

Para que el servidor PAcketFence tenga acceso a la red se debe confiruar el puerto del Switch en donde será conectado el servidor con los siguientes comandos:

```
Configure terminal
interface FastEthernet0/1
 description TO_PACKETFENCE_SERVER
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

De esta manera el servidor PF debe integrarse al entorno de red sin mayor inconveniente, se recomienda realizar pings de prueba a la interface de administración del SW Core (10.10.10.2) y viceversa para verificar la conectividad de ambos equipos.

4.3.6. PASOS DE CONFIGURACIÓN DEL SERVIDOR

Abrir un navegador dentro del mismo equipo Ubuntu apuntando a la siguiente dirección:

https://10.10.10.10:1443/configurator

- **Paso 1: Ejecución**

El primer y más importante de los pasos de configuración es este ya que aquí se escogerá el tipo de implementación q puede ser por VLANs o INLINE (con equipos de red en capa 2 que no permiten el ruteo de paquetes). La opción seleccionada en este paso influenciara los siguientes pasos de la configuración. El laboratorio posee equipos Cisco capa 3 por lo tanto se selecciona el método de configuración por VLAN como se muestra en la figura.

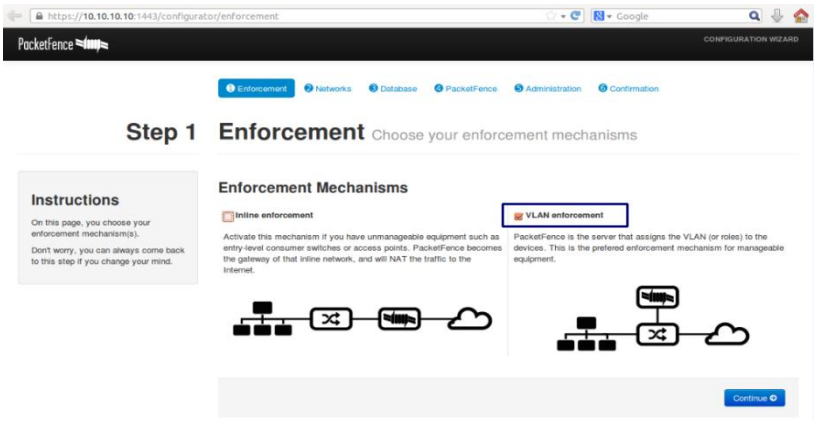

Figura 4.27: Paso 1 de configuración PacketFence

- **Paso 2: Redes**

Este paso trata sobre la configuración estática de las interfaces de red. De acuerdo a la opción seleccionada en el paso 1 aparecerá un listado de las interfaces de red activas en el servidor para nuestro caso serán las interfaces VLAN 10, 70 y 80. En esta pantalla se debe definir tres tipos de interfaces: *Administración (management), Registro (registration) y aislamiento (isolation).*

Solo se puede seleccionar una interface de mantenimiento (VLAN 10: 10.10.10.10) destinada a la comunicación con los equipos de red y administración de plataforma.

La interface de registro (VLAN 70: 10.10.70.10) sirve para monitorear los usuarios conectados a la red inalámbrica. La VLAN 70 denominada RESTRINGIDA en los switches fue creada con la finalidad de albergar a los usuarios invitados en la red que permanecerán dentro de un corto periodo de tiempo en las instalaciones. Esta VLAN cumple con la función de restringir el acceso de los usuarios invitados que se conecten ya sea via cableada o inalámbrica impidiendo que tengan comunicación con los diferentes equipos de red y su único vínculo de comunicación es hacia el internet y hacia los servidores FreeNAC y PacketFence que controlan a estos usuarios.

La VLAN 80 (AISLADOS) es la encargada de ubicar a los equipos que infringen las políticas de seguridad configuradas en PacketFence como por ejemplo: limite de ancho de banda, falta de parches instalados en sus sistemas operativos, falta de antivirus, direcciones MAC definidas como atacantes anteriores, equipos que utilizan programas malware, entre otros. Como se indico en la introducción de esta sección, la configuración integra de PacketFence requiere varios pasos adicionales y agregar más paquetes extra que en conjunto fácilmente puede abarcar un nuevo proyecto independiente, es por este motivo que en el proyecto actual la función de PacketFence es registrar y monitorear a los usuarios invitados conectados en la red inalámbrica la función de la VLAN 80 (AISLADOS) no está activada, pero la VLAN debe ser configurada en la instalación de la plataforma de lo contrario el asistente web no nos permite avanzar con el siguiente paso.

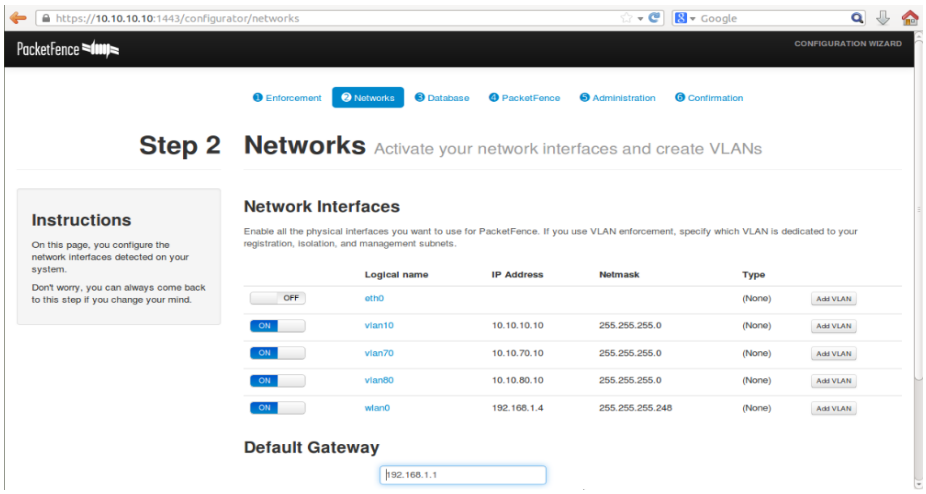

Figura 4.28: Paso 2, configuración de redes

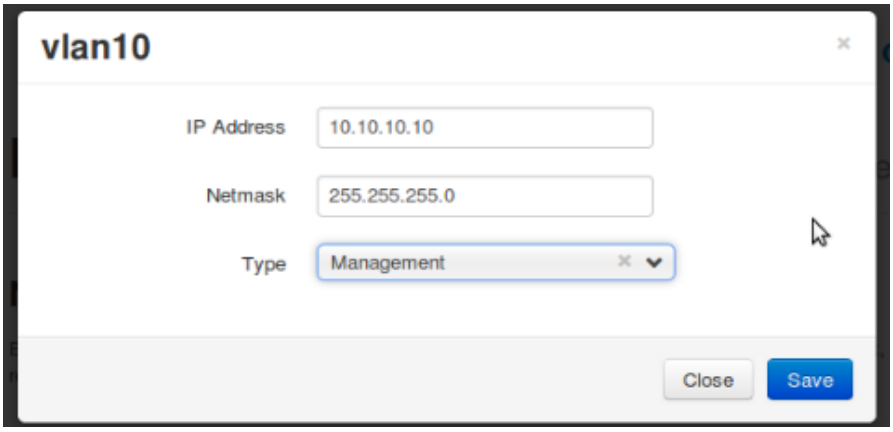

Figura 4.29: selección de la interface de mantenimiento PF

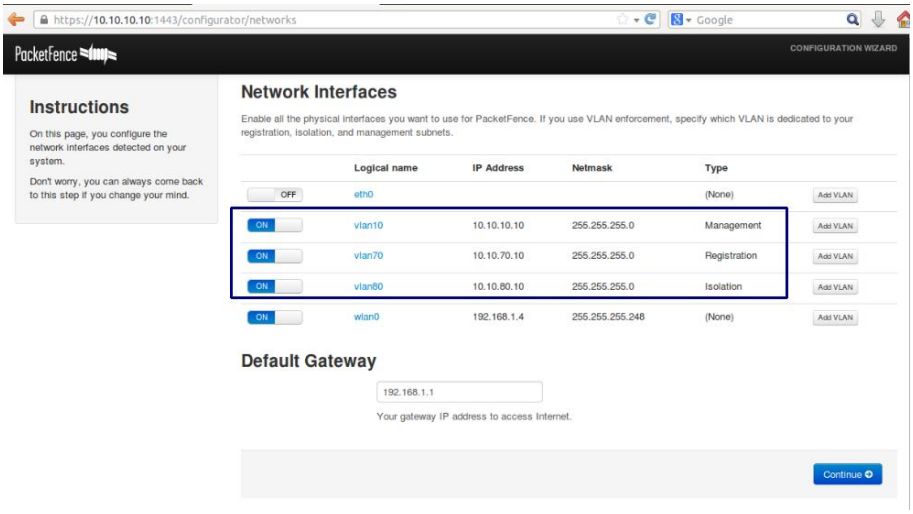

Figura 4.30: configuración final del paso 2

- **Paso 3: Base de Datos**

Este paso muestra la configuración del servidor MySQL necesitado por PacketFence. Las bases de datos y los esquemas son creados automáticamente por el sistema según las opciones activadas y configuradas en PacketFence.

La instalación de MySQL necesita utilizar el usuario "root" y un password que debe ser creado como se visualiza en la figura que se muestra a continuación de esta manera autorizamos la creación automática de bases, tablas y esquemas.

La siguiente sección crea la base de datos y carga el esquema correcto en ella. Se deja el nombre "pf" creado por default y se da click en *Create database and tables.*

La tercera sección crea una cuenta a nivel usuario para PacketFence dentro de MySQL simplemente se deja la cuenta "pf" creada por default y escogemos el password.

Si todos los pasos resultaron exitosos se podrá continuar con el siguiente paso de configuración.

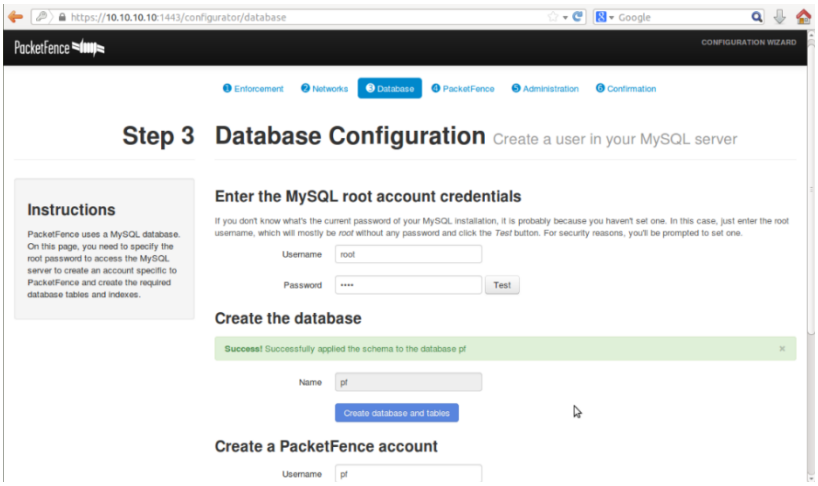

Figura 4.31: Paso 3, configuración de base de datos

- **Paso 4: Configuración PacketFence**

Aquí se configuran las opciones generales. Estas configuraciones son muy importantes porque definen las funcionalidades que el usuario la dará a la plataforma dentro de la red.

Casi toda la información solicitada aquí es auto explicativa. El campo que nos puede confundir es la selección de los servidores DHCP, aquí se ingresan las direcciones

IP de las redes en las cuales PacketFence actuara como servidor DHCP, que en nuestro caso será para la VLAN 70 de Registro de invitados y en la VLAN 80 de usuarios Aislados, el resto de servicios DHCP en las diferentes VLANs será entregado por el router de telefonía.

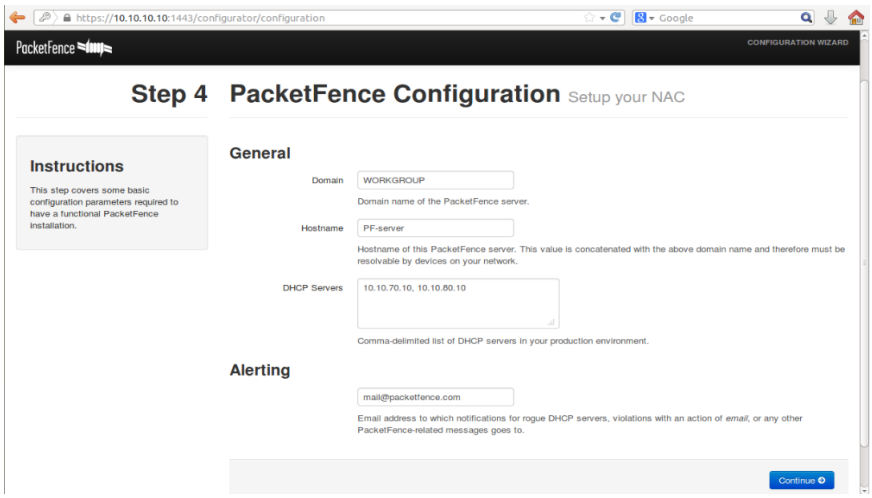

Figura 4.32: Paso 4, configuración de PacketFence

- **Paso 5: Administración**

En este paso se crea el usuario administrador de PacketFence que será utilizado cuando se acceda a través de la interface de administración WEB por medio de cualquier navegador.

Se crea el ***usuario: admin*** con *password:* ***admin.***

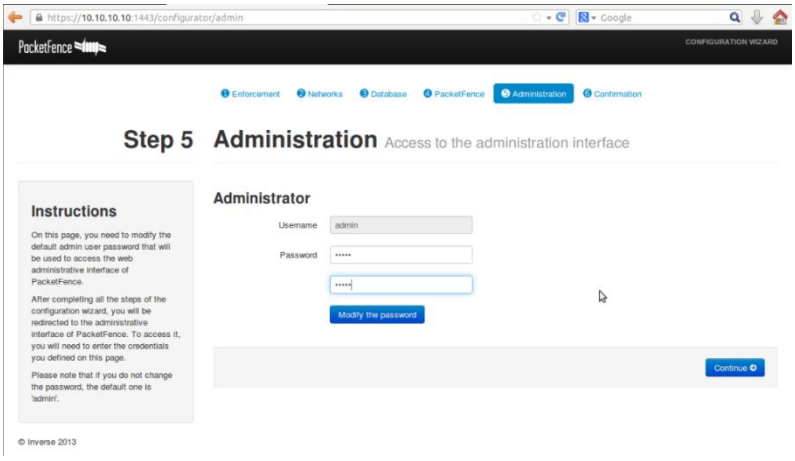

Figura 4.33: Paso 5, credenciales de usuario de administración

- **Paso 6: Inicio de Servicios**

Este es el último paso de la configuración de PacketFence, en esta pantalla se pueden ver todos los servicios que se ejecutan en segundo plano, estos servicios deben iniciar con normalidad para asegurar que al menos la configuración básica de PacketFence ha sido realizada con éxito. Si el inicio de todos los servicios es exitoso el usuario ya podrá configurar los parámetros de su red de acuerdo a sus necesidades.

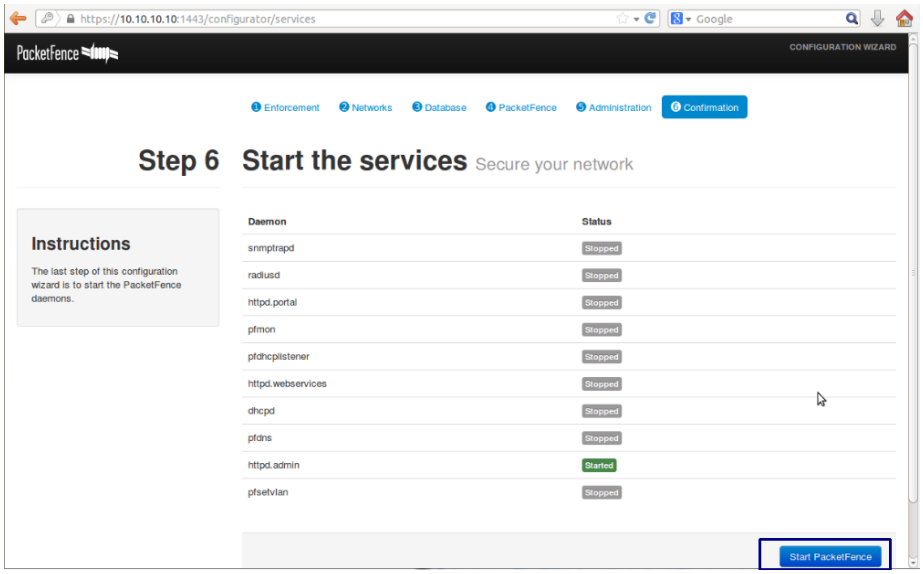

Figura 4.34: Paso 6, Inicio de servicios

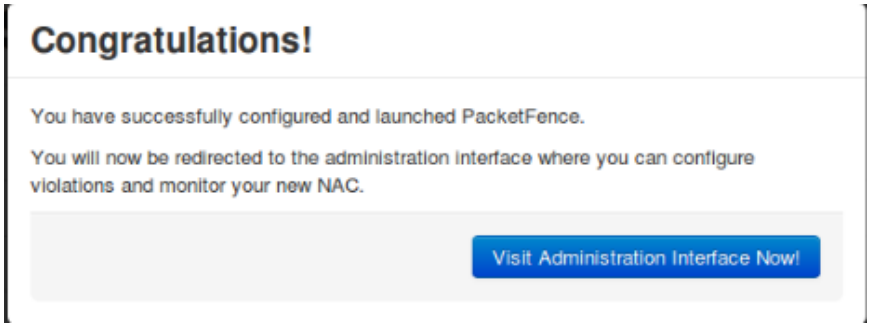

Figura 4.35: Pantalla de finalización exitosa de configuración.

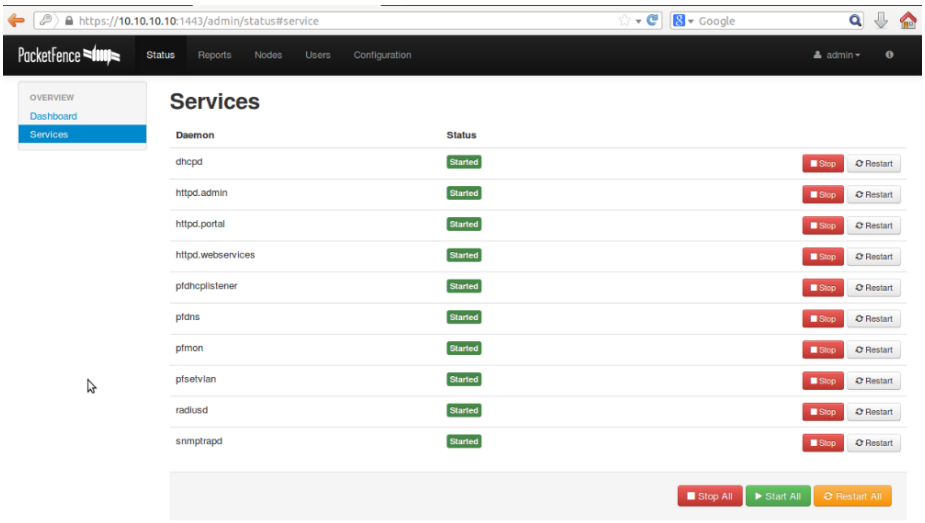

Figura 4.36: Servicios Iniciados.

4.3.7. CONFIGURACIÓN PERSONALIZADA DE PACKETFENCE SEGÚN LAS NECESIDADES DEL LABORATORIO

- **Archivo de configuración Global**

El archivo de configuración global de PacketFence se encuentra ubicado dentro de la localidad: /usr/local/pf/conf/pf.conf.

En este archivo se van a configurar y agregar parámetros importantes de la plataforma, es importante tener un respaldo de estos archivos. La edición de los parámetros de este archivo se lo realiza con el siguiente comando ejecutado dentro del terminal del servidor:

Nano /usr/local/pf/conf/pf.conf

Los datos agregados en estos campos son reflejados de forma inmediata en la página web del servidor. Se debe tener especial cuidado en los parámetros que aquí se escriben. Este archivo es la principal fuente de configuración de la plataforma como tal.

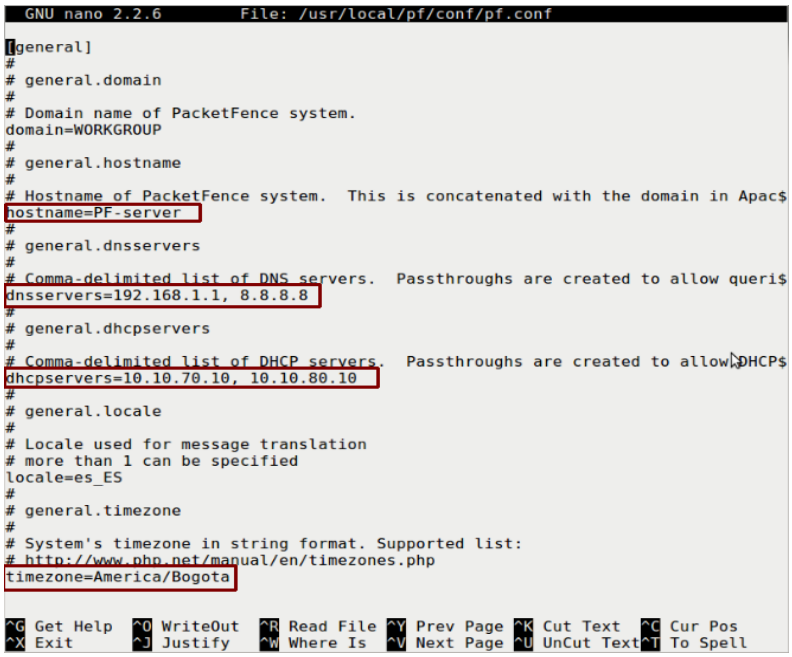

Figura 4.37: archivo pf.conf, parte 1

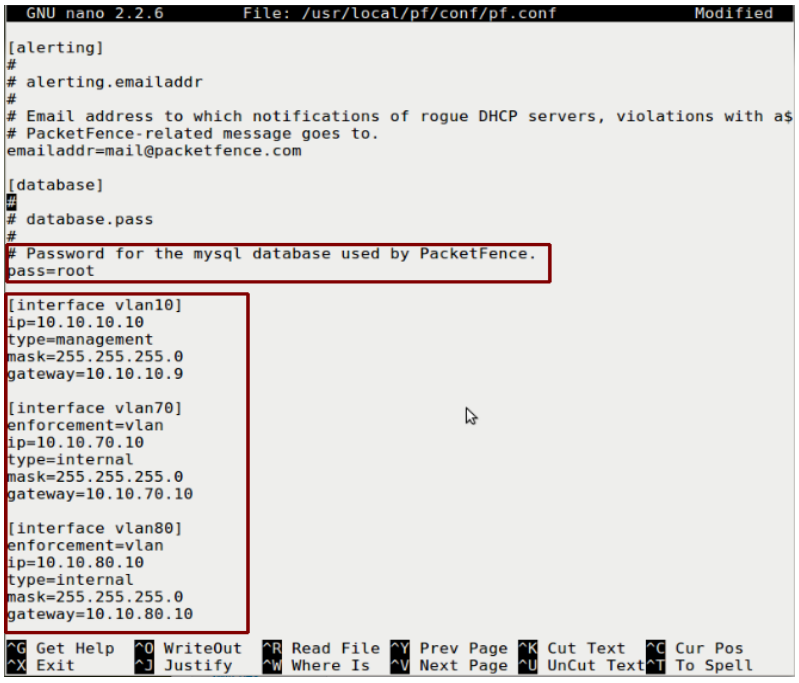

Figura 4.38: archivo pf.conf, parte 2

- **Definición de Dispositivos de red (switches.conf)**

Aquí se guarda la configuración relacionada con los equipos de Networking de la red. PacketFence necesita saber que switches, access points o controladoras administra, así como su tipo y configuración. Toda esta información se almacena en el directorio

/usr/local/pf/conf/switches.conf. es posible modificar la información de los dispositivos de red a través del comando:

Nano /usr/local/pf/conf/switches.conf

O a través del navegador web bajo la pestaña ubicada en Configuration>Network>Switches, como lo vemos en las siguientes pantallas.

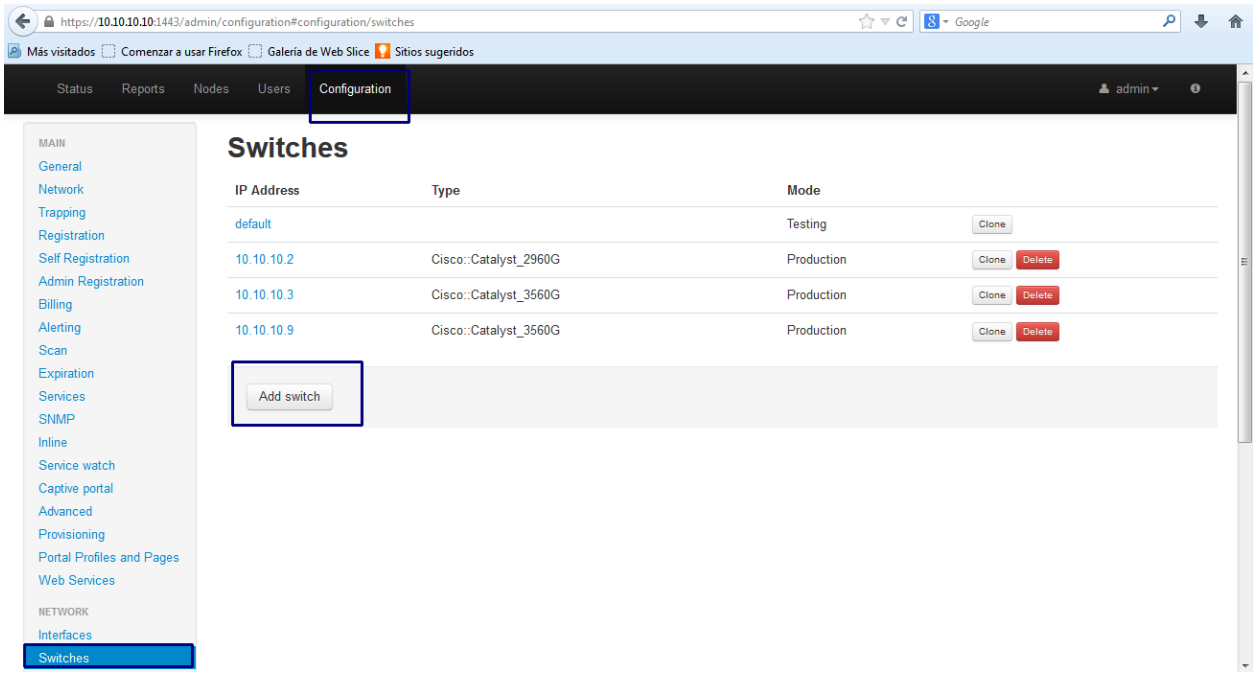

Figura 4.39: dispositivos de red

Al dar click en la opción “Add Switch”, se abre el asistente de configuración de switches. Es muy importante seguir estas instrucciones o modificarlas de acuerdo al modelo de la red con la que se trabaje.

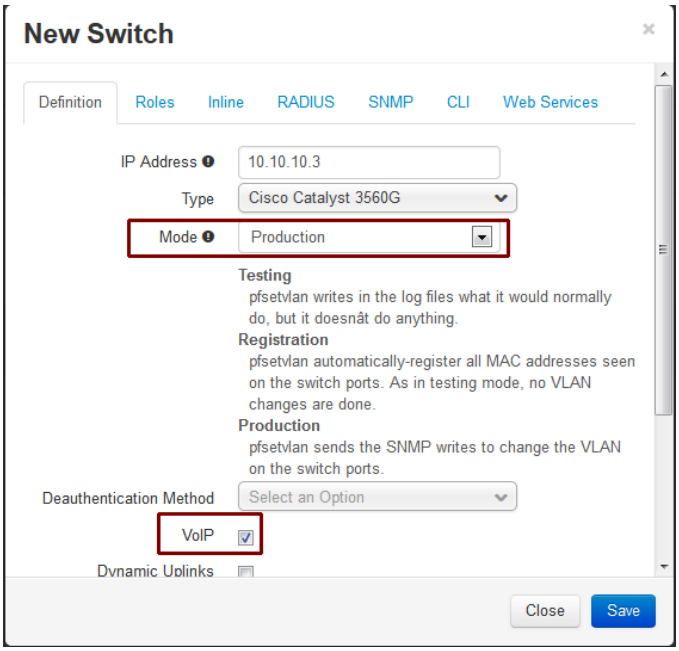

Figura 4.40: Nuevo switch, Definición

La siguiente pestaña “Roles” es en donde se agregan las VLAN necesarias para el funcionamiento del servidor. Para nuestro proyecto se hace especial énfasis en la VLAN de registro

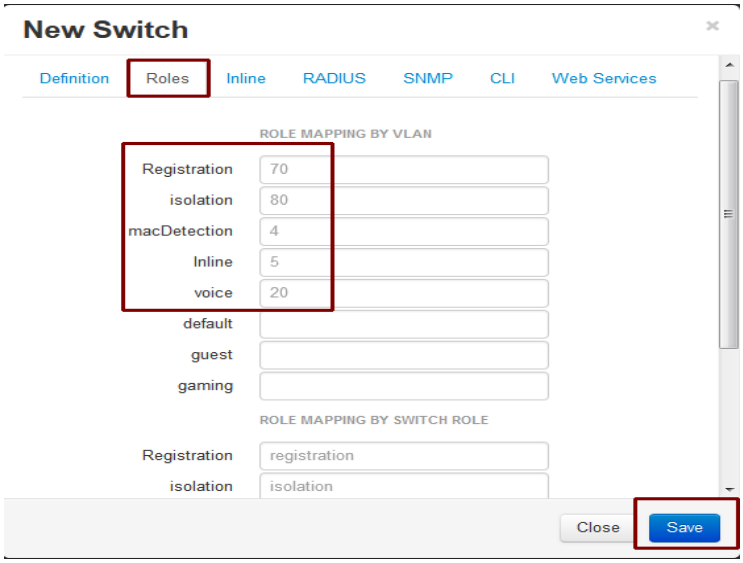

Figura 4.41: Nuevo switch, roles

La siguiente pantalla muestra la configuración del protocolo SNMP que es la principal forma de comunicación e interacción entre el servidor PacketFence y los equipos de

red. Los principales parámetros de configuración en estos equipos son las la versión del SNMP que en este caso es 2c y los nombres de las comunidades de lectura y escritura que deben ser idénticas a las configuradas en los switches (*public y prívate*).

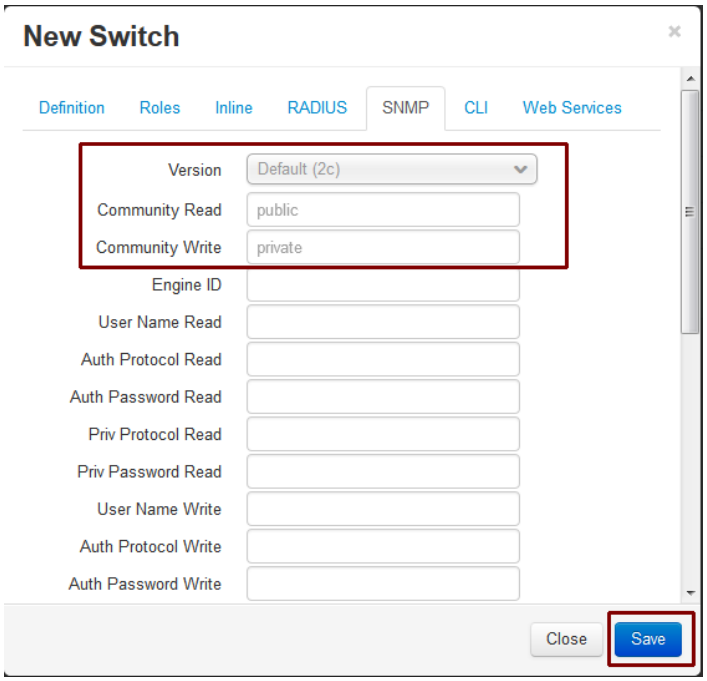

Figura 4.42: Nuevo switch, SNMP parte 1

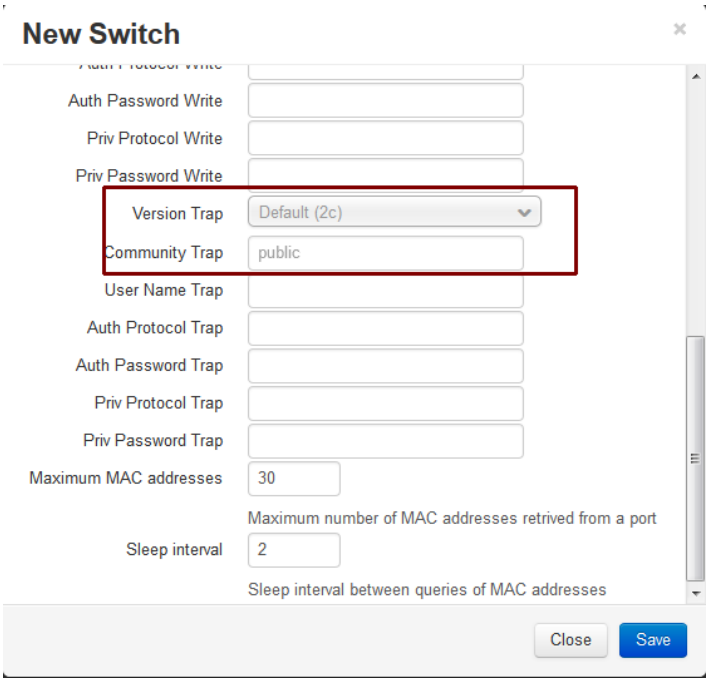

Figura 4.43: Nuevo switch, SNMP parte 2

4.3.8. CONFIGURACIÓN DE DISPOSITIVOS FLOTANTES (ACCESS POINTS INALÁMBRICOS)

En esta sección se agregan los dispositivos inalámbricos presentes en la red, ya sean puntos de acceso autónomos (access points) o equipos controladores que son utilizados para administrar redes inalámbricas de gran extensión geográfica que requieren varios access points para cubrir su superficie.

l actual proyecto que se enfoca en brindar conexión inalámbrica a los usuarios invitados en las instalaciones. Se cuenta access point Cisco AIR AP1142N por la ventajas de irradiar dos redes a la vez, una que será utilizada por los usuarios que cuenten con las claves de acceso autorizado a la red y la otra que se encargara de albergar a los dispositivos invitados de forma temporal, la actividad de los usuarios presentes en la red y autorización de nivel de acceso de usuario es asignado por el servidor PacketFence.

La descripción de cada una de las redes inalámbricas así como la configuración del Access point fue detallada previamente en este capítulo y en la sección anexos se muestra la configuración completa de access point Cisco para mayor referencia.

Las siguientes figuras muestran la configuración realizada para agregar al access point dentro de la plataforma PacketFence.

Ingresando a través del navegador web nos dirigimos hacia:

Configurator>Network>Floating devices>Add floating device.

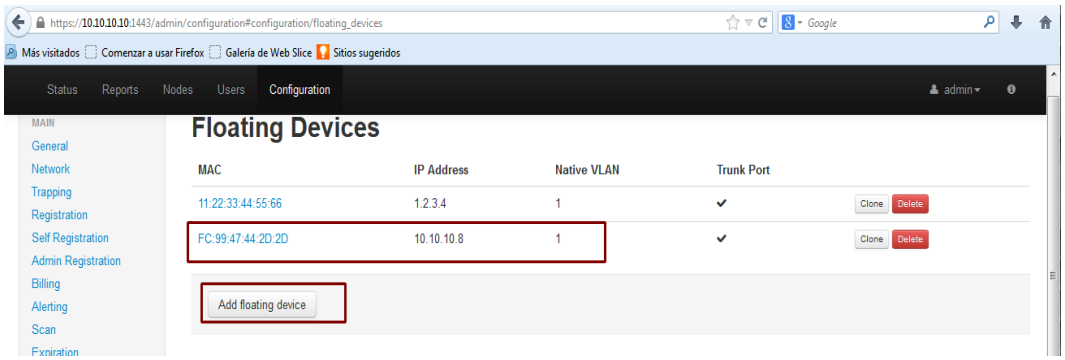

Figura 4.44: ingreso de acess point Cisco a PacketFence

Es importante ingresar a la VLAN 1 como nativa de esta manera los paquetes sin etiquetado del servidor PF podrán llegar al access point sin problema. Es necesario definir únicamente las VLANs que serán utilizadas por PF que son mantenimiento, registro y aislamiento. Nuestra diseño de red cuenta con mas VLANS pero no es necesario ingresarlas o todas.

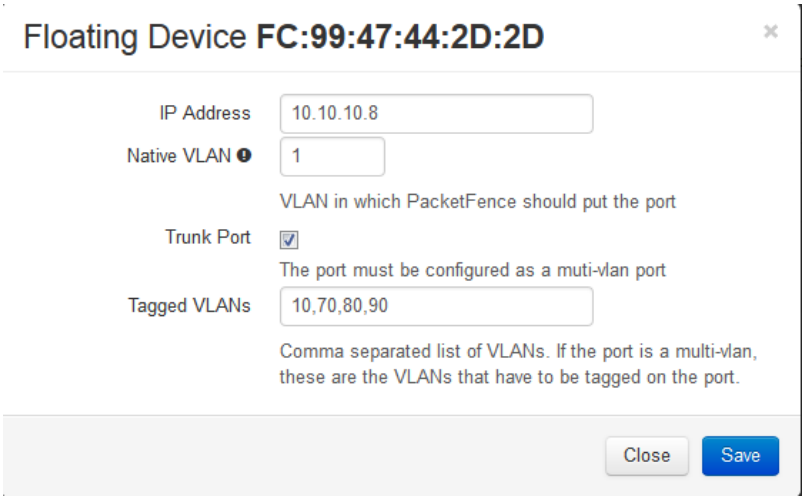

Figura 4.45: ingreso access point Cisco a PacketFence parte 2

4.3.9. UTILIZACIÓN DE PACKETFENCE

Una vez finalizada la instalación de PF es momento de configurarlo según las necesidades del laboratorio. Como primer paso ingresamos por medio de un navegador de internet desde cualquier computadora que se encuentre en la misma VLAN del servidor y apuntamos hacia la siguiente dirección:

https://10.10.10.10:1443/

Nos presentara un mensaje preguntando si aceptamos los riesgos de la conexión y si aceptamos los certificados emitidos por el emisor, a todo esto contestamos de forma afirmativa.

Una vez establecida la conexión se presenta la pantalla de bienvenida solicitando el nombre de usuario y contraseña para lo que utilizamos la cuenta *"admin"* con contraseña *"admin".*

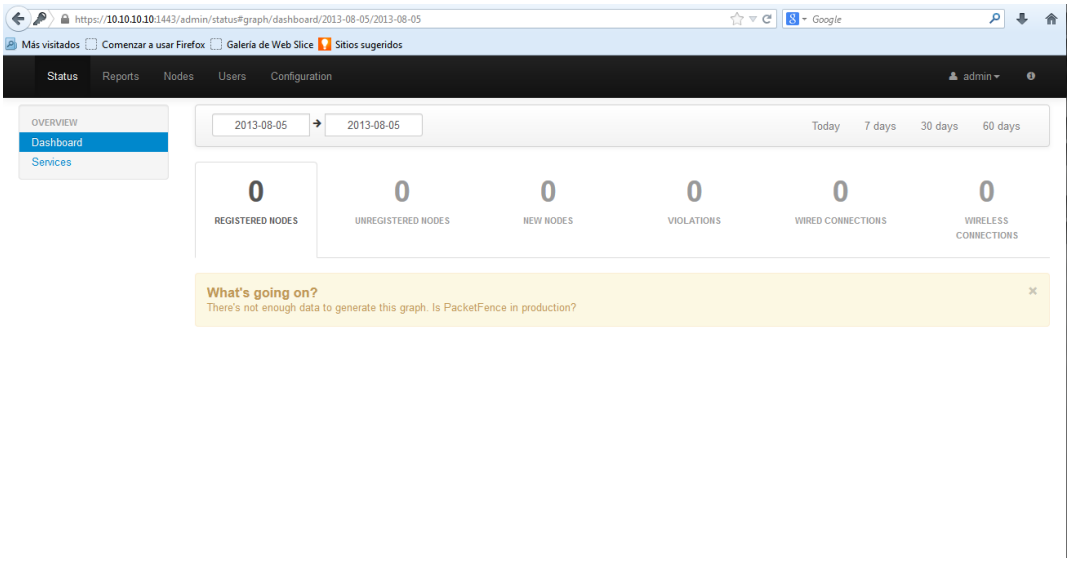

Figura 4.46: Pantalla inicial de PacketFence

PacketFence cuenta con 5 menús presentes en la parte superior de la pagina web, estos menús cumplen con diferentes funciones de configuración para satisfacer los requerimientos del usuario y son detallados a continuación.

- **Menú Configuration:**

Este es el menú más importante de todos porque es aquí en donde vamos a realizar la configuración de PF para adaptarlo a nuestra red, los resultados mostrados en el resto de menús son el resultado directo de la configuración del servidor.

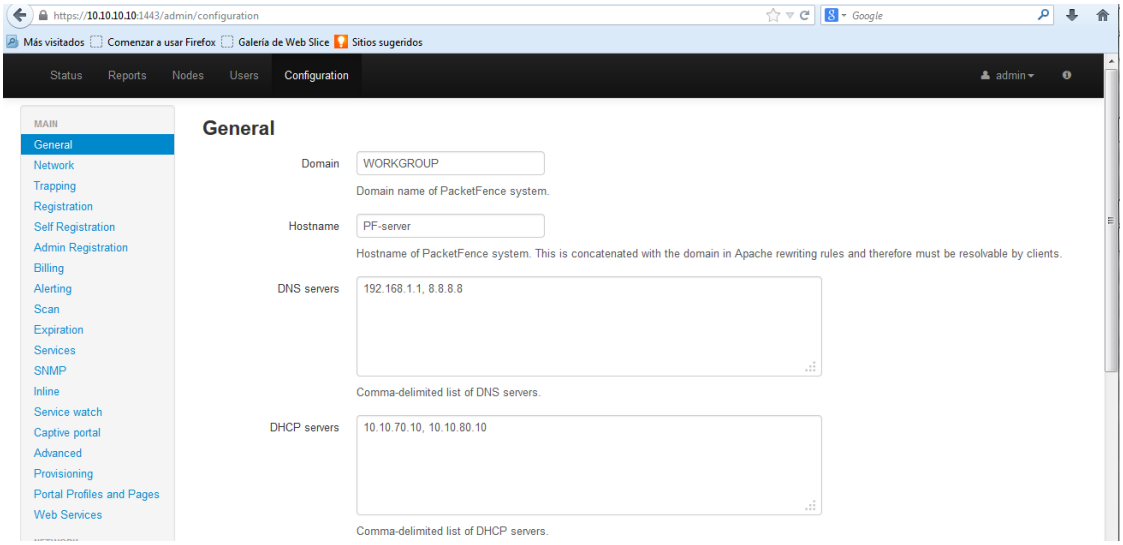

Figura 4.47: Menú Configuration

- **Menú Status:**

Aquí se muestran las estadísticas de conexión que han sido detectados por PacketFence de forma general así como la opción de administrar los servicios activos

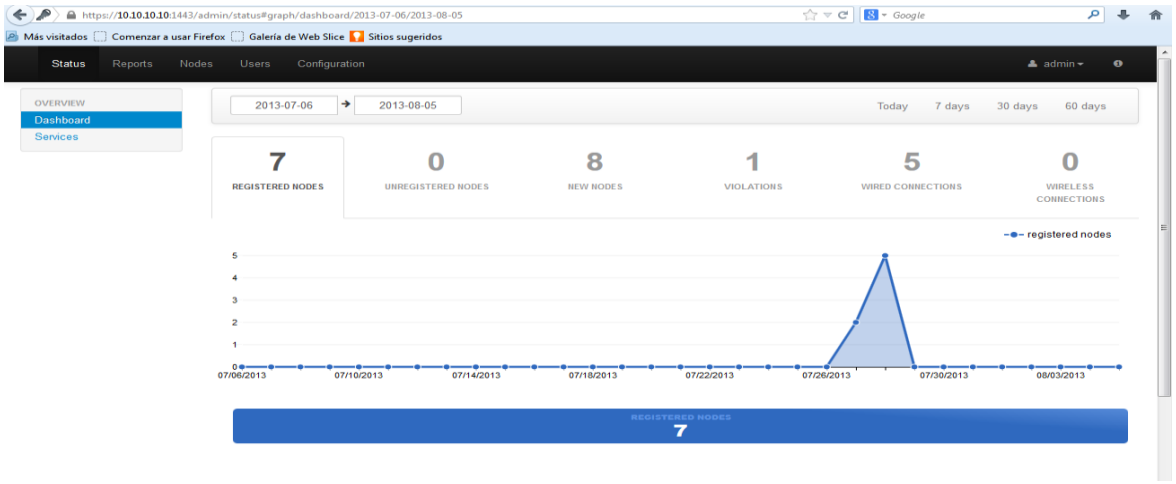

Figura 4.48: Menú Status

- **Menú Reports**

Abarca los reportes de forma más detallada sobre los eventos mostrados en el menú status. Detalla reportes de nodos, conexiones y auditoria. Los reportes se muestran en formatos estadísticos

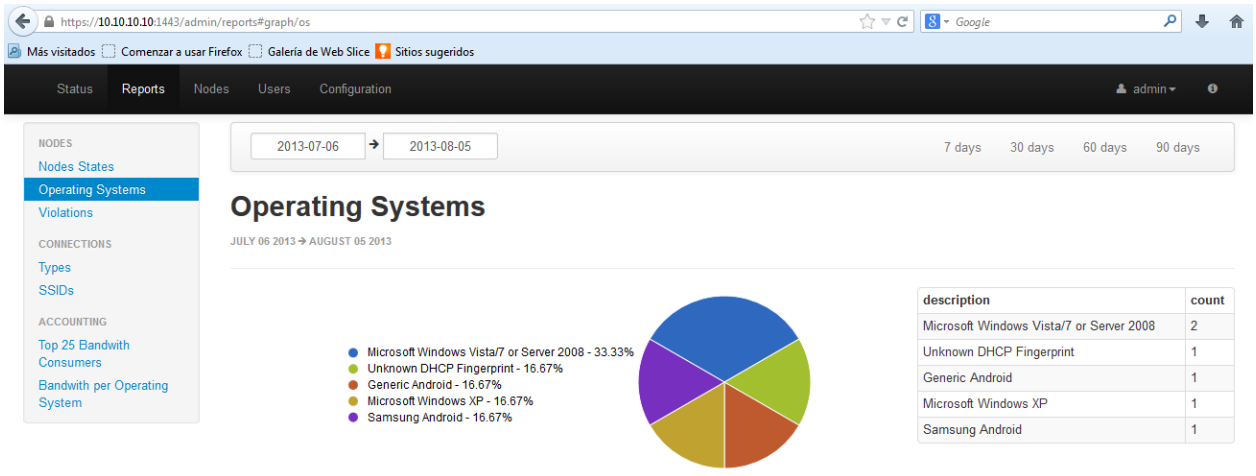

Figura 4.49: Menu Reportes

- **Menú Nodes**

Este menú es de los más importantes ya que aquí se llevara el control sobre los dispositivos conectados a la red inalámbrica. Los usuarios conectados a la red inalámbrica son identificados por medio de su dirección MAC, una vez identificada la dirección MAC el administrador decide si el usuario tiene privilegios de red o se le concede acceso restringido.

A los equipos desconocidos que no pueden ser identificados por el administrador se les concede la etiqueta de "No Registrado" (UNREGISTERED) y no tendrán acceso a la red.

La siguiente figura muestra el registro de los usuarios administrados por PacketFence así como sus direcciones MAC, IP, sistema operativo entre otros.

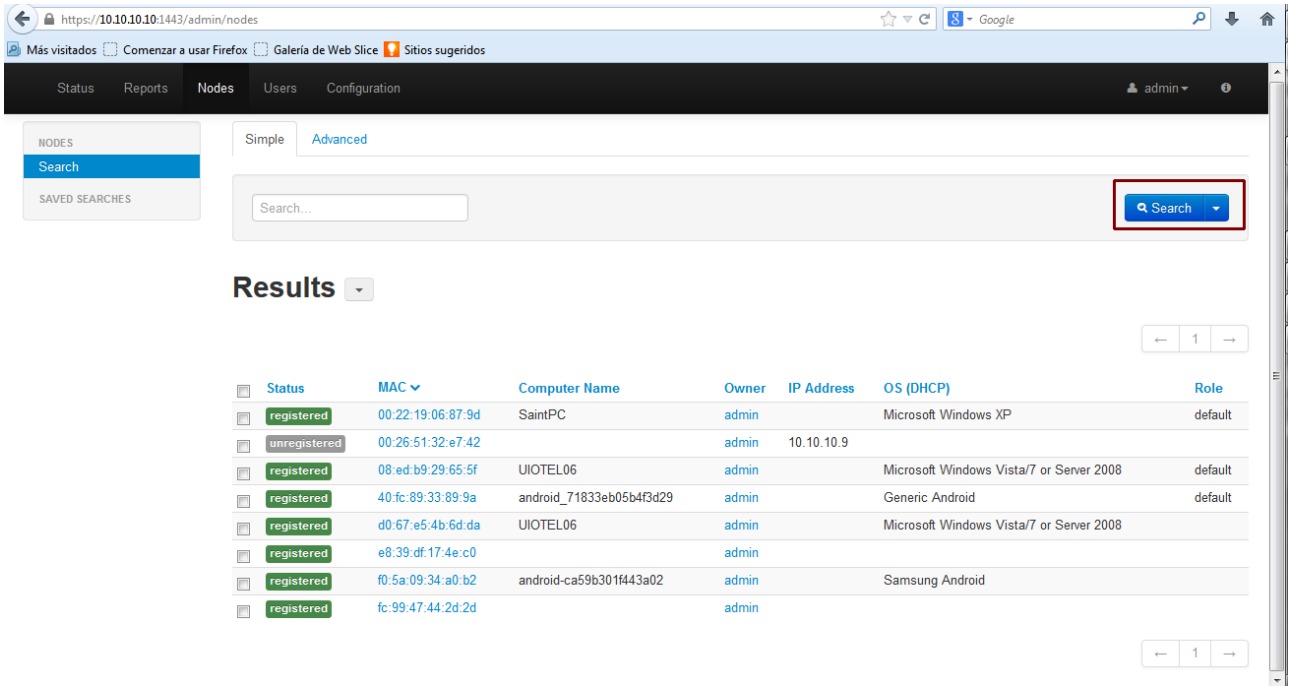

Figura 4.50: Menú nodos

El capitulo 5 cuenta con un ejemplo de utilización de PacketFence en los entornos de laboratorio simulando las alternativas de conexión que pueden presentarse en la red inalámbrica para mejor entendimiento.

CAPITULO V

5. VALIDACION Y PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA DE HERRAMIENTAS NAC DE SOFTWARE LIBRE

5.1. ADMINISTRACIÓN FreeNAC Y EJEMPLO DE FUNCIONAMIENTO

Una vez finalizada la instalación y configuraciones básicas de FreeNAC es posible administrar la herramienta de acuerdo a las necesidades del usuario. Esta sección se enfoca en bridar las pautas necesarias para la personalización de la herramienta brindando ejemplos de configuración con los equipos de laboratorio y usuarios de prueba.

Se recomienda utilizar la interface grafica GUI para modificar los parámetros de funcionamiento de FreeNAC y para la administración de equipos conocidos, desconocidos y agregar nuevos usuarios se recomienda administrar el servidor a través de web browser porque de esta manera se tiene acceso limitado y no es posible cambiar configuraciones críticas de que pueden afectar el funcionamiento del servidor.

5.2. UTILIZACIÓN DE WINDOWS GUI

Al iniciar la interface Windows GUI (*vmps.exe*) y presionar el botón *"Connect"* la interface intentara conectarse con la base de datos FreeNAC por lo que se recomienda que el equipo Windows en el que se ejecute el GUI este en la misma VLAN que el servidor FreeNAC para evitar problemas de conectividad además de deshabilitar restricciones de seguridad como antivirus y firewalls

Si el proceso de comunicación entre equipos es exitoso se mostrara la pantalla de bienvenida como se muestra en la figura.

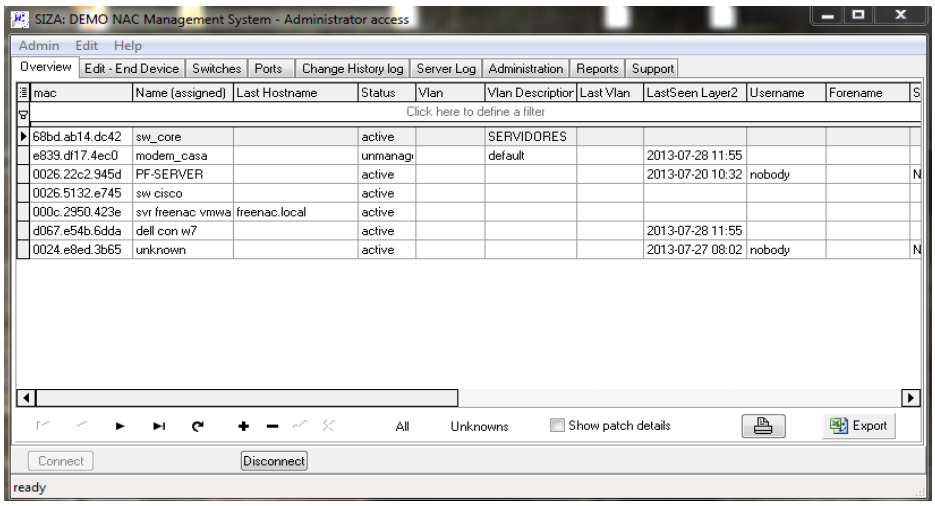

Figura 5.1: pantalla de bienvenida de FreeNAC Windows GUI

5.3. CONFIGURACIÓN DE PARÁMETROS DE RED

Aquí se detallan las configuraciones realizadas para personalizar del servidor FreeNAC de acuerdo a los datos de la red de laboratorio. Para esto se ingresa a la pestaña ***Administration> Config***

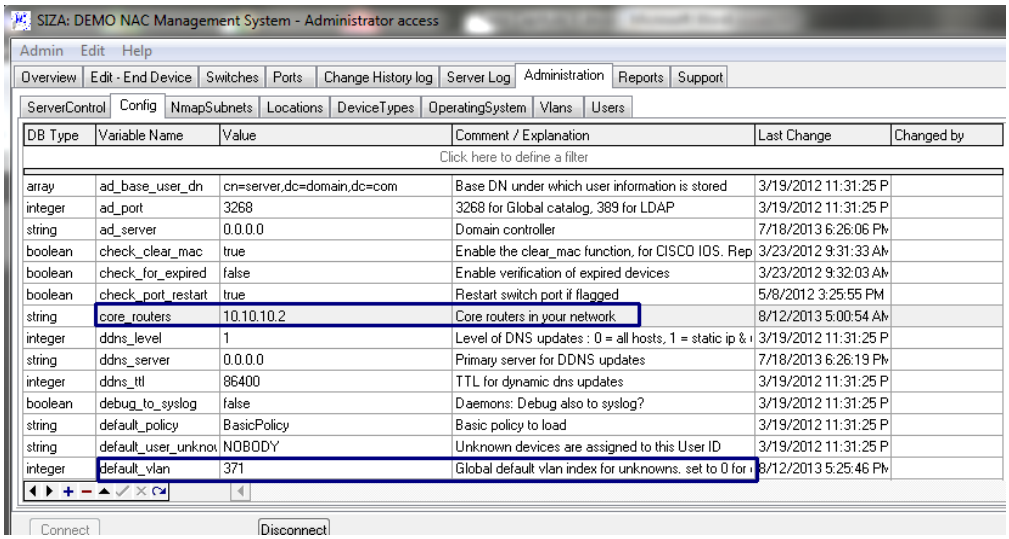

Figura 5.2: Pestaña de configuración parte 1

Core_routers: dirección IP del switch CORE

Default_vlan: 371, ingresar numero del índice que pertenece a la VLAN 80 (AISLADOS) que será asignada por defecto a los usuarios desconocidos. El índice de VLAN puede ser consultado en la pestaña ***Administration>Vlans***

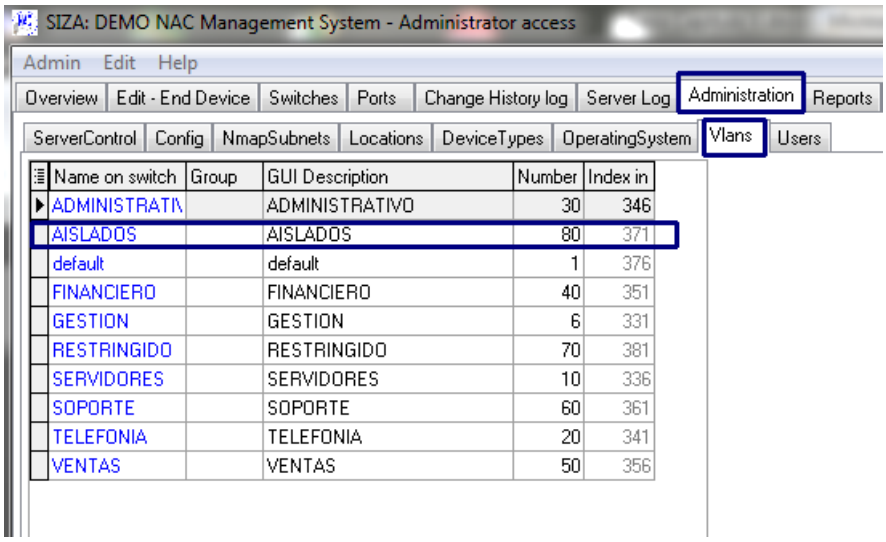

Figura 5.3: verificación de índices de VLANs

DemoMode: 1, Permite que acceso de administrador desde cualquier computador que tenga instalado los archivos vmps.exe

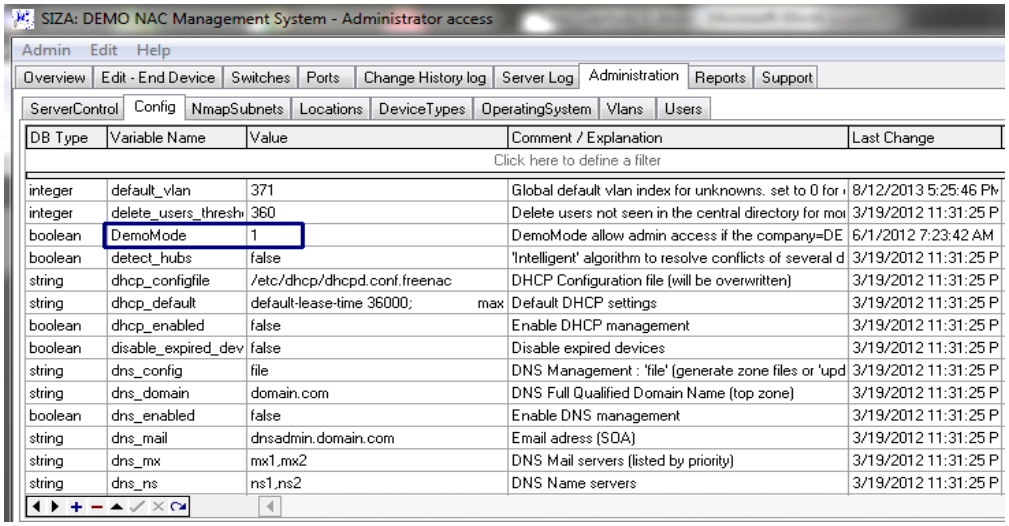

Figura 5.4: Pestaña de configuración parte 2

Dns_subnets: direcciones IP de los redes de los servidores DNS

Entityname: Nombre de la Empresa en donde se implementa la solución

Guidomain: Nombre del dominio de la empresa

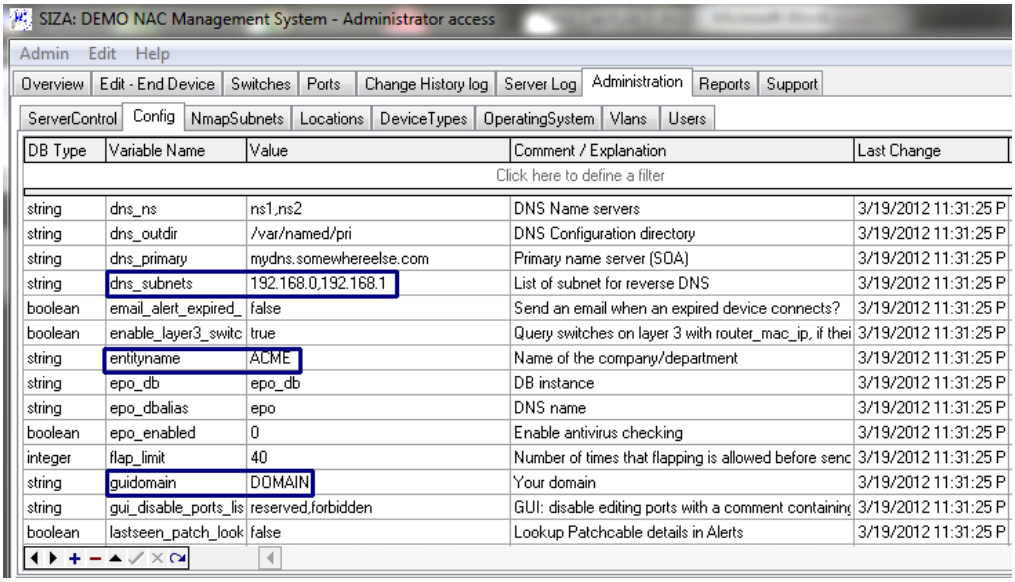

Figura 5.5: Pestaña de configuración parte 3

Scan_unmanaged: true, activación de escaneo de equipos no administrados

Set_vlan_for_unknows: 371, ingresar el índice de la VLAN designada para los equipos desconocidos VLAN 80 (AISLADOS)

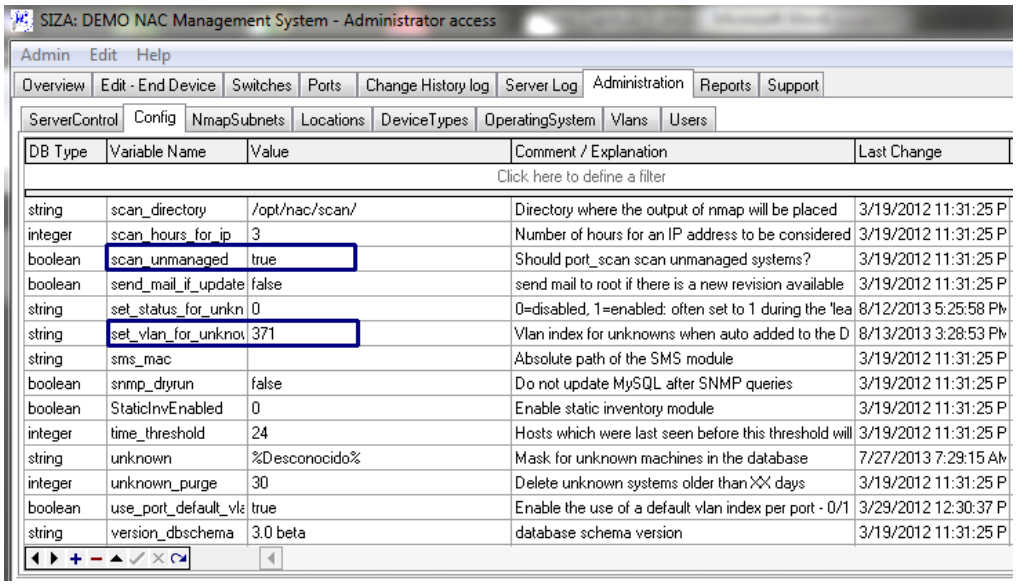

Figura 5.6: Pestaña de configuración parte 4

5.4. EJEMPLO DE FUNCIONAMIENTO FreeNAC

Para ilustrar de mejor manera la administración de FreeNAC, se agregan capturas de pantalla pertenecientes a un ejemplo de funcionamiento, el cual consiste en todo el proceso necesario para habilitar a una usuario otorgándole acceso a la red, es decir, un ejemplo que inicia desde la detección de la dirección MAC en una de las interfaces del switch de acceso en modo desconocido (*Unknown*) hasta su designación en la VLAN que corresponde y posteriores pruebas de conectividad.
Los equipos utilizados en este ejemplo son los siguientes:

MARCA	EQUIPO	MODELO	MNEMONICO	IP / Mac Address
DELL	PC	OPTIPLEX 740	Usuario1	0022.1906.879D
CISCO	SWITCH	Catalyst 3560	SWITCH_PRUEBAS	10.10.10.9
DELL	LAPTOP	Latitude E5520	FreeNAC_SVR	10.10.10.20 (Virtual)

Tabla 5.1: Equipos utilizados en ejemplo FreeNAC

- **Pestaña Overview:**

Esta pestaña contiene la información de las direcciones MAC de los equipos conectados a la red sean conocidos o desconocidos. Brinda estadísticas muy importantes como estado de administración (status), VLAN a la que pertenece la dirección MAC, switch en el que fue identificada, fecha de monitoreo, entre otras.
Esta ventana es de vital importancia para la gestión e identificación de usuarios desconocidos.

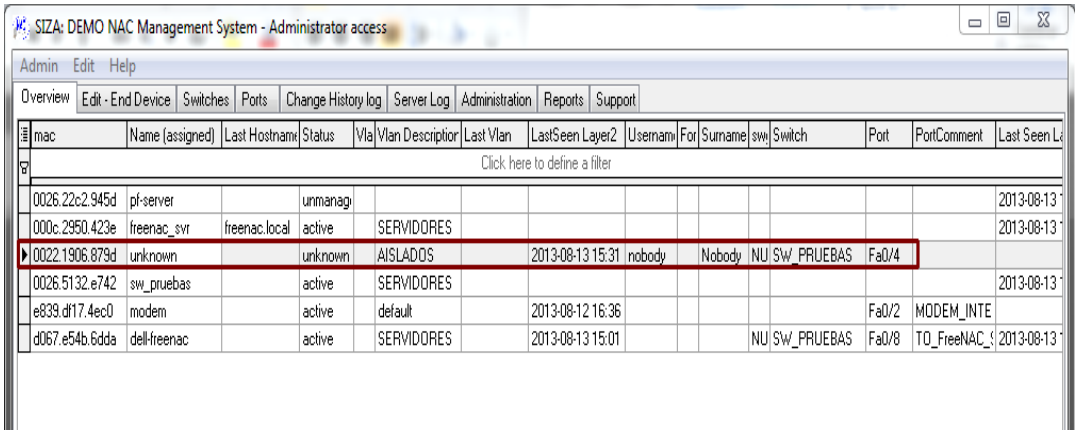

Figura 5.7: Pestaña Overview

En la figura anterior, claramente podemos visualizar que varias direcciones MAC han sido aprendidas por los switches y agregadas en la base de datos. Luego las direcciones MAC conocidas por el administrador fueron activadas y asignadas un nombre para poder identificarlas de mejor manera. Además podemos identificar la dirección MAC del equipo de pruebas (usuario1) que fue aprendida por el switch SW_PRUEBAS. Como esta dirección no consta en la base de datos se le asigna la etiqueta de desconocido *"unknown"* y el servidor FreeNAC le asigna un estatus de desconocido "unknown" y la ubica en la VLAN 80 (AISLADOS) para prevenir cualquier tipo de ataque.

La VLAN 80 es administrada por PacketFence y otorga el servicio DHCP para los usuarios de la VLAN 80 (AISLADOS) y VLAN 70 (RESTRINGIDO) que albergan a los usuarios no identificados e invitados respectivamente. La dirección IP asignada a él equipo **Usuario1: *10.10.80.20***. La siguiente figura muestra al equipo conectado a la VLAN 80 que apunta como DHCP y DNS server a la dirección IP 10.10.80.10 que pertenece a PacketFence y un intento de ping fallido hacia el servidor ***freeNAC*** (***10.10.10.20***).

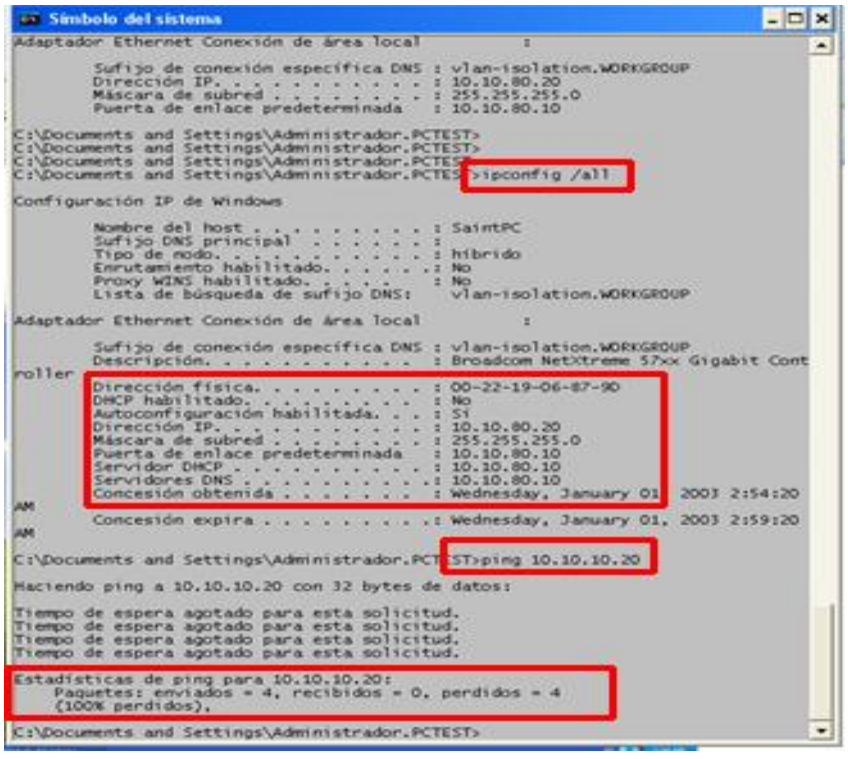

Figura 5.8: Equipo de Usuario1 en modo desconocido

Al realizar un ping desde cualquier computadora de la red hacia la dirección IP del usuario1 10.10.80.20, no es posible tener éxito ya que PacketFence aísla a este equipo del resto de la red. Para demostrar esta configuración se realiza un ping desde un equipo ubicado en la ***VLAN SERVIDORES (10.10.10.26)*** al equipo ***Usuario1 (10.10.80.20)*** como se muestra a continuación.

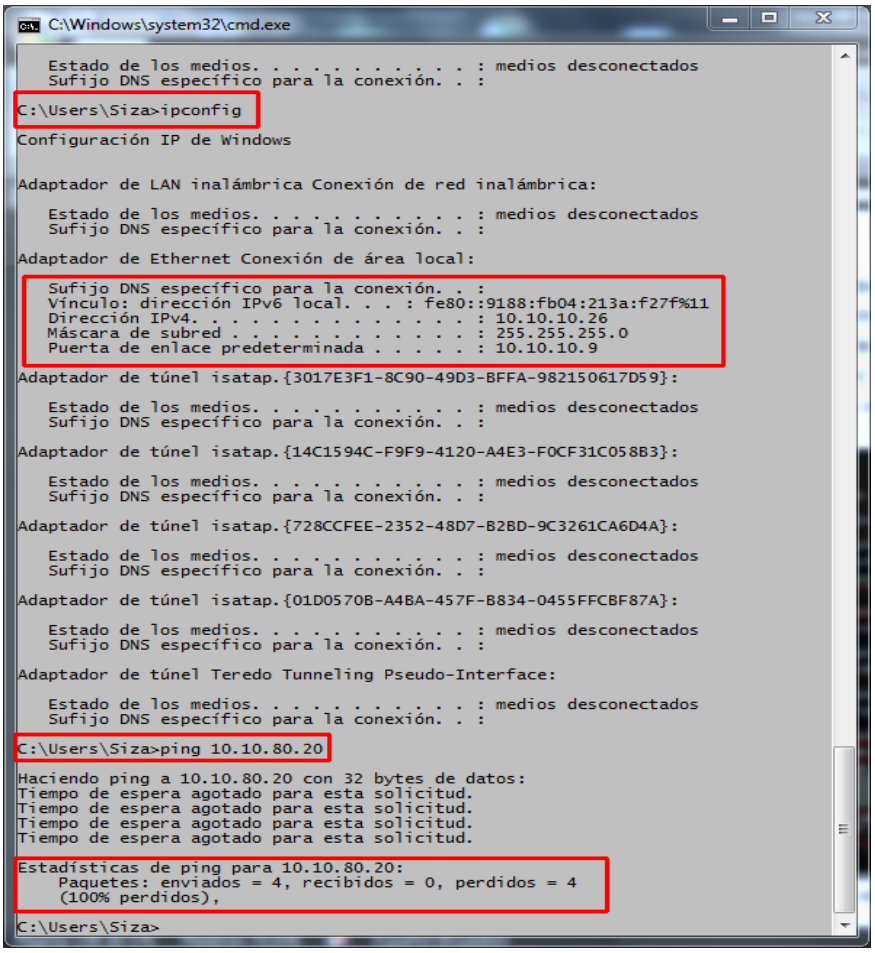

Figura 5.9: Prueba de conectividad hacia usuario desconocido

El puerto permanece en este estado hasta que el administrador de FreeNAC ingrese a través de GUI o Web Browser y autorice al usuario en la VLAN correspondiente.

A continuación se muestran los pasos necesarios para permitir el acceso de Usuario1 a la VLAN SOPORTE, para esto utilizamos las dos formas posibles: Windows GUI y Web Browser.

5.4.1. AUTORIZACIÓN DE ACCESO A RED POR MEDIO DE WINDOWS GUI

- Abrir Windows GUI (wmps.exe) desde la carpeta en donde fue extraído y configurado (ver configuración de Windows GUI dentro del Capítulo 3)
- Ubicar la dirección MAC del usuario que se desea habilitar ***(0022.1906.879D)***. En este caso la dirección MAC se encuentra en el SW_PRUEBAS puerto Fa0/4.

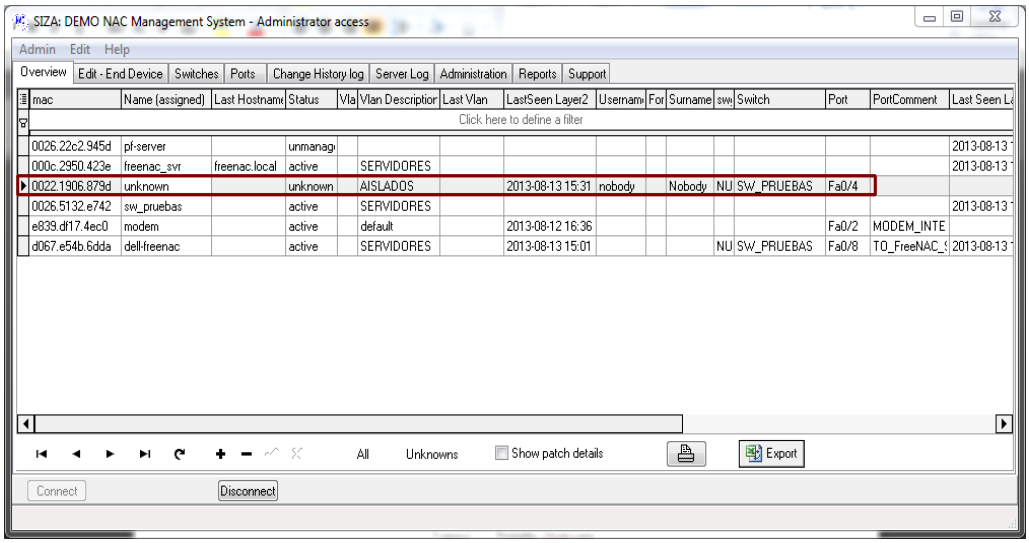

Figura 5.10: Ubicación de dirección MAC de Usuario dentro de GUI

- Una vez seleccionada la Dirección MAC del usuario. Ingresar a la pestaña: ***Edit-End Devices***. Nombrar al equipo para identificarlo de mejor manera, asignarle un usuario.

Nota: Es muy importante seleccionar la opción ***active-enabled*** ya que si no lo hacemos el equipo seguirá en estado *unknown* a pesar de que a esta dirección MAC se le asigne en una VLAN permitida

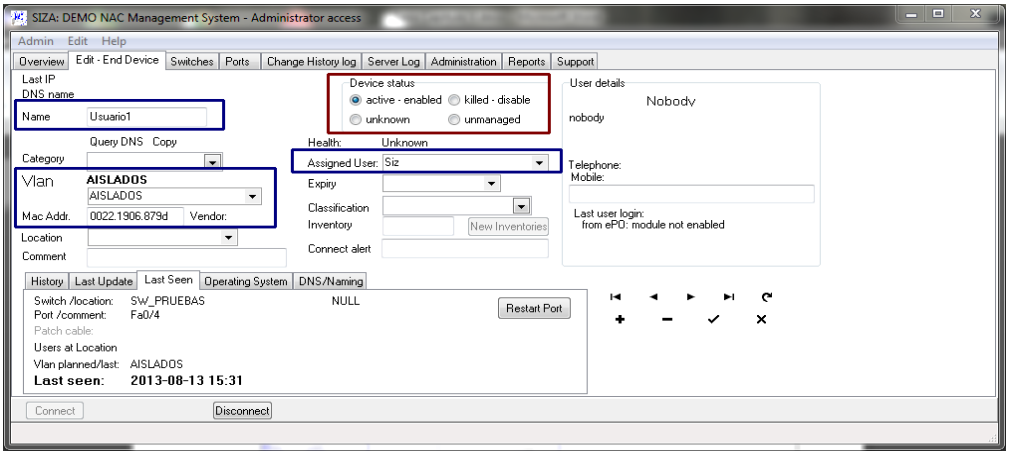

Figura 5.11: Activación de Dirección MAC

- Luego de activar el puerto, se debe asignarla la VLAN correspondiente. Se cambia su valor por defecto (VLAN AISLADOS) y se selecciona la VLAN SOPORTE designada para este ejemplo. Luego se da click en los botones: *Aplicar, Actualizar, Restart Port* para que los cambios surtan efecto. Los cambios se hacen efectivos durante el lapso de un minuto que es el tiempo por defecto que le toma al servidor enviar los comandos vía SNMP al puerto del switch respectivo.

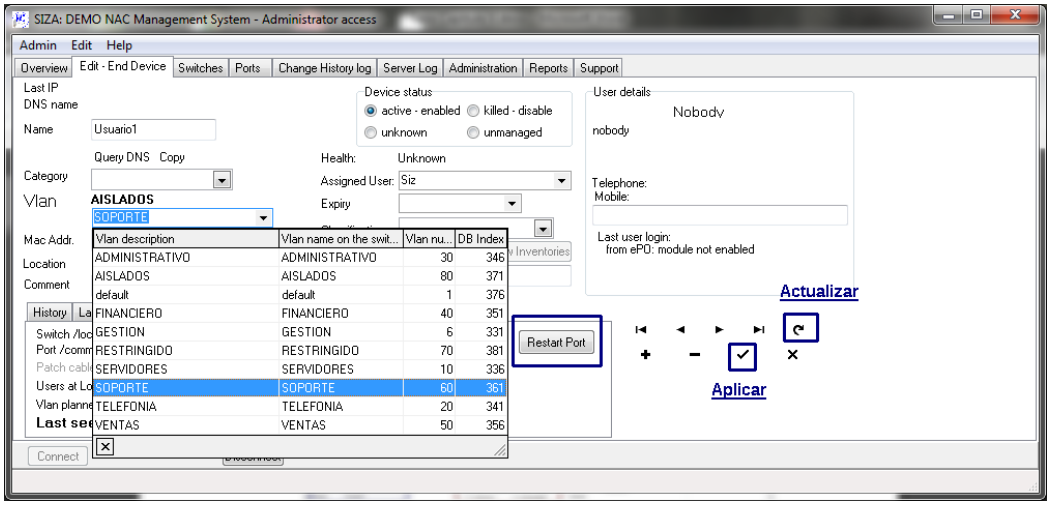

Figura 5.12: Asignación de VLAN SOPORTE al Usuario1

- Luego de realizados los cambios y reiniciado el puerto Fa0/4 del SWITCH_PRUEBAS, podemos visualizar que el computador Usuario1 ahora tiene una dirección IP perteneciente a la ***VLAN SOPORTE (10.10.60.11)*** y tiene conectividad con los equipos de red.

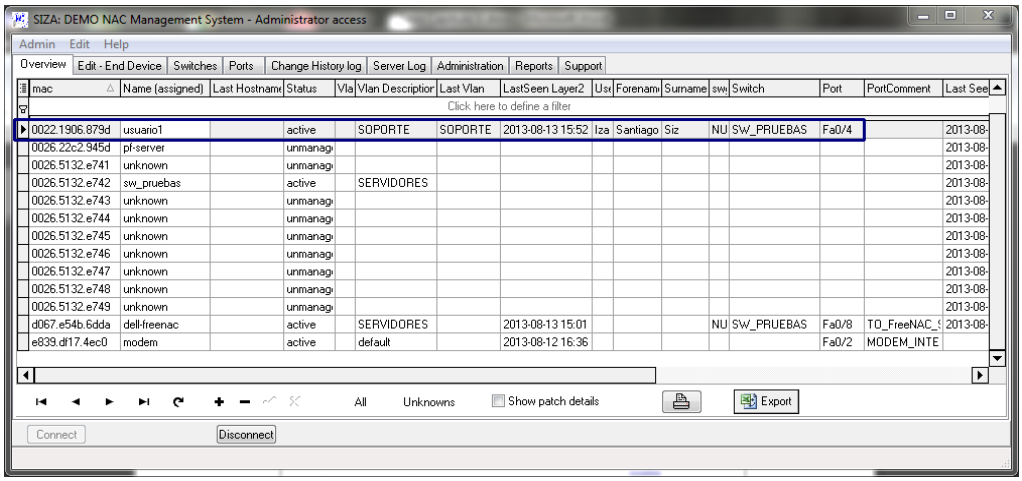

Figura 5.13: Usuario1 con acceso a la VLAN SOPORTE

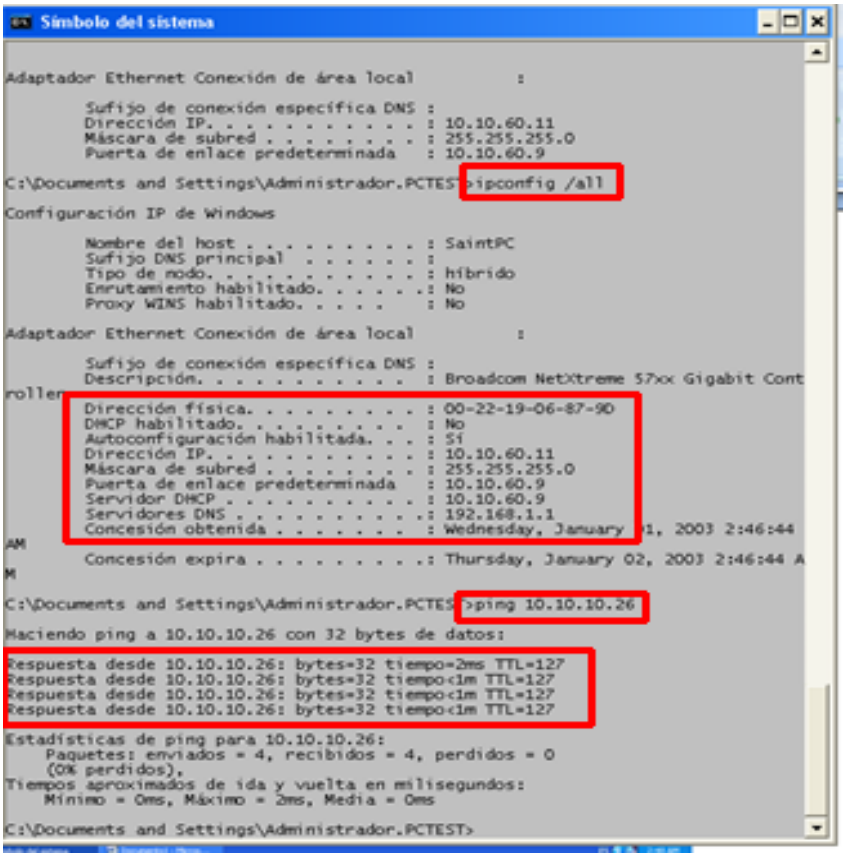

Figura 5.14: Usuario1 con dirección IP de la VLAN SOPORTE

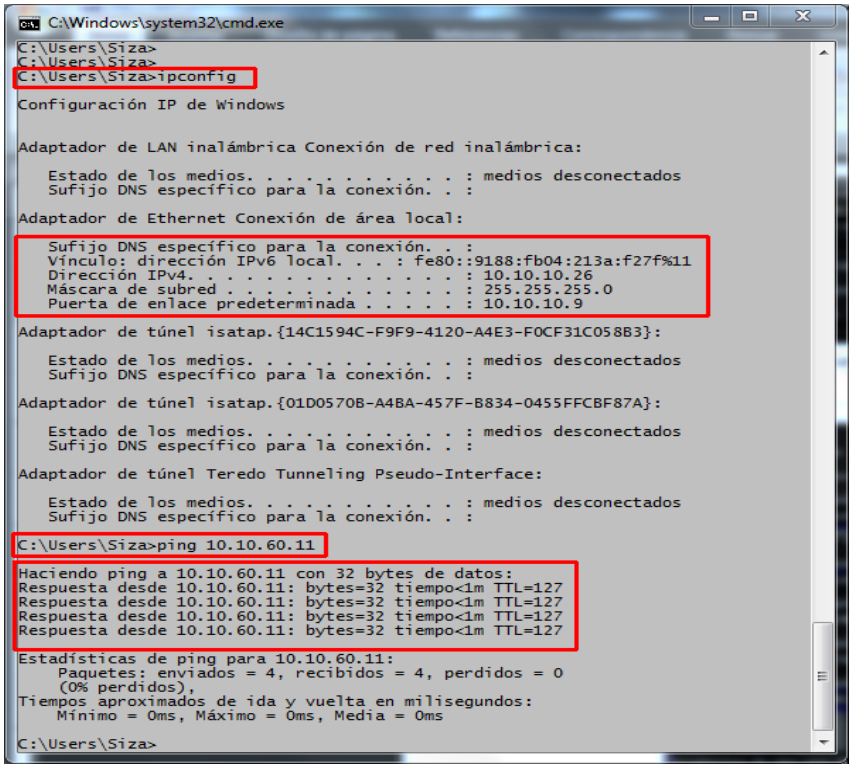

Figura 5.15: comprobación de conectividad entre equipos de red

5.4.2. AUTORIZACIÓN DE ACCESO A RED POR MEDIO DE WEB BROWSER

Esta sección se enfoca en la activación a través de la interface Web que es la forma de administración de usuarios recomendada ya que esta interface no tiene permisos de edición de los parámetros de configuración del servidor y no puede ocasionar mayores problemas de funcionamiento.

- Ingreso a FreeNAC a través de cualquier navegador de internet soportado, para lo cual se apunta a la dirección IP del servidor

http://10.10.10.20

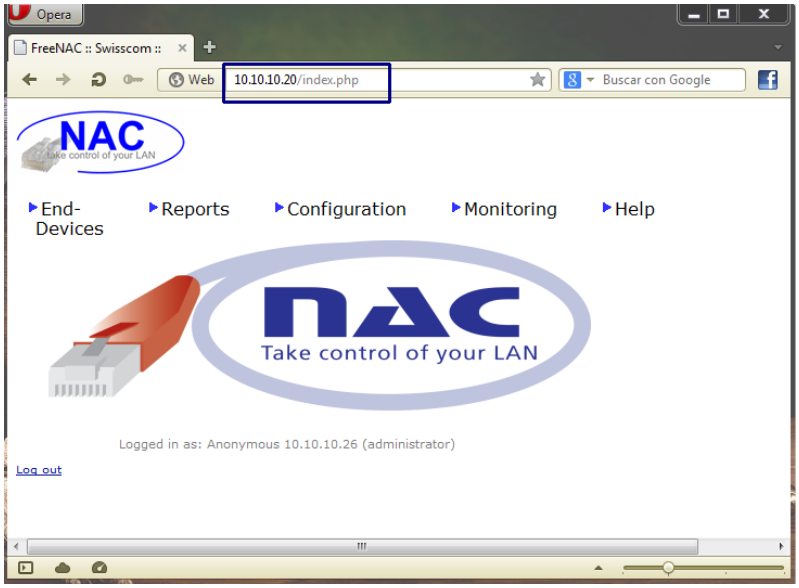

Figura 5.16: Pagina de Bienvenida FreeNAC Web Browser

- Luego ingresar en ***End-Devices> Find Unknowns***, podremos verificar los dispositivos desconocidos presentes en la red. Para modificar los parámetros del usuario se da click en el botón ***edit***

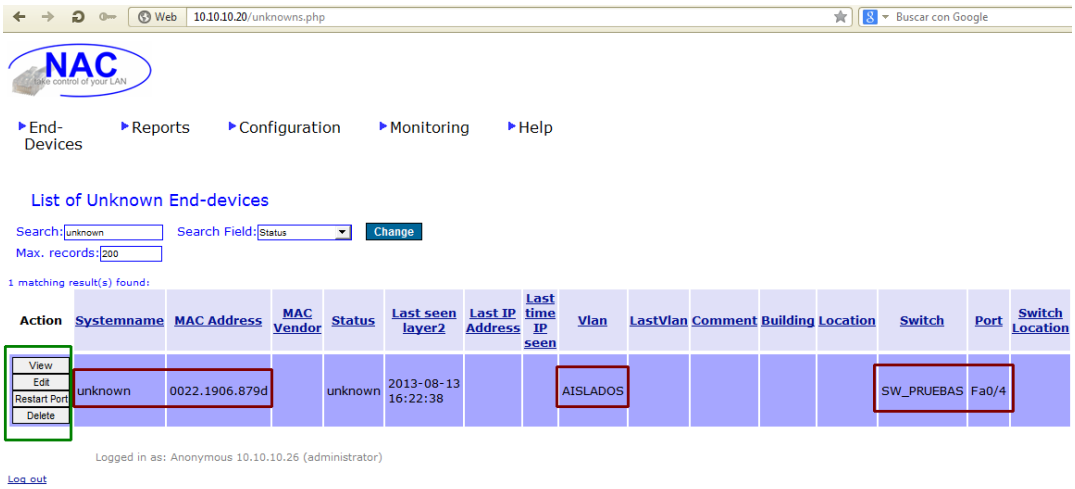

Figura 5.17: Lista de equipos desconocidos

- Dentro de la pantalla de edición le designamos un nombre (USUARIO1) y activamos la interface (Status=active)

.

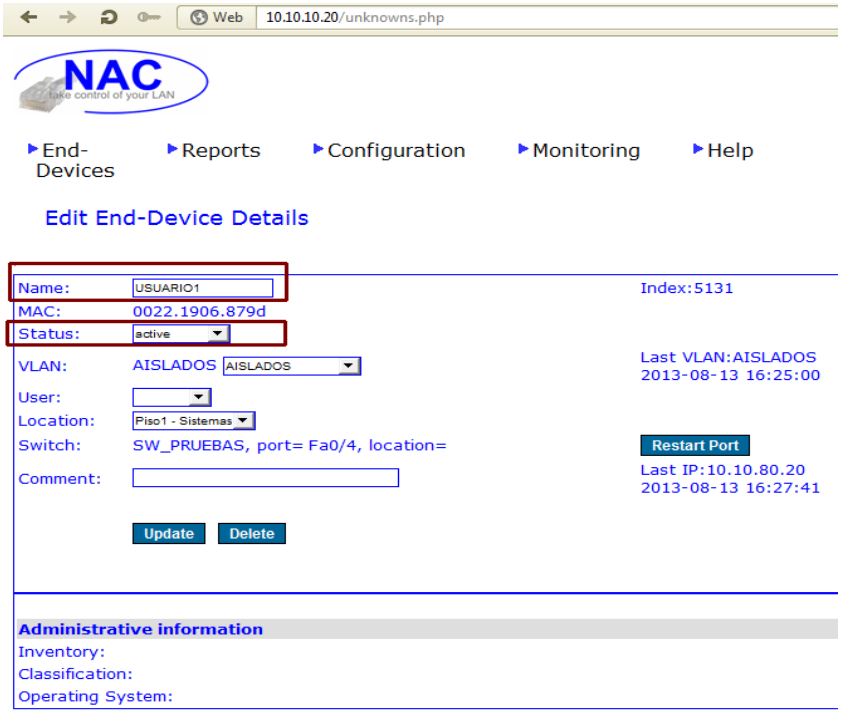

Figura 5.18: Activación de equipo desconocido

- El siguiente paso es asignar una VLAN a la dirección MAC del equipo desconocido. Se debe cambiar el valor de la VLAN AISLADOS configurada por

defecto y seleccionar la VLAN SOPORTE designada para este ejemplo. Luego para aplicar los cambios se debe presionar los botones ***Update*** y ***Restart Port***

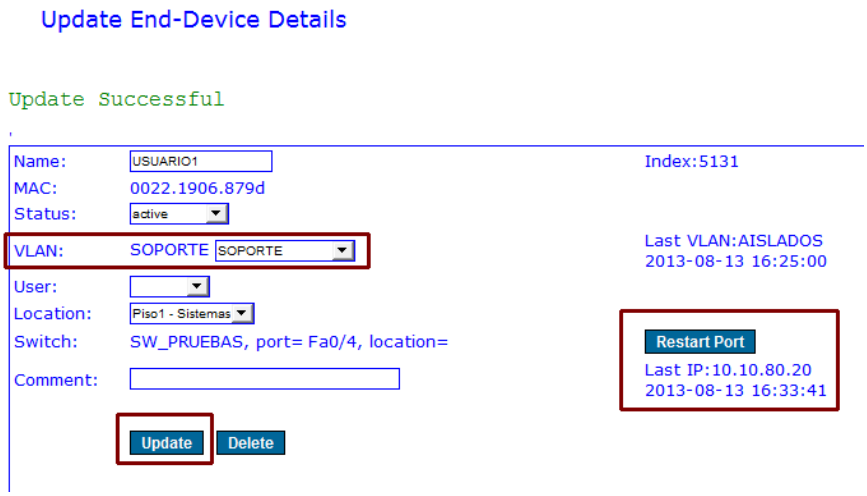

Figura 5.19: asignación de VLAN SOPORTE y aplicación de cambios

- Si el equipo fue agregado de forma exitosa debe desaparecer de la lista de desconocidos (***End-Devices>Find Unknowns***) y debe aparecer en la lista de agregados recientemente (***End-Devices> Find Recent***)
-

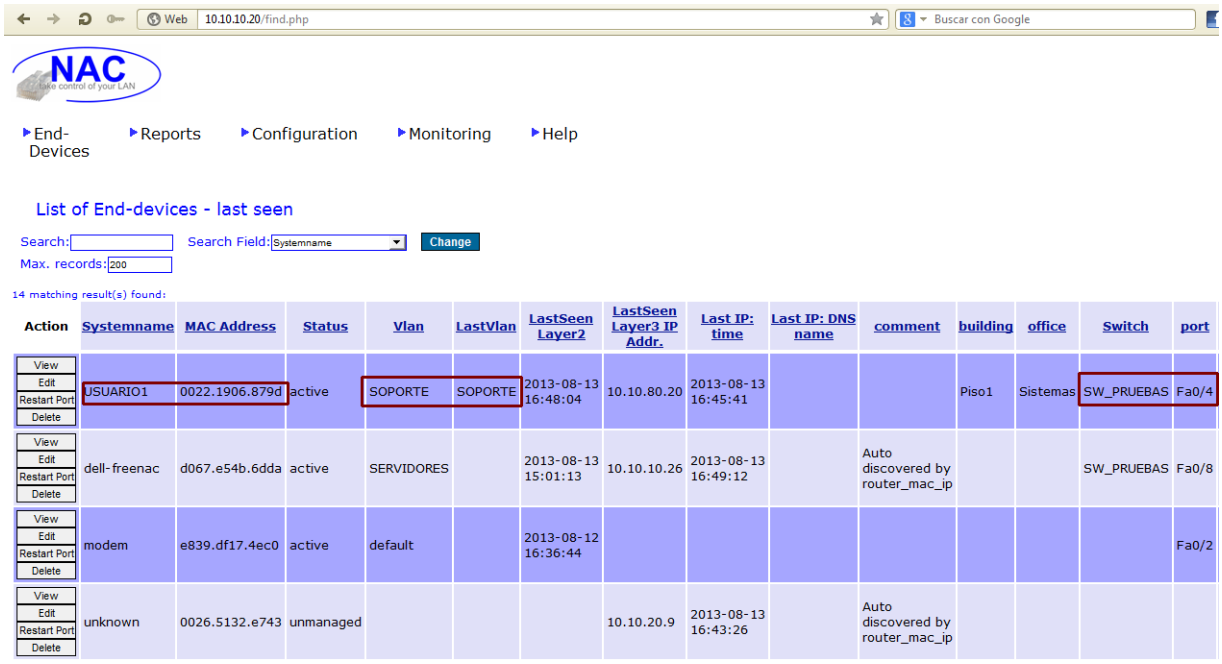

Figura 5.20: Visualización de dispositivos de red

- Para verificación de conectividad, se ejecuta el comando ping desde un equipo de la red a equipo Usuario1 como se realizo en el paso anterior

5.5. EJEMPLO DE FUNCIONAMIENTO PacketFence

PacketFence a diferencia de FreeNAC no requiere de parámetros de personalización adicionales, estos parámetros de red fueron ingresados en los pasos de instalación. Por lo tanto esta sección de enfoca en detallar un ejemplo de funcionamiento del servidor registrando equipos inalámbricos.

El laboratorio cuenta con dos redes inalámbricas configuradas en el access point las cuales son: LAB_GUEST, que es la red designada para los invitados ligada a la VLAN 70 (RESTRINGIDOS) la cual solo tendrá salida a internet y no puede comunicarse con ningún otro equipo de manera similar a los equipos invitados de la red cableada, y la red LAB_SOPORTE ligada a la VLAN 60 (SOPORTE) en la cual los usuarios que pertenecen a esta VLAN pueden conectarse, obtener una dirección IP y los derechos de acceso validos en este rango.

Nota: La red LAB_SORPORTE es un ejemplo de configuración que permite a los usuarios de la VLAN SOPORTE tener las mismas funciones de red que obtienen al conectarse a un puerto físico, de esta manera, los usuarios pueden ejercer sus funciones en cualquier lugar, en cualquier momento. Es posible crear una red inalámbrica por cada VLAN, pero antes de hacerlo es importante verificar si el access point puede irradiar más de una red inalámbrica a la vez.

Los equipos utilizados en este ejemplo son los siguientes:

MARCA	EQUIPO	MODELO	MNEMONICO	IP / Mac Address
Samsung	Tablet	Galaxy Tab 2	Usuario2	F05A.0934.A0B2
Motorola	Celular	Atrix 4G	Usuario3	40FC.8933.899A
Cisco	Access Point	AP-1142N	AP-LAB	10.10.10.8
HP	PC	Pavillion DV4	PF-Server	10.10.10.10

Tabla 5.2: Equipos utilizados en ejemplo PacketFence

Las contraseñas de las redes son:

SSID	CONTRASEÑA	VLAN ASOCIADA
LAB_GUEST	PUBLICO2013	70
LAB_SOPORTE	SOPORTE2013	60

Tabla 5.3: Contraseñas de redes inalámbricas

La clave de la red de LAB_GUEST será publicada dentro de las áreas en donde se encuentren los invitados, es decir, dentro de aulas, salas de reunión, espacios de recreación, entre otros. PacketFence aísla a todos los usuarios invitados para que no puedan comunicarse con el resto de equipos, por lo tanto, no es de gran importancia mantener la clave en secreto. La clave de la red LAB_SOPORTE, debe ser entregada a cada usuario para mayor seguridad. Se recomienda instalar un servidor Radius para incrementar el nivel de seguridad de las redes inalámbricas de usuarios autorizados.

PacketFence puede monitorear a las direcciones MAC de los usuarios conectados a las redes inalámbricas pero no tiene influencia sobre las claves de acceso, estas se configuran dentro de access point (ver Capitulo 4, Configuración de redes inalámbricas para mejor referencia).

A continuación se muestran los ejemplos de conexión de usuarios invitados y autorizados a las redes correspondientes.

5.5.1. ACCESO DE USUARIO A LA RED INALÁMBRICA DE INVITADOS (LAB_GUEST)

Para ilustrar este escenario el equipo Usuario2 (Tablet Samsung) ingresara a la red LAB_GUEST y se podrá observar a través de pantallas como se le concede acceso restringido, bloqueando cualquier tipo de conectividad a otros equipos de la red. PacketFence actúa como servidor DHCP para esta VLAN a través de la interface 10.10.70.10 y restringe la comunicación de los equipos conectados a esta red.

La siguiente figura muestra el estado inicial del equipo Usaurio2 el cual detecta las dos redes inalámbricas.

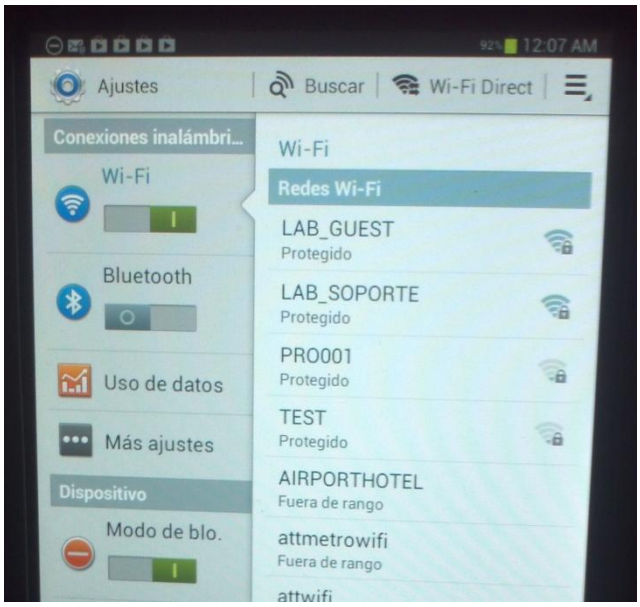

Figura 5.21: Detección de redes inalámbricas

El usuario ingresa la clave ***PUBLICO2013*** para conectarse a la red de invitados ***(LAB_GUEST).***

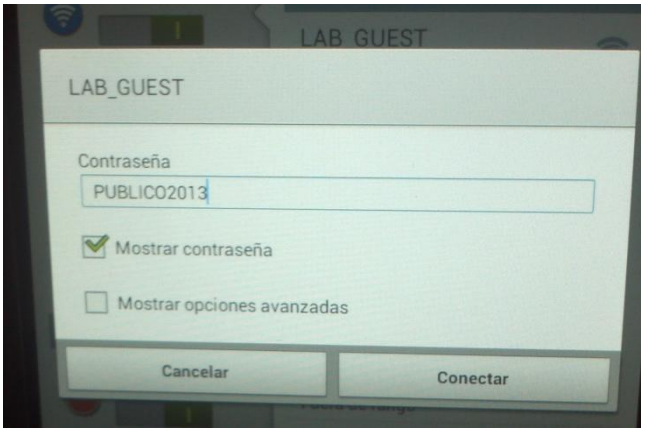

Figura 5.22: conexión a red inalámbrica LAB_GUEST

Si el ingreso de la contraseña es exitoso el equipo se conectara a la red de invitados y se le concederá una dirección IP. Para este caso se le asigno la dirección IP ***10.10.70.21.***

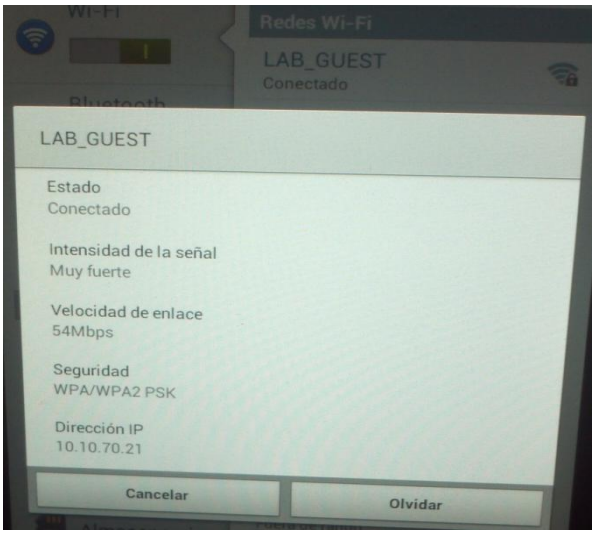

Figura 5.23: Verificación de conexión a red LAB_GUEST

Para comprobar que PacketFence impide que exista cualquier tipo de comunicación desde y hacia los equipos invitados, se realiza una prueba de conectividad desde el computador ***Usuario1*** que se encuentra en la ***VLAN 10 SERVIDORES (10.10.10.27)*** como se muestra en la siguiente figura. Los paquetes enviados a la dirección IP del ***Usuario2 (10.10.70.21)*** no son exitosos mientras que los paquetes enviados al ***Gateway (10.10.10.9)*** de la VLAN SERVIDORES son contestados sin inconveniente.

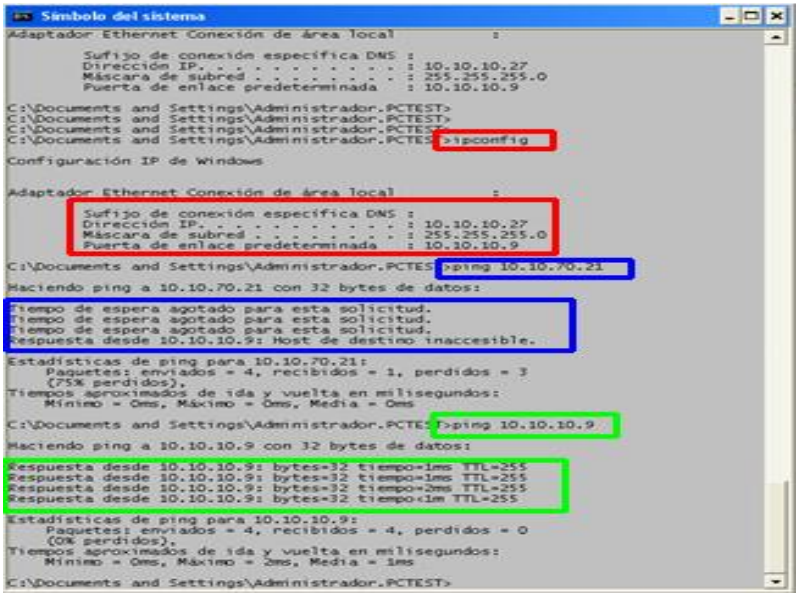

Figura 5.24: prueba de conectividad hacia la red de invitados

La conectividad entre equipos dentro de la misma ***VLAN 70 (RESTRINGIDOS)*** está permitida en el servidor PacketFence, en este caso el equipo ***Usuario1 (10.10.70.22)***

es cambiado a la VLAN 70 al igual que ***Usuario2 (10.10.70.21)*** y los dos están aislados del resto de equipos como se comprueba al realizar ping al servidor ***FreeNAC (10.10.10.20).***

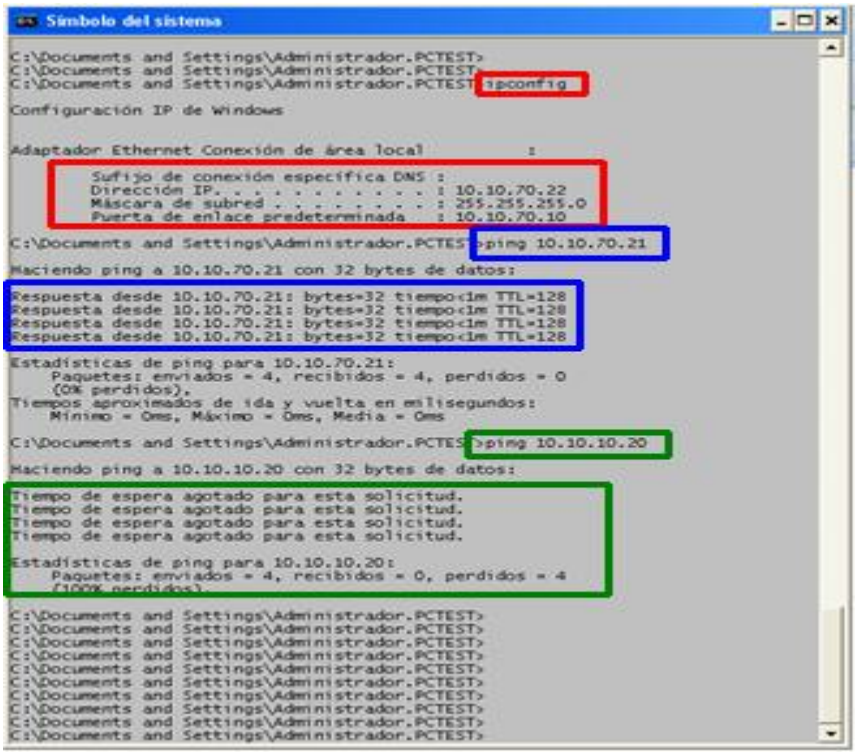

Figura 5.25: Prueba de conexión entre equipos Invitados

La administración de equipos conectados a la red inalámbrica se realiza por medio del portal web del servidor Packetfence por medio de cualquier navegador soportado apuntando a la siguiente dirección utilizando el usuario ***admin.***

https://10.10.10.10:1443/

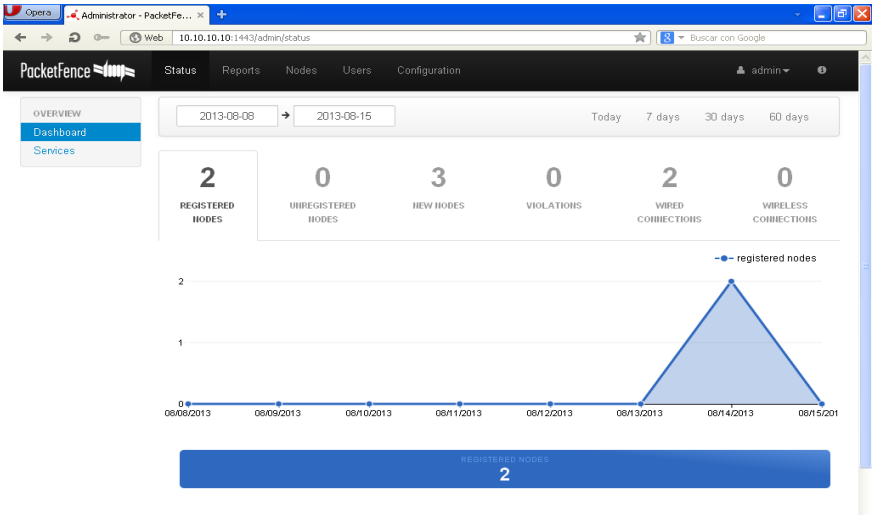

Figura 5.26: Pantalla inicio de PacketFence

Al ingresar a la pestaña NODES, en donde se lleva el control de los usuarios conectados al servidor podemos identificar la dirección MAC del equipo Usuario2 (F05A.0934.A0B2), el fabricante (Samsung) y el sistema operativo (android).

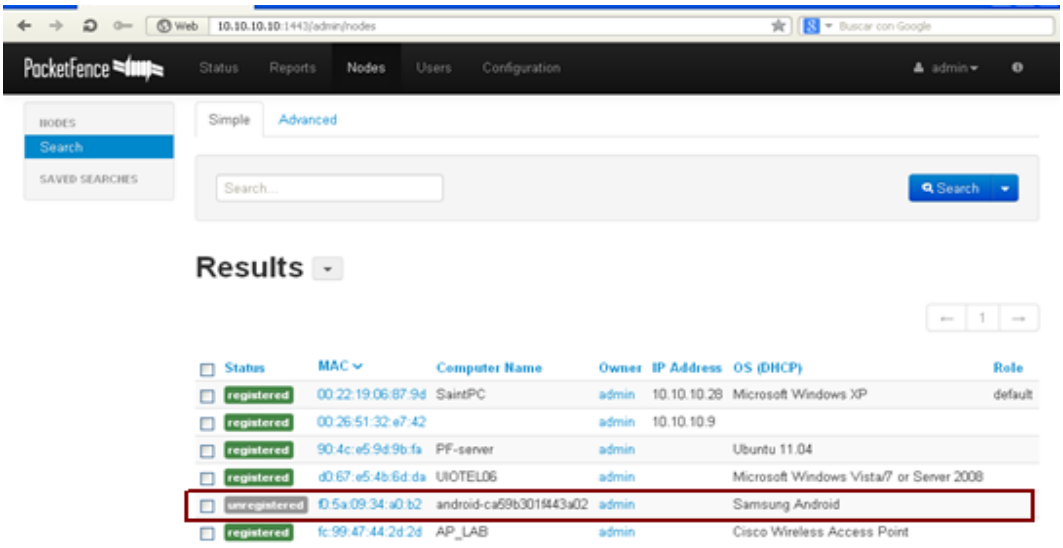

Figura 5.27: Equipo Invitado en PacketFence

Para registrar el equipo y visualizar un mejor detalle de los datos del equipo podemos ingresar a la ventana de estado dando click sobre la dirección MAC del equipo. El registro del equipo se logra al cambiar el estado ***unregistered*** a ***registered*** y guardando los cambios.

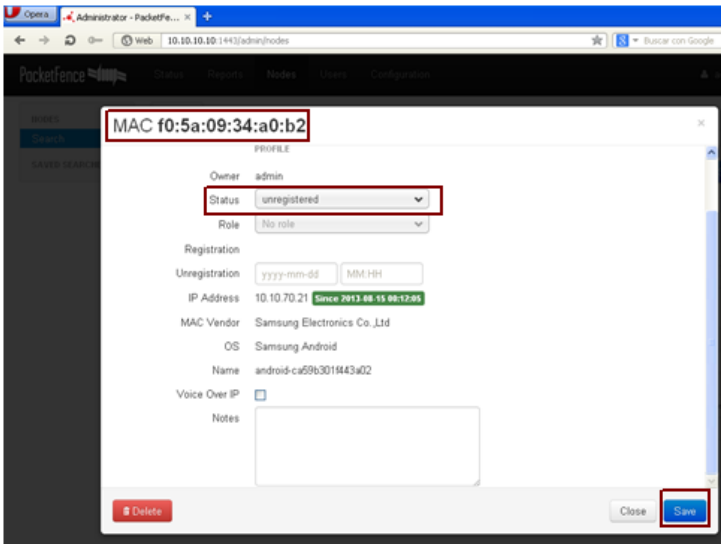

Figura 5.28: Registro de equipo invitado

5.5.2. ACCESO DE USUARIO A LA RED INALÁMBRICA DE USUARIO AUTORIZADO (LAB_SOPORTE)

En este caso el equipo Usuario3 se conecta a la red inalámbrica LAB_SOPORTE. El usuario debe ingresar la contraseña de acceso y será dirigido hacia el servidor DHCP de la VLAN 60 para obtener una dirección IP valida del rango (10.10.60.11)

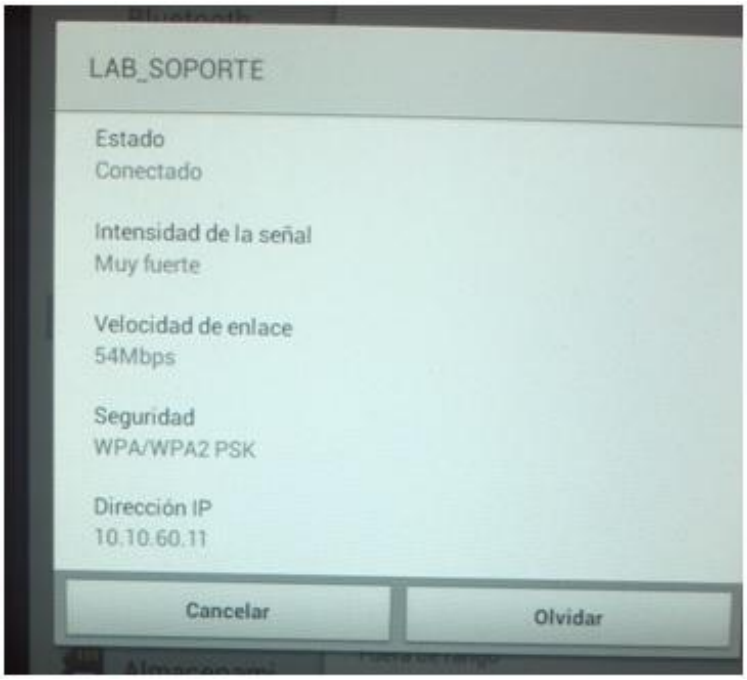

Figura 5.29: Verificación de conexión a red LAB_SOPORTE

Como esta red no está disponible para los usuarios invitados y no requiere de aislamiento, PacketFence no la administra, pero si puede llevar un control de las direcciones MAC de los equipos que se conectan a ella, de esta manera el administrador de red fácilmente puede identificar los equipos autorizados o no.

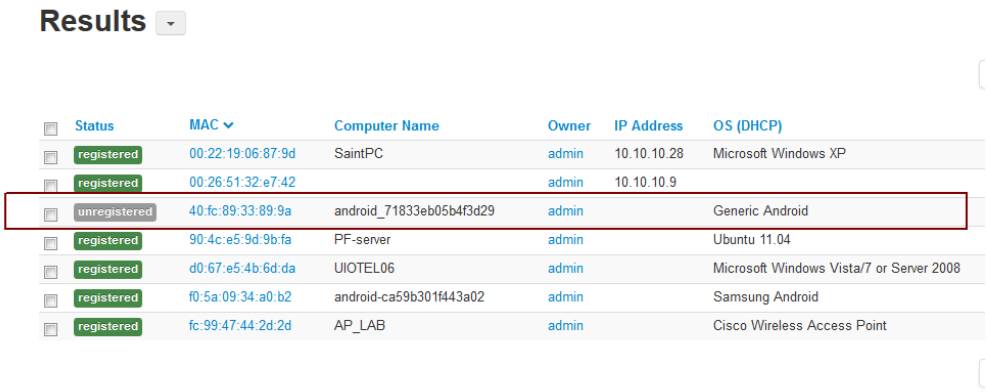

Figura 5.30: Equipo autorizado en PacketFence

En la figura anterior se aprecia que el servidor detecto un nuevo equipo inalámbrico que aparece como no registrado (***unregistered***), para visualizar de mejor manera los datos del nuevo equipo se da click en su dirección MAC.

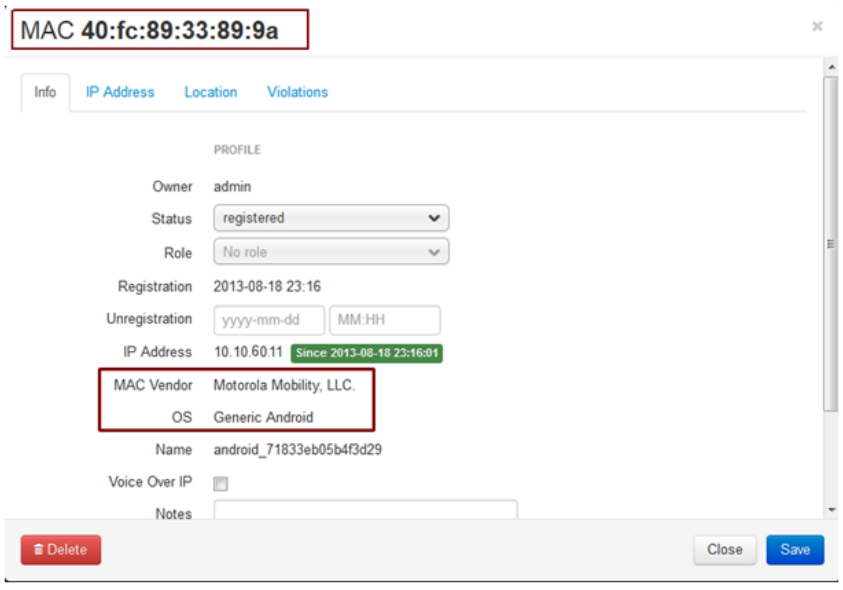

Figura 5.31: Identificación de usuario conectado en red SOPORTE

Una vez confirmado que se trata de la dirección MAC del equipo Usuario3 que tiene como IP asignada 10.10.60.11. Se realizan las pruebas de conectividad de la misma manera que fueron realizadas en el ejemplo de conexión de un usuario invitado. El

ping lo realiza el equipo ***Usuario1 (10.10.10.26)*** conectado en la VLAN SERVIDORES hacia el equipo ***Usuario3 (10.10.60.11)*** conectado en la VLAN SOPORTE y como se puede visualizar la conexión es exitosa. De esta manera se verifica que el equipo conectado en la VLAN SOPORTE posee acceso a los servicios de red otorgados a esta VLAN.

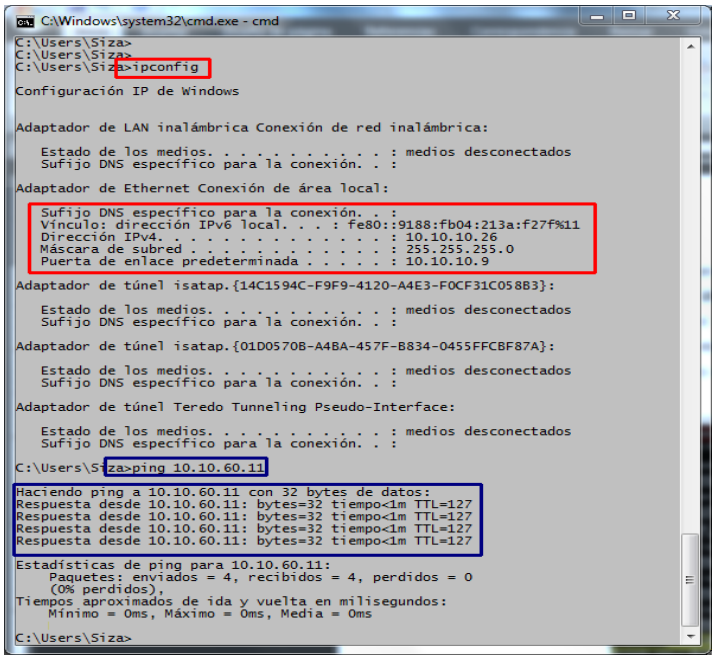

Figura 5.32: Prueba de conectividad entre equipos autorizados

5.6. ANÁLISIS ECONÓMICO DE HERRAMIENTAS DE CONTROL DE ACCESO PROPIETARIAS Y DE SOFTWARE LIBRE

Esta sección está dedicada al análisis de costos de implementación de sistemas de control de acceso de red de tres marcas propietarias (Cisco, Enterasys, ConSentry), las cuales poseen sus propias características y funcionalidades incluidas o no dentro de su esquema de licenciamiento. Adicionalmente, esta sección también presenta un análisis de costos de implementación del sistema de herramientas basadas en Software Libre que cubren y reemplazan las funcionalidades presentes en las soluciones propietarias.

Las funciones y características de cada sistema analizado se encuentran detalladas de mejor manera dentro del capítulo II que se dedica en énfasis a esta tarea.

5.6.1. ANÁLISIS DE COSTOS DE IMPLEMENTACIÓN DE SOLUCIONES PROPIETARIAS

- **Presupuesto de Implementación de la solución CISCO NAC**

Descripción	Cantidad	Características Principales	Soporte Inalámbrico	Precio Referencial
Cisco NAC Appliance 3350	1	**Tipo:** Servidor **Procesador:** Intel Xeon 3 GHz Dual core **Memoria:** 2 Gb DDR2 SDRAM **Disc Duro:** HDD 2 x 72 GB **Interfaces** 1 x Serial, 1 x PS/2 mouse, 1 x PS/2 keyboard, 1 x VGA, LAN (Gigabit Ethernet), 4 x USB **Sistema Operativo:** Cisco Clean Access Server **Cantidad de Usuarios permitidos:** 1500 usuarios	NO	$ 42.000[42]
Montaje, configuración e implementación de solución NAC (llave en Mano)	1	La solución llame en mano incluye todas las configuraciones necesarias para que la solución sea entregada al cliente probada y operativa de acuerdo a sus requerimientos de funcionamiento para 1500 usuarios	N/A	$ 6.000[43]
Capacitación y/o transferencia de conocimientos	1	Incluye capacitación formal sobre el funcionamiento de la plataforma a un grupo de administradores durante 40 horas	N/A	$ 2.000[44]
			TOTAL	**$ 50.000**

Tabla 5.4: Presupuesto Solución Cisco NAC

Nota:

- Costo estimado para instalación en una localidad dentro de la Cuidad de Quito.

[42] Precio referencial Cisco NAC Appliance. Recuperado de: http://shopper.cnet.com/soho-servers/cisco-nac-appliance-3350/4014-3125_9-32204743.html
[43] Precio referencial tomando en cuenta el valor de Hora Ingeniero en 50 usd. Referencia: ComWare S.A
[44] Precio referencial tomando en cuenta el valor de Hora Ingeniero en 50 usd. Referencia: ComWare S.A

- No incluye trabajos de cableado estructurado o provisión de cualquier elemento pasivo
- No incluye instalación y /o configuración adicional
- No incluye mantenimiento Preventivo, ni correctivo

- **Presupuesto de Implementación de la solución ENTERASYS NAC SOLUTION**

Descripción	Cantidad	Características Principales	Soporte Inalámbrico	Precio Referencial
Enterasys NAC-A-20	1	**Tipo:** Security appliance **Procesador:** 1 x Intel Quad-Core Xeon 5500 series **Memoria:** 12 GB (max) **Disc Duro:** 250 GB x 2 - Serial ATA-150 **Interfaces** 1 x Gigabit Ethernet 4 x USB **Sistema Operativo:** NAC v3.3 **Cantidad de Usuarios permitidos:** 3.000 usuarios	NO	$ 13.429[45]
Montaje, configuración e implementación de solución NAC (llave en Mano)	1	La solución llame en mano incluye todas las configuraciones necesarias para que la solución sea entregada al cliente probada y operativa de acuerdo a sus requerimientos de funcionamiento para 3000 usuarios	N/A	$ 3.500
Capacitación y/o transferencia de conocimientos	1	Incluye capacitación formal sobre el funcionamiento de la plataforma a un grupo de administradores durante 40 horas	N/A	$ 2.000
			TOTAL	**$ 18.929**

Tabla 5.5: Presupuesto Solucion Enterays

Nota:

- Costo estimado para instalación en una localidad dentro de la Cuidad de Quito.
- No incluye trabajos de cableado estructurado o provisión de cualquier elemento pasivo
- No incluye instalación y /o configuración adicional
- No incluye mantenimiento Preventivo, ni correctivo

[45] Precio Referencial Enterasys NAC Solution. Recuperado de: http://shopper.cnet.com/networking/enterasys-nac-out-of/4014-3243_9-33836558.html

- **Presupuesto de Implementación de la solución ConSentry LanShield**

Descripción	Cantidad	Características Principales	Soporte Inalámbrico	Precio Referencial
Consentry LANshield Controller, CS1000-ACAC	1	**Interfaces** 4 x puertos SFP de datos seguros 1 x Puerto mantenimiento **Sistema Operativo:** LANShield OS 3.0 **Cantidad de Usuarios permitidos:** 1.000 Usuarios **Funciones:** El Controlador LANShield está detrás de los switches existentes para aumentar el control LAN con el de usuario y la aplicación	NO	$ 17.995[46]
Consentry LANShield Switch, CS4048	1	**Funciones:** seguimiento de toda la actividad del usuario para la auditoría, soporta una fuerza de trabajo más dinámica y diversa	NO	$ 13.955
Montaje, configuración e implementación de solución NAC (llave en Mano)	1	La solución llame en mano incluye todas las configuraciones necesarias para que la solución sea entregada al cliente probada y operativa de acuerdo a sus requerimientos de funcionamiento para 1.000 usuarios	N/A	$ 4.000
Capacitación y/o transferencia de conocimientos	1	Incluye capacitación formal sobre el funcionamiento de la plataforma a un grupo de administradores durante 40 horas	N/A	$ 0.00[47]
			TOTAL	**$ 31.954**

Tabla 5.6: Presupuesto Solución ConSentry

Nota:

- Costo estimado para instalación en una localidad dentro de la Cuidad de Quito.
- No incluye trabajos de cableado estructurado o provisión de cualquier elemento pasivo
- No incluye instalación y /o configuración adicional

[46] Precio referencial ConSentry LanShield. Recuperado de: http://www.itsecurity.com/press-releases/press-release-consentry-lan-security-110606/

[47] ConSentry Sield Incluye la capacitación formal sin ningún costo adicional con la compra de sus equipos.

5.6.2. ANÁLISIS DE COSTOS DE IMPLEMENTACIÓN DE SOLUCIONES SOFTWARE LIBRE

- **Presupuesto de Implementación de la solución de Herramientas NAC basadas en Software Libre**

Descripción	Cantidad	Características Principales	Soporte Inalámbrico	Precio Referencial
Servidor para instalación de herramientas FreeNAC y PacketFence	2	**Tipo:** Destop PC, Laptop o Server **Procesador:** Intel or AMD CPU 3 GHz dual-core **Memoria:** 2G B of RAM (minimo) **Disc Duro:** 20 GB of disk space minimo (RAID 1 recommended) **Interfaces** 1 x Serial, 1 x PS/2 mouse, 1 x PS/2 keyboard, 1 x VGA, 1x LAN (Gigabit Ethernet), 4 x USB **Sistema Operativo:** FreeNAC: Ubuntu server 8.4.04 custom release PacketFence: Ubuntu 12.04 LTS	NO	$ 2.800
Licencia FreeNAC	1	**Funciones:** Software dedicado a control de Acceso NAC para red cableada. **Cantidad de Usuarios permitidos:** **SIN RESTRICCION**	NO	$ 0.00
Licencia PacketFence	1	**Funciones:** Software dedicado a control de Acceso NAC para red Inalámbrica. **Cantidad de Usuarios permitidos:** **SIN RESTRICCION**	**SI**	$ 0.00
Montaje, configuración e implementación de solución NAC (llave en Mano)	1	La solución llame en mano induye todas las configuraciones necesarias para que la solución sea entregada al cliente probada y operativa de acuerdo a sus requerimientos	N/A	$ 2.000
Capacitación y/o transferencia de conocimientos	1	Incluye capacitación formal sobre el funcionamiento de la plataforma. 20 horas	N/A	$ 1.000
			TOTAL	**$ 5.800**

Tabla 5.7: Presupuesto Solución Software Libre

Nota:

- Costo estimado para instalación en una localidad dentro de la Cuidad de Quito.
- No incluye trabajos de cableado estructurado o provisión de cualquier elemento pasivo de red
- No incluye instalación y /o configuración adicional
- No incluye mantenimiento Preventivo, ni correctivo

5.7. MATRIZ FODA DEL PROYECTO

CAPITULO VI

6. CONCLUSIONES Y RECOMENDACIONES

6.1.CONCLUSIONES

- El análisis de funcionalidad de las herramientas NAC facilito la selección de las herramientas Software Libre utilizadas en el sistema al comparar sus funciones con respecto a las ofrecidas por los fabricantes líderes del mercado.
- El implementar el laboratorio de red basado en las premisas de diseño ayudo a llevar un control de los resultados deseados al seguir de forma ordenada el proceso de diseño y limitando el alcance del proyecto hacia la meta planteada.
- Los ejemplos de utilización de la plataforma sirvieron como protocolo de pruebas para validar la configuración del sistema. Estos ejemplos ayudaron a corregir errores de funcionamiento modificando configuraciones en tiempo real.
- Mediante las pruebas realizadas se pudo verificar que la asignación dinámica de VLANs optimizo el tiempo empleado por los administradores de red y usuarios para permitir su acceso a la red, ya que el tiempo es menor al utilizado por el administrador al configurar los puertos del switch de forma manual.
- El protocolo SNMP constituye una parte primordial de la configuración en los equipos del sistema. Este protocolo es el encargado de comunicar a los servidores NAC y equipos de red para que los comandos de configuración sean ejecutados de forma automática sin necesidad de intervención por parte del personal de administración.
- Es importante crear VLANs dentro del diseño de la red de cualquier institución, de esta manera en más fácil agrupar usuarios con funciones similares, identificar de mejor manera errores y aplicar correctivos sin afectar a todos los usuarios de red.
- La utilización de la VLAN RESTRINGIDOS facilita de gran manera la administración de usuarios invitados de permanencia corta en la red. La

limitación de acceso y bloqueos que tienen los usuarios de esta VLAN ayuda a mejorar la seguridad informática de las empresas evitando posibles ataques de equipos desconocidos.

- La asignación dinámica de VLANs no afecta el funcionamiento de otros servicios asignados a los usuarios como por ejemplo DHCP, DNS, telefonía IP, etc. Se demostró con ejemplos prácticos la funcionalidad de la plataforma en un sistema de red en producción sin inconvenientes en su operación.
- El incremento de ambientes de redes inalámbricas en las empresas de la actualidad, obliga a que también existan controles de acceso de usuarios. Se comprobó que al utilizar un sistema de acceso a la red basada en Software Libre como PacketFence es posible llevar a cabo un control no invasivo sobre los usuarios que se comunican a por medio de red inalámbrica.
- Aunque en la actualidad muchas empresas no confían en gran manera en los sistemas basados en Software Libre, a través de este proyecto se demostró que su implementación puede ser llevada a cabo en empresas que cumplan con los requerimientos mínimos de equipamiento de hardware, software y personal con experiencia básica en manejo de tecnologías de información sin necesidad de invertir grandes cantidades de dinero en comprar equipos propietarios, contratación de personal especializado o capacitar a su personal por largos periodos de tiempo en estas tecnologías.

6.2.RECOMENDACIONES

- La tecnología VMPS utilizada en este proyecto esta implementada íntegramente en equipo de red marca *CISCO* por lo tanto es imperativo que el personal que configure los equipos tenga conocimientos básicos en manejo de esta plataforma.
- Si los servidores van a ser instalados en forma de maquina virtual, se recomienda que se deshabiliten los programas de seguridad como firewalls, antivirus, etc. De esta manera se permitirá el establecimiento de sesiones y apertura de puertos para la comunicación entre equipos.

- Utilizar el protocolo SNMP en versión 3 para mejorar los niveles de seguridad de la red ya que en esta versión los mensajes viajan encriptados y requieren inicio de sesión por medio de ingreso de usuario y contraseña antes de enviar cualquier mensaje entre equipos.
- El personal encargado de configurar FreeNAC y PacketFence debe tener conocimientos básicos de administración de servidores Linux, bases de datos MySQL para facilitar la detección y corrección de problemas presentes en el proceso de implementación del sistema.
- Los switches deben tener una dirección IP en la misma VLAN que el servidor FreeNAC para facilitar el envió de paquetes SNMP entre equipos, si estos se encuentran en VLANs diferentes es probable que el switch de Core no realice el ruteo de todos los paquetes enviados.
- En los servidores Linux se debe instalar herramientas gratuitas de administración como netstat, BUM o zenmap para monitorear el estado de los puertos abiertos o servicios activos en cada servidor esto facilita la administración sin necesidad de ingresar varios comandos en la terminal.
- Antes de realizar ediciones a cualquier archivo de configuración de los servidores se recomienda realizar una copia de respaldo del mismo para evitar posibles problemas ocasionados por configuraciones erróneas.
- La radiación de varias redes inalámbricas desde un mismo access point es una característica propia del modelo de equipo instalado, se recomienda verificar si el modelo de access point seleccionado cumple con esta característica ya que la mayoría de equipos para interiores pueden radiar una sola red a la vez.

Bibliografía:

- Deal, R. (2008) *Cisco Certified Network Associate Study Guide*. United States: McGraw-Hill. Copyright 2008 by The McGraw-Hill Companies
- Esmoris, D. *Control de Acceso a Redes* (Trabajo Investigativo*).* Facultad Informática de la Universidad Nacional de la Plata.
- Junta de Comunidades de Castilla-La Mancha (2009). *Taller de Migración al Software Libre*. Centro de Excelencia de Software Libre (Versión 1.0) Castilla: La Mancha. Creative Commons by-Sa
- *Network Admission Control (NAC) Framework.* Recuperado de: http://www.cisco.com/en/US/netsol/ns617/index.html
- *Consentry LanShield*. Recuperado de: http://www.ruthvictor.com/pdf/NAC/Datasheet/ConSentry_LANShield_controller_DS_012608.pdf
- *Elemental Security Plataform*. Recuperado de: http://www.elementalsecurity.com/network-access-control/
- *Enterasys NAC.* Recuperado de: http://www.enterasys.com/company/literature/nac-ds.pdf
- *PacketFence*. Recuperado de: http://www.packetfence.org/about/overview.html
- *FreeNAC*. Recuperado de: http://freenac.net/es
- *Precio referencial Cisco NAC Appliance*. Recuperado de: http://shopper.cnet.com/soho-servers/cisco-nac-appliance-3350/4014-3125_9-32204743.html
- *Precio Referencial Enterasys NAC Solution*. Recuperado de: http://shopper.cnet.com/networking/enterasys-nac-out-of/4014-3243_9-33836558.html
- *Precio referencial ConSentry LanShield.* Recuperado de: http://www.itsecurity.com/press-releases/press-release-consentry-lan-security-110606/

ANEXOS

Anexo I

CONFIGURACION DE SWITCH CORE

```
LAB_SWITCH_CORE#sh run
Building configuration...

Current configuration : 4402 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname LAB_SWITCH_CORE
!
boot-start-marker
boot-end-marker
!
no logging console
enable password cisco
!
username cisco privilege 15 password 0 cisco
username Comware privilege 15 password 0 comware2013
!
!
no aaa new-model
clock timezone EC -5
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
!
spanning-tree mode mst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
spanning-tree mst configuration
 name LAB
!
spanning-tree mst 0 priority 24576
spanning-tree vlan 6 priority 4096
!
vlan internal allocation policy ascending
!
!
interface GigabitEthernet0/1
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/2
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/3
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/4
 switchport access vlan 6
 switchport mode access
```

```
 switchport nonegotiate
!
interface GigabitEthernet0/5
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/6
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/7
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/8
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/9
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/11
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/13
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/14
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/15
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/16
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/17
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
```

```
!
interface GigabitEthernet0/18
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet0/21
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/22
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/23
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/24
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/25
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/26
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/27
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/28
 switchport access vlan 6
 switchport mode access
 switchport nonegotiate
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan6
 description GESTION_LAB
 ip address 10.6.0.10 255.255.255.0
!
interface Vlan10
 ip address 10.10.10.2 255.255.255.0
```

```
interface Vlan20
 ip address 10.10.20.2 255.255.255.0
!
interface Vlan30
 ip address 10.10.30.2 255.255.255.0
!
interface Vlan40
 ip address 10.10.40.2 255.255.255.0
!
interface Vlan50
 ip address 10.10.50.2 255.255.255.0
!
interface Vlan60
 ip address 10.10.60.2 255.255.255.0
!
ip default-gateway 10.6.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.6.0.1
no ip http server
no ip http secure-server
!
!
ip sla enable reaction-alerts
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 privilege level 15
 login local
 transport input all
line vty 5 15
 exec-timeout 15 0
 privilege level 15
 login local
 transport input all
!
ntp source Vlan6
ntp server 10.6.0.10
end

LAB_SWITCH_CORE#
```

Anexo II

CONFIGURACION DE SWITCH ACCESO (SW_PRUEBAS)

```
SW_PRUEBAS#sh run
Building configuration...

Current configuration : 5357 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW_PRUEBAS
!
boot-start-marker
boot-end-marker
!
!
username cisco privilege 15 password 0 cisco
username comware privilege 15 password 0 comware2013
no aaa new-model
clock timezone ec 0
system mtu routing 1500
ip subnet-zero
ip routing
no ip dhcp use vrf connected
!
vmps reconfirm 120
vmps retry 5
vmps server 10.10.10.20 primary
vmps server 10.10.10.18
!
spanning-tree mode mst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 description TO_SW_CORE
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan dynamic
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport access vlan dynamic
 switchport mode access
 spanning-tree portfast

interface FastEthernet0/4
 switchport access vlan dynamic
 switchport mode access
 spanning-tree portfast
!

interface FastEthernet0/5
 switchport access vlan dynamic
```

```
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan dynamic
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan dynamic
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/8
switchport access vlan dynamic
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/1
!
interface Vlan6
 ip address 10.6.0.24 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.6.0.10
ip http server
ip http secure-server
!
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.10.10.10 version 2c public  mac-notification snmp
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 login local
line vty 5 15
 exec-timeout 0 0
 privilege level 15
 login local
!
mac address-table notification change interval 0
mac address-table aging-time 3600
end

SW_PRUEBAS#
```

Anexo III

CONFIGURACION DE ACCESS POINT INALAMBRICO

```
AP_LAB#sh runn
Building configuration...
Current configuration : 5350 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname AP_LAB
!
aaa new-model
!
aaa session-id common
clock timezone 1 -5
ip domain name WORKGROUP
!
dot11 syslog
dot11 vlan-name RESTRINGIDO vlan 70
dot11 vlan-name SOPORTE vlan 60
!
dot11 ssid LAB_GUEST
  vlan 70
  authentication open
  authentication key-management wpa
  mbssid guest-mode
  wpa-psk ascii 0 PUBLICO2013
!
dot11 ssid LAB_SOPORTE
  vlan 60
  authentication open
  authentication key-management wpa
  mbssid guest-mode
  wpa-psk ascii 0 SOPORTE2013
!
power inline negotiation prestandard source
!
username cisco privilege 15 password 0 cisco
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm tkip
 !
 encryption vlan 60 mode ciphers aes-ccm tkip
 !
 encryption vlan 70 mode ciphers aes-ccm tkip
 !
 ssid LAB_GUEST
 !
 ssid LAB_SOPORTE
 !
 antenna gain 0
 traffic-metrics aggregate-report
 mbssid
 speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
```

```
 no preamble-short
 station-role root access-point
!
interface Dot11Radio0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.60
 encapsulation dot1Q 60
 no ip route-cache
 bridge-group 60
 bridge-group 60 subscriber-loop-control
 bridge-group 60 block-unknown-source
 no bridge-group 60 source-learning
 no bridge-group 60 unicast-flooding
 bridge-group 60 spanning-disabled
!
interface Dot11Radio0.70
 encapsulation dot1Q 70
 no ip route-cache
 bridge-group 70
 bridge-group 70 subscriber-loop-control
 bridge-group 70 block-unknown-source
 no bridge-group 70 source-learning
 no bridge-group 70 unicast-flooding
 bridge-group 70 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm tkip
 !
encryption vlan 60 mode ciphers aes-ccm tkip
 !
 encryption vlan 70 mode ciphers aes-ccm tkip
 !
 ssid LAB_GUEST
 !
 ssid LAB_SOPORTE
 !
 antenna gain 0
 no dfs band block
 mbssid
 speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
 channel dfs
 station-role root access-point
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1.60
 encapsulation dot1Q 60
```

```
 no ip route-cache
 bridge-group 60
 bridge-group 60 subscriber-loop-control
 bridge-group 60 block-unknown-source
 no bridge-group 60 source-learning
 no bridge-group 60 unicast-flooding
 bridge-group 60 spanning-disabled
!
interface Dot11Radio1.70
 encapsulation dot1Q 70
 no ip route-cache
 bridge-group 70
 bridge-group 70 subscriber-loop-control
 bridge-group 70 block-unknown-source
 no bridge-group 70 source-learning
 no bridge-group 70 unicast-flooding
 bridge-group 70 spanning-disabled
!
interface GigabitEthernet0
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 duplex auto
 speed auto
 no keepalive
!
interface GigabitEthernet0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface GigabitEthernet0.60
 encapsulation dot1Q 60
 no ip route-cache
 bridge-group 60
 no bridge-group 60 source-learning
 bridge-group 60 spanning-disabled
!
interface GigabitEthernet0.70
 encapsulation dot1Q 70
 no ip route-cache
 bridge-group 70
 no bridge-group 70 source-learning
 bridge-group 70 spanning-disabled
!
interface BVI1
 ip address 10.10.10.8 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.10.10.2
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
logging source-interface BVI1
radius-server host 10.10.10.10 auth-port 1812 acct-port 1813 key useStrongerSecret
!
!
!
line con 0
line vty 0 4
!
end

AP_LAB#
```

Anexo IV

CONFIGURACION DE CENTRAL TELEFONICA – Cisco Communication Manager Express

```
CME_CW_UIO#sh runn
Building configuration...
current configuration : 9010 bytes
!
! No configuration change since last restart
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CME_CW_UIO
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
clock timezone ec -5 0
!
no ipv6 cef
ip source-route
ip cef
!
ip dhcp excluded-address 10.10.20.1 10.10.20.20
ip dhcp excluded-address 10.10.10.1 10.10.10.25
ip dhcp excluded-address 10.10.30.1 10.10.30.10
ip dhcp excluded-address 10.10.40.1 10.10.40.10
ip dhcp excluded-address 10.10.50.1 10.10.50.10
ip dhcp excluded-address 10.10.60.1 10.10.60.10
ip dhcp excluded-address 10.10.70.1 10.10.70.10
!
ip dhcp pool TELEFONIA
 network 10.10.20.0 255.255.255.0
 option 150 ip 10.10.20.1
!
ip dhcp pool SOPORTE
 network 10.10.60.0 255.255.255.0
 dns-server 10.6.0.1
 default-router 10.10.60.1
!
ip dhcp pool SERVERS
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.2
 dns-server 10.6.0.1
!
ip dhcp pool FINAN
 network 10.10.40.0 255.255.255.0
 default-router 10.10.40.1
 dns-server 10.6.0.1
!
ip dhcp pool ADMIN
 network 10.10.30.0 255.255.255.0
 default-router 10.10.30.1
 dns-server 10.6.0.1
!
ip dhcp pool VENTAS
 network 10.10.50.0 255.255.255.0
 default-router 10.10.50.1
 dns-server 10.6.0.1
```

```
!
no ip domain lookup
multilink bundle-name authenticated
crypto pki token default removal timeout 0
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 h323
 sip
  registrar server expires max 3600 min 3600
  localhost dns:10.2.0.18
  no call service stop
!
voice class codec 1
 codec preference 1 g711alaw
 codec preference 2 g711ulaw
 codec preference 3 g729r8
!
!
voice register global
 mode cme
 source-address 10.10.20.1 port 5060
 max-dn 15
 max-pool 15
 load 9971 sip9971.9-1-1SR1
 authenticate register
 authenticate realm all
 dialplan-pattern 2 25.. extension-length 4
 dialplan-pattern 4 60.. extension-length 4
 tftp-path flash:
 create profile sync 1322633207226396
!
voice register dn  1
 number 6003
 shared-line
 label User 3
 mwi
!
voice register dialplan 1
 type 7940-7960-others
 pattern 1 60..
 pattern 2 25..
!
voice register pool  1
 id mac 04C5.A4B0.D825
 type 9971
 number 1 dn 1
 dialplan 1
 dtmf-relay rtp-nte
 voice-class codec 1
 username 6003 password 6003
!
license udi pid CISCO2911/K9 sn FTX1541AJZZ
license accept end user agreement
license boot module c2900 technology-package uck9
hw-module pvdm 0/0
```

```
!
!
!
username comware privilege 15 secret 5 $1$upjN$TQtsoTWIxJHxu50M8Hwi9/
username cisco privilege 15 password 0 cisco
!
redundancy
!
no ip ftp passive
ip ssh version 2
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
 no cdp enable
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.6
 description Vlan Gestion
 encapsulation dot1Q 6
 ip address 10.6.0.51 255.255.255.0
!
interface GigabitEthernet0/0.10
 description vlan DATOS
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 description Vlan TELEFONIA
 encapsulation dot1Q 20
 ip address 10.10.20.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip default-gateway 10.6.0.1
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip http path flash0:
!
ip route 0.0.0.0 0.0.0.0 10.6.0.1
ip route 10.20.0.0 255.255.0.0 GigabitEthernet0/2
!
control-plane
!
mgcp profile default
!
gatekeeper
 shutdown
!
ephone-type 7937g
 device-name Conference Station 7937G
 device-type 7937
 num-buttons 1
 max-presentation 6
```

```
telephony-service
 max-ephones 15
 max-dn 15
 ip source-address 10.10.20.1 port 2000
 max-redirect 5
 system message LAB CISCO UC COMWARE
 cnf-file location flash:
 load 7906 SCCP11.9-1-1SR1S.loads
 load 7937 apps37sccp.1-4-4-0.bin
 load 7945 SCCP45.9-1-1SR1S.loads
 load 7975 SCCP75.9-1-1SR1S.loads
 max-conferences 8 gain -6
 moh flash:/cucme-mlpp/G729/UPA.wav
 web admin system name comware secret 5 $1$1d5A$BNcAirI1FrhtMx8sUGUit1
 transfer-system full-consult
 create cnf-files version-stamp 7960 Aug 09 2013 16:17:21
!
ephone-dn  1  dual-line
 number 6001
 label prueba1
!
ephone-dn  2  dual-line
 number 6002
 label 6002
 description Usuario 2
!
ephone-dn  3  dual-line
 number 6004
 label USER 4
 description USER 4
!
ephone  2
 mac-address 8CB6.4F57.A691
 username "User2"
 type 7945
 button  1:2
!
ephone  4
 mac-address 0004.F2EB.8DBC
 type 7937
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login local
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 privilege level 15
 login local
 transport input ssh
line vty 5 15
 privilege level 15
 login local
 transport input all
!
scheduler allocate 20000 1000
ntp master
end
```