ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

ESTUDIO PARA LA ASIGNACION DINAMICA DE ACCESO Y DIRECCIONAMIENTO DE VLAN's (RED INTELIGENTE) PARA LA SECRETARÍA NACIONAL DE TELECOMUNICACIONES (SENATEL)

DIEGO JAVIER JARAMILLO DE LA CRUZ

SANGOLQUÍ – ECUADOR

ENERO 2011

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: "ESTUDIO PARA LA ASIGNACIÓN DINÁMICA DE ACCESO Y DIRECCIONAMIENTO DE VLAN'S (RED INTELIGENTE) PARA LA SECRETARÍA NACIONAL DE TELECOMUNICACIONES (SENATEL).", ha sido desarrollado en su totalidad por el señor DIEGO JAVIER JARAMILLO DE LA CRUZ con CC: 1713729885, bajo nuestra dirección.

Atentamente

_____

Ing. Darwin Aguilar

DIRECTOR

_____

Ing. Carlos Romero

CODIRECTOR

RESUMEN

Con el análisis del proyecto se podrá plantear el diseño de una nueva red de administración y de control dentro de la Secretaría Nacional de Telecomunicaciones para la asignación dinámica de las VLAN's, las que serán asignadas a través de un servidor VMPS para los equipos de los funcionarios y poder entregar los servicios correspondientes, así como para los visitantes y asignar el acceso a Internet a los mismos.

Con el objetivo de trabajar con los mismos equipos de la Institución, se utilizó un software con las especificaciones de la red existente que cumple con las necesidades de asignación dinámica, además de poseer una interfaz web en tiempo real para observar todas las actividades que se vayan desarrollando dentro de la red.

Se presenta todo el desarrollo de configuración del servidor, así como de las pruebas que se han desarrollado para los múltiples casos que se puedan presentar y ver los resultados en la interfaz anteriormente mencionada.

Finalmente el estudio de una nueva red dinámica dio como resultado un modelo que se adapta a la presente red dentro de la Secretaría Nacional de Telecomunicaciones alcanzando un mayor rendimiento y facilidades de control para el administrador y la obtención de los diferentes servicios para cada uno de los funcionarios.

DEDICATORIA

Este proyecto se lo dedico a mis padres, hermanos, familia y amigos que durante el transcurso de mi vida me han demostrado un apoyo completo para cumplir cada una de mis metas, y que están en todo momento en mi corazón y son mi fuerza para continuar adelante. Al esfuerzo de mis padres así como el amor y la confianza de creer en mí cada día, para mí siempre serán un ejemplo de superación en todos los ámbitos los que me impulsan para crecer cada día y dar mi mejor esfuerzo para todo lo que me proponga.

Diego J. Jaramillo C.

AGRADECIMIENTOS

Gracias en primer lugar a Dios por todo lo que Él ha hecho en mi vida y que por su gran voluntad, quiso que yo esté en este mundo y pueda demostrar al mundo y a mí mismo que cuando uno se plantea metas, el creer en sí mismo, el esfuerzo y las ganas de continuar adelante, nada de imposible.

A mis padres Gustavo y Sonia, que han sido mis pilares en la vida, los que me han enseñado a dar mis primeros pasos para salir al mundo como una persona de bien y buenos valores, además de compartir todos los momentos importantes de mi vida y su apoyo incondicional para seguir creciendo en la vida.

A mis hermanos Andrés y Carolina, los que han crecido conmigo y juntos hemos aprendido a ser un equipo y nunca soltarnos de la mano, siempre para ver por cada uno de nosotros y mantener el lazo que nos une cada vez mas fuerte durante toda nuestra vida.

A mis amigos, gracias por haber compartido esos momentos inolvidables que quedarán en mis recuerdos y espero seguir viviendo muchos más, además que me han demostrado ser un apoyo para esos momentos difíciles y me han sabido dar una mano para levantarme y darme fuerza para continuar.

A mi novia Carolina porque además de ser la persona que se gano mi corazón y mi apoyo para mis metas, me ha demostrado ser una persona de superación y de que en verdad cuando uno se propone no rendirse ante un error es capaz de todo en la vida y de que el amor y el respeto perdure por el resto de nuestras vidas.

A mis profesores, los que han dedicado su tiempo para transmitir sus conocimientos y corregir mis errores además de la gran amistad que me han brindado, y me han mostrado lo primordial para salir a luchar en la vida como persona y profesional.

Diego J. Jaramillo C.

PROLOGO

El desarrollo de este proyecto permitirá desarrollar una red inteligente que automatice las configuraciones que se han venido realizado de forma manual dentro de la Institución, cuando un funcionario cambie de Dirección no haya la necesidad de que una persona del departamento de Informática tenga que volver a configurar los parámetros en el equipo sino que esto lo haga directamente el servidor.

Este estudio se va a implementar con el fin de facilitar el control por parte del administrador de la red y de aumentar la seguridad de acceso a la red ya que dentro de la Secretaría Nacional de Telecomunicaciones se maneja información sumamente importante que las personas fuera de ella no deben por ningún motivo tener acceso y mucho menos de modificar la misma.

Este proyecto busca realizar un análisis comparativo entre el actual procedimiento de asignación a las redes de área local virtuales para ofrecer los servicios y el manejo de la información correspondiente así como de la detección de los equipos que no consten dentro de los registros y establecer la conexión correspondiente a los servicios establecidos.

INDICE GENERAL

CAPÍTULO I

INTRODUCCION

CAPÍTULO II

ESTADO ACTUAL DE LA RED INFORMATICA DE LA SENATEL

CAPÍTULO III

REDISEÑO DE RED INTELIGENTE DINAMICA DE EQUIPOS

CAPÍTULO VI

PRUEBAS Y ANALISIS DE DESEMPEÑO DEL DISEÑO

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

ANEXOS

INDICE DE TABLAS

INDICE DE FIGURAS

CAPITULO I

INTRODUCCIÓN

1.1. Redes Informáticas

1.1.1. Concepto

En la actualidad existen millones de redes con el fin de realizar la comunicación entre dos o más ordenadores que se encuentran en ubicaciones distantes.

Figura 1.1.Redes Informáticas

Las redes informáticas son una serie de computadoras, dispositivos móviles o ambos que se encuentran conectados entre sí, sea por un medio físico (cable) o de manera inalámbrica, para el transporte de archivos y repartir recursos tales como impresoras, faxes así mismo como correo electrónico, juegos, aplicaciones, etc.

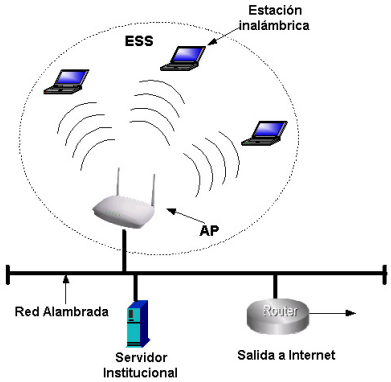


Figura 1.2. Red alámbrica e inalámbrica

Dentro de todas las redes siempre existe un equipo denominado administrador, el cual es el encargado de permitir o restringir el acceso hacia los recursos de su red, lo cual lo asignará de acuerdo a las necesidades que cada uno de los usuarios requiera.

1.1.2. Clasificación

Las redes informáticas se pueden clasificar de varias maneras, estas pueden ser de acuerdo a su direccionalidad, alcance, topología, método de conexión y relación funcional.

El objetivo de clasificar las redes informáticas de acuerdo a estos parámetros es de buscar el diseño más óptimo para los diferentes requerimientos o situaciones geográficas en las que se encuentren los elementos que conformaran la red. [1]

A continuación se muestra la clasificación de las redes de acuerdo a lo señalado anteriormente:

Tabla 1.1. Clasificación de las redes informáticas

	TIPO	DESCRIPCIÓN
Direccionalidad	Simplex	Los paquetes viajan en un solo sentido
	Half-Dúplex	Los paquetes viajan en cualquier sentido pero en tiempos diferentes
	Full-Dúplex	Los paquetes viajan en cualquier sentido a cualquier tiempo

Alcance	PAN	Redes de Área Personal
	LAN	Redes de Área Local
	CAN	Redes de Área de Campus
	MAN	Redes de Área Metropolitana
	WAN	Redes de Área Amplia
	SAN	Red de Área de Almacenamiento
Topología	Bus	Un solo canal de comunicaciones
	Estrella	Todas las comunicaciones se originan en un punto central
	Anillo	Todos los equipos están conectados entre sí en un lazo cerrado
	Malla	Cada nodo está conectado a todos los nodos de la red
	Árbol	Varias redes estrella entre si
	Mixta	Combinaciones entre cualquiera de las redes anteriores
Método de conexión	Medios guiados	Cable coaxial, fibra óptica
	Medios no guiados	Infrarrojo, bluetooth, láser
Relación Funcional	Cliente- servidor	Requisito-Respuesta
	Igual-a-Igual	Todos los elementos de la red actúan por igual

1.1.2.1. Por direccionalidad

En esta clasificación se hace referencia a la orientación en la cual son transportados los paquetes dentro de una red.

1.1.2.1.1. Simplex

En este tipo de comunicación un ordenador está definido como transmisor, mientras tanto que otro equipo es el receptor y la información es enviada desde el equipo transmisor hacia el receptor, solo existe un canal físico y un canal lógico unidireccional.

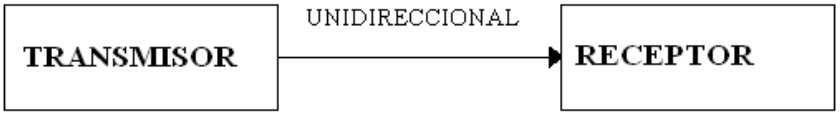


Figura 1.3.Transmision Simplex

1.1.2.1.2. Dúplex

Esta comunicación ya se la considera bidireccional en donde ambos equipos pueden ser transmisores y receptores, pero no a la vez, primero se envía información de un equipo hacia otro, y luego se puede enviar información desde el equipo que lo recibió anteriormente.

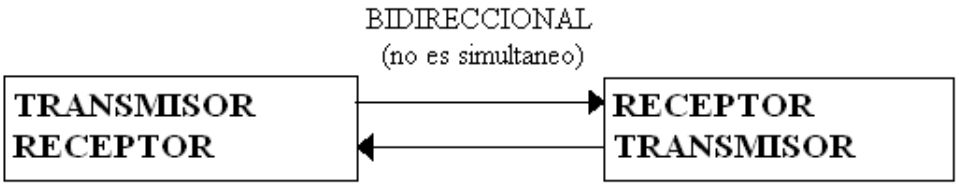


Figura 1.4.Transmision Dúplex

1.1.2.1.3. Full Dúplex

Aquí el emisor y el receptor no están definidos, ya que la comunicación es simultanea, los dos equipos pueden estar enviando y recibiendo información al mismo tiempo, existe un único canal físico y dos canales lógicos.

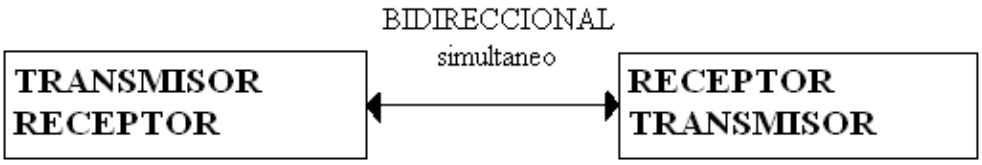


Figura 1.5.Transmision Full Dúplex

1.1.2.2. Por su alcance

El diseño de una red se lo hace para cubrir una determinada área específica, esto quiere decir que puede ser desde el área que cubre a una persona hasta mayores distancias entre dos países.

1.1.2.2.1. PAN (Redes de Área Personal)

Es una red implementada con el fin de comunicar dos o más dispositivos que se encuentran dentro de un entorno personal, entre estos dispositivos existen los PDA´s, laptops, cámaras, teléfonos celulares, etc.

Además estas redes sirven para conectar con otras redes de mayor jerarquía o Internet para obtener mayores prestaciones de servicios.

Para acceder a estas redes si se lo realiza de modo alámbrico se lo puede realizar mediante cables por medio de los buses de un computador como son FireWire y el mismo USB, al realizarlo de modo inalámbrico existen diversas tecnologías de acceso; entre las principales existen el infrarrojo y el bluetooth.

Figura 1.6.Red PAN

1.1.2.2.2. LAN (Redes de Área Local)

Las redes de área local son aquellas que ya interconectan varios ordenadores y periféricos en donde su extensión puede llegar desde un hogar, hacia varios metros, generalmente puede ser hasta de 200 metros. Dentro de estas redes se puede compartir información, recursos y aplicaciones entre equipos.

Cuando las redes LAN son sumamente grandes se las puede dividir en grupos de trabajo (Workgroups), este grupo posee un sistema común de determinados recursos que son compartidos entre todos los miembros dentro de la VLAN.

Figura 1.7.Red LAN

1.1.2.2.3. CAN (Redes de Área de Campus)

Estas redes son el conjunto de dos redes LAN que se encuentran distanciadas geográficamente y que pertenecen a una misma Institución como puede ser una empresa, universidad, gobierno, etc.

Estas redes pueden estar interconectadas para compartir recursos o la misma información, un ejemplo de estas redes se lo podría aplicar dentro de una universidad que dispone de varios campus distribuidos dentro de una misma ciudad y que deben compartir una misma información en común.

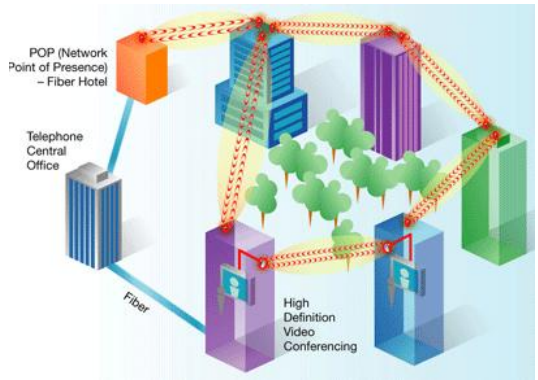


Figura 1.8.Red CAN

1.1.2.2.4. MAN (Redes de Área Metropolitana)

Estas redes son una versión de mayor capacidad y de cobertura que las redes de área local, que buscan cubrir toda una ciudad, en estas redes ya se pueden abarcar varias redes de diferentes instituciones, proporcionan múltiples servicios como la transmisión de datos, de video y voz a altas velocidades, un claro ejemplo de este tipo de redes metropolitanas se lo atribuye al área de telecomunicaciones, en donde un operador busca cubrir todo un distrito metropolitano para brindar el servicio de voz.

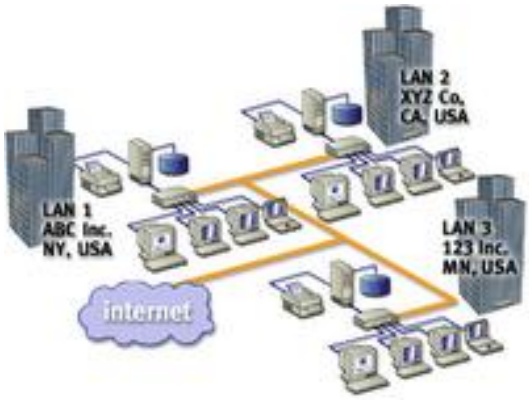


Figura 1.9.Red MAN

1.1.2.2.5. WAN (Redes de Área Extensa)

Es una red que cubre un área geográfica sumamente extensa, generalmente las empresas de servicios de telefonía brindan servicios para conectar a redes WAN, estas redes son de tipo convergente, es decir que transportan datos, voz y video.

La cobertura que ofrecen las redes WAN puede ser de tipo internacional, más comúnmente usado por empresas para conferencias desde distintas partes del mundo, ó enviar información desde dos puntos geográficamente distanciados de manera considerable.

Figura 1.10.Red WAN

1.1.2.2.6. SAN (Redes de Área de Almacenamiento)

La red SAN es una arquitectura que maneja altas velocidades, creada para el almacenamiento de la información que es enviada por grandes redes en donde existen varios servidores que poseen gran variedad de datos.

En estas redes se diferencian así mismo dos tipos de redes:

- La red de área local (LAN)
- La red de acceso de datos

Debido a la alta capacidad y velocidad que maneja la SAN estas redes se manejan a través de canales de fibra óptica, tanto para la transmisión de mensajes entre nodos así como para la estructura de switches, todos los elementos de esta red son conectados por este medio.

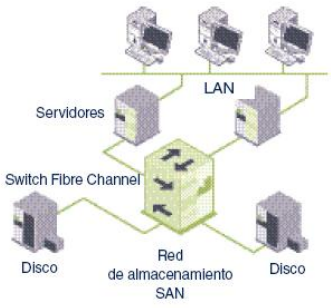


Figura 1.11.Red SAN

1.1.2.3. Por su topología

Se implementará una red por su topología de acuerdo a los elementos físicos y la disposición de cada uno de ellos con el fin de alcanzar el máximo rendimiento y el aprovechamiento de todos los recursos.

1.1.2.3.1. Bus

La topología bus es aquella donde todos los ordenadores se encuentran conectados a un único canal de comunicaciones conocido también como backbone, por el cual cruza toda la información y este será el encargado de clasificar por medio de identificadores de paquetes IP para determinar a cual de todos los ordenadores pertenece dicha información.

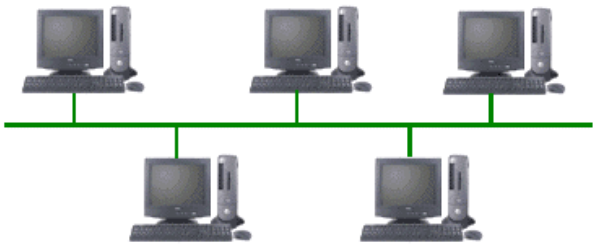


Figura 1.12.Topologia tipo Bus

1.1.2.3.2. Estrella

Aquí todos los equipos se encuentran conectados directamente a un ordenador central el cual es el encargado de distribuir la información y los recursos de la red así como la dirección IP para cada uno de los equipos, cuando dos equipos de la red comparten información lo hacen por medio del ordenador, y si existiera un fallo en el ordenador central toda la red quedará sin comunicación ya que el punto de enlace quedaría inactivo.

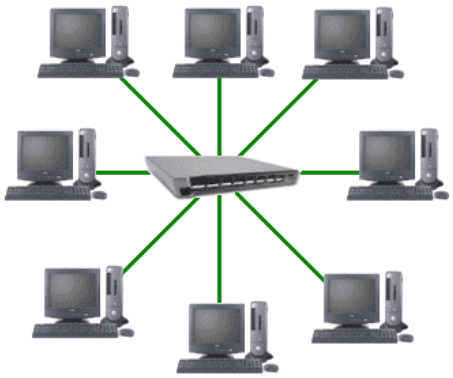


Figura 1.13.Topologia tipo Estrella

1.1.2.3.3. Anillo

Todos los equipos se encuentran conectados al equipo más cercano hasta que se cierre por completo, los equipos serán transmisores y receptores a la vez así como nodos de transmisión, el momento que existe un envió de datos entre terminales, el crecimiento en estas redes implica abrir un punto para implementar un nuevo equipo la comunicación se perderá hasta que nuevamente el anillo se vuelva a cerrar.

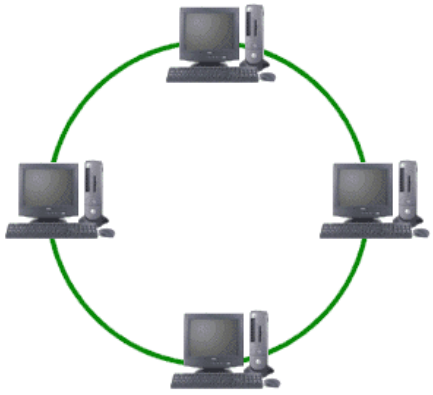


Figura 1.14.Topologia tipo Estrella

1.1.2.3.4. Malla

El principal aspecto en esta topología es la de ofrecer redundancia, esto quiere decir que un equipo se encuentra conectado con todos los equipos de la red al mismo tiempo, esto ayuda para que la información pueda ir por cualquier otro camino en el caso de que la

conexión directa no esté en funcionamiento, los nodos no dependen de algún otro para realizar la comunicación, el inconveniente de estas redes es su costo ya que se debe implementar mayor cantidad de cableado.

La disponibilidad de esta red es mucho mayor y mejor eficiencia el momento de la compartición de recursos.

Figura 1.15.Topologia tipo Malla

1.1.2.3.5. Árbol

La topología árbol es una combinación entre las topología tipo estrella y tipo bus, aquí el servidor es el elemento de donde sale el backbone principal, el cual se extenderá por toda la red y en la cual las subredes estrella se unen, conocidas también como ramificaciones y de estas pueden salir más subredes, se suelen utilizar hubs o switches en los cuales se producen las ramificaciones correspondientes.

Figura 1.16.Topologia tipo Árbol

1.1.2.3.6. Mixta

Son aquellas en las cuales se implementan dos o más tipos de las topologías anteriores dentro de una misma red.

1.1.2.4. Por su método de conexión

El método de conexión indica la manera física de cómo se realiza la comunicación entre los equipos o la de acceder hacia los recursos de la red.

1.1.2.4.1. Medios guiados

En los medios guiados las señales tienen que seguir un camino físico (cable) por el cual toda la información es transmitida.

Algunos ejemplos de medios guiados son:

- Cable coaxial

Figura 1.17.Cable Coaxial

- Par trenzado

Figura 1.18.Par Trenzado

- Fibra Óptica

Figura 1.19.Fibra Óptica

1.1.2.4.2. Medios No Guiados

En la transmisión con medios no guiados, es el medio el cual determina todos los parámetros de la comunicación como la velocidad de transmisión, el ancho de banda y la distancia entre el transmisor y el receptor.

Los ejemplos más conocidos de este tipo de medios son:

- Señales de rayo infrarrojo

Figura 1.20.Rayo Infrarrojo

- Señales de bluetooth

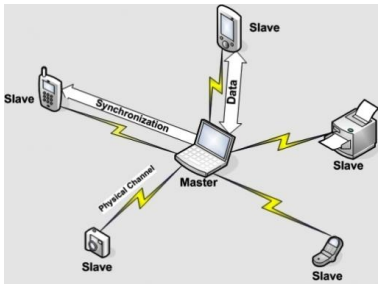


Figura 1.21.Senal Bluetooth

- Señales de rayo láser

Figura 1.22.Rayo Laser

1.1.2.5. Por su relación funcional

La relación funcional de una red implica definir las funciones de todos los equipos involucrados en la red, y como actúan entre ellos.

1.1.2.5.1. Cliente-Servidor

En estas redes el ordenador (cliente), busca acceder a los recursos que posee el administrador de la red también conocido como servidor, para esto el cliente envía mensajes de solicitud al servidor para acceder a dichas aplicaciones, en donde el servidor debe enviar un mensaje de respuesta sea de confirmación o negación, todos los permisos de acceso son controlados por el servidor.

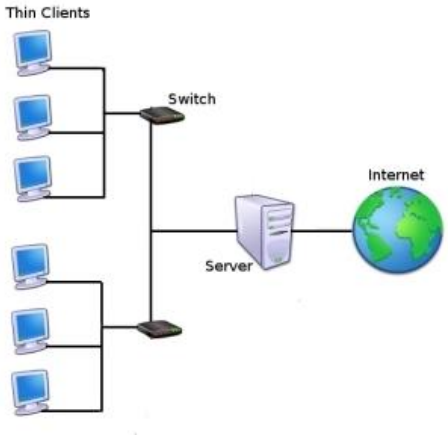


Figura 1.23.Relacion Cliente-Servidor

1.1.2.5.2. Cliente-Cliente (Peer to Peer)

En estas redes todos los equipos actúan por igual, se basan en una serie de nodos que actúan por igual, es decir que pueden ser clientes y servidores de forma simultánea.

Permiten el intercambio de la información en cualquier formato, se lo hace de forma directa por lo que se optimiza el ancho de banda del resto de ordenadores de la red.

Cuando se busca obtener transmisiones en tiempo real son aplicadas estas redes tales como en las redes de telefonía IP.

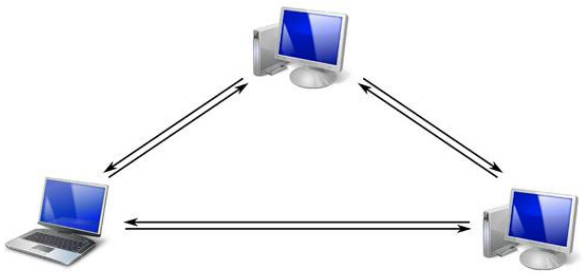


Figura 1.24.Relacion Peer to Peer

1.2. Elementos de una Red

Una red de computadoras está conectada tanto por hardware como por software. El hardware incluye tanto las tarjetas de interfaz de red como los cables que las unen, y el software incluye los controladores (programas que se utilizan para gestionar los dispositivos y el sistema operativo de red que gestiona la red. A continuación se listan los componentes: [2]

- Servidor.

- Estaciones de trabajo.

- Placas de interfaz de red (NIC).

- Recursos periféricos y compartidos.

Dentro de una red observamos siempre distintos dispositivos por los cuales serán enviados los paquetes de información, cada uno de estos cumplen distintas funciones para permitir conectividad entre todos los equipos.

Servidor: este ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo.

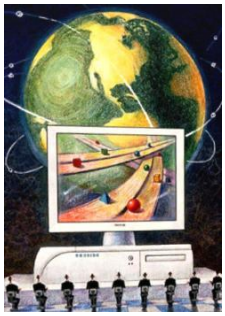


Figura 1.25.Servidor

Estaciones de Trabajo: Cuando una computadora se conecta a una red, la primera se convierte en un nodo de la última y se puede tratar como una estación de trabajo o

cliente. Las estaciones de trabajos pueden ser computadoras personales con el DOS, Macintosh, Unix, OS/2 o estaciones de trabajos sin discos.

Figura 1.26.Estacion de trabajo

Tarjetas o Placas de Interfaz de Red: Toda computadora que se conecta a una red necesita de una tarjeta de interfaz de red que soporte un esquema de red específico, como Ethernet, Arc Net o Token Ring. El cable de red se conectara a la parte trasera de la tarjeta.

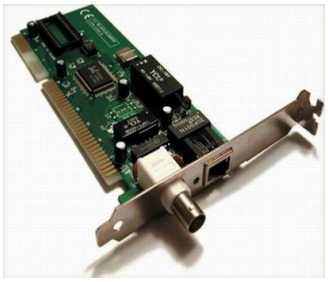


Figura 1.27.Tarjetas de Interfaz de Red

Sistema de Cableado: El sistema de la red está constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo.

Figura 1.28.Cableado

Recursos y Periféricos Compartidos: Entre los recursos compartidos se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores y el resto de equipos que puedan ser utilizados por cualquiera en la red.

Figura 1.29.Periféricos

Dentro de los elementos más relevantes para llevar a cabo la comunicación y el envío de paquetes se encuentran el switch y el router, los cuales se los analizara desde su funcionamiento básico hasta las aplicaciones de cada uno de ellos.

1.2.1. Arquitectura Jerárquica

Cuando se diseña una red, con el fin de evitar mayores problemas en recursos y administración se aplica un modelo de diseño jerárquico, esto implica en dividir en capas jerárquicas a la red para que el rendimiento y la escalabilidad. [3]

A continuación se indica la manera de cómo dividir una red en tres capas.

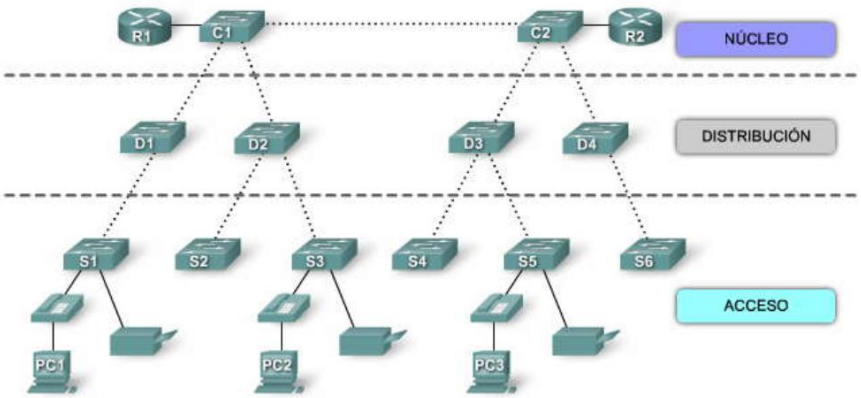


Figura 1.30.Arquitectura Jerárquica

1.2.1.1. Capa de acceso

Esta capa de acceso es la manera de cómo llegar hacia los dispositivos finales de la red y controlar los equipos que se pueden comunicar a la red.

Hace interfaz con los dispositivos finales como son impresoras, scanner, teléfonos IP y hosts para permitir el acceso al resto de la red.

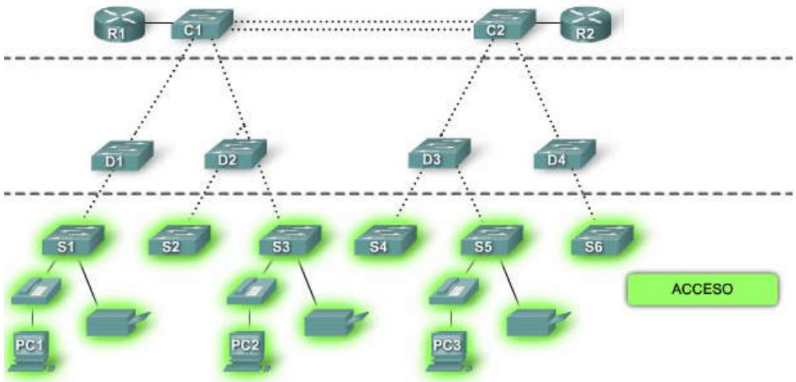


Figura 1.31.Capa de Acceso

1.2.1.2. Capa de distribución

La capa de distribución es aquella que controla el flujo de la información entre la capa de acceso y la capa de núcleo, este control se lo realiza por medio de políticas y

dominios de broadcast en el enrutamiento de las funciones de las respectivas VLAN's que se hayan conformado en la red.

En esta capa se agrega la información que entregan los switches de la capa de acceso que van a ser enrutados en la capa de núcleo para que lleguen hasta su destino final.

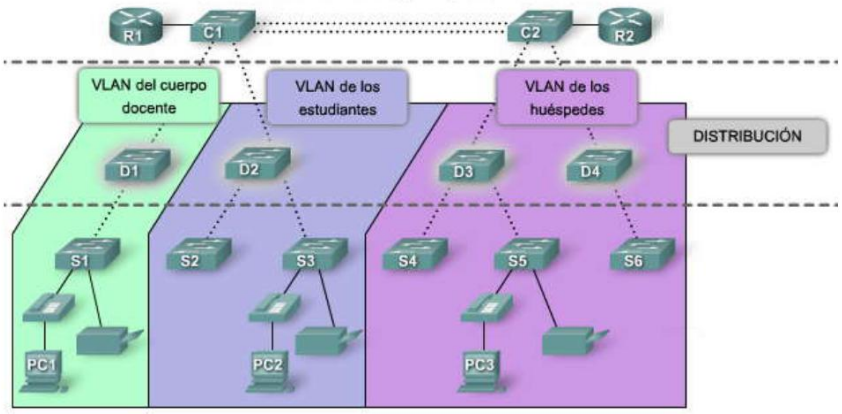


Figura 1.32.Capa de Distribución

1.2.1.3. Capa de núcleo

La capa de núcleo es el medio de interconexión ya sea entre diferentes capas de distribución o hacia los recursos de Internet, por lo que esta capa debe manejar grandes cantidades de tráfico a altas velocidades.

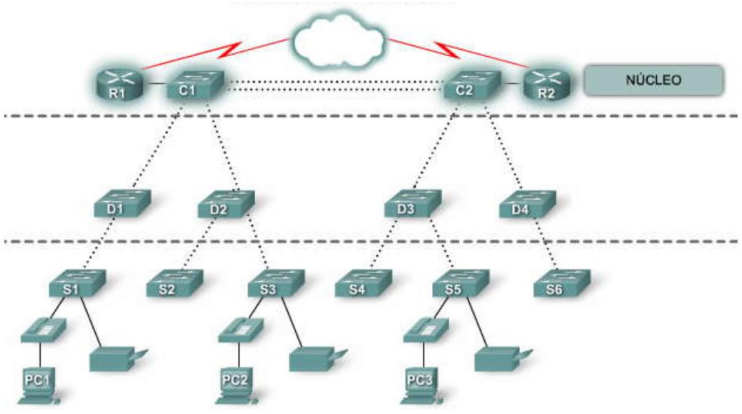


Figura 1.33.Capa de Núcleo

1.2.2. Diseño de redes Jerárquicas

Para poder diseñar redes jerárquicas hay que tomar en cuenta parámetros previos tales como el diámetro de la red, agregado de ancho de banda y redundancia. [4]

1.2.2.1. Diámetro de la red

El diámetro de la red es la cantidad de equipos que debe cruzar un paquete para llegar hacia el destino, si el diámetro de la red es bajo se puede asegurar una latencia baja entre los equipos interconectados.

1.2.2.2. Agregado de ancho de banda

Este parámetro puede ser aplicado en cualquiera de las capas jerárquicas, se deben conocer los valores necesarios de ancho de banda para poder implementar enlaces entre los switches previamente determinados para combinar los enlaces de puerto de múltiples switches para aumentar el rendimiento.

1.2.2.3. Redundancia

El buscar redundancia en una red indica que siempre debe estar disponible, para esto se pueden incrementar los enlaces entre los equipos o aumentar los equipos por lo que buscar mayor redundancia es más costoso de acuerdo al tamaño de la red.

1.2.3. Router

El router es un equipo que trabaja en la capa 3 del modelo OSI, el cual corresponde a la capa de red, esto quiere decir que toma decisiones en base al grupo de direcciones de una red, para conmutar los paquetes y enviarlos a través del puerto de salida correspondiente.

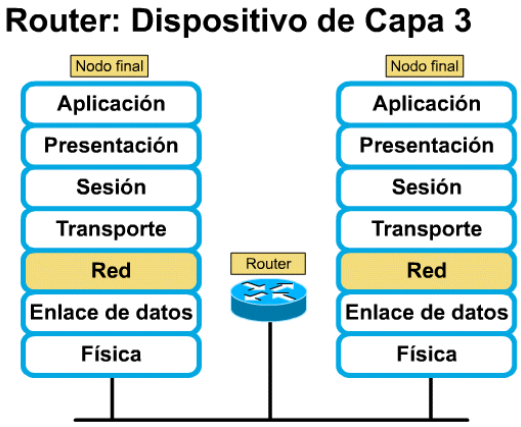


Figura 1.34.Router Capa 3

El router es el encargado de interconectar varias redes en un mismo punto, permite el paso de los paquetes tomando en cuenta la base de información de la capa de red, además siempre busca la mejor ruta o camino para que los paquetes lleguen a esa red, para definir la ruta más eficiente se realiza mediante el valor de la métrica que debe cruzar por todas las redes y siempre se lo hará por la que tenga el menor número de saltos. [5]

Es el último dispositivo físico entre la red y los recursos como Internet, aplicaciones entre otros.

Figura 1.35.Funcionamiento Router

En el aspecto físico para que se lleve a cabo la conectividad en toda la red, debemos tomar en cuenta las interfaces de cada dispositivo y el tipo de cable se va a utilizar, para comunicar dos o más routers se lo hace mediante las interfaces seriales de los equipos y para salir hacia cada una de sus redes mediante cable directo sea hacia un hub, switch o de manera directa hacia un ordenador.

A continuación se muestra el esquema de una red distribuida para recibir los recursos del servidor y que mediante el router central los distribuye hacia cada una de las redes correspondientes.

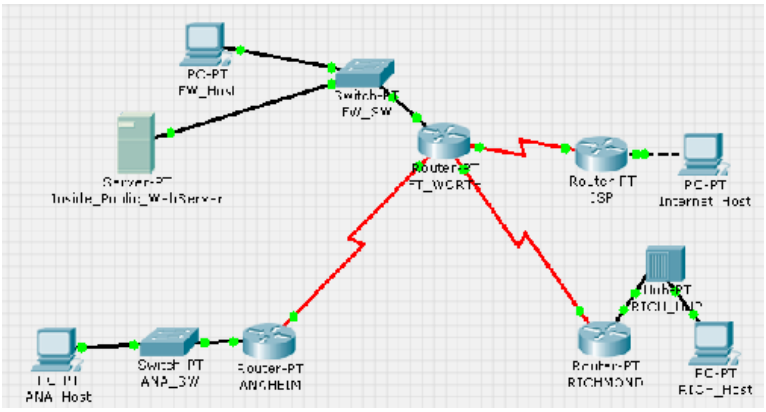


Figura 1.36.Conexiones del Router

Como se indico anteriormente el router debe conocer todas las redes conectadas directamente a el, inclusive los routers vecinos, se debe verificar de alguna manera que el equipo reconozca todas estas redes para que pueda enviar los paquetes ya sea dentro de su propia red o tenga que direccionarlos hacia otra que se encuentre alejada físicamente.

Para llevar a cabo este proceso el router tiene una tabla de enrutamiento la cual realiza las búsquedas del mejor camino a una red destino, así como la de mostrar todas las rutas que conoce.

RRAS-ROUTER1 - IP Routing Table

Destino	Máscara de red	Puerta de en...	Interfaz	Métrica	Protocolo
10.57.76.0	255.255.255.0	10.57.76.1	Local Area C...	1	Local
10.57.76.1	255.255.255.255	127.0.0.1	Loopback	1	Local
10.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.45.0	255.255.255.0	192.168.45.1	Local Area C...	1	Local
192.168.45.1	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	224.0.0.0	192.168.45.1	Local Area C...	1	Local
224.0.0.0	224.0.0.0	10.57.76.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	192.168.45.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local

Figura 1.37.Tabla de Enrutamiento

En la tabla anterior se observa un ejemplo de una tabla de enrutamiento donde se muestran diferentes parámetros para determinar todas las redes que el router conoce.[6]

- **Destino**

El destino es el host, la dirección de subred, la dirección de red o la ruta predeterminada de destino. El destino para una ruta predeterminada es 0.0.0.0.

- **Máscara de red**

La máscara de red se utiliza en conjunción con el destino para determinar cuándo se utiliza una ruta, cuando la máscara es 255.255.255.255, indica que la ruta tiene una máscara 0.0.0.0 y cuando la máscara es 0.0.0.0, indica que cualquier destino puede utilizar esta ruta.

La máscara 255.255.255.255 significa que sólo utilizará esta ruta un destino que coincida exactamente. La máscara 0.0.0.0 significa que cualquier destino puede utilizar esta ruta. Si una máscara se escribe en binario, un **1** es significativo (debe coincidir) y un **0** no lo es (no es necesario que coincida).

- **Puerta de enlace**

La puerta de enlace es la dirección IP del siguiente router al que se debe enviar un paquete. En los vínculos LAN (como Ethernet o Token Ring), este router debe tener acceso directo a la puerta de enlace a través de la interfaz indicada en la columna **Interfaz**.

En los vínculos LAN, la interfaz y la puerta de enlace determinan cómo va a reenviar el tráfico el router. En el caso de una interfaz de marcado a petición, la dirección IP de puerta de enlace no es configurable. En los vínculos punto a punto, la interfaz determina cómo reenvía el tráfico el router.

- **Interfaz**

Indica la interfaz LAN o de marcado a petición que se va a utilizar para alcanzar el siguiente router.

- **Métrica**

La métrica indica el costo relativo por utilizar la ruta para alcanzar el destino. La métrica típica son los saltos, o número de routers que se atraviesan para alcanzar el destino. Si existen varias rutas al mismo destino, la ruta con menor métrica es la ruta más adecuada.

- **Protocolo**

El protocolo muestra cómo se aprendió la ruta. Si en la columna **Protocolo** se enumeran los protocolos RIP o OSPF (o cualquier otro que no sea Local), el router está recibiendo las rutas. [2]

Todos los routers que se encuentren interconectados entre sí, deben enviar su tabla de enrutamiento cada cierto periodo con el fin de actualizar la información del resto de routers para que estos aprendan las rutas y pueda existir conexión en toda la red.

Además de estos parámetros la tabla de enrutamiento nos muestra las redes asociadas y el siguiente salto para pasar a otra red. [7]

Para esto podemos clasificar a las rutas de la siguiente manera:

- Rutas conectadas directamente
- Rutas estáticas
- Rutas dinámicas

1.2.3.1. Rutas conectadas directamente

Este tipo de rutas, se establecen cuando se configura la interfaz de un router y una PC dentro de la misma red, y será la máscara de subred la que determinara a que red pertenece, la interfaz debe esperar recibir una señal portadora de otro dispositivo de red como un hub o un Switch para que se active la interfaz.

Figura 1.38.Rutas conectadas directamente

El router automáticamente detectara todas las conexiones físicas hacia el y las mostrara en su tabla de enrutamiento como rutas directamente conectadas como se muestra en la siguiente figura:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

Figura 1.39.Tabla de Enrutamiento Rutas conectadas directamente

1.2.3.2. Rutas estáticas

Las rutas se las establecen de manera manual por medio del administrador y no se adaptan a cambios en la topología de la red, además estas rutas utilizan procesos de recursos del equipo y el control se hace más complejo conforme el tamaño de la red aumenta.

Estas rutas incluyen una única dirección de la red, la máscara de la red destino y la dirección IP que tiene la interfaz del router, ya sea para el siguiente salto o de interfaz de salida.

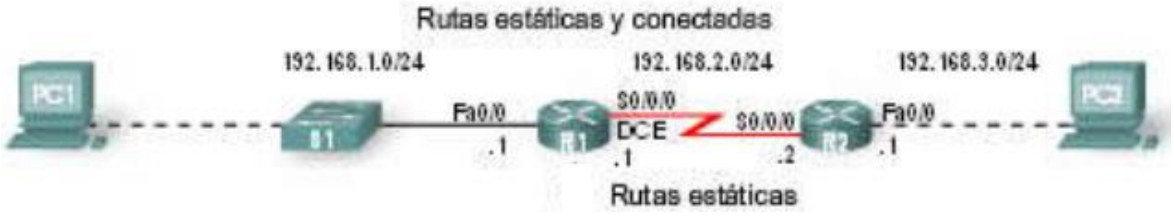


Figura 1.40. Rutas conectadas estáticas

La información de la tabla de enrutamiento mostrara los siguientes detalles de esta conexión:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

Figura 1.41.Tabla de Enrutamiento Rutas Estáticas

1.2.3.3. Rutas dinámicas

Las rutas dinámicas son aquellas que el router aprende por medio de los protocolos de enrutamiento para descubrir nuevas rutas hacia otras redes que están conectadas a otros routers y otros posibles caminos para llegar hacia un mismo destino con el fin de reducir el tráfico que cruza por toda la red.

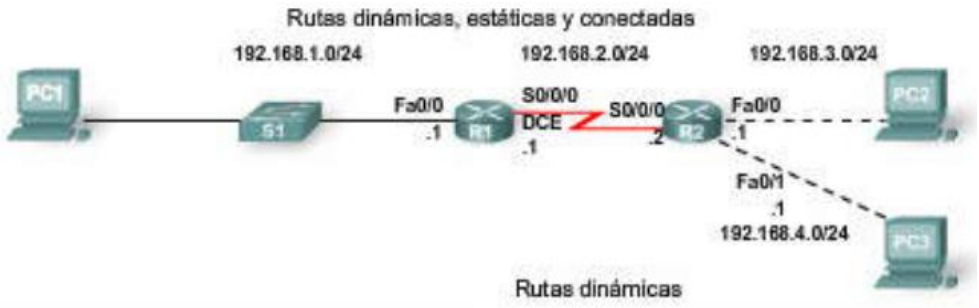


Figura 1.42. Rutas conectadas dinámicas

En este ejemplo por medio de los protocolos de enrutamiento el R1 ha aprendido nuevas rutas las cuales las publica en su tabla de enrutamiento donde aprendió una ruta a través del protocolo de enrutamiento y otra que fue configurada como ruta estática.

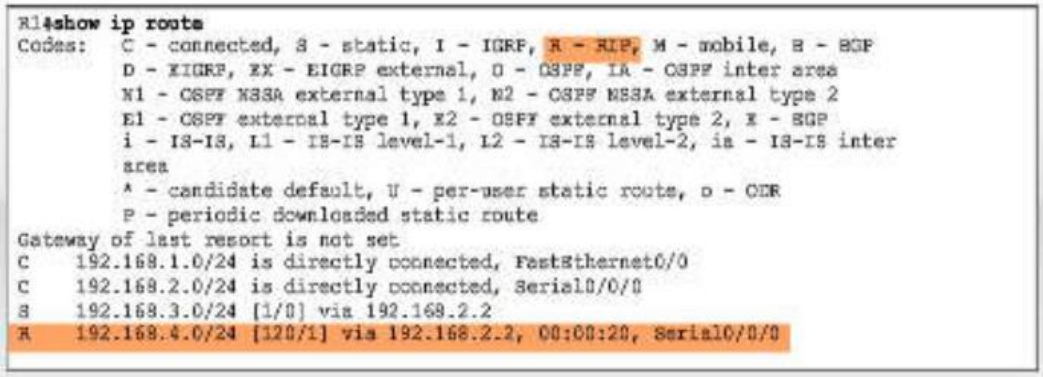


Figura 1.43.Tabla de Enrutamiento Rutas Dinámicas

Para llevar a cabo la comunicación entre dos routers con el fin de obtener comunicaciones entre equipos de diferentes redes, los routers se manejan a través de protocolos de enrutamiento los cuales se basan en diferentes parámetros para obtener una red global convergente.

Los protocolos principales para la comunicación entre routers son:

- RIP V1
- RIP V2
- IGRP
- EIGRP
- OSPF

1.2.3.4. Protocolos de enrutamiento

1.2.3.4.1. Rip V1

Es un protocolo de vector distancia, esto quiere decir que se maneja a través de un módulo y una dirección, calcula la distancia en función de cuantos routers debe cruzar hasta el host de destino, las actualizaciones de la tabla de enrutamiento se las ejecuta cada 30 segundos, este protocolo tiene un máximo de 15 saltos y en el caso de ser mayor indica que la red es inalcanzable.

Además RIP V1 no soporta el VLSM (Máscara de Subred de Longitud Variable), no envía las máscaras de subred en las actualizaciones y es propenso a lazos de enrutamiento.

1.2.3.4.2. Rip V2

La versión 2 de RIP se maneja de similar manera que la anterior con la diferencia de que esta ya soporta VLSM y cuando envía las tablas de enrutamiento ya lo hace con la máscara, estas actualizaciones son mediante multicast el cual es el tipo del flujo de los datos, siempre antes de permitir la recepción de la tabla solicita credenciales de autentificación y sigue presentando los mismos inconvenientes que su versión anterior como el número limitado de saltos y el momento de enviar toda la tabla de enrutamiento genera mayor tráfico en toda la red.

RIP V2 envía las actualizaciones de enrutamiento a través de la dirección de multicast 224.0.0.9.

1.2.3.4.3. IGRP

IGRP usa una métrica compuesta que consiste en diferentes variables de red, como son el ancho de banda, unidades máximas de transmisión (MTU), confiabilidad, carga y el retardo. Este protocolo envía las actualizaciones de las tablas cada 90 segundos.

Está diseñada para operar en redes de gran tamaño, usa el ancho de banda y el retardo como la métrica, además cada router muestra destinos con su distancia correspondiente y la envía al resto de routers, estos se ajustan a los valores obtenidos para obtener las rutas más eficientes.

1.2.3.4.4. EIGRP

Es una versión mejorada de IGRP, utiliza la misma métrica compuesta que IGRP pero que es multiplicada por un valor de 256:

$$Métrica = [BandW + Delay] \times 256 \quad \text{(Ecuación 1.1)}$$

Donde BandW y Delay corresponden al ancho de banda y al retardo respectivamente.

A diferencia de los otros protocolos que reciben la tabla periódicamente, EIGRP las envía únicamente cuando detecta un cambio dentro de la red.

Además tiene la ventaja de contar con paquetes de saludo para detectar que los routers vecinos siguen activos o si alguno dejo de funcionar, con el fin de calcular la nueva métrica y obtener nuevas rutas para llegar a los mismos destinos.

1.2.3.4.5. OSPF

Este es un protocolo de estado de enlace, esto quiere decir que un router comunica a todos los demás cuáles son sus vecinos y a que distancias se encuentran de ellos.

Un solo router al recibir la información de todos los routers puede construir un mapa global sobre el cual puede calcular cuales son las rutas más optimas.

Este protocolo utiliza áreas siendo el área 0 también conocida como backbone. Al hablar de áreas se define a reducir el procesamiento de tráfico a una determinada parte de la red mejorando el rendimiento y la convergencia.

Todos los routers configurados mediante este protocolo contienen la misma información sobre sus propios estados de enlace y de los vecinos de cada uno de los demás routers.

1.2.4. Switch

Un switch, al igual que un puente, es un dispositivo de capa 2. De hecho, el switch se denomina puente multipuerto, así como el hub se denomina repetidor multipuerto. La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión.

Como los switches son capaces de tomar decisiones, hacen que la LAN sea mucho más eficiente. Los switches hacen esto conmutando los datos sólo hacia el puerto al que está conectado el host destino apropiado. Por el contrario, el hub envía datos desde todos los puertos, de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos.

A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión, dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red). La diferencia entre un hub y un switch está dada por lo que sucede dentro del dispositivo.

El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, pensar en el switch como un elemento que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto.

El switch conmuta paquetes desde los puertos (interfaces) entrantes a los puertos salientes, suministrando a cada puerto el ancho de banda total (la velocidad de transmisión de datos en el backbone de la red). [8]

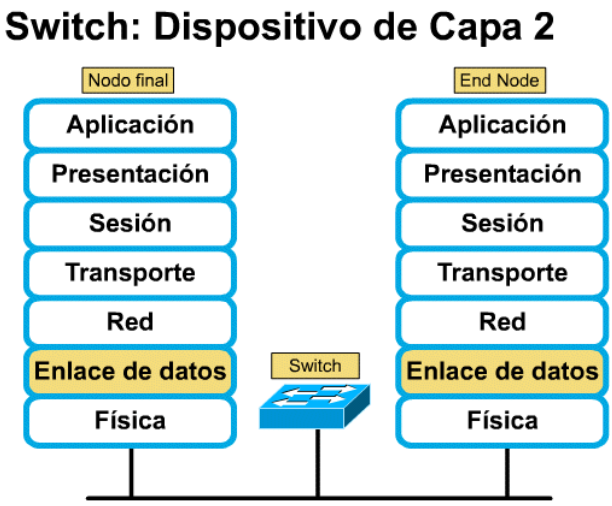


Figura 1.44.Switch Capa 2

1.2.4.1. Switches en redes Jerárquicas

Los switches dentro de las redes jerárquicas deben ser implementados de acuerdo a ciertas especificaciones como son: [9]

- Flujo de tráfico objetivo
- Comunidades de usuario
- Servidores de datos
- Servidores de almacenamiento de datos

1.2.4.1.1. Análisis del flujo de tráfico

Es el proceso de medición del ancho de banda que se utiliza así como de los datos para mejorar el rendimiento y tomar las mejores decisiones en la parte física.

En la actualidad no existe una definición concreta sobre el flujo de tráfico por lo que se lo define como la cantidad de paquetes en un determinado tiempo. Todos los paquetes son tomados en cuenta para este análisis sin importar el propósito que cumplan.

Para controlar el flujo de tráfico en la red se pueden manipular los puertos del Switch con el fin de gestionar el ancho de banda a los caminos por donde existe mayor cantidad de congestión de datos.

1.2.4.1.2. Análisis de comunidades de usuario

Este análisis es aquel para identificar los grupos establecidos y el uso que cada uno de ellos le da a la red. Esto conlleva a determinar la selección de equipos cuando se realiza el diseño de una red, ya que de acuerdo a las tareas que cada usuario realiza y el tráfico que lleva, se determinaran los dispositivos para conformar la red.

Siempre se debe analizar para un crecimiento a futuro de la red y que siga manteniendo las mismas prestaciones a todos los usuarios, para esto se debe observar en base a años anteriores ya que debe mantener una constante de crecimiento para seleccionar los switches necesarios.

1.2.4.1.3. Almacenamiento de datos y servidores de datos

Los medios de almacenamiento de datos pueden ser de varios tipos como servidores, redes SAN, almacenamiento adjunto a redes (NAS), o cualquier otro que tenga la capacidad de almacenar grandes cantidades de datos.

Aquí se debe tomar en cuenta el análisis de flujos de tráfico ya que varios equipos solicitan información de los servidores produciendo que haya congestiones en la red, por lo que el ancho de banda y tasas de reenvío son importantes para tratar de solucionar este problema.

El tráfico que se origina entre los dispositivos de almacenamiento pueden ocupar grandes volúmenes de tráfico y una manera de optimizar esto es que estos equipos se encuentren a distancias cortas para disminuir el tráfico entre ellos y no afectar al resto de la red.

El trafico que existe entre el cliente y el servidor es mucho menor ya que únicamente es con el fin de acceder a la información como medio de solicitud y esperando una respuesta, en base a esto los switches entre los servidores deben poseer un alto rendimiento a diferencia de los que son implementados en las capa de acceso.

A continuación se muestra como viaja el tráfico cuando el flujo es entre cliente servidor y entre dos servidores o un dispositivo de almacenamiento.

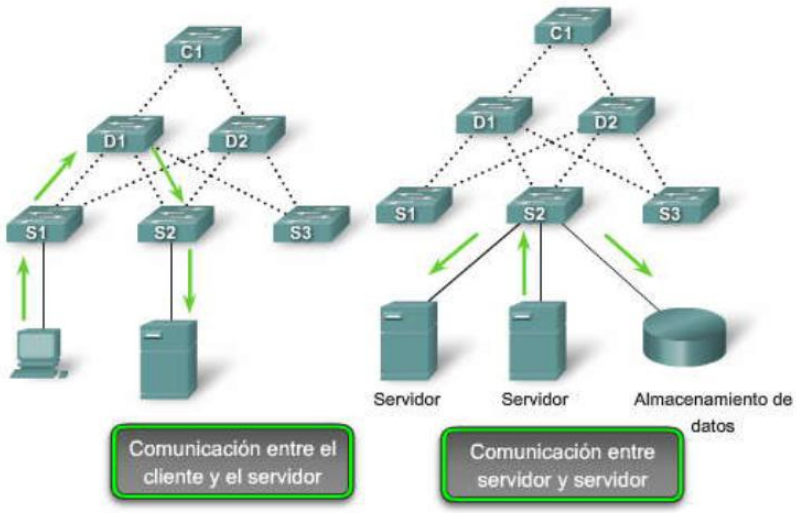


Figura 1.45.Tipos de tráfico de flujo en el Switch

1.2.4.2. Métodos de conmutación

En la conmutación de paquetes el switch establece un enlace de comunicación entre dos tramas durante el tiempo necesario para el envío de paquetes.

Existen 3 métodos para llevar a cabo el proceso de conmutación de paquetes:

- Store and forward (Almacenamiento y envío)
- Cut through (pasar a traves)
- Adaptative Cut through (cortar y enviar adaptativo)

1.2.4.2.1. Store and forward

En este modo los paquetes previo a ser enviados son guardados en un buffer, hasta que se revise si se tienen errores de redundancia cíclica denominados CRC, para lo que se recibe un flujo de datos de cualquier trama de entrada y devuelve una longitud fija de salida, si encuentra un error en la trama esta será descartada, caso contrario si no detecta errores verifica la dirección MAC de destino y envía el paquete.

Requiere de un mayor tiempo para poder verificar las tramas por lo que el delay será cada vez más grande.

1.2.4.2.2. Cut Through

Aquí se busco reducir el tiempo de verificación de las tramas, solamente se verifican los primeros 6 bytes de la trama e inmediatamente se procede a enviar el paquete hacia su destino.

Los switches que utilizan este método no pueden detectar si hay errores en las tramas ocasionados por colisiones de las tramas o CRC's, por tanto el ancho de banda será cada vez mayor para encaminar los paquetes que contienen errores.

1.2.4.2.3. Adaptative Cut Through

Este método soporta cualquiera de los dos métodos mencionados anteriormente. Esto puede ser configurado mediante el administrador o por el mismo switch si está en capacidad de hacerlo dependiendo de las tramas errores que pasan por los puertos.

Cuando se establece un cierto nivel de margen de paquetes errados se puede cambiar el modo de conmutación a store and forward y cuando el tráfico se normalice y disminuyan estos paquetes corruptos volver al modo de cut through.

1.2.4.3. Tramas Ethernet

Dentro de los switches se establecieron dos tamaños para las tramas que cruzan por medio de las interfaces de Ethernet. [10]

Tamaño mínimo de la trama Ethernet: 64 bytes a 1518 bytes estructurada de la siguiente manera:

- Preámbulo: 7 bytes
- Inicio: 1 byte
- MAC destino: 6 bytes
- MAC origen: 6 bytes
- Tipo/ Tamaño: 2 bytes
- Relleno: 46 bytes (min) a 1500 bytes (Max)

Se agregan 4 bytes más a esta trama cuando se manejan VLAN's y muestran el identificador de la VLAN correspondiente, dando como resultado una trama máxima de 1522 bytes.

- Checksum (CRC) 4 bytes

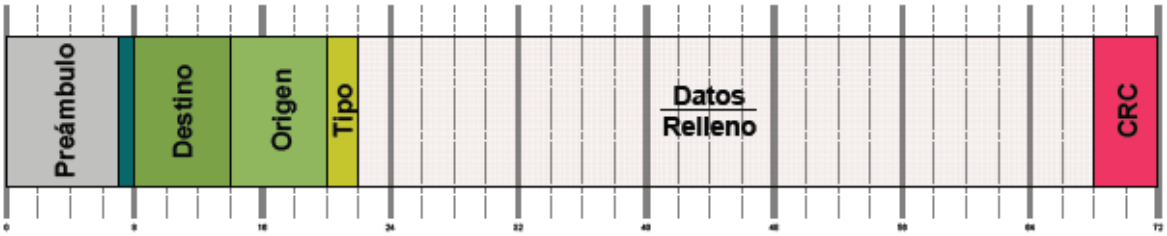


Figura 1.46.Formato de una trama Ethernet en el Switch

1.2.4.4. Buffer de memoria

Es la memoria del switch encargada del manejo de los datos, existen 2 tipos de memorias:

- **Puerto:** cada puerto del switch maneja su propio espacio de memoria.
- **Compartido:** el switch tienen un solo buffer de memoria, apunta a una dirección de la cual empieza por lo que implica mayor costo.

1.2.4.5. Tabla MAC

La tabla MAC es en la cual se guardan todas las direcciones físicas de los dispositivos conectados a los puertos del switch y que es por medio de la cual el equipo se maneja para realizar el envío de los paquetes.

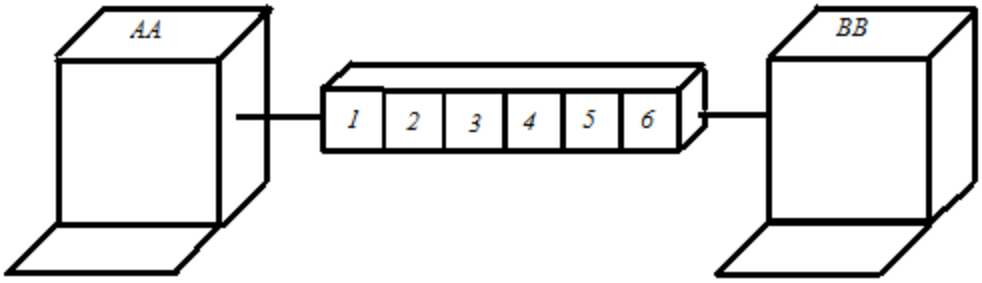


Figura 1.47.Conexión de equipos a los puertos del Switch y elaboración de la Tabla MAC

La tabla MAC de este switch se presentara así:

Tabla 1.2. Tabla MAC registrada en el SW

# puerto	*MAC*
1	AA
6	BB

Es una dirección de 48 bits expresados como 12 dígitos hexadecimales única de cada equipo que se registra en la NIC (Tarjeta de Interfaz de Red) y sirve de identificador para las tramas que lleguen al puerto, cuando detecta que la dirección MAC de la trama es la misma del equipo deja pasar hacia las capas de mayor nivel. [11]

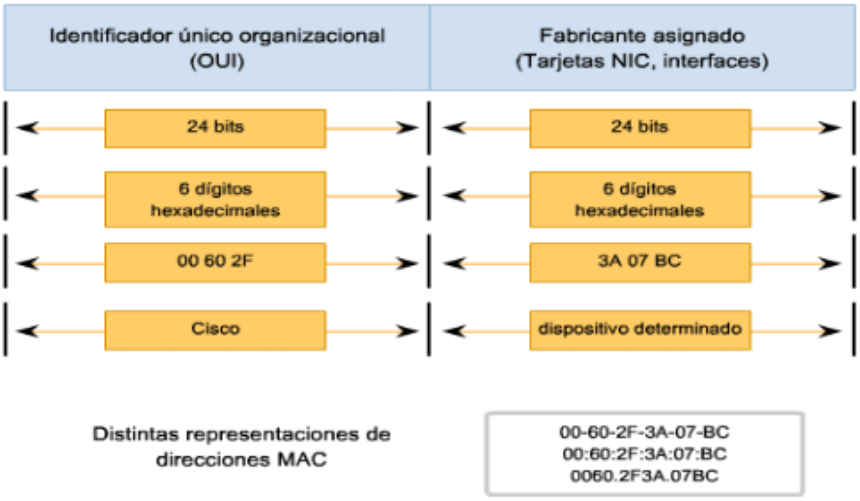


Figura 1.48.Esquema interno de la dirección MAC

1.2.5. VLAN'S

Las VLAN's son redes locales que agrupan a ciertos equipos de manera lógica, está conformada por varios dispositivos como hubs, routers, switches para conformar una subred mediante software y además tiene su propio dominio de broadcast. [12]

Es una agrupación lógica de puertos dentro de un switch para formar una red LAN independiente, que supera el inconveniente de la agrupación geográfica de los equipos y que se crea la segmentación de acuerdo a los criterios que el administrador necesite.

A continuación se puede observar la diferencia entre una LAN tradicional y una VLAN para el mismo propósito.

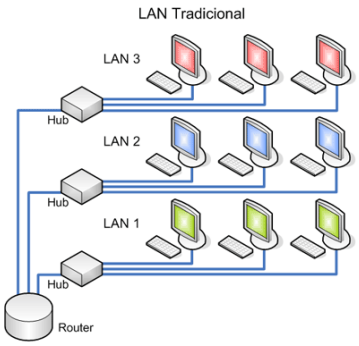


Figura 1.49.Diseño de una Red LAN básica

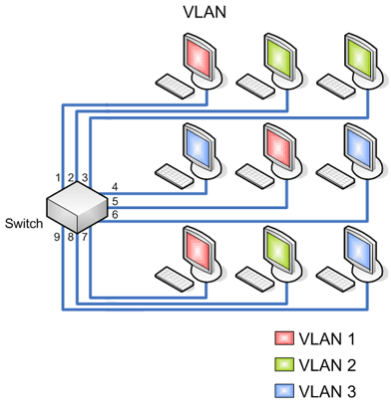


Figura 1.50.Diseño de Múltiples redes VLAN's

La implementación de VLAN's se la emplea mediante switches, esto permite un control más inteligente en lo que refiere a tráfico ya que puede aislarlo dando como resultado un incremento en la eficiencia de la red.

Cuando se distribuyen los diferentes usuarios a los respectivos grupos se lo hace mediante segmentación lo que ocasiona un incremento del ancho de banda en dichos grupos.

1.2.5.1. Segmentación

La segmentación es la creación de dominios para los grupos de trabajo mediante la conexión física de los equipos y servidores a los puertos del switch, teniendo una conexión dedicada hacia la red.

Esta es una ventaja considerable ya que reduce el tráfico dentro de la red, porque solo se transmiten los paquetes que están dentro del dominio de la VLAN, un mejor ancho de banda así como la confidencialidad de los datos, y una disminución de la latencia.

Para comunicar los switches que comunican las VLAN se utiliza el proceso denominado Trunking, el protocolo encargado de llevar esto acabo es el VTP (VLAN Trunking Protocol).

1.2.5.2. Clasificación de las VLAN's

Existen diversos tipos de VLAN's, están pueden ser diseñadas de acuerdo a lo que el administrador así lo requiera, tales como:

- VLAN de puerto central
- VLAN estáticas
- Por puerto
- Por dirección MAC
- Por protocolo
- Por dirección IP
- Por nombre de usuario
- VLAN dinámicas (DVLAN)

1.2.5.2.1. VLAN's de puerto central

Son aquellas que unen sus nodos en un puerto común del switch.

1.2.5.2.2. VLAN's estáticas

Se encuentran previamente definidas por el administrador, los puertos del switch están asignados a una única estación de trabajo.

1.2.5.2.3. VLAN's por puerto

Se definen de acuerdo a los puertos del switch para establecer los grupos de trabajo, a continuación se indica cómo se distribuye de acuerdo a los puertos las VLAN's respectivas.

Tabla 1.3. Configuración VLAN mediante puerto

Puerto	VLAN
1	1
2	2
3	2
4	3
5	1
6	3
7	1
8	2
9	3

1.2.5.2.4. VLAN's por dirección MAC

Se establecen los grupos de trabajo de acuerdo a la dirección física de la estación de trabajo.

Tabla 1.4. Configuración VLAN mediante dirección MAC

MAC	VLAN
12.15.89.bb.1d.aa	1
12.15.89.bb.1d.aa	2
aa.15.89.b2.15.aa	2
1d.15.89.6b.6d.ca	2
12.aa.cc.bb.1d.aa	1

1.2.5.2.5. VLAN's por protocolo

En base a la forma de comunicación, el switch va agrupando los equipos para formar los grupos de trabajo.

Tabla 1.5. Configuración VLAN mediante protocolo

Protocolo	VLAN
IP	1
IPX	2
IPX	2
IPX	2
IP	1

1.2.5.2.6. VLAN's por dirección IP

Se basa en el encabezado de la capa 3 del modelo OSI, esto no quiere decir que actúe como router, sino que únicamente realiza una inspección de las direcciones autorizadas a ingresar a la red, conlleva un gran ahorro de tiempo debido a que no se debe configurar nuevamente el switch y la dirección IP de la estación siempre será la misma.

1.2.5.2.7. VLAN's por nombre de usuario

Para determinar un usuario permitido lo establece mediante certificación del usuario, independientemente del equipo en el que se esté trabajando.

1.2.5.2.8. VLAN's Dinámicas (DVLAN)

Estas VLAN emplean los recursos de todos los ejemplos anteriores de forma automática, previamente los puertos del switch deben estar configurados para determinar cualquiera de los parámetros como la dirección MAC, el protocolo o la dirección IP.

Para llevar esto acabo el switch deberá tener una base de datos anteriormente configurada por el administrador para que pueda comprobar los datos que provengan de los equipos que se conecten al switch e intenten acceder a una VLAN.

La mayor ventaja que se puede observar es que la administración de estas redes es mucho menor porque todo lo realiza automáticamente el switch, también si se agregan nuevos equipos a la red o cambian las estaciones de trabajo.

1.2.6. Métodos de encriptación

La encriptación de datos no es otra cosa que codificar o cambiar los datos los cuales se enviaran por canales sumamente inseguros y que pueden poseer información valiosa.

Para mantener una seguridad confiable de la información existen diversas clases de ocultar los datos, en la actualidad los más utilizados dentro de las empresas son las llaves que permiten codificar y decodificar la información el momento de que los paquetes han llegado hacia su destino. [13]

El encriptar los datos garantiza que cuando los datos confidenciales pasan a través de un medio susceptible de infiltración, no se puedan alterar ni observar.

1.2.6.1. Técnicas de encriptación

De forma general podemos clasificar estas técnicas en dos grupos:

- Simétricos
- Asimétricos

1.2.6.1.1. Simétricos

En los algoritmos simétricos la llave que se utiliza para la encriptación es la misma que se usa para la desencriptación del mensaje, estos son conocidos como algoritmos de llave privada.

Figura 1.51.Etapas de la técnica simétrica de encriptación

Mediante estos algoritmos los datos son enviados a través de la red, esta técnica usa una sola llave para la encriptación y la misma será utilizada en el receptor para decodificar la información.

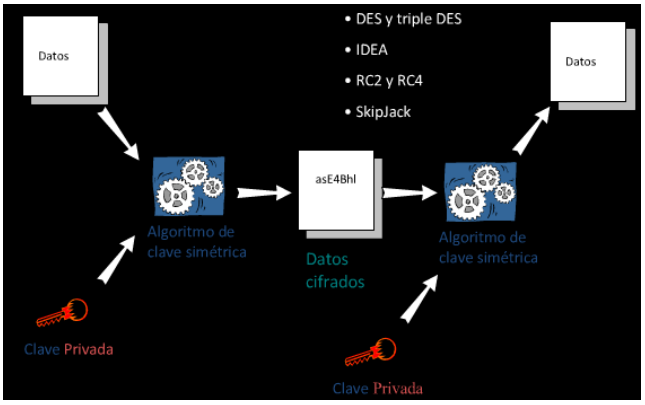


Figura 1.52.Descripción Interna de transporte de la técnica simétrica

1.2.6.1.2. Asimétricos

Estos algoritmos son conocidos como de llave pública debido a que pueden existir varios emisores que conocen la llave de encriptación, puede ser vista por todo el público, pero en la parte del receptor el usuario es el único que conoce la llave de desencriptación. Este algoritmo es mucho más eficiente para la transmisión de información ya que el atacante no sabe cuál es la única llave para decodificar los datos.

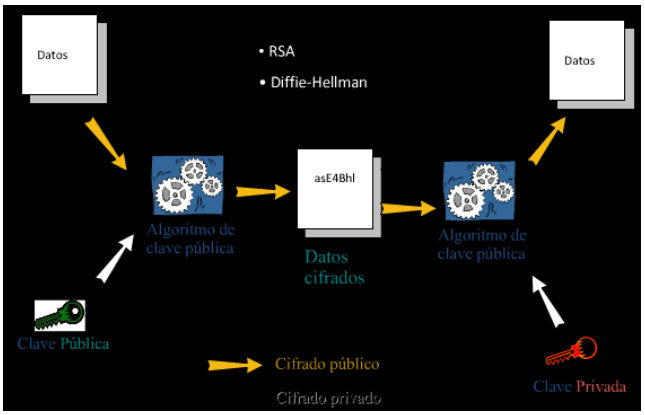


Figura 1.53.Descripción Interna de transporte de la técnica asimétrica

A partir de estos conceptos podemos mantener segura la información que se transmita a través de redes inseguras para llegar hacia su destino.

1.2.6.1.3. Firma digital

La firma digital son datos unidos al documento creados a partir de una llave privada y que de alguna forma tiene que ser verificada a través de las llaves públicas que la validez de esa firma proviene del usuario correspondiente, estos datos de la firma digital son generados mediantes funciones Hash.

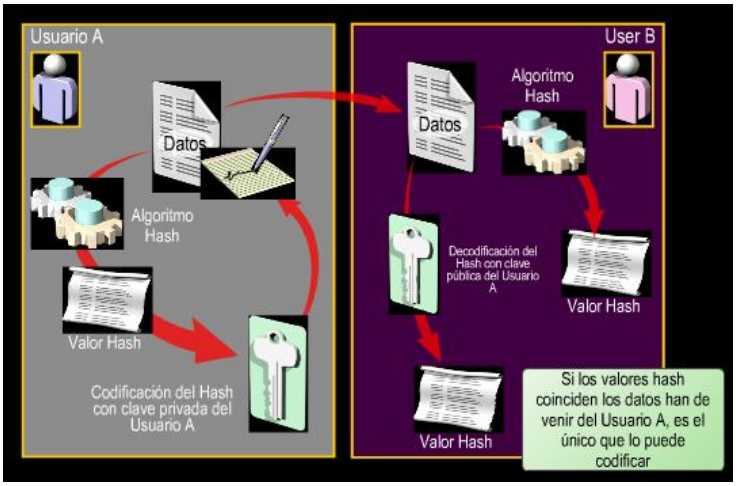


Figura 1.54.Técnica de encriptación mediante firma digital

Para la verificación de dicha firma el receptor deberá previamente conocer el algoritmo privado del que lo envía, cuando se desencripta este debe coincidir con la que el receptor conoce utilizando la llave pública, si lo hace de manera correcta se puede decir que la firma enviada es válida y se puede confiar de la información que se recibió.

1.2.6.2. Funciones Hash

Las funciones Hash sirven para comprimir el resumen del mensaje cuando se firma un documento, los bits de este mensaje se reducen a valores Hash predeterminados de tamaño fijo con el fin de distribuir estos mensajes en posibles valores Hash.

Las funciones Hash producen valores de 128 bits o mayores, por lo que el número de diferentes valores que se obtiene es de $2^{(128)}$ que supera al valor de mensajes por día que circulan alrededor de todo el mundo.

A continuación están algunos tipos de algoritmos criptográficos de Hash elaborados para generar los datos de encriptación.

- **SHA-1:** Este algoritmo genera un valor de 160 bits partiendo de la longitud aleatoria.

- **MD5:** Es conocido como el algoritmo de resumen de mensaje, que genera un valor Hash de 128 bits de cualquier trama que tenga una longitud de bits arbitraria.

- **RIPEMD-160:** Fue diseñado con el fin de superar a las versiones anteriores de MD que generan un valor de 128 bits por uno de 160 bits (20 bytes) para que sea mayor la seguridad en lo que se refiere a la firma digital. Los pasos para obtener los valores Hash son el doble en referencia con SHA-1.

A continuación se muestra una tabla comparativa entre estos algoritmos Hash con sus respectivos parámetros.

Tabla 1.6. Tabla de Parámetros de las Funciones Hash

	MD5	SHA-1	RIPEMD-160
Longitud del resumen	128 bits	160 bits	160 bits
Unidad básica de procesamiento	512 bits	512 bits	512 bits
Número de pasos	64 (4 etapas de 16)	80 (4 etapas de 20)	160 (5 pares de etapas de 16)
Tamaño máximo del mensaje	∞	$2^{64} - 1$ bit	∞
Funciones lógicas primitivas	4	4	5
Constantes adicionales usadas	64	4	9

1.2.7. Seguridades de una red

Hoy en día la información que circula a través del internet se ha visto vulnerable por medio de diferentes ataques para obtenerlas, siempre se busca evadir las seguridades que las protegen, por lo que se deben implementar mayores protecciones para mantener privada la información de nuestra red. [14]

Conforme las redes y las aplicaciones crecen, se hace más difícil un control de los múltiples ataques que pueden ingresar; para mantener a salvo una red se deben conocer previamente todas las posibles amenazas para la utilización de herramientas y aplicaciones de futuros que ataques que se originen fuera o dentro de la Institución.

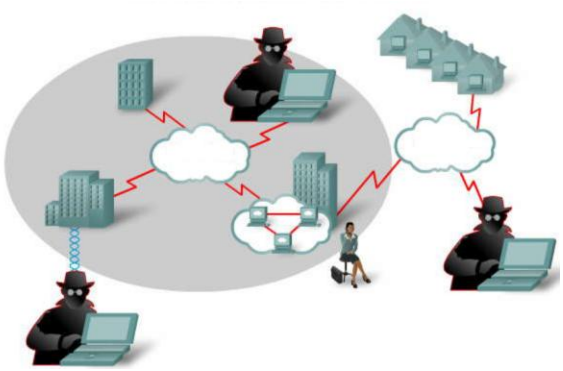


Figura 1.55.Formas de acceso de los Hackers

1.2.7.1. Tipos de delitos informáticos

Conforme han ido en evolución las tecnologías de redes, también lo han hecho las maneras de ataque a los usuarios para extraer información, dentro de los más comunes que se presentan en las redes tenemos: [15]

- Abuso de las mismas personas de una Institución
- Virus
- Suplantación de identidad
- Fraude financiero
- Robo de contraseñas

1.2.7.2. Tipos de ataques a la red

Los atacantes informáticos han desarrollado una gran variedad de ataques, desde dañar únicamente un equipo hasta la obtención de claves de cuentas bancarias sin ser detectados por las protecciones de seguridad.

A continuación vamos a ver los tipos de ataques y las finalidades que poseen cada uno de ellos.

Figura 1.56.Tipos de ataques al equipo

1.2.7.2.1. Contagio de virus

Es el ataque más común, conocido por todo el mundo con el fin de afectar el sistema operativo o dañar archivos importantes, su elaboración es muy simple en comparación a ataques de mayor escala.

1.2.7.2.2. Vulnerabilidades

Son errores que se originan en la configuración de un software por el cual se originan fallos que los atacantes utilizan para la exploración remota dentro del equipo.

1.2.7.2.3. Ataque de Layer 7

Explotan vulnerabilidades conocidas en el equipo de las aplicaciones, se encuentran directamente en los servicios ofrecidos al público, y una manera de evitarlo es mediante la instalación de parches fabricados por los mismos autores de dichas aplicaciones.

1.2.7.2.4. Tecnología mutante

Son virus que cambian su código, utilizando procesos de encriptación y los mismos antivirus, su detección se hace bastante compleja ya que al no tener un código fijo los programas de seguridad no pueden detectarlos.

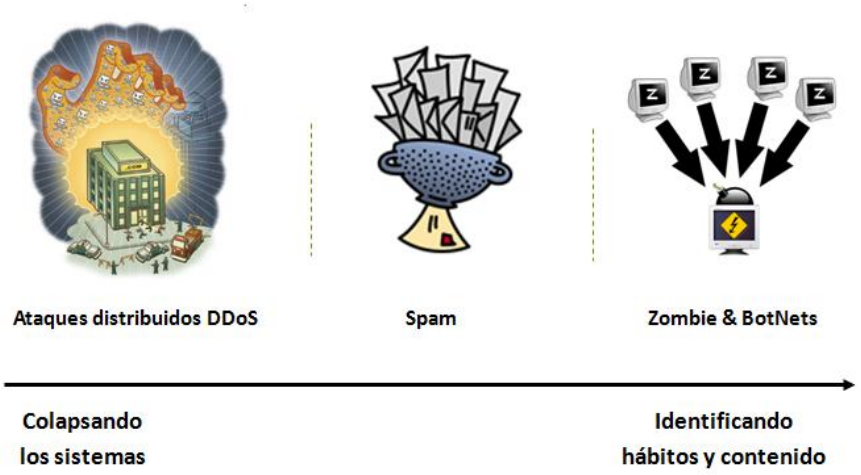


Figura 1.57.Tipos de ataques masivos

1.2.7.2.5. Ataques distribuidos de denegación de servicio (DDOS)

Esto se produce cuando varios servidores o PC's desde distintos lugares para bajar el servicio de un servicio, lo realizan tratando de colapsarlo por medio de varias solicitudes de este servicio hasta que dejen de brindarlo.

1.2.7.2.6. Spam

También conocidos como correo basura, lo que buscan es atacar los correos electrónicos con información que el usuario nunca solicito, utilizan direcciones de empresas, y el momento de aceptar este mensaje se está confirmando a este servidor de que ese correo es válido y está abierto para futuros ataques.

1.2.7.2.7. Zombie & BotNets

Las red Zombie son aquellas donde miles de ordenadores han sido infectados por un software malicioso denominado bot con el fin de obedecer todas las instrucciones que un atacante las establezca, un equipo Zombie recibe órdenes de propagar el mismo así mismo el de enviar correo Spam hacia distintas redes con el objetivo de infectar a nuevos usuarios.

Phishing & Pharming

Perfeccionando las técnicas mediante el uso de recursos de red

Figura 1.58.Tipos de ataques de violación de seguridad

1.2.7.2.8. Phishing

Esto consiste en obtener información confidencial, como números de tarjetas de crédito, contraseñas, números de cuenta entre otros, esto lo hacen enviando correos con la imagen de la Institución bancaria ya sea por motivos de mantenimiento o verificación de los datos, el fin es conseguir la información para posteriormente ser utilizados de forma ilegal.

1.2.7.2.9. Pharming

Es una derivación del phishing que es de mayor peligro, donde se envían correos que aparentan estar vacios, que tienen un programa que manipula la dirección de dominio y la direcciona a una que el atacante haya definido anteriormente. Cuando el usuario ingresa la dirección de su entidad financiera luego de haber ejecutado este correo, se lo direcciona a un dominio falso donde se le pedirán todos sus datos personales y jamás podrá darse cuenta que se está entregando información confidencial a otra persona.

1.2.7.3. Seguridad de la información

Hoy en día se engloba a todos los términos informáticos que interactúan como información, así mismo se lo tiene que hacer en el aspecto de seguridad, por lo tanto se lo hace tanto para hardware como para software.

En este punto se toma en cuenta tres aspectos importantes que se muestran en el siguiente gráfico:

Figura 1.59.Seguridad de la Información

1.2.7.4. Objetivos de la información

Con el fin de mantener segura una red se detallan ciertos objetivos con el fin de garantizar que toda la información que se maneja es segura, estos parámetros son:

- **Integridad:** Los datos que se envían no fueron alterados durante su transmisión hasta llegar a su destino.

- **Confidencialidad:** La información que se transmite debe ser manejada únicamente por los usuarios autorizados.

- **Disponibilidad:** Esto se refiere a garantizar que en cualquier momento se pueden acceder a los recursos de la información.

- **Evitar el rechazo:** ninguna de las operaciones que realice un usuario autorizado sea negado más adelante ya cuando esta haya sido realizada.

- **Autenticación:** La verificación de los usuarios permitidos para el manejo de la información.

En base a estos factores se podría decir que la red que se maneja es segura pero siempre se están evolucionando los métodos con el fin de acceder a estos datos, ahora es común ver que una persona se conecte desde cualquier parte del mundo hacia las redes informáticas por lo que las protecciones que se brinden deben estar un paso siempre delante de los atacantes.

1.2.7.5. Métodos de protección

En una empresa donde se trabaja con varios equipos que buscan información de toda la red de información (Internet), debe haber protecciones en todos los puntos por donde pasara dicha información, por lo que para cada área existen programas que ayudaran

a que esta información sea libre de programas maliciosos que puedan afectar a los usuarios.

Se han dividido en cuatro categorías para proteger la información las cuales son:

- Inicial
- Contenido
- Avanzado
- Profesional

1.2.7.5.1. Inicial

En esta área se encuentran los servicios de seguridad perimetral, es decir entre la red de equipos y la información externa (Internet).

- **FW & IDP:** estos son los requerimientos mínimos en una red para detección de virus y de intrusos, estos equipos se encuentran implementados dentro de un mismo hardware.

- **VPN:** son servicios que permiten conectar dos puntos de manera segura a través del internet.

- **Teleworkers:** este es un servicio pensado para usuarios que se encuentran fuera de la empresa y que les permite conectarse de forma segura a la red para que puedan seguir realizando sus actividades con normalidad.

1.2.7.5.2. Contenido

Los servicios del área de contenido se encargan de profundizar la seguridad que en el área inicial no pudo ser detectada.

- **AV & AS:** servicios designados para el control del correo electrónico.

- **Webfilter:** encargado del contenido de las páginas que se visiten durante la navegación en internet.

1.2.7.5.3. Avanzado

Es la categoría de analizar todo lo referente a los segmentos que se maneja de manera interna en la red.

- **FW interno:** administra el control del tráfico que circula en los segmentos definidos en la red interna.

- **IDP interno:** detiene el ataque que se haya realizado a uno de los segmentos internos.

- **ADS (sistema de detección de anomalías):** en base a como se encuentre el tráfico actual en la red, se encarga de analizar ataques sumamente peligrosos que puedan acceder a los servidores.

- **Parche Virtual:** es el encargado de simular parches de protección y de actualizaciones de los servidores, con el fin de que los ataques a estos no se produzcan el momento de que los servidores en verdad los realicen.

1.2.7.5.4. Profesional

Esta categoría está dirigida a los servicios de consultoría, es decir para verificar la eficiencia de las seguridades implementadas en la red.

- **Prueba de penetración:** se trata de realizar todos los pasos que realizaría un atacante para acceder a la información de la empresa, esto es realizado mediante programas de simulación o personas de la misma empresa.

- **Análisis de brecha:** se basa en determinar el nivel en el cual se encuentra la seguridad de la información en base a la norma ISO 27001.

CAPITULO II

ESTADO ACTUAL DE LA RED INFORMÁTICA DE LA SENATEL

2.1. Situación actual de la red informática

La Secretaría Nacional de Telecomunicaciones actualmente está constituida por Departamentos, los cuales se encuentran distribuidos en cada piso de la infraestructura, para una administración más fácil de la red global se han dividido estos Departamentos dentro de VLAN's por medio de la dirección física de cada uno de los equipos implementados en los puestos de trabajo. [16]

La administración de la red es realizada por el Departamento de Servicios Informáticos de la SENATEL, en donde se encuentran todos los equipos como: Servidores, Routers, Switches, y las aplicaciones para distribuir los diferentes servicios a todos los funcionarios de la SENATEL.

Estas VLAN's manejan un alto nivel de encriptación de seguridad por la importancia de datos que se maneja dentro de la Institución, para certificar la legitimidad de los documentos; los Directores de cada Departamento fueron provistos de llaves los cuales insertan una firma digital única de cada funcionario cuando se envían hacia distintas instituciones.

Para visitantes o funcionarios de otras instituciones que se vayan a conectar a la red, serán direccionados a una VLAN de uso temporal, en la cual podrán navegar por Internet de la misma manera que a los funcionarios internos con ciertos parámetros de seguridad como la prohibición a ciertas páginas asignadas por el servidor proxy, el cual asigna los permisos de acceso a ciertas páginas web determinadas anteriormente por el administrador de la red.

En la VLAN temporal cabe indicar que no se han asignado los recursos internos de la Institución tales como el correo o de intranet en la cual se manejan todos los oficios y documentos en los que trabajan los usuarios internos.

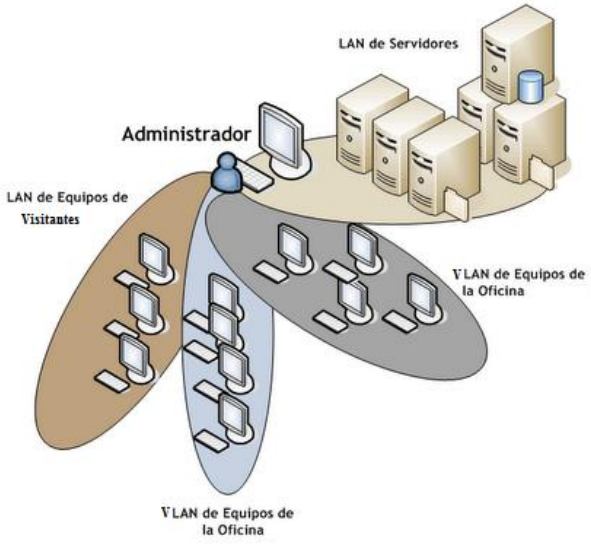


Figura 2.1.Distribucion de VLAN's

Dentro de la SENATEL se han elaborado de esta manera cada una de las VLAN's de acuerdo a como se distribuyeron los departamentos y puestos de trabajo en cada uno de ellos.

A continuación se muestra la disposición de cada una de las VLAN's que se han creado de acuerdo a los pisos y a los departamentos dentro de la Secretaría Nacional de Telecomunicaciones.

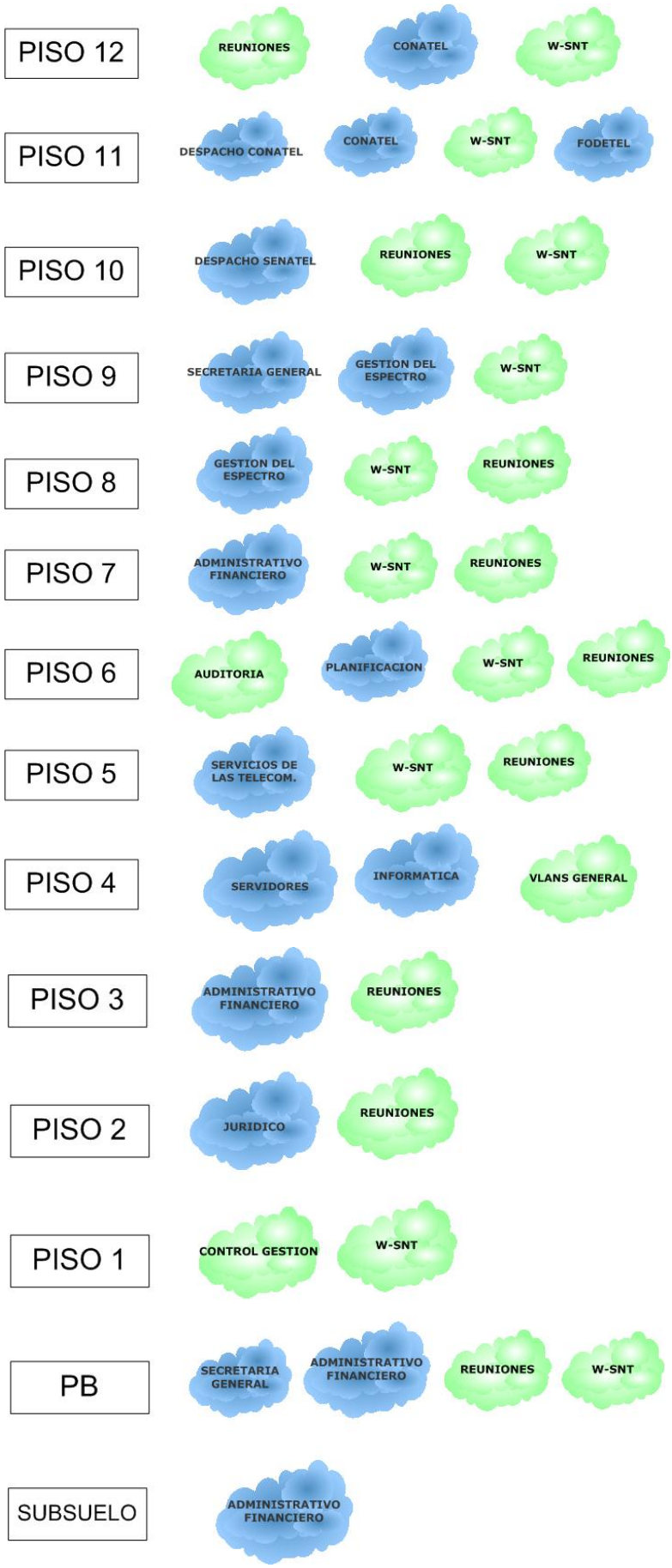


Figura 2.2.Distribucion de las VLAN's de la SENATEL

Desde un punto de vista lógico que se desea observar toda la red de manera general la Secretaría Nacional de Telecomunicaciones se encuentra implementada de la siguiente manera:

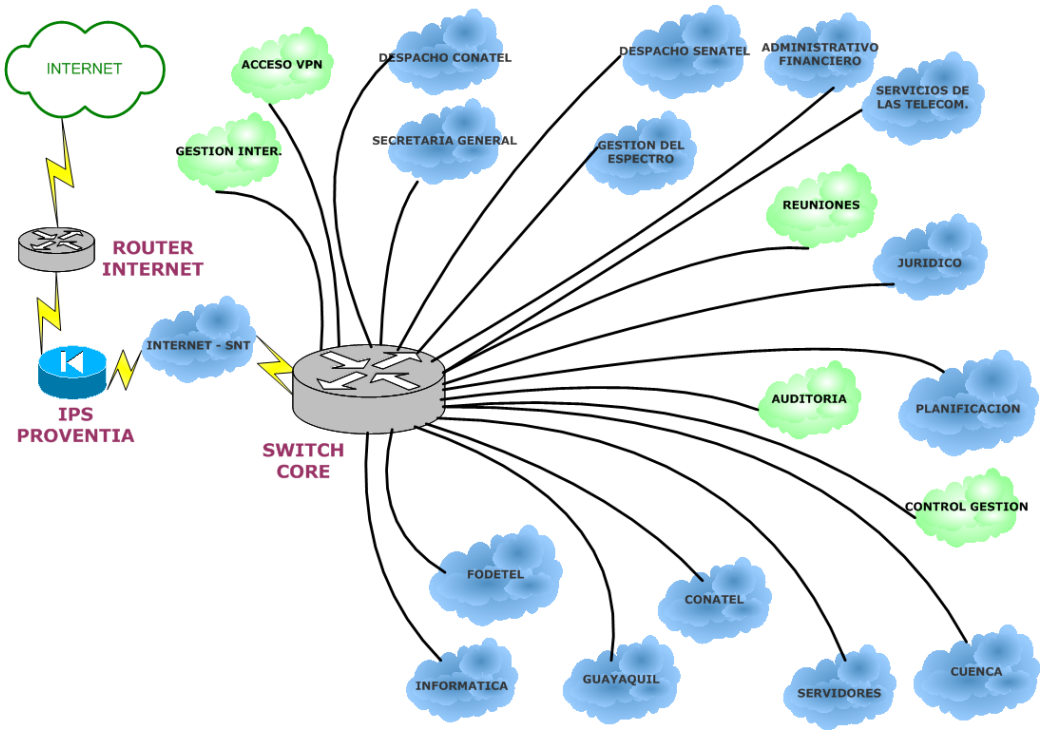


Figura 2.3.Distribucion lógica de la red informática de la SENATEL

En donde podemos observar que todos los departamentos se encuentran conectados a un elemento de capa 3, en este caso un Switch Core, el cual se encuentra previamente conectado a un servidor proxy para filtrar el contenido de la información de ciertas páginas y distribuir esta información hacia todas las VLAN's que se muestran en la figura anterior.

2.1.1. Modos de acceso

Para poder acceder a la red el usuario puede realizarlo de dos maneras, sea mediante un punto de acceso en cualquiera de los pisos o por medio de una computadora portátil que posea la unidad de wireless o punto de conexión inalámbrico.

2.1.1.1. Modo alámbrico

El modo alámbrico es aquel que permite al usuario acceder a la red por un medio físico, en este caso un cable cruzado que va desde el puerto del ordenador hacia el punto de red para establecer la conexión.

Figura 2.4.Modo de acceso alámbrico a la red

2.1.1.2. Modo inalámbrico

El modo inalámbrico es el cual no necesita de una medio físico para realizar la conexión, utiliza el aire como interfaz por la cual viajan los paquetes.

Figura 2.5.Modo de acceso inalámbrico a la red

2.2. Diseño actual de la red

Actualmente la red de la Secretaría cuenta con los dos modos de acceso que se detallaron anteriormente, por lo que para cada uno de ellos se ha estructurado una red diferente y que llegan a los mismos servidores.

En primera instancia se muestra el esquema de la red alámbrica y como acceden los funcionarios a los recursos y son asignados a los respectivos grupos de trabajo, luego se mostrara la red de acceso inalámbrico, el servidor encargado de permitir el acceso así mismo del protocolo de comunicación que está configurado actualmente.

2.2.1. Diseño actual de la red alámbrica de la SENATEL

La red alámbrica se encuentra distribuida en toda la infraestructura partiendo desde los servidores, hacia cada uno de los equipos como se muestra en la siguiente figura.

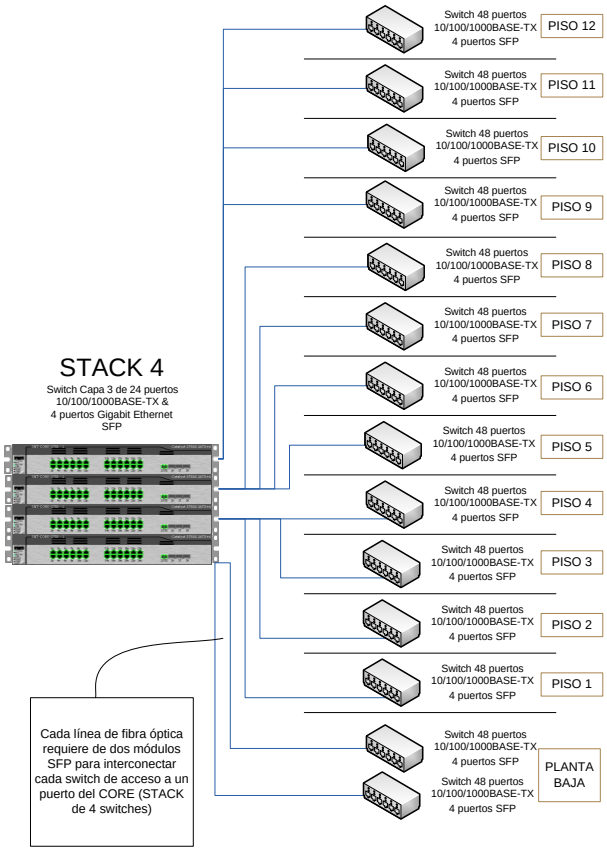


Figura 2.6.Estructura de la red alámbrica SENATEL

En cada piso se encuentra instalado un switch CISCO de 48 puertos, de los cuales se distribuyen hacia cada uno de los equipos que existan en ese piso, se hace una excepción en lo que corresponde a la planta baja ya que existen varios puntos de red por los visitantes que necesiten acceder a la red.

Para conectar todos los switches implementados en cada uno de los pisos con el switch central encargado de direccionar el tráfico se han utilizado líneas de fibra óptica con el objetivo de aumentar la eficiencia de la red como velocidad, disponibilidad, y evitar la pérdida de la información.

Cada usuario de la Institución tiene asignado su equipo el cual posee una única dirección física la cual se encuentra registrada y que indica que esa dirección pertenece a determinado usuario.

Los equipos de los funcionarios están conectados a la red por medio de cable cruzado hacia los distintos puntos de red, y esta configuración se la realiza cada vez que se agrega un nuevo equipo a la red de manera estática.

Además se realiza la configuración manual de todos los parámetros, como dirección del servidor, configuración del correo personal y de la red interna de la Institución para el manejo de trámites entre todos los usuarios.

2.2.2. Diseño actual de la red inalámbrica de la SENATEL

En lo que se refiere a dispositivos inalámbricos la Institución ha elaborado una red con puntos de acceso en cada uno los pisos, estos puntos conocidos como Access Point (AP) están configurados para permitir al equipo que acceda a la red por medio de un proxy determinado por el administrador y de la misma manera con una clave de seguridad para que únicamente los funcionarios de la Secretaría puedan acceder a la red.

En la siguiente figura se muestra el esquema de cómo se ha implementado la red inalámbrica de la Secretaría Nacional de Telecomunicaciones.

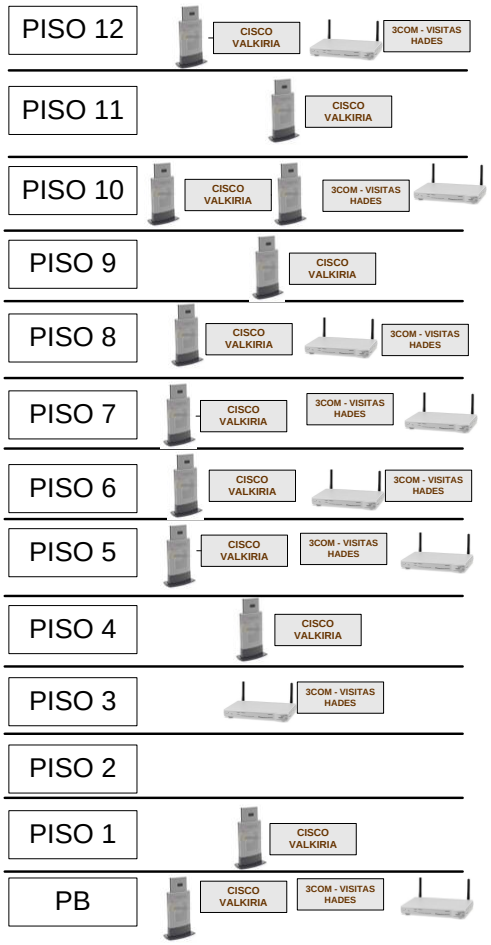


Figura 2.7.Estructura de la red inalámbrica SENATEL

Como se puede observar existen dos redes inalámbricas las cuales manejan dos tipos diferentes de acceso, ambas redes se configuraron con un servidor proxy así como de una clave de seguridad para su acceso.

La primera es la red VALKIRIA en la cual únicamente pueden acceder los directores de cada departamento por medio de las llaves digitales en donde el nivel de restricción de acceso es menor pero el nivel de encriptación es mucho mayor, esta red permite tener acceso a toda la red interna así como de los servicios que esta ofrece.

La segunda red es la red HADES la cual es destinada para visitantes en la cual el nivel de restricción de acceso es mucho mayor y el nivel de encriptación es menor, cuando un usuario está conectado a esta red, no puede ver ninguno de los equipos dentro de la Institución y solo está activa para la navegación a través de Internet.

2.2.2.1. Seguridad WPA- TKIP

El estándar WPA (Acceso Protegido Wi-Fi) es un estándar diseñado para la protección de redes inalámbricas en base a las deficiencias del estándar anterior WEP (Privacidad equivalente a Cableado), uno de esos defectos es que reutilizaba el vector de inicialización, lo cual era más vulnerable a ataques.

WPA también abarca lo que es la autentificación de usuarios a través de un servidor en el cual se guardan todas las contraseñas y autorizaciones de los usuarios de la red, con el objetivo de que el servidor se despliegue por todas las redes este estándar autoriza el acceso mediante una clave única para cada uno de los usuarios, en el caso de la Institución este servidor de autentificación es el servidor RADIUS.

Este servidor distribuye diferentes claves, estas claves son cifradas utilizando el algoritmo RC4, el mismo que es utilizado en WEP pero más sofisticado, genera una clave de acceso de 128 bits y un vector de inicialización de 48 bits.

El protocolo TKIP (Protocolo de Integridad mediante Llave Temporal) cambia las claves que son generadas por el servidor RADIUS de manera aleatoria de acuerdo como la red es utilizada, como estas claves se combinan con los vectores de inicialización más grandes, hacen un sistema relativamente más seguro contra ataques para la recuperación de contraseñas.

TKIP genera una clave temporal de 128 bits compartida entre cliente y punto de acceso, está clave se combina con la dirección física del usuario que más adelante se unirá que con el vector de inicialización, estas claves temporales son cambiadas en un tramo de cada 10000 paquetes de manera dinámica manteniendo así la confidencialidad de dicha contraseña.

2.3. Servidores

El servidor es un equipo o aplicación que se encuentra incorporada en la red para ofrecer un servicio al resto de ordenadores denominados clientes los cuales podrán solicitar está aplicación cuando ellos lo requieran.

Dentro de la Secretaría Nacional de Telecomunicaciones se encuentran varios servidores, que cumplen todo tipo de aplicaciones de los cuales se detallaran únicamente los más relevantes.

En la clasificación de los servidores podemos encontrar:

- Servidor de correo
- Servidor web
- Servidor proxy
- Servidor de base de datos
- Servidor de impresión

En la red de la Institución se encuentran estos servidores, así como de los servidores encargados de asignar las direcciones a cada ordenador y de establecer los permisos de acceso a los recursos anteriormente mencionados.

A continuación se detallan los servidores más importantes que se manejan dentro de la Secretaría Nacional de Telecomunicaciones.

2.3.1. Servidor DHCP

Un servidor DHCP es el encargado de asignar todos los parámetros necesarios a los equipos que se encuentren conectados a su red de forma automática, como la dirección de puerta de enlace, la máscara de subred, la dirección IP.

Las siglas DHCP en ingles son Dynamic Host Configuration Protocol, indica que este servidor provee el protocolo a todos los clientes de la red de poder conectarse entre sí, asignando de forma automática las direcciones a cada uno de ellos dentro de un rango determinado por el administrador.

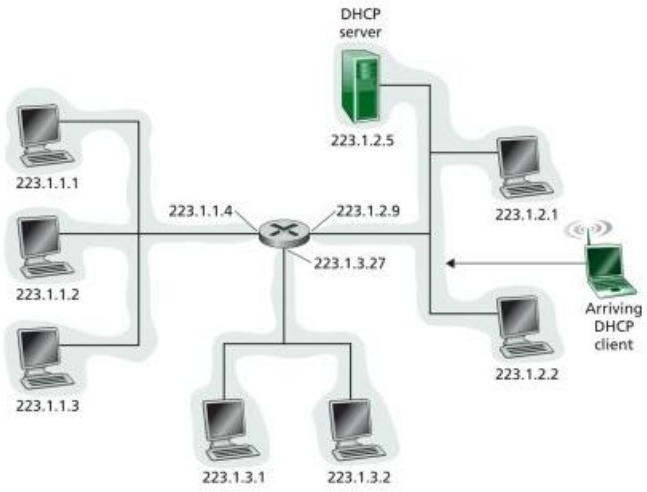


Figura 2.8.Asignacion de direcciones IP mediante servidor DHCP

El servidor DHCP asigna automáticamente la correspondiente dirección IP a todos los equipos que se conectan a la red, siempre asigna de acuerdo a la subred que se una el ordenador, en la figura podemos ver que a la red que se encuentra conectada el servidor directamente llega un nuevo equipo el cual será registrado y asignado todos los parámetros necesarios para que forme parte de la red.

DHCP se maneja básicamente en dos bases de datos, la primera consiste en una base de direcciones estática y otra que contiene varias direcciones que se encuentran disponibles y se irán asignando conforme los clientes así lo requieran.

Cuando un equipo se conecta a la red el servidor verifica la dirección física de la tarjeta de interfaz de red, si se comprueba que existe esa dirección en la base de datos estática se asigna la dirección IP correspondiente con todos los parámetros ya establecidos, y en el caso de no ser encontrada se le asigna una dirección IP disponible de la base de datos dinámica de manera temporal.

2.3.2. Servidor de dominio (DNS)

Un servidor de dominio es aquel que permite de cierta manera transformar la dirección IP de una página Web en un nombre denominado dominio el cual es con el que se busca dicha página en el explorador.

Sus siglas vienen del nombre en inglés Domain Name Server, nos ayuda a buscar las direcciones IP de los nombres que buscamos, ya sea de una página WEB, o de un host que se encuentra dentro de una red LAN.

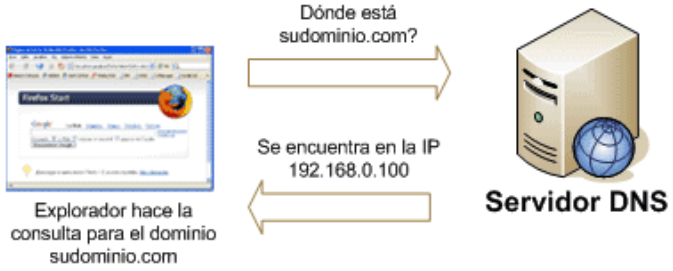


Figura 2.9.Solicitud de la dirección IP de una página Web al servidor DNS

Como se puede observar en la figura, cuando un usuario ingresa una dirección en el navegador, está ingresando el dominio al que desea ingresar, el servidor DNS devuelve la dirección IP del servidor WEB en la cual tiene que buscar.

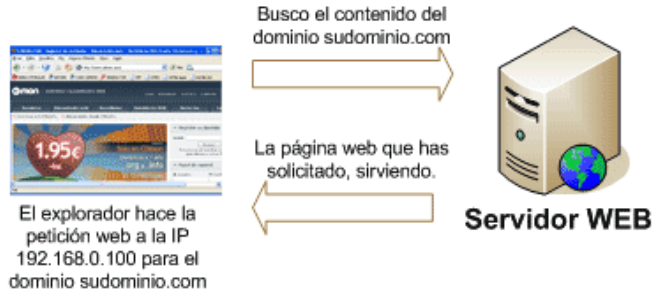


Figura 2.10.Busqueda de la página web a través del servidor WEB

Cuando el explorador envía la solicitud de búsqueda de ese dominio al servidor WEB, este devuelve la información de la página solicitada, todo esto ocurre en cuestión de instantes que son imperceptibles para el usuario.

2.3.3. Servidor RADIUS

Un servidor RADIUS es el encargado de verificar y autentificar la petición de un cliente RADIUS a través de credenciales de información así como de ciertos parámetros de conexión, todo esto lo realizan en base a un formato que solamente este servidor lo puede interpretar.

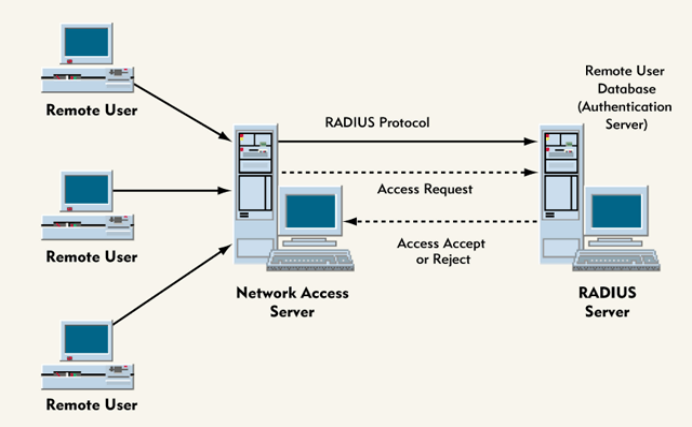


Figura 2.11.Esquema de funcionamiento del servidor Radius

El servidor responde a la solicitud de los clientes ya sea con una aceptación o un rechazo mediante el mismo formato el cual corresponde al mismo utilizado por UDP, este protocolo utiliza los mismos puertos que UDP para realizar está comunicación:

- **1812:** mensajes de autenticación RADIUS
- **1813:** mensajes de administración de cuentas RADIUS

Para algunos servidores de acceso de red (NAS) los puertos UDP de comunicación sean distintos:

- **1645:** mensajes de autenticación RADIUS
- **1646:** mensajes de administración de cuentas RADIUS

Mediante este servidor podemos verificar que los usuarios que solicitan acceso sean los que se encuentran dentro de la base de datos para poder acceder a los servicios.

2.3.3.1. IAS

El Servicio de autenticación de Internet es la implementación de Microsoft de un servidor y proxy del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS, *Remote Authentication Dial-In User Service*).

Como servidor RADIUS, IAS se encarga de manera centralizada de la autenticación, autorización y de las cuentas de conexión de muchos tipos de accesos a la red, como inalámbrico, conmutación de autenticación, acceso remoto de red privada virtual (VPN, Virtual Private Network) y acceso telefónico y conexiones de enrutador a enrutador. Como proxy RADIUS, IAS reenvía los mensajes de autenticación y cuentas a otros servidores RADIUS.

Active Directory® es un servicio de directorio que almacena información acerca de los objetos de una red y la pone a disposición de los usuarios y administradores de la red.

Cuando un servidor IAS es miembro de un dominio de Active Directory®, IAS utiliza el servicio de directorio como su base de datos de cuentas de usuario y forma parte de una solución de inicio de sesión único. El mismo conjunto de credenciales se utiliza para controlar el acceso a la red (autenticar y autorizar el acceso a la red) y para iniciar una sesión en un dominio de Active Directory.

Los proveedores de servicios de Internet (ISP, Internet Service Providers) y las organizaciones que mantienen el acceso a la red han visto incrementado el reto de administrar todos los tipos de acceso a la red desde un punto de administración único, con

independencia del tipo de equipamiento de acceso a la red utilizado. El estándar RADIUS admite está funcionalidad en entornos homogéneos y heterogéneos. RADIUS es un protocolo cliente-servidor que permite que el equipo de acceso a la red (utilizado como clientes RADIUS) envíe solicitudes de administración de cuentas y autenticación a un servidor RADIUS.

Un servidor RADIUS tiene acceso a información de cuentas de usuario y puede comprobar las credenciales de autenticación de acceso a la red. Si las credenciales del usuario son auténticas y se autoriza el intento de conexión, el servidor RADIUS autoriza el acceso del usuario basándose en las condiciones especificadas, y registra la conexión de acceso a la red en un registro de cuentas. El uso de RADIUS permite la recopilación y el mantenimiento de los datos de autenticación, autorización y cuentas de usuario para el acceso a la red en una ubicación central, en lugar de en cada servidor de acceso.

Con IAS, las organizaciones pueden también contratar una infraestructura de acceso remoto de un proveedor de servicios y conservar al mismo tiempo el control sobre la autenticación, autorización y cuentas de los usuarios.

Pueden crearse configuraciones IAS diferentes para las siguientes soluciones:

- Acceso inalámbrico
- Acceso remoto de la organización mediante red privada virtual (VPN) o acceso telefónico
- Acceso telefónico externo o acceso inalámbrico
- Acceso a Internet
- Acceso autenticado a recursos de la extranet para los socios comerciales

2.3.3.2. IAS como servidor RADIUS

IAS en esta función sirve para la autenticación, autorización y la administración de las cuentas de clientes RADIUS, siendo estos clientes servidores de acceso o de proxy.

Como servidor RADIUS, IAS proporciona lo siguiente:

- Un servicio central de autenticación y autorización así como de las cuentas para todas las peticiones de acceso enviadas por clientes RADIUS.

- Para autenticar las credenciales de usuario de un intento de conexión, IAS utiliza un dominio de Microsoft® Windows NT® Server 4.0, un dominio de Active Directory® o el Administrador de cuentas de seguridad (SAM, Security Accounts Manager) local.

- Para autorizar la conexión, IAS utiliza las propiedades de marcado de la cuenta de usuario y las directivas de acceso remoto.

- Un servicio central de registros de administración de cuentas para todas las solicitudes de administración de cuentas enviadas por clientes RADIUS. Las solicitudes de administración de cuentas se almacenan en un registro local para su posterior análisis.

A continuación se muestra un esquema de cómo IAS trabaja como un servidor RADIUS para el caso que hayan varios clientes y un proxy RADIUS. [3]

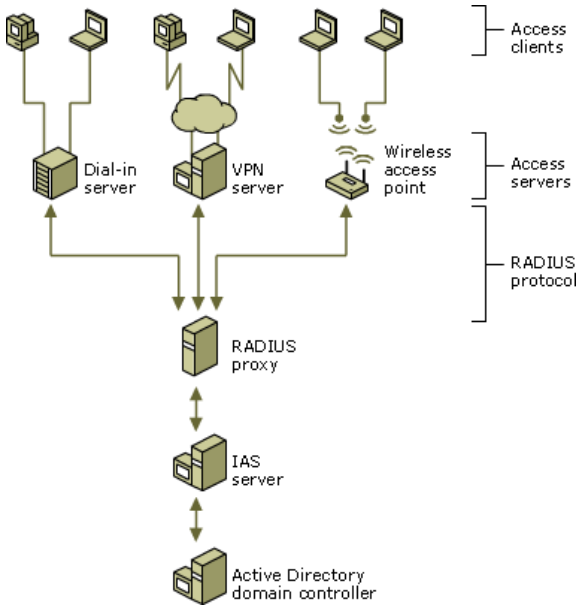


Figura 2.12.IAS como servidor RADIUS

2.4. Equipos utilizados y características de los mismos

Dentro de la Secretaría para poder conformar la red se han distribuido equipos para la elaboración de la redes de acceso alámbrico e inalámbrico, de acuerdo a las necesidades para la prestación de servicios en todo el edificio se han hecho uso de los siguientes equipos los cuales cuentan con sus características técnicas.

2.4.1. Switch de Capa 3

Este es el equipo encargado de distribuir los servicios de los servidores hacia todos los pisos de la Institución, esto lo hace mediante backbones de fibra óptica hacia cada uno de los switches ubicados en los departamentos.

A continuación se muestran las características físicas que posee este equipo así como de las especificaciones de red que maneja.

Figura 2.13.Switch de Capa 3

Características técnicas:

- Cantidad de puertos: 24 10/100/1000T
- Enhanced Multilayer Software Image encargado de QoS
- Maneja ACL's (Listas de control de acceso)

- Protocolo de enrutamiento estático RIP
- Ranuras vacías: 4 x SFP
- Modo de comunicación: Dúplex, Full Dúplex
- Soporte DHCP, soporte VLAN
- Tipo de conectividad: cableado
- Protocolo de conmutación: Ethernet
- Velocidad de transferencia de datos: 1 Gbps
- Protocolo de direccionamiento: OSPF, IGRP, RIP 1, RIP 2, EIGRP

2.4.2. Switch de Capa 2

Este equipo es el que se encuentra en cada uno de los pisos de la Institución y a donde llega la conexión del backbone de fibra óptica del switch de capa 3, a este equipo es donde se conectan cada uno de los ordenadores de los funcionarios de la Institución.

Figura 2.14.Switch de Capa 2

Características técnicas:

- Cantidad de puertos: 48 x Ethernet 10/100/1000t
- Velocidad de transferencia de datos: 1 Gbps
- Protocolo de interconexión de datos: Ethernet, Fast Ethernet, Gigabit Ethernet
- Tecnología de conectividad: cableado
- Modo de comunicación: Dúplex, Full Dúplex
- Protocolo de conmutación: Ethernet
- Conmutación Capa 2, auto-sensor por dispositivo, soporte de DHCP, soporte VLAN
- Total de ranuras de expansión (libres): 4 (4) x SFP
- Método de autenticación: RADIUS, TACACS+

2.4.3. Access Point WLAN

El AP es la interfaz inalámbrica para conectar a las redes de la SENATEL el cual se encuentra configurado para que se tenga acceso mediante un usuario y una contraseña además de todos los parámetros como un proxy y con los métodos de encriptación para la seguridad de la información.

Figura 2.15.Access Point Wireless LAN

Características técnicas:

- RAM instalada: 16 MB
- Memoria Flash: 8 MB
- Tecnología de conectividad: inalámbrico
- Protocolo de interconexión de datos: 802.11b (Wi Fi)
- Protocolo de gestión remota: HTTP, Telnet
- Soporta DHCP
- Soporte VLAN

CAPITULO III

REDISEÑO DE RED INTELIGENTE DINÁMICA DE EQUIPOS

3.1. Variable de detección de equipos

Para realizar la detección de los equipos que pertenecen a la Secretaría Nacional de Telecomunicaciones, se planteó obtener una base de datos que contenga todas las direcciones MAC de cada uno de los dispositivos así como de las VLAN's a las que corresponden cada uno de los mismos.

Con el fin de cumplir con este objetivo se planteó la implementación de un servidor que direccione de forma automática a las VLAN's correspondientes cuando detecte que un equipo se ha conectado a la red de la Institución.

El servidor encargado de esta función es el servidor VMPS (VLAN Membership Policy Server), el cual por medio de una solicitud que envía el switch al que se conecta un equipo asigna la VLAN correspondiente a la dirección MAC del equipo conectado, esto también se lo puede llevar a cabo por medio de la identificación del usuario el cual también se encontrara registrado dentro de la base de datos.

De acuerdo a los equipos actualmente instalados dentro de la Institución, la idea de implementar el servidor dentro del switch de capa 3 no se podía dar ya que debido a la versión y características del mismo no se lo podía implementar como servidor sino únicamente como cliente.

Teniendo en cuenta este inconveniente se tuvo que optar por implementar un servidor que se encuentre conectado al switch de capa 3 (Router) para que cumpla con está

función, por lo que era necesario realizar cambios en la configuración en los equipos con el fin de la implementación de la red inteligente.

A continuación de muestra un esquema de cómo se implementaría este nuevo servidor a la red y que será el encargado de direccionar la petición de cada una de las VLAN's, en pocas palabras el servidor VMPS.

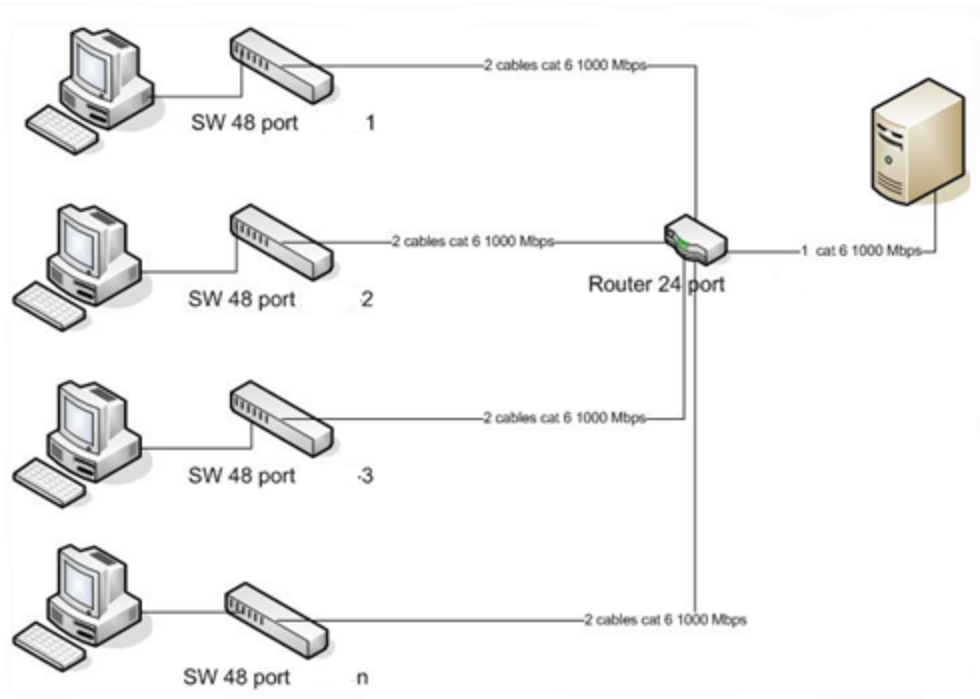


Figura 3.1.Esquema de implementación de servidor VMPS

El servidor VMPS recibirá todas las solicitudes que sean generadas por los switches en cada uno de los pisos de la Institución, previo a que se le asigne una VLAN este deberá consultar a la base de datos y determinar la procedencia del equipo que quiere conectarse a la red y lo hará en base a parámetros previamente establecidos, con esto cualquier funcionario podrá conectar su equipo sin la necesidad de volver a realizar la configuración que se realiza en las VLAN's estáticas. [17]

En este caso se utilizó el software denominado FreeNAC el cual posee internamente el servidor anteriormente mencionado y que deberá ser inicialmente configurado con los requerimientos que el administrador así lo requiera.

3.2. Software FreeNAC

FreeNAC es una herramienta de tipo OpenSource dirigida a la administración, autentificación y acceso dinámico para VLAN's.

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. [18]

Las características principales son:

- Asignación dinámica de redes virtuales
- Control de acceso a redes
- Flexibilidad en mecanismos de autentificación para redes: 802.1x, VMPS, Cisco Mac-Auth-Bypass
- 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 3.2. LOGO Software FreeNAC

FreeNAC provee una solución transparente para la administración dinámica de redes virtuales, a la vez que restringe la conectividad a la red. Desde el punto de vista de la seguridad, detecta dispositivos 'desconocidos' que están tratando de obtener acceso a través

de un conector de red Ethernet abierto, negando el acceso (y registrando el evento). Dispositivos conocidos y registrados son colocados a la red virtual que es atribuida a ellos.

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.

Con FreeNAC, 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.

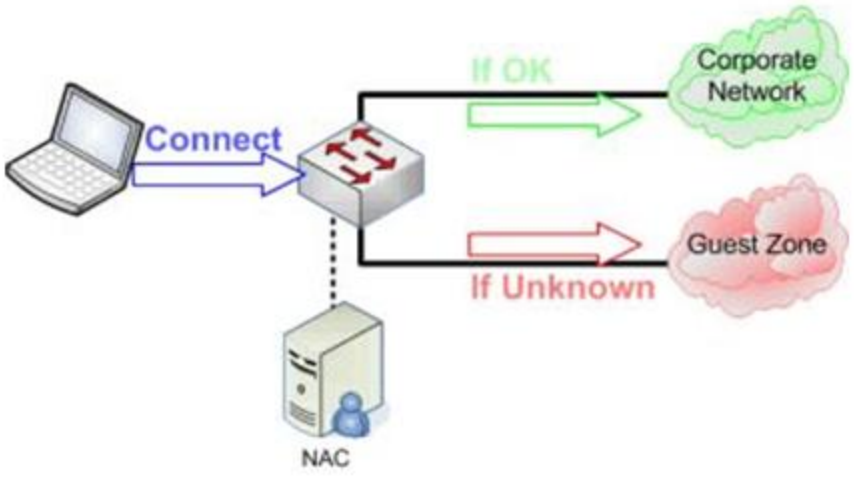


Figura 3.3. Direccionamiento de VLAN's con FreeNAC

FreeNAC tiene dos modos de operación:

- **VMPS**
- **802.1X**

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 física (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. [19]

A continuación se mostrara la configuración del programa para su correcto funcionamiento y todos los parámetros necesarios para cumplir con las metas que se plantearon para el direccionamiento dinámico de las VLAN's.

3.3. Programas

Para poder ejecutar el software FreeNAC se lo puede realizar utilizando una máquina virtual la cual ya viene con todos los elementos necesarios, o se lo puede hacer a través de la plataforma Linux ya que es el único entorno en el cual trabaja este software.

Para este estudio se decidió utilizar el programa mediante una máquina virtual la cual nos permite configurar el servidor únicamente a través de líneas de comandos en modo de terminal (Linux). [20]

En primer lugar se necesita un programa que permita ejecutar está máquina virtual, y para ello se decidió utilizar el conocido **VMware Workstation.**

3.3.1. VMware Workstation

VMware Workstation es un software que nos permite tener otro sistema operativo dentro del ordenador, y que permite realizar pruebas de software, componentes de PC para determinar su comportamiento o si puede llegar a ser dañino para el sistema operativo.

Figura 3.4. Logo VMware Workstation

Cuando el programa se encuentra instalado correctamente detecta automáticamente todos los programas que se encuentren con la extensión para iniciar el sistema operativo que se desea ejecutar.

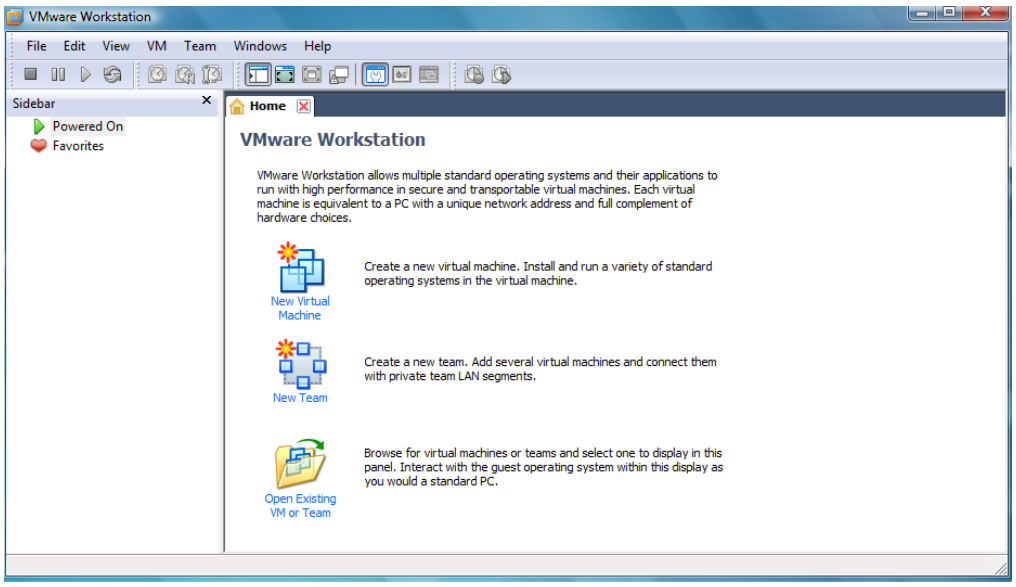


Figura 3.5. Menú inicial VMware Workstation

3.3.2. Máquina Virtual FreeNAC

La máquina virtual de FreeNAC viene equipada con todas las herramientas necesarias como Linux, los módulos necesarios y FreeNAC instalado en modo de prueba.

Podemos encontrar la máquina virtual de FreeNAC dentro de la siguiente dirección:

http://sourceforge.net/projects/opennac/files/

Y nos mostrara la siguiente pantalla:

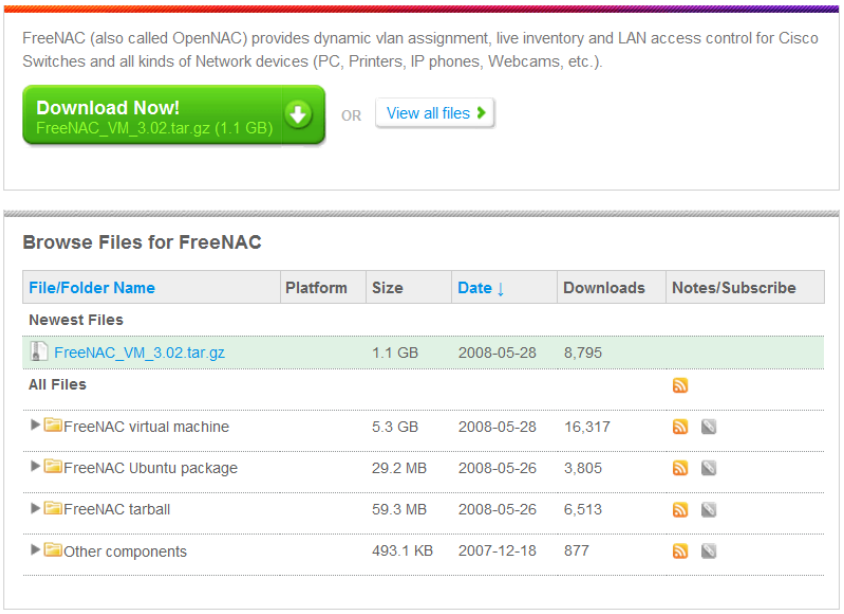


Figura 3.6. Página de descarga de Máquina Virtual FreeNAC

El archivo debido a que contiene todos los módulos necesarios para su funcionamiento, es sumamente extenso en tamaño por lo que se recomienda tener una conexión estable para obtenerlo en el menor tiempo posible.

Al terminar con el proceso de descarga se debe descomprimir esta carpeta y ser abierta desde el software VMware Workstation el cual buscara directamente el archivo para iniciar la máquina virtual.

3.3.3. Interfaz Gráfica de Usuario de Windows (Windows GUI)

La interfaz gráfica de usuario es la cual nos permite manipular los parámetros sobre los cuales va a trabajar el servidor, este será inicializado luego de haber configurado el servidor y establecer la comunicación entre los dos sistemas operativos.

Tabla 3.1. Funciones de los Sistemas Operativos

Sistema Operativo	*Función*
Linux	Servidor
Windows	Interfaz de usuario

Necesariamente debe trabajar con los 2 sistemas operativos anteriormente mencionados ya que en la parte del servidor los diseñadores del programa lo hicieron únicamente para trabajar en la plataforma de Linux, esto debido a que cualquier tipo de servidor presenta un mejor desempeño y menores vulnerabilidades, y en Windows porque la interfaz de usuario actualmente existe para este sistema operativo.

El enlace para descargar la Interfaz Gráfica de Usuario es la siguiente:

http://freenac.net/en/community/downloads

A continuación nos mostrara la siguiente página desde la cual procedemos a descargar los archivos del GUI:

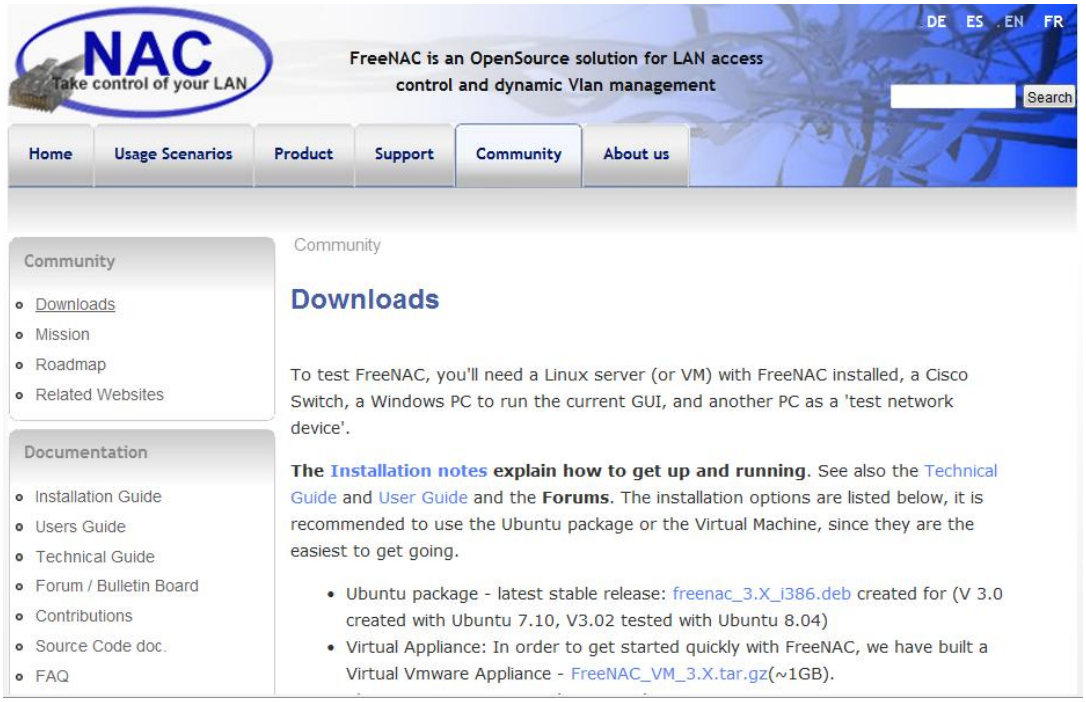


Figura 3.7. Página de descargas de FreeNAC

Los archivos para ejecutar la interfaz de usuario están con los nombres de: **vmps.exe** y **vmps.xml**, los cuales corresponden al archivo ejecutable y el archivo de configuración de aplicación.

Figura 3.8. Archivos de interfaz gráfica de usuario GUI

Estos archivos se ejecutarán luego de haber establecido inicialmente los parámetros del servidor FreeNAC.

Ya con todos los elementos necesarios a continuación se procederá a configurar los archivos, permisos, direcciones, etc. que requiere el servidor.

3.4. Conexión entre los sistemas operativos

Como se mencionó anteriormente FreeNAC funciona a través de los dos sistemas operativos, por lo que es necesario establecer la comunicación entre ambos.

FreeNAC por defecto viene configurado para utilizar el modo bridge el cual es necesario para estar corriendo activamente en la red y para recibir paquetes en una dirección IP dedicada.

Automáticamente el momento de instalar la aplicación de máquinas virtuales este asigna una dirección IP al adaptador de Ethernet de la red y en base a esta se procederá a configurar el adaptador Ethernet de la máquina virtual para que se encuentren dentro de la misma red y poder establecer la comunicación entre los dos sistemas operativos.

A continuación se muestra la configuración de la interfaz de Windows para el dispositivo Ethernet y del cual se debe configurar el de la máquina virtual.

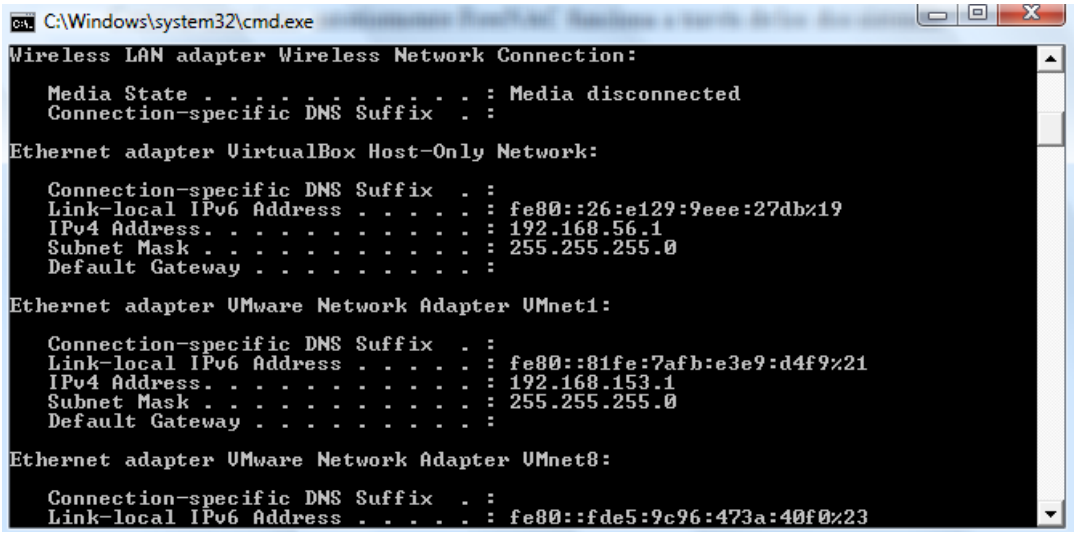


Figura 3.9. Configuración Ethernet Windows

El momento de arrancar la máquina virtual el momento de ingresar el nombre de usuario y contraseña, únicamente se permitirá el acceso con el usuario **freenac** y clave **freenac** lo cual no nos permitirán realizar cambios en los archivos necesarios, por lo que se

deberá cambiar al administrador de Linux que corresponde a **root,** lo cual se lo realiza utilizando el siguiente comando:

sudo bash

Al escribir este comando nos pedirá el nombre del nuevo usuario y contraseña y cambiamos a root y la contraseña para acceder con este usuario.

Ahora se debe revisar en primer lugar las interfaces activas de la máquina virtual para lo cual se ejecuta la siguiente línea:

ifconfig

Y nos mostrara lo siguiente:

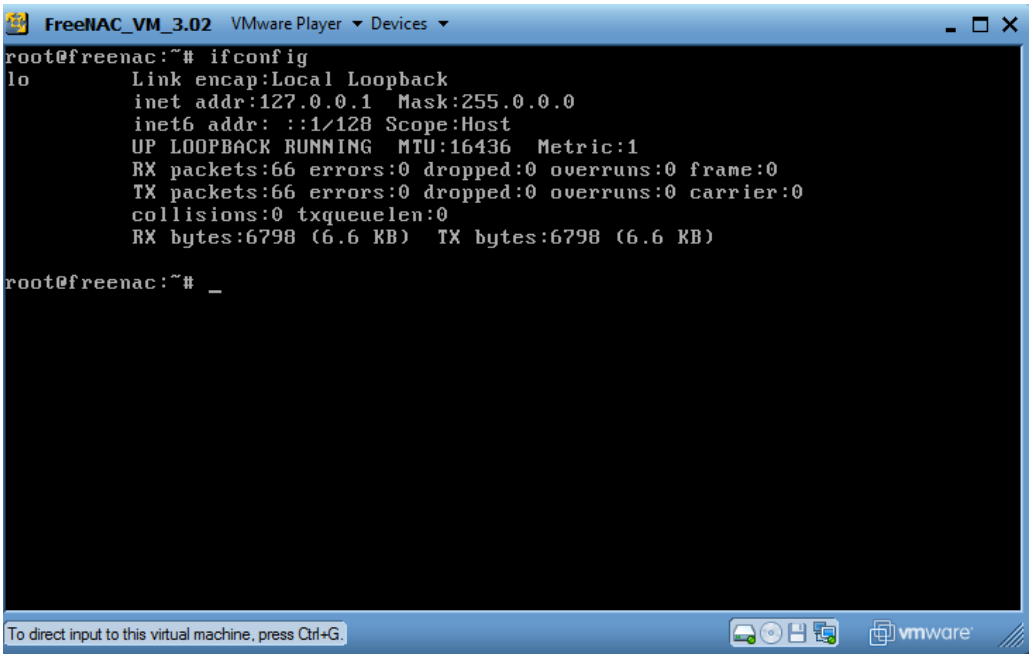


Figura 3.10. Configuración inicial de interfaces de FreeNAC

Para levantar la interface Ethernet y darle una dirección IP, se ejecutará lo siguiente:

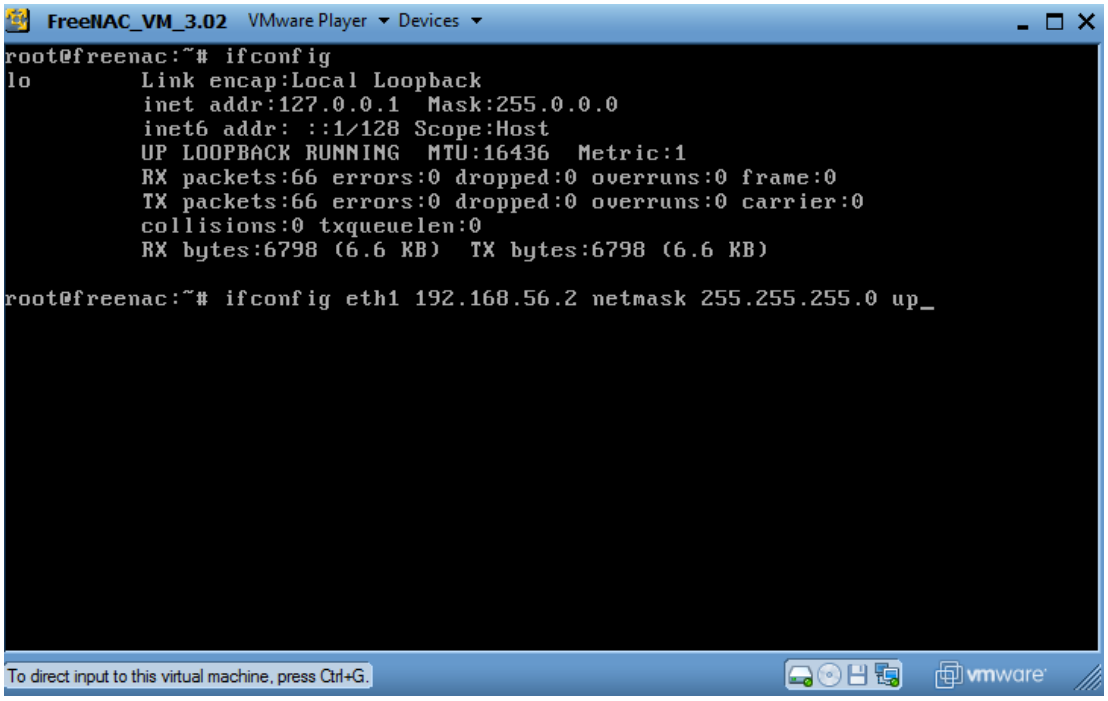


Figura 3.11. Comando para levantar una interfaz Ethernet FreeNAC

Luego de ejecutar este comando y volver a ejecutar **ifconfig** nos deberá aparecer lo siguiente:

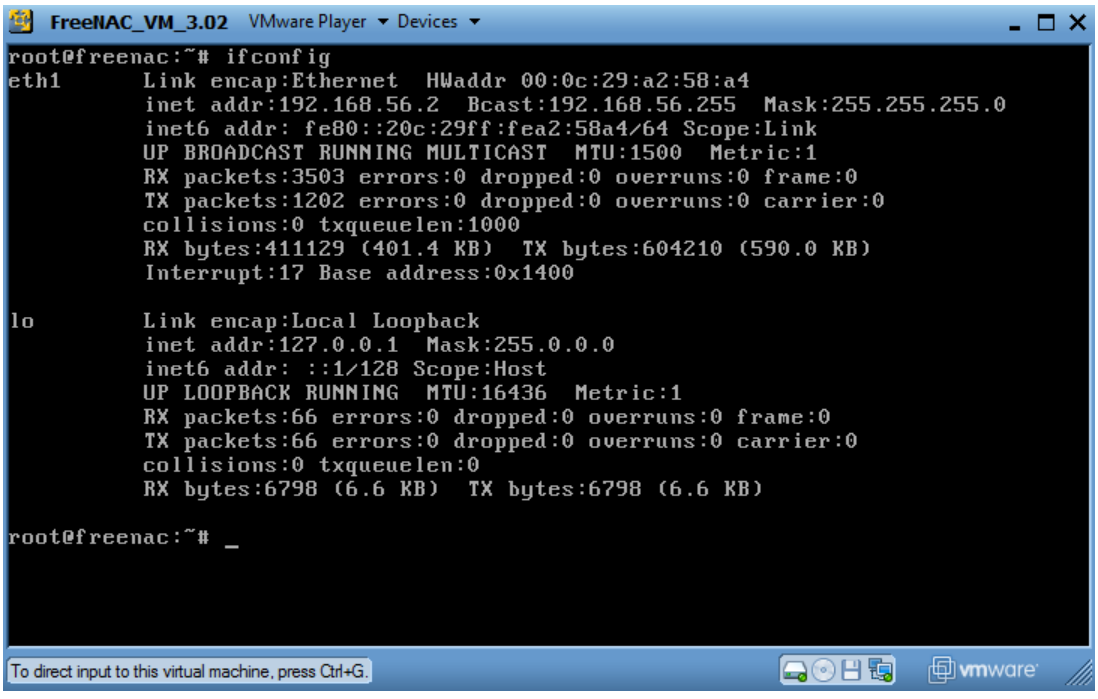


Figura 3.12. Interfaz Ethernet levantada y configurada

3.5. Conexión con la interfaz WEB

Con el fin de determinar que los dos sistemas operativos se han conectado satisfactoriamente y poder visualizar la administración del servidor, FreeNAC ha creado una interfaz Web la cual mostrara una página con varios enlaces de toda la información necesaria.

Para ello en primer lugar se deberá ingresar en el navegador y en la barra de dirección, colocar la IP de la máquina virtual:

Figura 3.13. Ingreso de IP en la barra del navegador

Si se despliega la siguiente página en el navegador, indica que el servidor se está ejecutando correctamente y se ha establecido la conexión entre la máquina virtual y el ordenador.

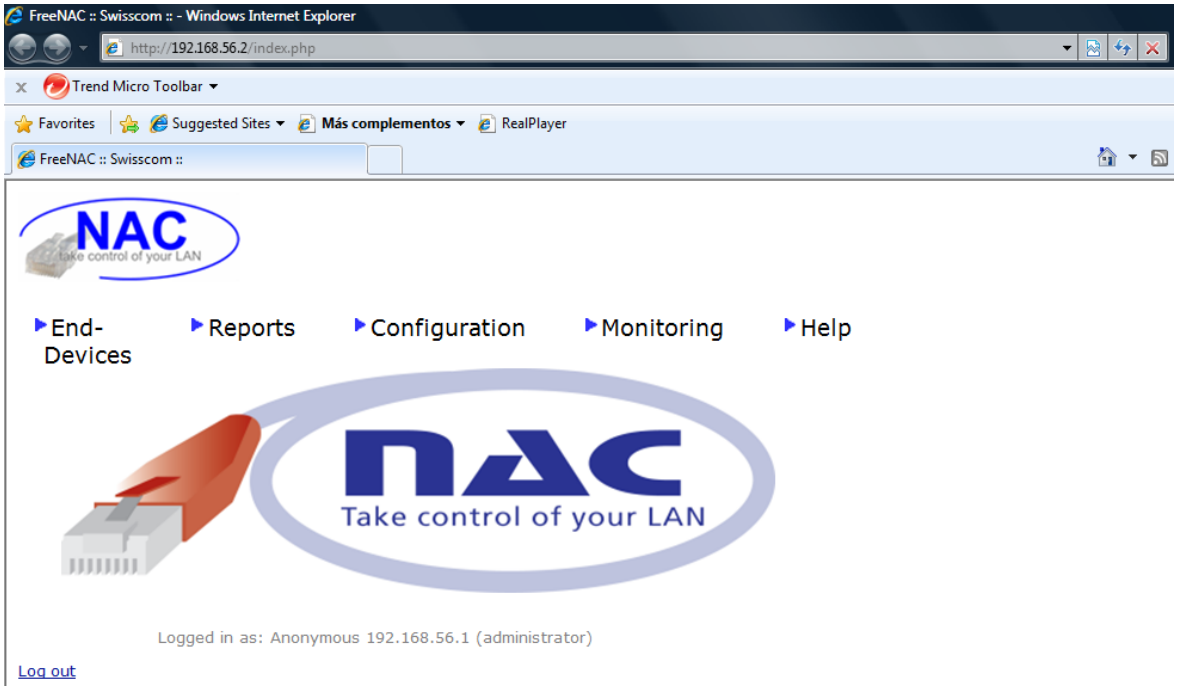
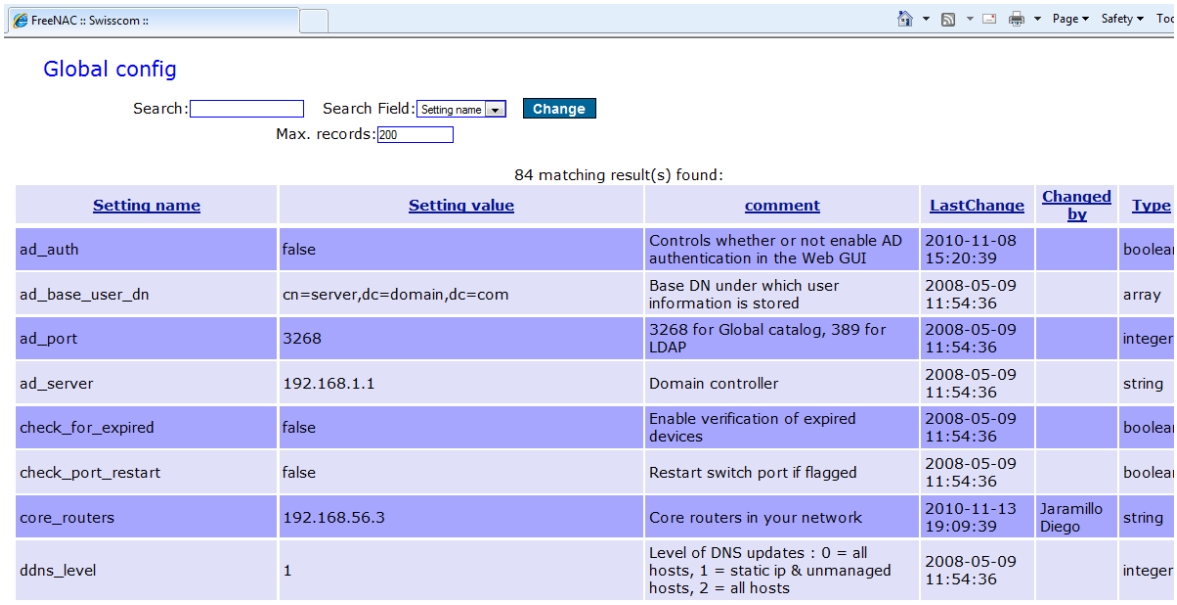


Figura 3.14. Página de inicio de la interfaz Web de FreeNAC

Aquí se podrá observar todos los parámetros con los cuales el servidor trabajará con la red, así como de varias opciones como dispositivos conectados, switches, routers, direcciones permitidas, rendimiento del sistema entre otros, lo primero será revisar la configuración global que abarca todos los parámetros principales.



Setting name	Setting value	comment	LastChange	Changed by	Type
ad_auth	false	Controls whether or not enable AD authentication in the Web GUI	2010-11-08 15:20:39		boolean
ad_base_user_dn	cn=server,dc=domain,dc=com	Base DN under which user information is stored	2008-05-09 11:54:36		array
ad_port	3268	3268 for Global catalog, 389 for LDAP	2008-05-09 11:54:36		integer
ad_server	192.168.1.1	Domain controller	2008-05-09 11:54:36		string
check_for_expired	false	Enable verification of expired devices	2008-05-09 11:54:36		boolean
check_port_restart	false	Restart switch port if flagged	2008-05-09 11:54:36		boolean
core_routers	192.168.56.3	Core routers in your network	2010-11-13 19:09:39	Jaramillo Diego	string
ddns_level	1	Level of DNS updates : 0 = all hosts, 1 = static ip & unmanaged hosts, 2 = all hosts	2008-05-09 11:54:36		integer

Figura 3.15. Parámetros de la configuración global de FreeNAC

Para poder modificar todos estos valores, se lo podrá hacer únicamente mediante la interfaz de Windows la cual se configurará más adelante.

3.6. Configuración de la base de datos (MySQL)

Inicialmente se deberá asegurar que mysql comience de forma automática cada vez que se inicia el servidor, en el sistema operativo con el que se está trabajando se lo hace mediante:

update-rc.d mysql defaults

Para acceder con mayor brevedad hacia el directorio de la base de datos mysql se establece un enlace simbólico que apunte hacia esta dirección, por ejemplo /var/lib/mysql, esto con el fin de agilitar el acceso hacia este directorio.

3.6.1. Archivo de configuración (my.cnf)

Este es el archivo encargado de iniciar la base de datos y contiene los datos de quienes pueden acceder a la base de datos, el nombre de la base de datos que va a ejecutar, el puerto por el cual va a escuchar entre otras.

En la máquina virtual existen dos archivos que se encuentran en dos rutas diferentes y que deben contener los mismos datos, ya que podrían existir conflictos el momento de la conexión y el servidor no trabajará.

Las direcciones donde se encuentra este archivo son:

- /etc/mysql/**my.cnf**
- /opt/nac/contrib/etc/**my.cnf**

Dentro de este archivo se deben revisar los siguientes parámetros:

```
log-bin = vmps1-bin
log-warnings
report-host = vmps1
server-id       = 10                    [10 for master, 20 for slave1, 20 for slave 2 etc..]
relay-log=vmps1-relay-bin
replicate-do-db= opennac
replicate-wild-ignore-table= opennac.vmpsauth%
```

Figura 3.16. Parámetros de configuración de archivo my.cnf

El parámetro server-id se indica a través de un número indicando cual es el servidor maestro y cuáles son los secundarios, en este caso 10 es para el servidor maestro y tiene el nombre de vmps1.

Además se debe tener en cuenta el incremento de los tiempos de espera para evitar una desconexión en redes de tráfico bajo, se agrega lo siguiente:

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

Figura 3.17. Incremento de tiempo de espera

MySQL tiene que escuchar a la red a través del puerto 3306 (por defecto de MySQL), pero podría estar vinculado únicamente para localhost (parámetro por defecto de Ubuntu) por lo que dentro del archivo se deberá comentar este comando:

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

Figura 3.18. Parámetros de enlace de dirección

Cada servidor puede insertar datos a nivel local, los cambios se replican en otros servidores y estos no entran en conflicto. Los conjuntos de datos deben ser configurados mediante las teclas de autoincremento y este valor deberá ser diferente en cada uno de los servidores, esto con el fin de evitar conflictos de replicación.

Si el valor fuera de 5 significa que permite un máximo de 5 servidores, cada servidor deberá tener un valor de auto incremento de desplazamiento diferente (1 para el principal, 2 para el segundo, etc).

```
auto_increment_increment= 5
auto_increment_offset   = 1    [1 for vmps1, 2 for vmps2, 3 for vmps3 ...]
```

Figura 3.19. Valores de auto incremento para los servidores

3.6.2. Permisos

Hay que asegurarse que el usuario de MySQL pueda escribir en la base de datos, por lo que se le deberán dar los permisos pertinentes:

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

Figura 3.20. Permisos para escribir en la base de datos MySQL

3.6.3. Reinicio MySQL

Primero se deberá verificar que el archivo ubicado en /etc/init.d/mysql existe y el inicio automático se encuentra habilitado. Finalmente debemos reiniciar mysql en orden para que se puedan ejecutar los cambios que se realizaron en el archivo **my.cnf**.

```
/etc/init.d/mysql restart
```

Figura 3.21. Reinicio del servicio mysql

Para verificar que mysql está corriendo correctamente a través de netstat, se podrá observar que mysql está obligado a escuchar cualquier dirección 0.0.0.0 y no 127.0.0.1 de localhost.

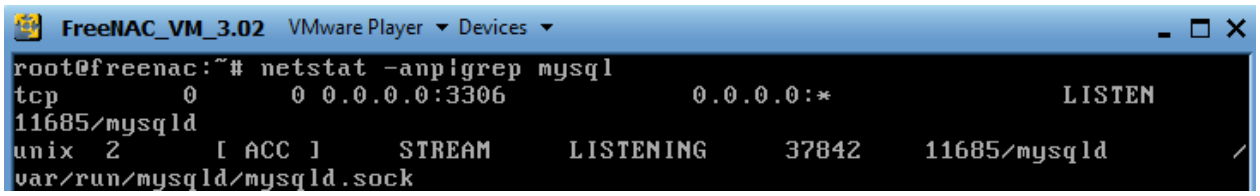


Figura 3.22. Verificación de reinicio de mysql

3.6.4. Conjunto de datos inicial de FreeNAC

La máquina virtual FreeNAC viene incluida con los scripts necesarios así como de dos bases de datos, una con el nombre "opennac" la cual se encuentra vacía y será modificada por medio del administrador y la otra con el nombre de "nacdemo" que viene con un ejemplo de cómo trabaja el sistema de FreeNAC.

Para el objetivo de estudio y de pruebas, se utilizará la base ya creada que viene con el software FreeNAC, en este caso **opennac,** ya que a continuación se podrecerá a descomprimir los archivos necesarios correspondientes a la base de datos en el directorio de mysql:

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

Figura 3.23. Archivos de la base de datos opennac

3.6.5. Creación de nueva base de datos vacía (solo servidores principales)

Para un nuevo servidor principal, se debería instalar un nuevo conjunto de tablas vacías FreeNAC en la base de datos **opennac**, por lo que primero se deberán respaldar las tablas anteriores:

```
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
```

Figura 3.24. Creación de nueva base de datos

3.6.6. Configuración de permisos de la base de datos

A partir de la versión 2.2 se ha proporcionado el archivo **permission.sql**, por lo que no hay que preocuparse sobre la configuración de los permisos.

```
cd /mysqldata
mysql -u root opennac < permissions.sql
```

Figura 3.25. Permisos de acceso para la base de datos opennac

Para determinar que existe conectividad con la base de datos **opennac** se ingresa como se muestra a continuación:

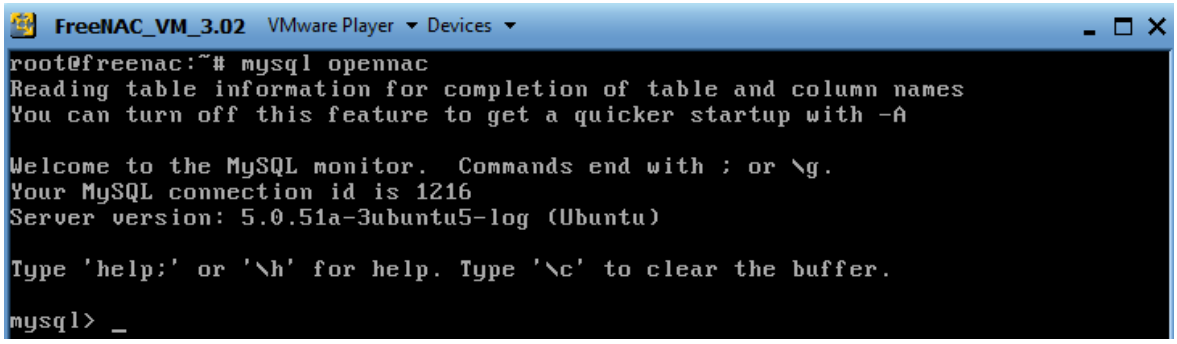


Figura 3.26. Conectividad con la base de datos opennac

Para verificar las tablas que posee esa base de datos o seleccionar algo en específico se pueden utilizar los siguientes comandos:

```
show tables;
select * from port;
```

Figura 3.27. Comando SQL

3.6.7. Configuración de usuarios mysql para scripts PHP

Por defecto para los permisos de scripts y la configuración del archivo **config.inc**, está determinada la clave "PASSWORD2" para acceder a la base de datos y habilitar la ejecución de los demonios.

Por seguridad se debe cambiar de contraseña de los valores preestablecidos del programa.

En primer lugar se deberá ingresar a la base de datos mysql en modo privilegiado (root):

```
mysql -u root -p mysql
```

Figura 3.28. Acceso a la base de datos como root

Para cambiar las contraseñas de acceso dentro de la base de datos se ejecutarán las siguientes líneas de comando:

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

Figura 3.29. Cambio de contraseñas de acceso

NEW_PASSWORD2 es la clave que se usará en el archivo **config.inc** y NEW_PASSWORD1 es el que se usará para acceder desde la interfaz gráfica de usuario.

3.7. Archivo de configuración (config.inc)

El archivo de configuración inicial es el que permitirá el arranque de los demonios del servidor para el usuario y contraseña que se hayan especificado en todos los archivos como la interfaz Web, para la base de datos SQL y el archivo de configuración **config.inc.**

3.7.1. Creación de grupo y usuario

Se necesita crear un grupo y un usuario freenac, esto es útil si se desea que el archivo de configuración sea accesible para otros demonios tales como Apache o Radius.

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

Figura 3.30. Creación de grupo y usuario freenac

3.7.2. Configuración FreeNAC

Para el servidor maestro se deberá crear un nuevo archivo de configuración a partir de la plantilla que se tiene de este archivo **config.inc** y establecer los parámetros de conexión hacia la base de datos, este debe contener a la misma contraseña que se estableció en la configuración de la base de datos:

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

Figura 3.31. Configuración de parámetros de conexión y contraseña

Luego de ejecutar estos comandos, se abrirá el archivo de configuración en el cual se deberán modificar los siguientes parámetros:

```
## MySQnL DB settings for all scripts
  $dbhost="localhost";
  $dbname="opennac";
  $dbuser="inventwrite";
  $dbpass="xxxxxxx";
```

Figura 3.32. Parámetros del archivo config.inc para la base de datos

3.7.3. Políticas de uso

Un cambio sustancial en la versión 3.0 de FreeNAC es la introducción a una política de interfaz orientada a objetos (OO), la cual proporciona una mayor flexibilidad y encapsulación de decisiones individuales sobre el acceso a la red.

Se debe especificar un archivo de política sobre el cual se va a trabajar. Existen varios tipos de políticas y de acuerdo a lo requerido por el administrador se determinara la más óptima.

Para este estudio se utilizará la política **policy5.php** la cual es muy útil en varios sitios, por lo que se establecerá un enlace entre el archivo de política y el archivo que se desea utilizar:

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

Figura 3.33. Políticas de uso

3.7.4. Inicio del demonio VMPS

En primera instancia se debe crear un archivo de arranque y después iniciar el servicio:

```
cp /opt/nac/contrib/startup_init.d/vmps /etc/init.d/vmps
chmod 750 /etc/init.d/vmps
```

Figura 3.34. Creación y ejecución del archivo startup

Y activarlo para que inicie automáticamente en función de su distribución:

```
update-rc.d vmps defaults
```

Para observar los eventos se inicia el syslog:

```
/etc/init.d/vmps start
ps -ef | grep vmps
tail -f /var/log/messages
```

Figura 3.35. Comandos para observar los eventos realizados del demonio VMPS

3.7.5. Inicio del demonio postconnect

El procedimiento de inicio y ejecución de este demonio es similar al que se realizó con el demonio VMPS.

```
cp /opt/nac/contrib/startup_init.d/postconnect /etc/init.d/postconnect
chmod 750 /etc/init.d/postconnect
```

Figura 3.36. Creación y ejecución del archivo startup

Inicio automático en función de su distribución:

```
update-rc.d postconnect defaults
```

Observar los eventos mediante syslog:

```
/etc/init.d/postconnect start
tail -f /var/log/messages
```

Figura 3.37. Comandos para observar los eventos realizados del demonio postconnect

3.8. Configuración de derechos de usuarios GUI

En la parte de configuración, existen dos niveles de autorización y de autentificación:

3.8.1. Usuario mysql

La interfaz gráfica de usuario de Windows utiliza un usuario específico y una contraseña para acceder a la base de datos.

El usuario mysql es creado como parte de la configuración de la base de datos mysql y otorgado derechos de acceso a determinadas tablas de forma remota. Este usuario es usualmente llamado **"inventwrite"** por razones históricas. La contraseña designada para este usuario tiene que ser codificada y almacenada en el archivo de configuración de Windows.

Para determinar que este usuario existe, se ingresa el siguiente comando dentro de la base de datos "mysql":

```
select * from user where user='inventwrite';
```

Figura 3.38. Comprobación de existencia de usuario inventwrite en la tabla user

A continuación se nos desplegará en la pantalla el nombre del usuario especificado:

```
            0 |                       0 |
inventwrite | *D6FE9112648082EB3EA19FCEA45F4A1F9C4BE801
    | N            | N              | N              | N
```

Figura 3.39. Visualización del usuario en la base de datos mysql

Finalmente se debe informar a la interfaz gráfica de Windows cual es el usuario y la contraseña que va a utilizar. El nombre de usuario y contraseña se almacenaran en una cadena cifrada llamada 'auth' en el archivo de configuración **vmps.xml.**

- Iniciar la aplicación **vmps.exe**

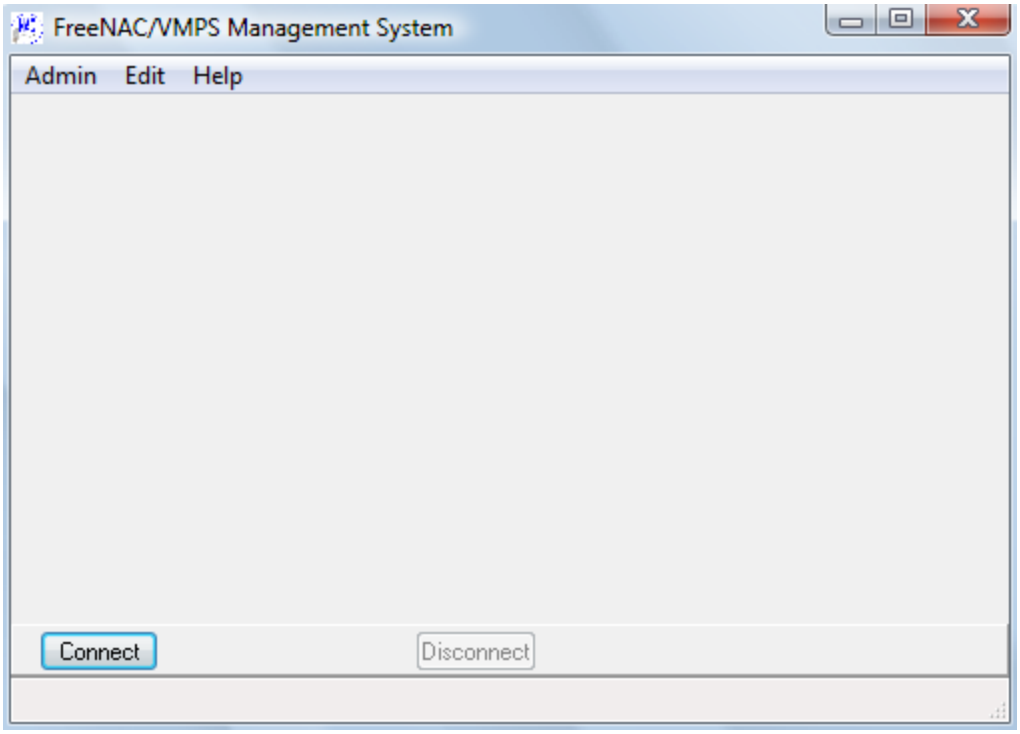


Figura 3.40. Inicio de la interfaz Gráfica de Usuario

- Seleccionar Admin -> Encrypt User

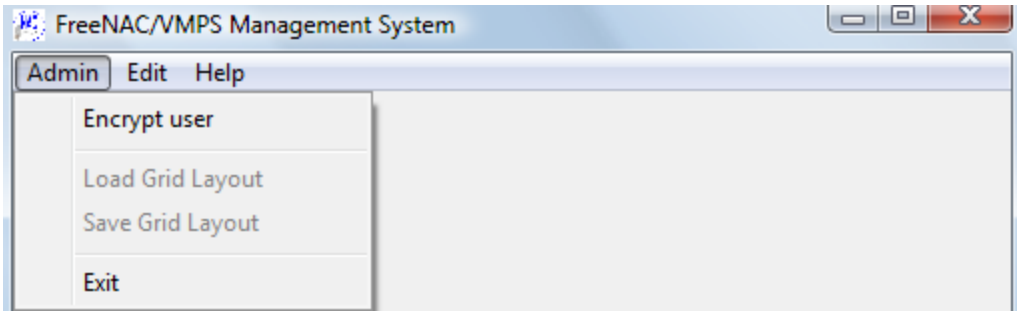


Figura 3.41. Encriptación de usuario

- Ingresar el usuario y la contraseña, luego presionar el botón "generate"

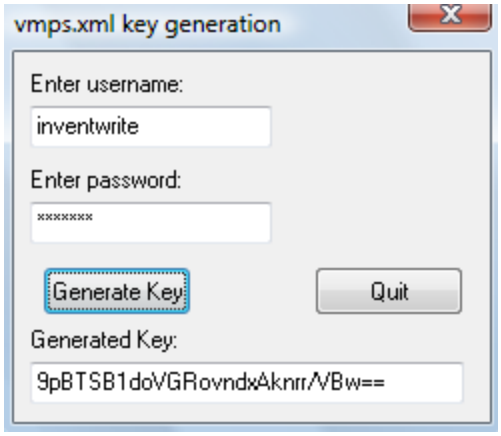


Figura 3.42. Generación de clave para usuario inventwrite

- Copiar el valor generado en el campo Generated key en el campo "auth" del archivo **vmps.xml**

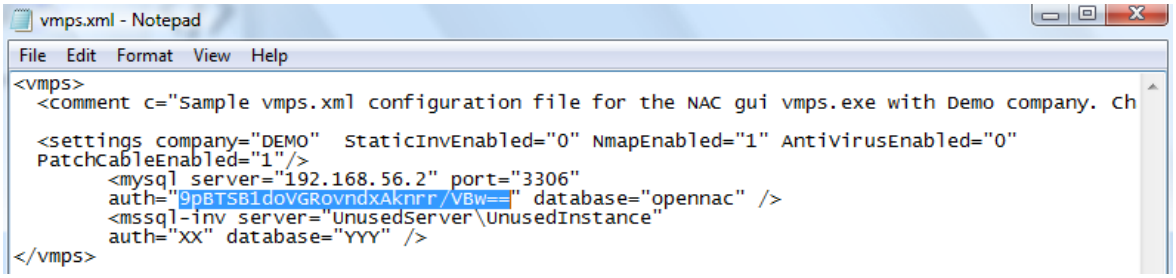


Figura 3.43. Almacenamiento de clave en el archivo vmps.xml

3.8.2. Usuario NAC

La interfaz gráfica de usuario utiliza el nombre registrado de Windows para identificar dicho usuario, y coloca este valor en el campo **nac_rights** para este usuario y controlar lo que puede hacer (ejecución del lado del cliente), la interfaz a la vez envía al servidor el dominio de Windows.

Dependiendo de los derechos de usuario de este nombre de usuario en la tabla 'usuarios', la interfaz gráfica le permitirá el acceso o se negara a trabajar.

Existen tres tipos de permisos que pueden tomar los usuarios para acceder a la base de datos:

- **Solo Lectura:** los usuarios pueden observar la información, pero no realizar ningún cambio desde la interfaz gráfica de usuario.

- **Escritura:** Se pueden realizar cambios en la información general así como editar las etiquetas, pero no con los switches, puertos, registros o las etiquetas de administración.

- **Administrador:** En modo de administrador se pueden realizar cambios en todas las configuraciones tanto general, como para los switches y puertos que se encuentren conectados al servidor.

Cada uno de estos permisos debe tener un valor en el campo de **nac_rights** de la tabla los cuales se indican en la siguiente tabla:

Tabla 3.2. Tabla de permisos de usuarios NAC

Tipo de permiso	Valor nac_rights
Read-only	1
Write	2
Administrator	99

Para insertar un nuevo usuario en la tabla de la base de datos, el siguiente comando SQL dentro de la base de datos deberá ser ejecutado:

```
mysql> insert into opennac.users (username, Surname, GivenName, nac_rights) valu
es ('djaramillo', 'Diego', 'Jaramillo', 99);_
```

Figura 3.44. Comando para agregar un nuevo usuario con permisos de escritura

Una vez que fueron insertados, los permisos y otros detalles, estos pueden ser modificados a través de la interfaz gráfica de usuario.

3.9. Verificación del domino de Windows

La interfaz gráfica de usuario (GUI) también se puede restringir al dominio en el cual está trabajando Windows, si el campo "guidomain" en la tabla de configuración en el servidor está configurado.

Por ejemplo si se establece a "DOMINIO", la interfaz gráfica de usuario solo podrá permitir conectarse a los usuarios que se encuentren registrados bajo dicho dominio.

La variable **$dbhost** del archivo "config.inc" debe tener el mismo nombre que el domino del sistema operativo Windows para evitar conflictos el momento de conectar la interfaz gráfica de usuario.

3.10. Conectar a la interfaz gráfica de usuario (GUI)

Ya que todos los parámetros del servidor se encuentran configurados, se procede a conectar a través de la interfaz gráfica de Windows.

Si todo se encuentra correctamente establecido al momento de presionar el botón "connect" deberá aparecer la siguiente ventana:

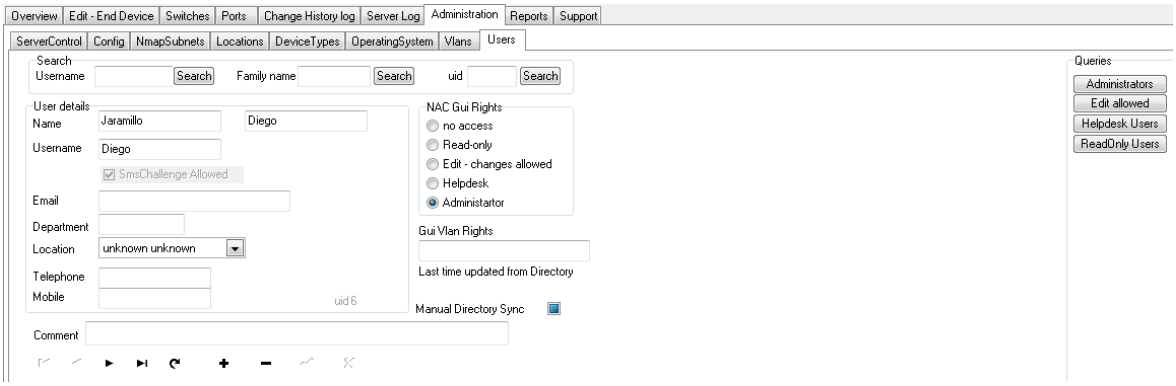


Figura 3.45. Ventana de la interfaz gráfica de usuario (GUI)

Por medio de esta interfaz se configurará la base de datos de las VLAN's así como de los usuarios a través de las direcciones físicas (MAC's) y en la cual se observará el direccionamiento dinámico que ejecutará el servidor.

Esta es la única manera de modificar todos los parámetros con los cuales trabajará el servidor FreeNAC y en donde se establecerán las direcciones IP de los equipos de red como switches y routers así como de los nombres de los mismos.

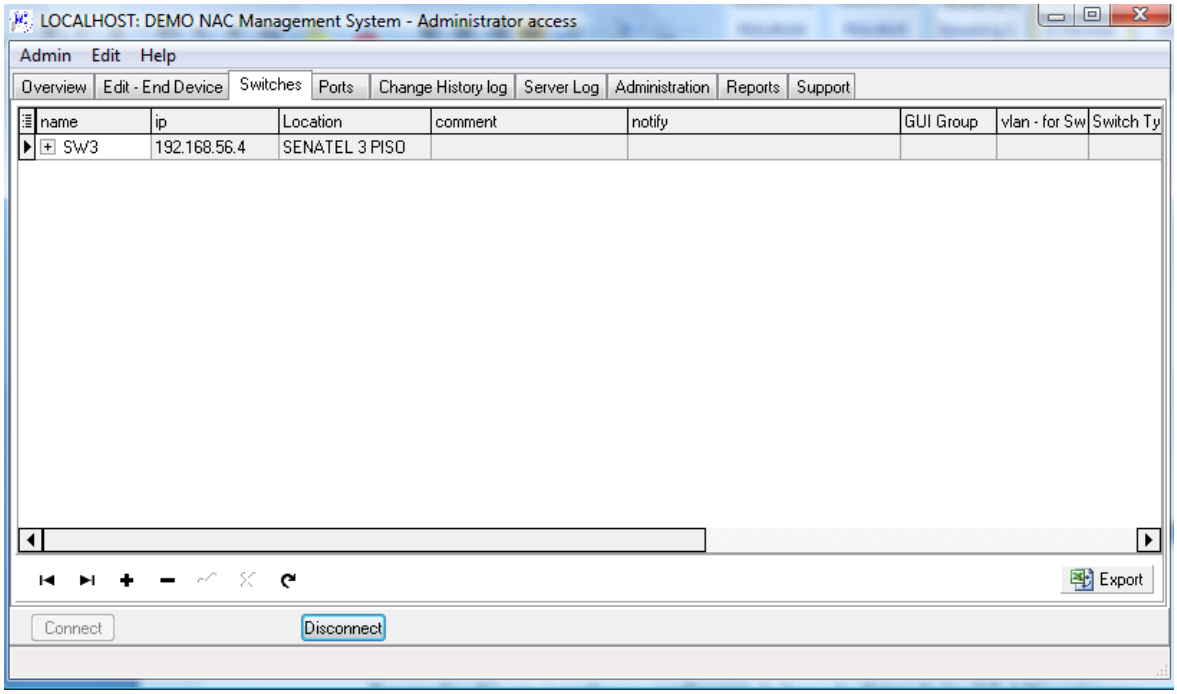


Figura 3.46. Registro de un switch en el servidor

La ventaja que presenta el software FreeNAC es la de ofrecer un menú de fácil uso para la administración de la red, en esta gráfica se muestra como se ingresa un switch así como de su dirección IP y su nombre.

3.11. Registro de equipos y usuarios en el servidor FreeNAC

Si se ingresó como usuario **Administrador** en la parte superior aparecerá una pestaña con este nombre y donde se crearán las VLAN's correspondientes.

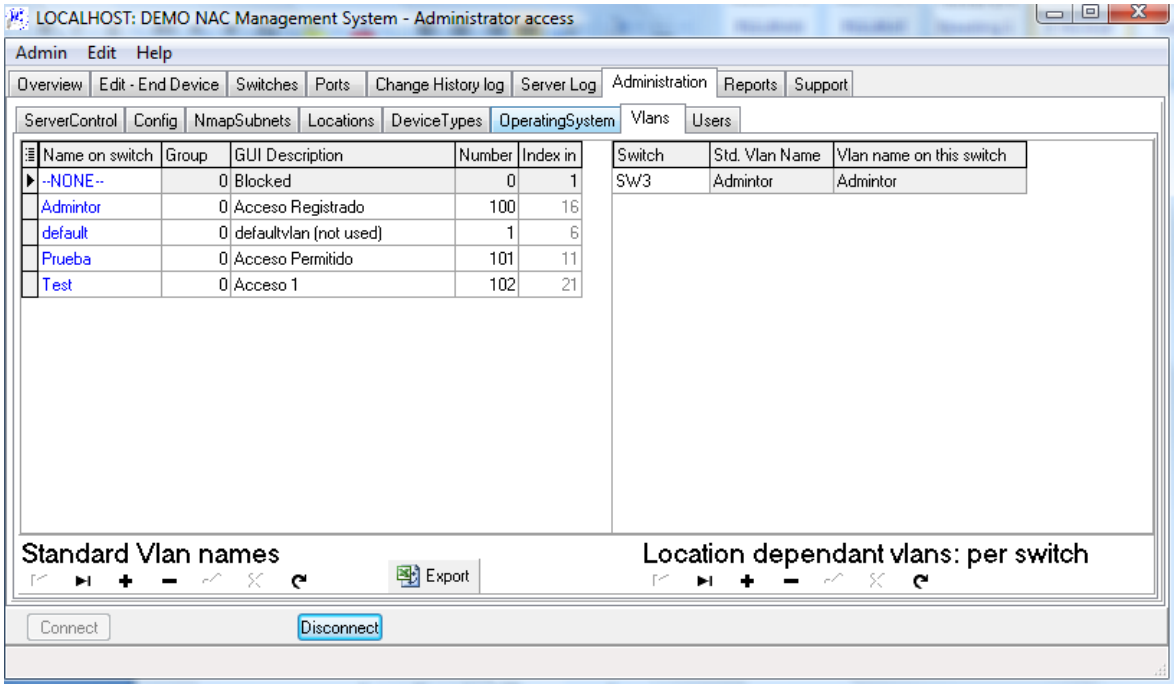


Figura 3.47. Pestana de creación de VLAN's

Aquí se registrarán las VLAN's para los usuarios como para los equipos, ya creadas estas se procederá a ingresar a los usuarios que pertenecen a la Institución clasificándolos de acuerdo a su área de trabajo y a la VLAN que pertenece.

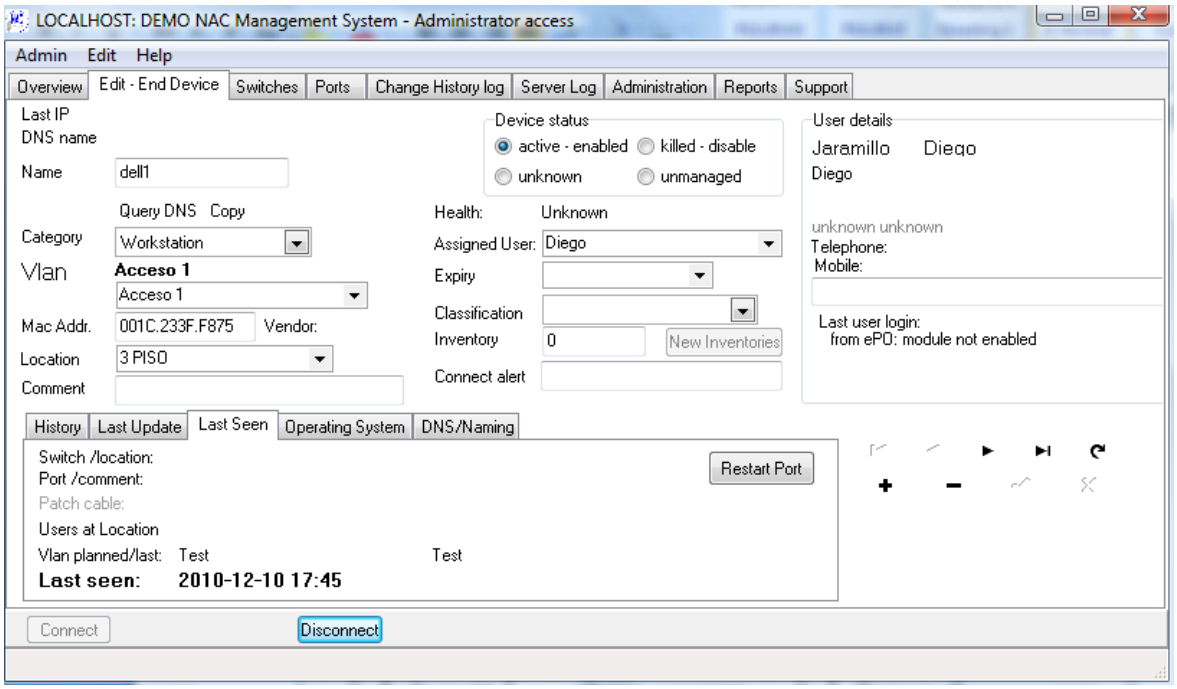


Figura 3.48. Registro de usuario a la Base de Datos

Todos los usuarios que hayan sido ingresados se presentarán en una sola tabla en la pestaña **Overview** como se muestra a continuación.

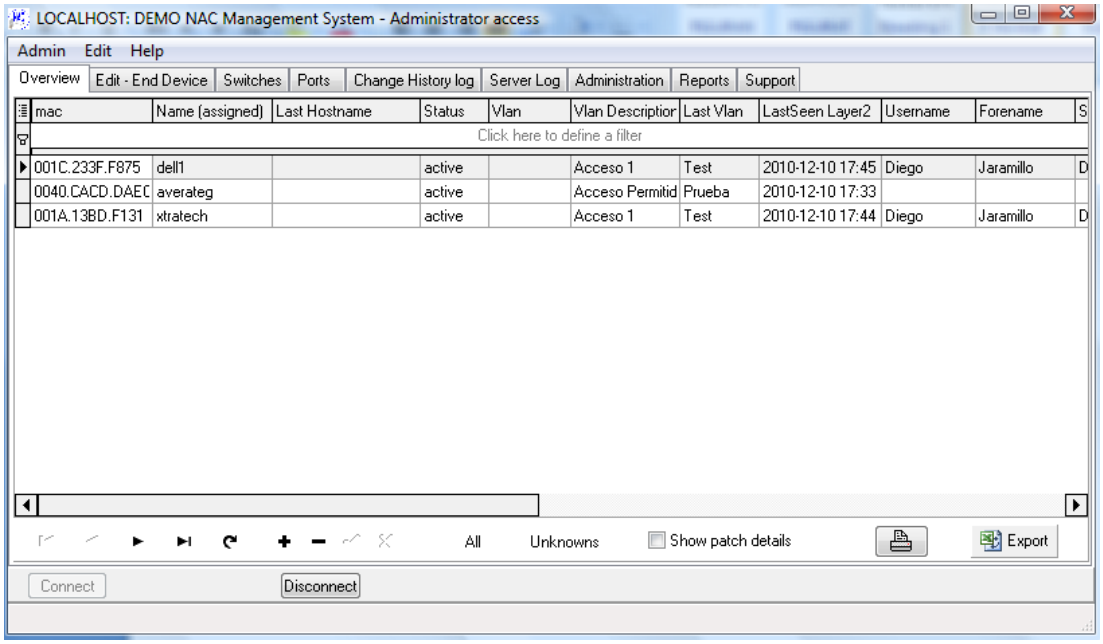


Figura 3.49. Tabla de usuarios registrados en el servidor

Ahora que estos parámetros han sido ingresados en el servidor, se debe configurar el switch para que trabaje como cliente VMPS con los datos que han sido ingresados en las tablas del servidor.

3.12. Integración Switch CISCO

Los switches de CISCO para que puedan trabajar con el programa FreeNAC se los puede configurar mediante cinco formas:

1. "Pasiva" la exploración de direcciones MAC visible en todos los puertos.
2. Consulta de estado de puerto
3. Puerto de control (arranque/parada/reinicio/establecer VLAN estática/establecer el modo de VMPS)
4. Atención de consultas VMPS
5. Atención de consultas 802.1x/Radius

3.12.1. Exploración Pasiva de las tablas MAC a través de SNMP

FreeNAC incluye la herramienta snmp_scan.php que consulta la información de los switches:

- Hardware del switch y la versión del software
- Descubrimiento de nuevos puertos
- Actualización de nombres de puertos, estado (up, down), perfil de autentificación (VLAN estática, dinámica / VMPS o troncal)
- Actualización de la última VLAN en un puerto, para los puertos estáticos
- Para cada dirección MAC encontrada en los campos "Última Vez", "Última VLAN", "Ultimo Puerto" estos se actualizan, o para los nuevas MAC's una nueva entrada es agregada con el nombre "unknown"

La secuencia de comandos solo analiza los switches que tengan la bandera de exploración activada (1) en la tabla del switch.

Los ajustes se configuran en dos lugares, en el archivo de configuración **config.inc** y en la tabla de configuración.

3.12.1.1. Configuración: Switch

SNMP debe estar habilitado y establecer ACL (Listas de control de acceso) para que las consultas sean posibles a partir de la dirección del servidor FreeNAC. Si existe un firewall entre FreeNAC y los switches, el puerto SNMP (udp/161) tiene que estar abierto.

3.12.1.2. Configuración: Config.inc

Este archivo que se encuentra en la dirección /opt/nac, contiene datos confidenciales así como las contraseñas de acceso, aquí se debe establecer una cadena de comunidad SNMP para leer la configuración del switch:

$snmp_ro

3.12.1.3. Configuración: Tabla de configuración

Los parámetros de la tabla de configuración pueden ser modificados desde la línea de comandos mysql (usar 'describe switch' y 'select * from config' si está a gusto con SQL) o mediante la interfaz gráfica de usuario de Windows (Pestaña de Administración en la pestaña 'Config').

La opción snmp_dryrun debe ser falso (0)

3.12.1.4. Configuración: Tabla del switch

En primer lugar se tiene que declarar los switches que van a ser escaneados, ya sea a través de la interfaz gráfica de usuario o por línea de comandos:

```
insert into switch set ip='1.2.3.4', name='swXX', location='1';
```

Figura 3.50. Declaración de un switch para ser analizado por el servidor

Para que un switch se analice automáticamente, establecer la bandera de 'exploración' en 1:

update switch set scan='1' where ip='1.2.3.4';

Se deben cambiar los valores de acuerdo a su sistema y activar **snmp_scan**.

Una vez configurado ejecutarlo desde la línea de comandos para probar que está funcionando correctamente:

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

Figura 3.51. Activación del escaneo SNMP de los switches

A través del syslog se podrá observar cómo está funcionando esta herramienta, puede tardar algún tiempo, dependiendo del número de switches de la red. Si los tiempos de espera o demora demasiado significa que SNMP no está correctamente configurado en el switch, o la comunidad no está correcta dentro del archivo **config.inc**.

Para ejecutar con regularidad, por ejemplo a las 11:05 todos los días, se debe añadir una entrada en el **cron** como root:

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

Figura 3.52. Habilitación diaria mediante cron del root

3.12.2. Consulta de estado de conmutación de puerto

A partir de la versión 3.0 de FreeNAC, se ha introducido la herramienta **ping_switch.php** la cual consulta el estado del puerto del switch (up/down), que puede ser vista en la interfaz gráfica de usuario.

Para activarla, agregar el switch al FreeNAC, establecer la exploración automática en 1, y añadir una entrada dentro del cron como root, si se desea hacerlo cada hora se hará lo siguiente:

```
10   8-17   * * 1-5 /opt/nac/bin/ping_switch.php 2>&1   | logger -t ping_switch.php
```

Figura 3.53. Activación de la herramienta ping_switch para cada hora

3.12.3. Puerto de Control

La programación activa de ciertos parámetros es posible desde la interfaz gráfica de Windows. Estos parámetros se almacenan en la base de datos, y luego escritos en los switches a través de la herramienta **cron_restart_port.php** en el servidor.

Para cada puerto los parámetros que pueden ser establecidos son los siguientes:

- Restart
- Clear_mac
- Shutdown
- Atribución VLAN estática o dinámica
- Si es estática, la vlan puede ser definida

3.12.3.1. Configuración

Ajustar la comunidad snmp ($snmp_rw) en el archivo config.inc. Probar la herramienta cron_restart_port.php en la línea de comandos y verificar los resultados mediante la revisión del syslog y el registro del servidor 'server log' en la interfaz gráfica de usuario. A continuación activar en el cron para cada minuto:

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

3.12.3.2. Configuración clear_mac

Es necesario como complemento de port_restart para los switches con las versiones más recientes del IOS. Para activarlo se realizará lo siguiente:

1. Configurar los valores de $sw_user, $sw_pass y $sw_en_pass en el archivo **config.inc.**

   Estas variables son necesarias para acceder al switch a través de telnet y llamar al comando IOS para limpiar la dirección MAC del switch.

   Los comandos para el switch son enviados en texto claro (vía telnet). Si un switch de administración dedicado de red no está disponible, esto puede aumentar los riesgos de seguridad.

2. Activar esta función: establecer el valor de la variable de configuración **check_clear_mac** de falso a verdadero.

3. Seleccionar el IOS de los switches donde clear_mac será utilizado.

   Esto puede hacerse desde la interfaz gráfica de usuario en la pestaña de configuración, estableciendo la variable **switch_type** en 1 o mediante MySQL a través del siguiente comando:

```
mysql> UPDATE switch SET switch_type='1' WHERE name='mysuperswitch';
```

Figura 3.54. Configuración de la variable switch_type desde MySQL

3.12.4. Atención de consultas VMPS

La característica principal de FreeNAC fue originalmente para responder a las solicitudes VMPS, y responder con un PERMITIR o DENEGAR. La respuesta es hecha por el demonio **vmpsd_external** en acuerdo con la política de uso configurada.

Aunque los puertos individuales pueden ser establecidos en modo estático o dinámico, desde la interfaz gráfica de usuario, los principales parámetros VMPS deben ser programados directamente en cada switch (mediante telnet o SSH).

- Dirección IP del servidor VMPS

- Tiempos de espera
- Intervalos de confirmación

3.12.5. Atención de consultas 802.1x/Radius

Las solicitudes 802.1x para autentificar dispositivos finales basados en el protocolo 802.1x, por lo general ya sea un Dominio de Usuario de Windows, o un certificado.

Esto involucraba los módulos FreeRadius y Samba, y también se requiere de la programación manual de puerto en los switches (vía telnet o SSH).

3.13. Configuración Switch CISCO

Para este estudio y de acuerdo a las necesidades de la Institución para la cual se elabora el presente proyecto se ha decidido trabajar con las solicitudes VMPS, de manera general que un switch detecte en uno de sus puertos que un equipo desea conectarse a la red y entregar su dirección MAC para que el servidor sea el encargado de direccionarlo hacia su VLAN respectiva.

3.13.1. Parámetros VMPS

Los nombres y números de VLAN's deben ser configurados en los switches exactamente igual que los que se han creado en la tabla VLAN dentro del servidor FreeNAC.

Este proceso deberá ser llevado a cabo manualmente por el administrador en cada uno de los equipos ya que FreeNAC únicamente trabaja con los parámetros ingresados.

A continuación se indica cómo se establece la comunicación desde el switch hacia el servidor FreeNAC como cliente VMPS y la configuración de los puertos dinámicos que trabajarán con las VLAN que hayan sido registradas en la tabla del servidor:

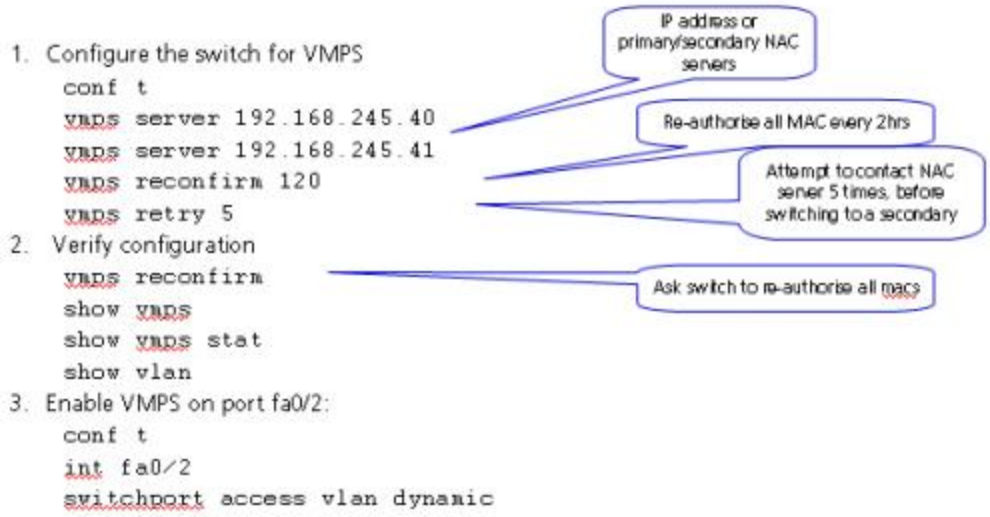


Figura 3.55. Configuración del switch para VMPS

El punto 1 establece la configuración IP del servidor VMPS donde se realizarán todas las consultas, así como del tiempo en el que volverá a reconfirmar todas las conexiones actuales (vmps reconfirm) y el número de veces que intentara en contactar al servidor antes de pasar al servidor secundario o indica la conexión como no valida.

El punto 2 verifica el estado actual y muestra el estado de las vlan así como de la conexión con el servidor vmps.

El punto 3 es un ejemplo de cómo habilitar un puerto como dinámico en la cual luego de verificar la dirección MAC del servidor establecerá la VLAN correspondiente en el puerto.

3.13.2. Función clear_mac

Cuando un equipo no registrado se conecta, un NEGAR de parte de FreeNAC es recibido y el puerto del switch bloquea el acceso. Si más adelante las propiedades del dispositivo de conexión son modificadas con el fin de permitir el acceso a una VLAN, el

puerto permanecerá bloqueado para ese dispositivo evitando que más peticiones VMPS lleguen al servidor FreeNAC. La cantidad de tiempo que el puerto permanece bloqueado es variable. Un reinicio del puerto no cambia el estado del puerto, ni tampoco la desconexión del cable de red del puerto del switch.

Se ha descubierto que la eliminación de la dirección MAC del switch remueve el estado de bloqueo y el puerto funcionara como se espera. Por lo tanto una función 'clear_mac' debe ser agregada en el servidor FreeNAC como complemento de 'port_restart'.

3.14. Integración Router CISCO

Los routers pueden ser consultados regularmente para descubrir las direcciones IP, así como los nombres DNS atribuidos a las direcciones MAC. Esta es una parte importante del "descubrimiento automático" de los equipos finales.

Si la variable **router_mac_ip_discoverall = true** en la tabla de configuración, el módulo **router_mac_ip** documentara todos los pares MAC/IP que encuentre en la red, no solo los que se encuentren como activos con el protocolo VMPS.

De esta manera los dispositivos finales son marcados con el estado "unmanaged" (no administrado).

3.14.1. Configuración

Los ajustes son configurados en dos lugares, en el archivo **etc/config.inc** y en la tabla mysql **config.**

3.14.1.1. Configuración config.inc

Este archivo contiene datos confidenciales como contraseñas, además para este módulo se debe establecer una cadena SNMP para realizar consultas de los ajustes del router:

$snmp_ro

3.14.1.2. Configuración tabla 'config'

La tabla 'config' puede ser configurada desde la línea de comandos mysql (a través de 'describe config' y 'select * from config'), o a través de la interfaz gráfica de usuario de Windows GUI.

Existen algunas variables de configuración que deben ser establecidas.

Cuáles son las direcciones IP de los routers que contienen las tablas ARP que van a ser consultadas:

```
core_routers=192.168.245.3 192.168.245.6 192.168.245.30
```

Figura 3.56. Dirección IP routers en la tabla config

Se deben documentar todas las nuevas direcciones IP o únicamente las que se encuentren en la tabla **sistemas**:

```
router_mac_ip_discoverall=true
```

Figura 3.57. Registro de todas las direcciones IP

La dirección IP y dirección MAC que van a ser ignoradas durante el proceso de consulta:

```
router_mac_ip_ignore_ip= /^(127.0.0|192.168.|193.5.238)/
```

```
router_mac_ip_ignore_mac= /^(00d0.0064.d000|0008.02a1.a3b3)/
```

Figura 3.58. Dirección IP y MAC que no van a ser consultadas

Deben las direcciones IP ser trasladadas en nombres de DNS y actualizadas:

```
router_mac_ip_update_from_dns=true
```

Figura 3.59. Traslado de dirección IP a nombre de DNS

Los nombres también pueden ser actualizados desde NMB (Windows Naming), en lugar de nombres de dominio DNS. La mayoría de sitios deben seguir con DNS:

```
router_mac_ip_update_from_nmb=false
```

Figura 3.60. Traslado de dirección IP a nombre NMB

3.14.2. Instalación

Luego de haber realizado la configuración anterior a través de la interfaz gráfica de usuario GUI, ejecutar el archivo /opt/nac/bin/**router_mac_ip.php** desde la línea de comandos, previo a esto se debe aumentar el nivel de depuración de 0 a 3.

```
$logger->setDebugLevel(3);
```

Figura 3.61. Nivel de depuración

Para entender mejor el comportamiento de lo que hace este archivo, se puede revisar los mensajes a través del syslog. Asegurarse de que las consultas del router están trabajando y que sean rápidas (ej. 20 seg.), todos los equipos finales tienen que ser visualizados en la interfaz gráfica de usuario.

Cuando esté trabajando como se lo espera, a continuación se debe agregar una entrada en el cron del root, por ejemplo, las consultas del router cada 6 minutos:

```
*/6 *    * * *   /opt/nac/bin/router_mac_ip
```

Figura 3.62. Tiempo de verificación de las consultas del router

La configuración que se implementó en los equipos para este estudio se encuentra en la sección **Anexos**.

CAPITULO IV

PRUEBAS Y ANALISIS DE DESEMPEÑO DEL DISEÑO

4.1. Resultados obtenidos mediante FreeNAC

De acuerdo a todo lo que se realizó en el capítulo anterior, FreeNAC ha presentado los resultados esperados que se plantearon para ser implementado en la Institución.

Para demostrar que esto se llevó a cabalidad se creó dentro de la Secretaría Nacional de Telecomunicaciones un ambiente de pruebas con los equipos que son utilizados y haciendo las pruebas correspondientes en los múltiples casos que se pueden presentar.

Estos resultados se ven directamente a través de la interfaz gráfica de usuario, registrando todas las actividades de conexión ya sea en hora, fecha, switch, el puerto del switch donde se ha conectado un equipo y si este se encuentra o no registrado dentro de la base de datos creada.

Si se desea observar lo que está sucediendo dentro de la red, se lo puede verificar a través de las interfaces que ofrece FreeNAC, tanto por la interfaz gráfica de usuario de Windows, como de la interfaz Web.

En la interfaz gráfica de usuario podremos observar de manera más detallada el número de puerto y de que switch ha sido conectado con la fecha de ejecución mientras tanto que en la interfaz Web nos muestra de forma general el número de equipos que se ha conectado a dicho dispositivo de red en los últimos 30 días y de igual manera por usuario en el caso de que se encuentre registrado.

A continuación se mostrarán todos los casos con los cuales se trabajó y como funciona en cada uno de ellos el servidor FreeNAC, los casos con los que se trabajó son los siguientes:

Tabla 4.1. Cuadro de posibles casos para la detección de equipos

Servidor	***Equipo de red***	***Equipo final***		
		VLAN 1	***VLAN 2***	***Visitante***
FreeNAC	*Switch*	*X*	*X*	
		X X		
			X	*X*
	Switch – Core	*X*	*X*	
		X X		
			X	*X*
	Switch – Core --Switch	*X*	*X*	
		X X		
			X	*X*

Para cualquiera de los casos presentados el servidor FreeNAC deberá responder de la misma manera ya que prácticamente todos los equipos de red y equipos finales deberán estar registrados en las tablas y en el caso de los switches, que todos tengan la misma dirección IP del servidor así como las VLAN's que hayan sido creadas.

4.2. Casos posibles

A continuación se presentan los resultados obtenidos durante el estudio con el servidor FreeNAC para los casos anteriormente mencionados y reflejados en las interfaces gráficas de usuario y Web.

4.2.1. Switch

En este caso se trabajó directamente la detección de los equipos a través de un switch, entre el servidor y los dispositivos finales como se muestra a continuación:

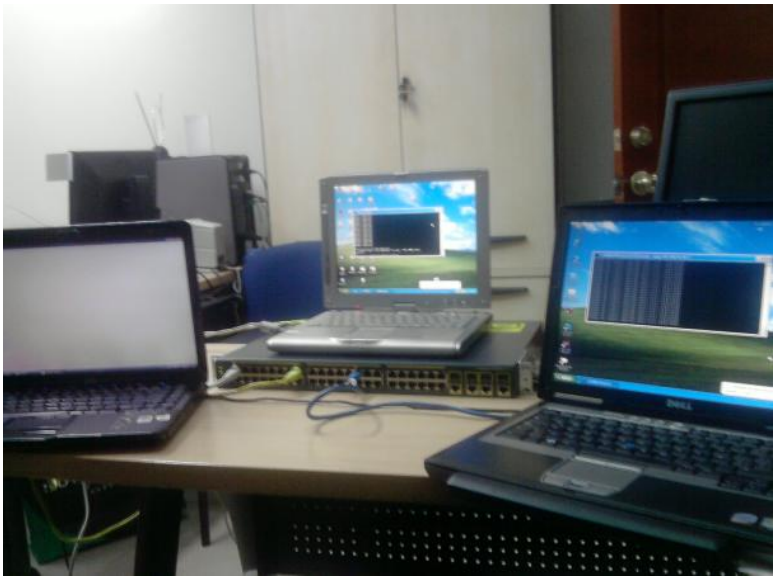


Figura 4.1. Equipos para detección de equipos utilizando un Switch CISCO

El momento de realizar el registro del equipo en la base de datos, previamente se debe establecer la dirección IP del equipo tomando en cuenta que este debe encontrarse dentro de la red y el servidor pueda devolver el requerimiento del mismo.

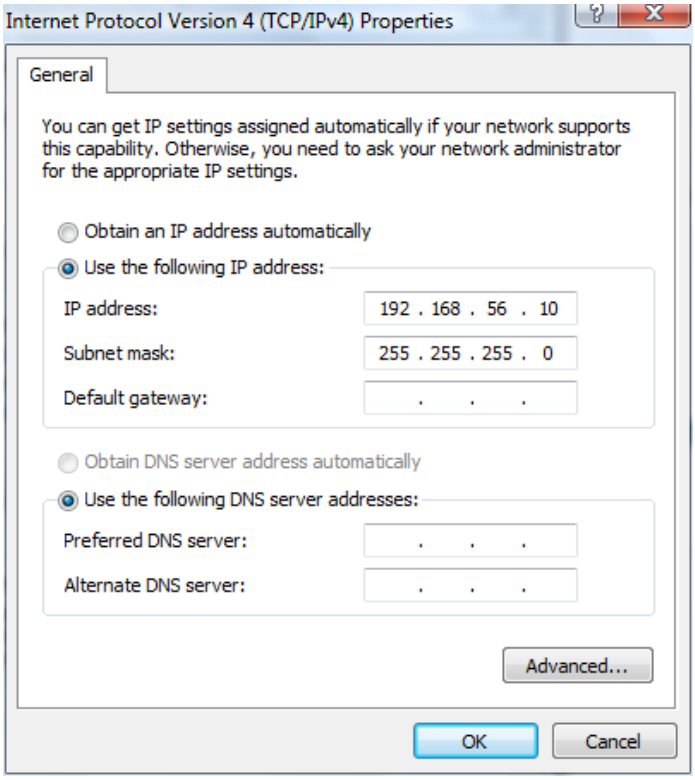


Figura 4.2. Registro dirección IP del equipo de usuario

Este proceso se lo realizará para todos los equipos que se desean registrar dentro de la base de datos del servidor para que puedan ser direccionados automáticamente a sus respectivas VLAN's.

El switch toma la dirección MAC del equipo y la envía hacia el servidor para que compare con la que ha sido registrada anteriormente con su VLAN correspondiente, mientras se lleva a cabo este proceso el puerto no se levantará hasta que entregue el resultado.

4.2.1.1. VLAN1 – VLAN2

Para este caso se trabajó con dos equipos que se encuentren registrados en la base de datos pero en VLAN's diferentes, en el caso de la Secretaría que los equipos se encuentran en diferentes direcciones.

El primer paso es registrar los equipos dentro del servidor FreeNAC como se muestra a continuación:

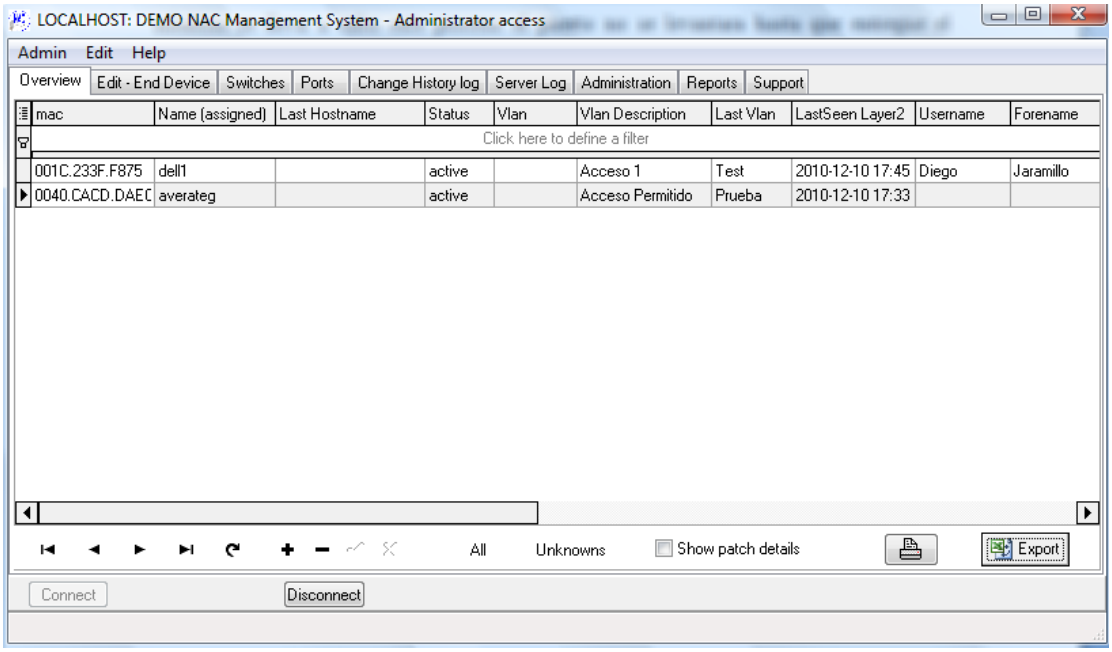


Figura 4.3. Registro de equipos en diferentes VLAN's

Luego de esto y haber configurado las direcciones IP en los mismos únicamente se procede a conectarlos al switch a cualquier puerto dinámico para esperar el resultado que entregue el servidor FreeNAC.

El servidor levantará el puerto y lo registrará con la VLAN correspondiente para cada uno de los equipos conectados como se muestra a continuación:

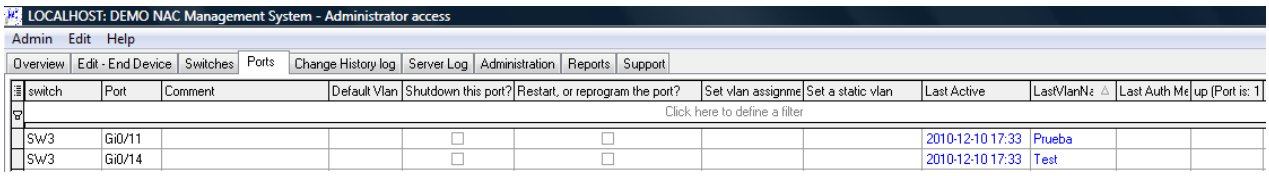


Figura 4.4. Detección de los equipos en el servidor FreeNAC

De igual manera se puede observar a través de la interfaz Web los reportes gráficos de los últimos 30 días conectados a los equipos de red, como los más representativos

tenemos los que son en función del switch y el número de dispositivos conectados al mismo:

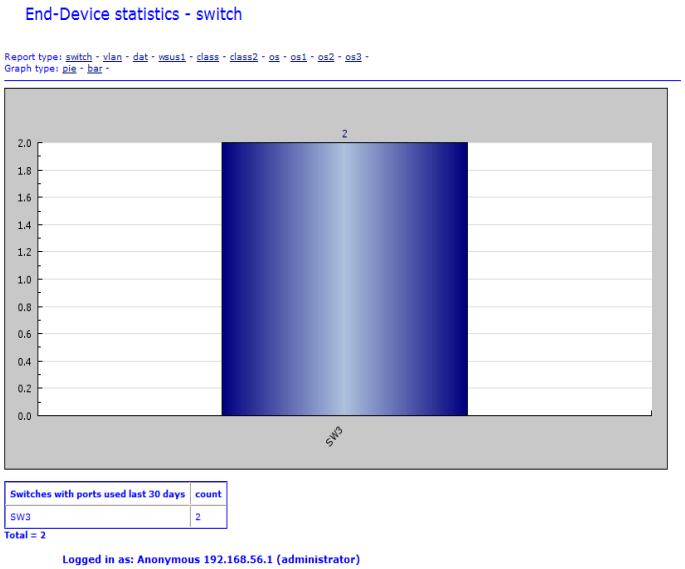


Figura 4.5. Gráfica interfaz Web (Switch – Dispositivos finales)

Igualmente se puede observar la gráfica en función de las VLAN's y el número de equipos que se han conectado a esta:

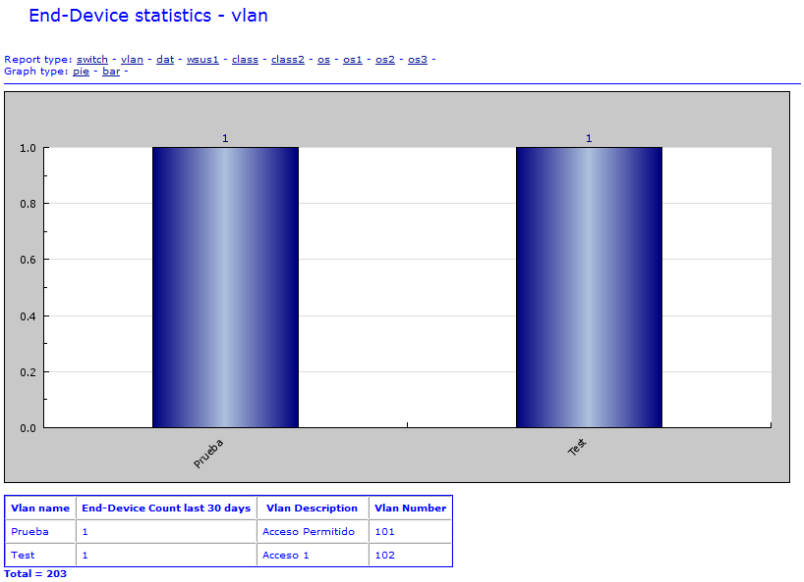


Figura 4.6. Gráfica interfaz Web (VLAN's – Dispositivos finales)

4.2.1.2. VLAN1 – VLAN1

Para este caso ahora se registró otro equipo que pertenezca a cualquiera de las dos VLAN's registradas anteriormente, en este caso se la registró en la VLAN con el nombre 'Acceso 1', como se muestra en la siguiente imagen:

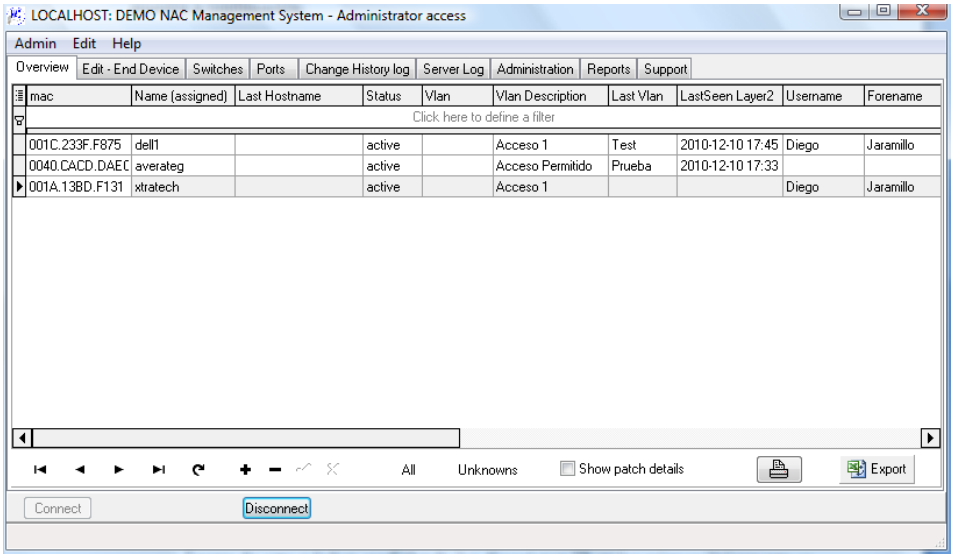


Figura 4.7. Registro de usuario a la VLAN (Acceso 1)

Ahora se conecta el equipo igualmente a cualquiera de los puertos del switch y esperar que el servidor sea el encargado de levantar el puerto y direccionarlo a su VLAN correspondiente, si todos los parámetros fueron ingresados correctamente en la pestaña de puertos en la interfaz gráfica de usuario nos aparecerá lo siguiente:

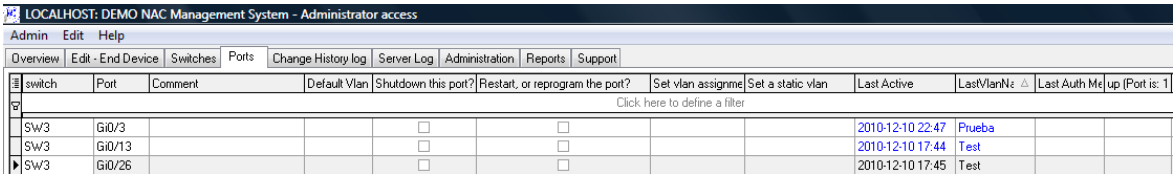


Figura 4.8. Detección del nuevo equipo en el servidor FreeNAC

Si se actualiza la interfaz Web nos deberá mostrar las gráficas con la nueva detección del equipo ingresado en la red:

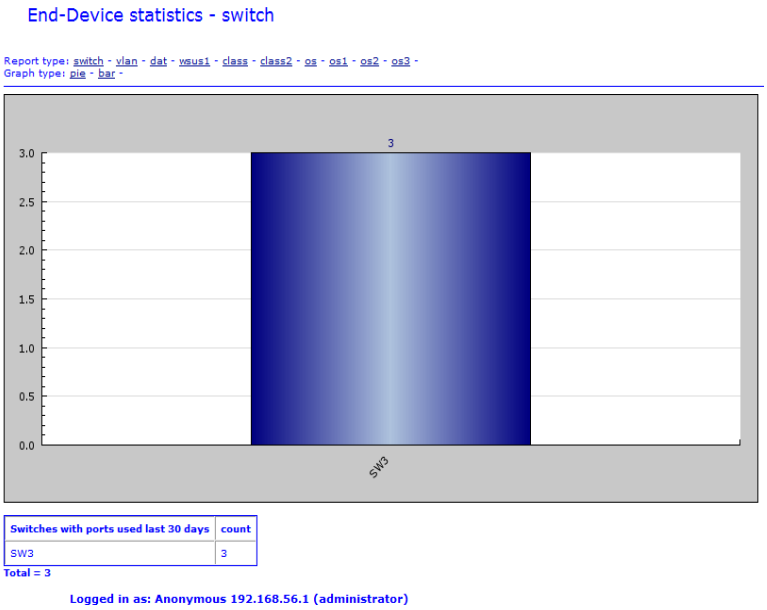


Figura 4.9. Gráfica interfaz Web (Switch – Dispositivos finales)

En relación al reporte de las VLAN's nos mostrará un incremento en la VLAN que se ha registrado el nuevo equipo en relación al caso anterior:

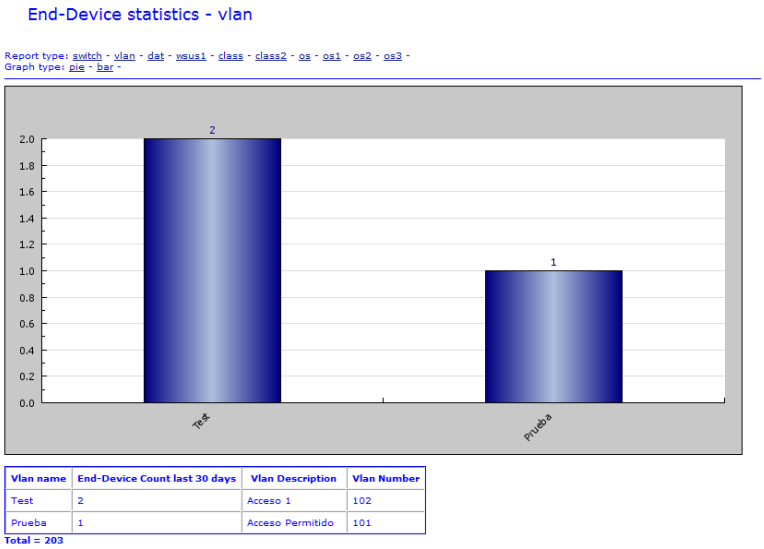


Figura 4.10. Gráfica interfaz Web (VLAN's – Dispositivos finales)

4.2.1.3. VLAN2 – Visitante

Para los usuarios externos a la Institución, se ha configurado para que al momento de que ingresen a la red sean direccionados a una VLAN donde tengan únicamente acceso a Internet, en este caso se lo hizo para la VLAN por defecto (VLAN 1).

De acuerdo a la política de uso establecida, indica que los equipos que se encuentren registrados en la base de datos sean direccionados a las VLAN's correspondientes, mientras que los equipos desconocidos lo harán a la que se haya indicado en el parámetro de la tabla de configuración **default_vlan**.

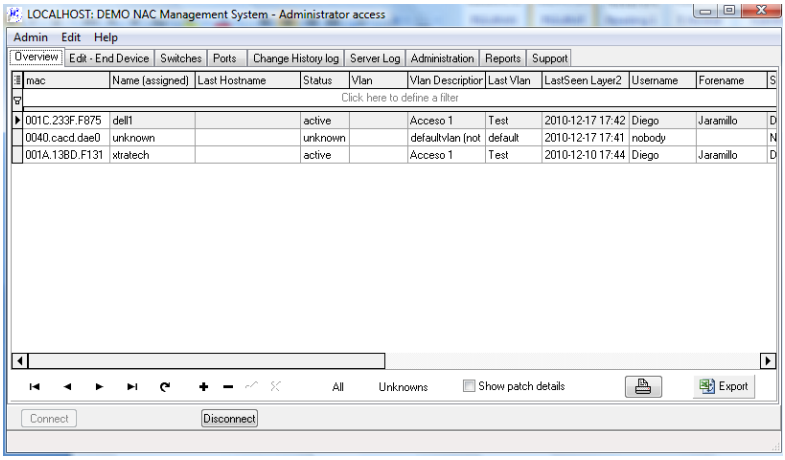


Figura 4.11. Detección del equipo desconocido en la tabla del servidor

Cuando un equipo se conecta, este siempre será registrado en la tabla de la interfaz gráfica de usuario como se muestra en la figura, en la pestaña **puertos** nos deberá aparecer lo siguiente:

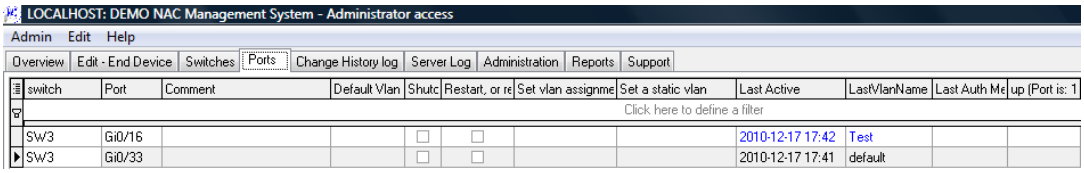


Figura 4.12. Registro del equipo desconocido a la VLAN por defecto

En la interfaz Web nos aparecerá la siguiente gráfica:

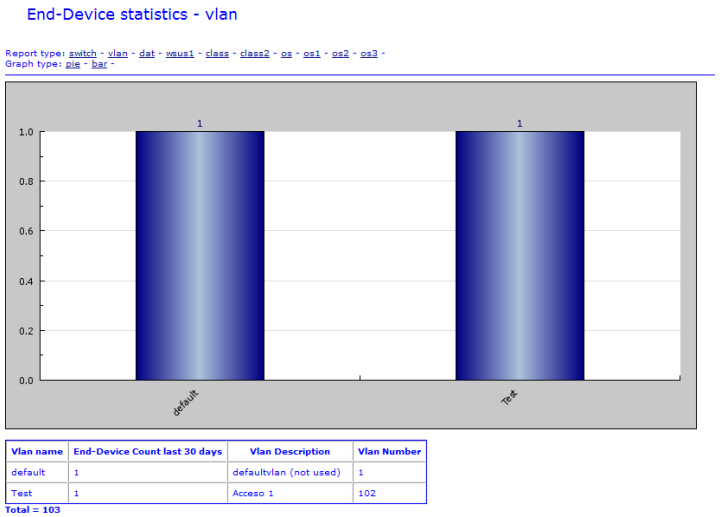


Figura 4.13. Gráfica interfaz Web (VLAN's – Dispositivos finales)

4.2.2. Switch – Core

En esta etapa se ha implementado el dispositivo de capa 3, la cual será la que recepte todas las solicitudes de los switches, a continuación se muestra el diseño de este caso:

Figura 4.14. Equipos para detección de equipos utilizando un Switch y un Core CISCO

4.2.2.1. VLAN1 – VLAN 2

La detección es la misma que en el caso anterior, se debe tomar en cuenta la configuración del Core en los puertos como troncales y el que se dirige hacia el servidor, tanto para la VLAN de administración como para las de ubicación de los dispositivos finales:

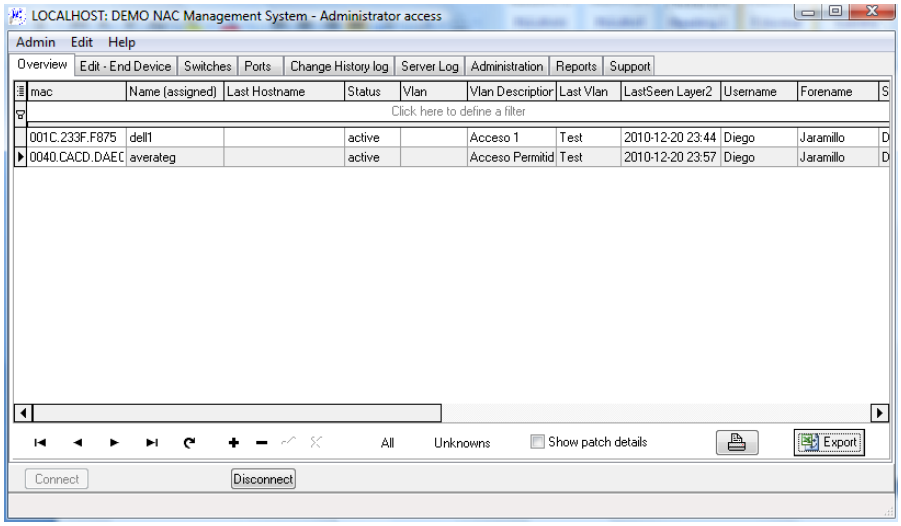


Figura 4.15. Detección de los equipos en el mismo switch conectados al Router

En la interfaz nos desplegará el mismo resultado que el caso anterior, ya que únicamente esta interfaz nos presenta las gráficas en relación al Switch y no al Router.

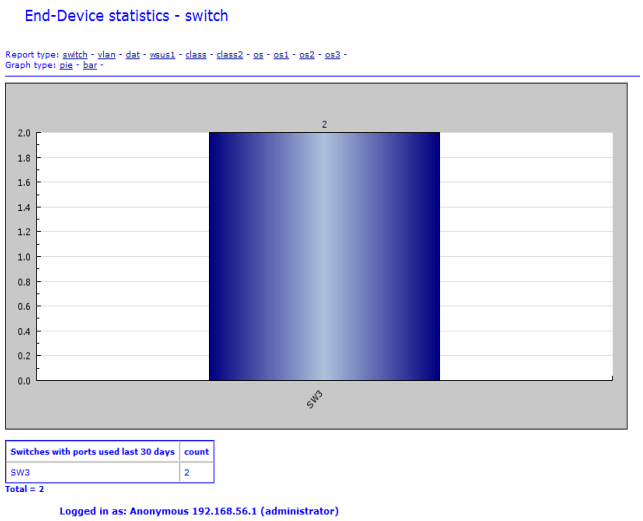


Figura 4.16. Gráfica interfaz Web (Switch – Dispositivos finales)

El único cambio realizado para este caso es la implementación del Core a la red y que será la encargada de la administración de todas las peticiones que realicen todos los switches hacia el servidor FreeNAC.

En el caso del gráfico con respecto a las VLAN´s y los dispositivos finales será el siguiente:

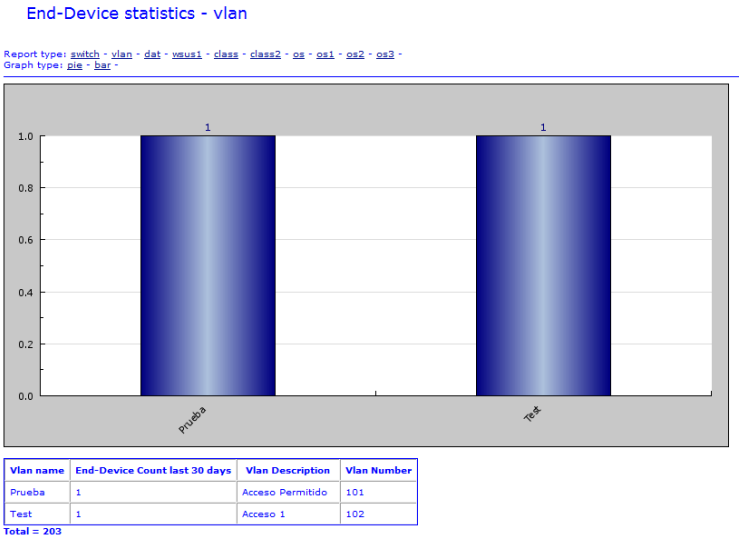


Figura 4.17. Gráfica interfaz Web (VLAN's – Dispositivos finales)

4.2.2.2. VLAN1 – VLAN 1

Para los equipos que se encuentran dentro de la misma VLAN de igual manera que para el caso anterior, estos se mostrarán en la pestaña **Ports** como se muestra en la figura:

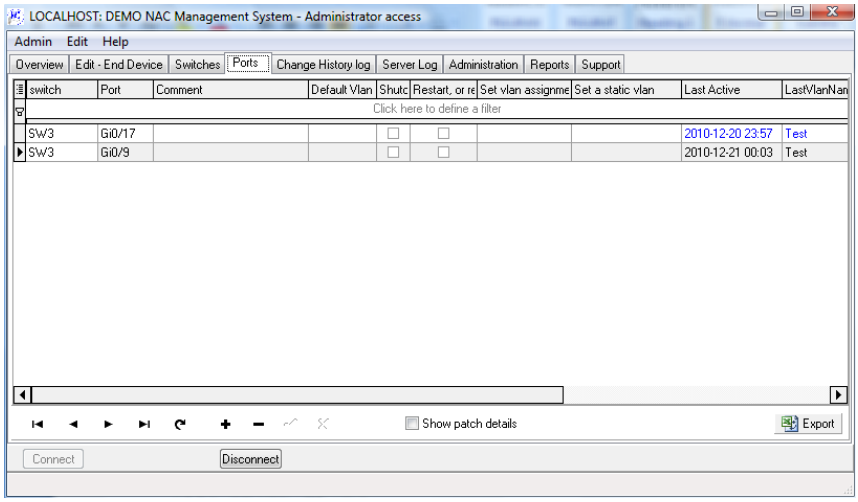


Figura 4.18. Detección de los equipos en el mismo Switch conectados al Router

En la interfaz Web nos mostrará los siguientes resultados:

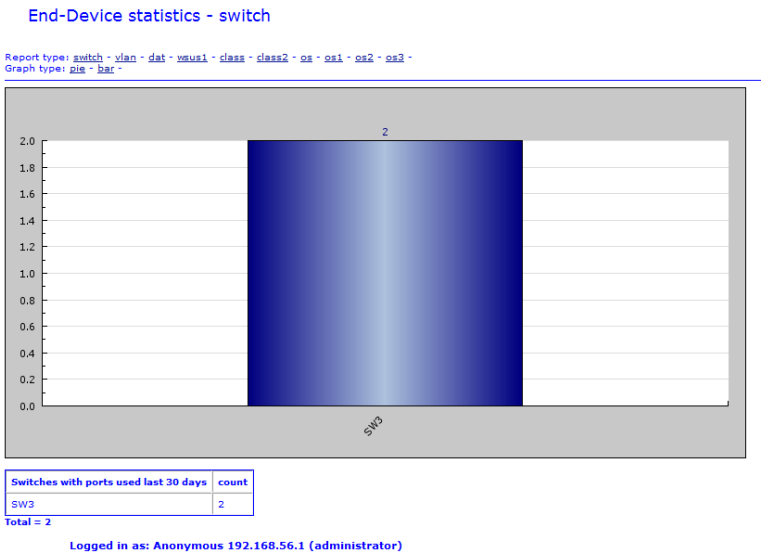


Figura 4.19. Gráfica interfaz Web (Switch – Dispositivos finales)

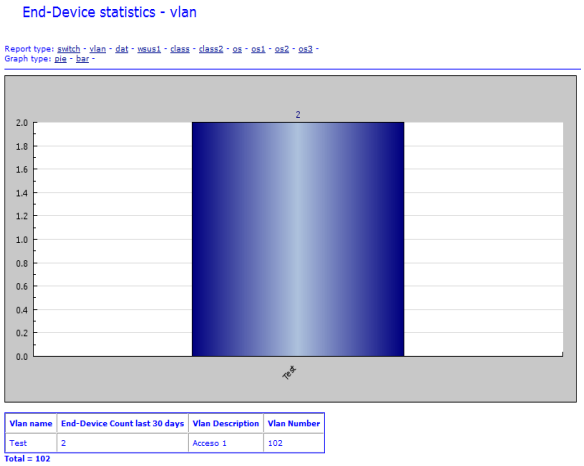


Figura 4.20. Gráfica interfaz Web (VLAN's – Dispositivos finales)

4.2.2.3. VLAN2 – Visitante

La lógica no cambia con la implementación del Core, para cuando un visitante se conecta a la red más allá del puerto que sea, en la siguiente gráfica se muestra la conexión de un equipo registrado en la base de datos y de un visitante que se han conectado en el mismo Switch:

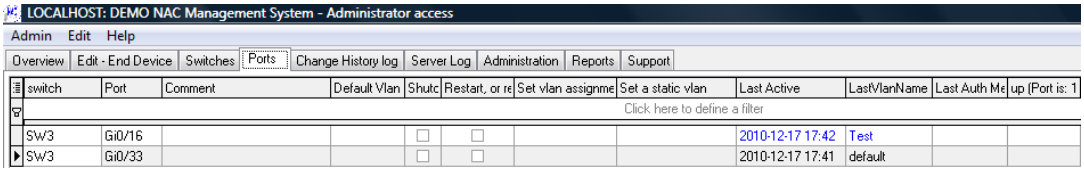


Figura 4.21. Detección de un equipo registrado y un desconocido en el servidor

En las gráficas de la interfaz Web veremos lo siguiente:

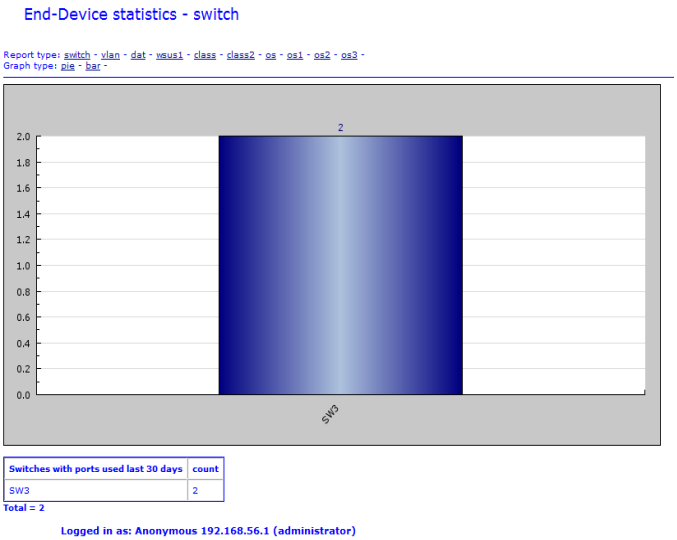


Figura 4.22. Gráfica interfaz Web (Switch – Dispositivos finales)

La gráfica de las VLAN´s respecto a los dispositivos finales no mostrará ningún cambio respecto a los casos anteriores ya que la topología es la única que se ha modificado y ambos equipos se conectaron al mismo dispositivo:

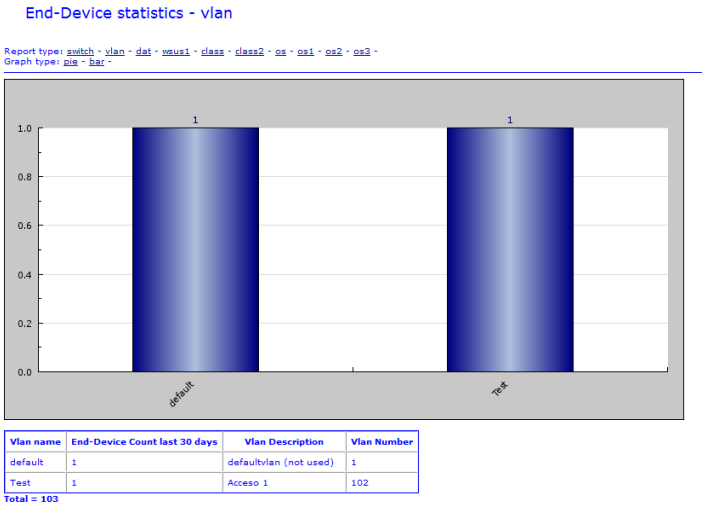


Figura 4.23. Gráfica interfaz Web (VLAN's – Dispositivos finales)

4.2.3. Switch – Core - Switch

Finalmente para este caso se implementaron 2 switches que fueron previamente registrados en el servidor FreeNAC y que poseen la misma configuración a diferencia de su nombre y dirección IP la cual deberá estar dentro de la red:

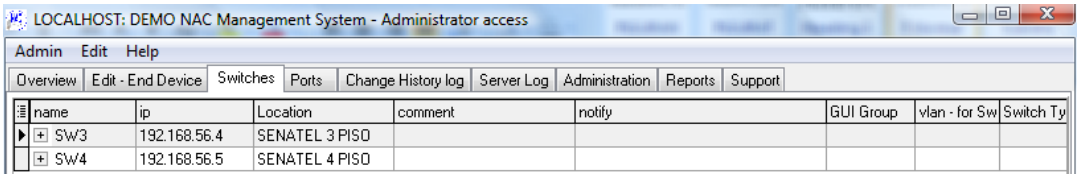


Figura 4.24. Registro nuevo Switch en el servidor FreeNAC

Los resultados serán exactamente los mismos a los que se presentaron en los casos anteriores, la diferencia se muestra en las interfaces gráficas y Web para cada una de las posibilidades.

A continuación se muestra el esquema que se utilizó para realizar este caso:

Figura 4.25. Equipos para detección de equipos utilizando dos Switch y un Core CISCO

4.2.3.1. VLAN1 – VLAN2

El procedimiento de prueba es el mismo utilizado en los casos anteriores, se registraron 2 equipos que se encuentren en VLAN´s diferentes y a su vez se conectaron en Switches diferentes, al final si se encuentran registrados deberán ser direccionados automáticamente a las VLAN´s correspondientes.

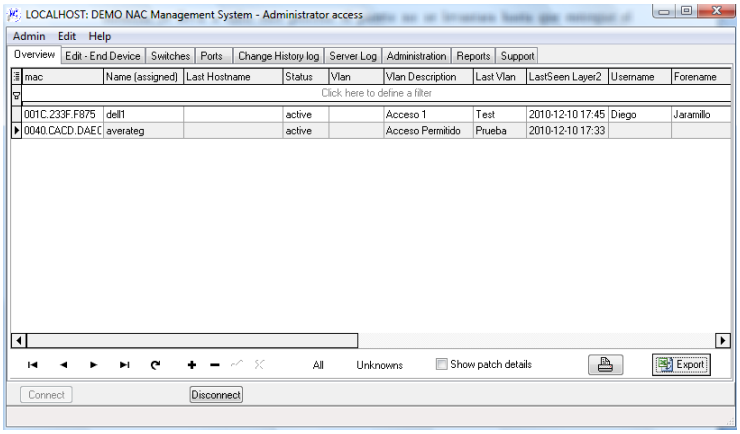


Figura 4.26. Registro de los equipos en VLAN's diferentes

Ahora en la interfaz Web, como se ha registrado la integración de un nuevo Switch a la red, el servidor FreeNAC lo registra y envía a las estadísticas la inclusión del nuevo equipo:

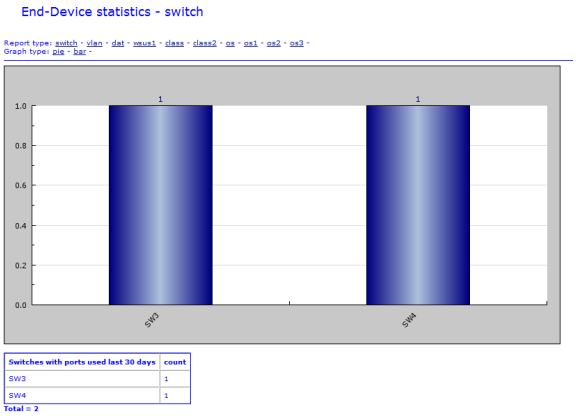


Figura 4.27. Gráfica interfaz Web (Switch – Dispositivos finales)

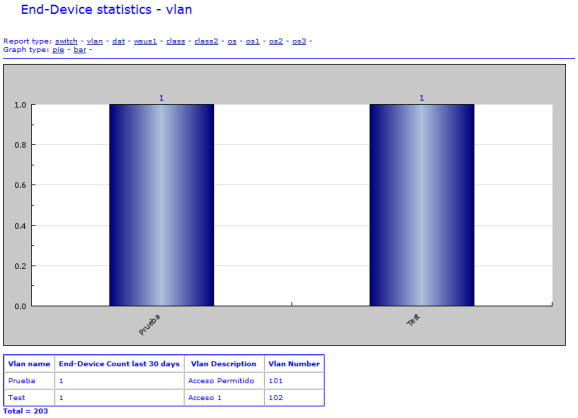


Figura 4.28. Gráfica interfaz Web (VLAN's – Dispositivos finales)

4.2.3.2. VLAN1 – VLAN1

La diferencia que se puede observar es que los equipos que se encuentran en la misma VLAN se encuentran en switches diferentes, si observamos desde la interfaz gráfica de usuario GUI observaremos lo siguiente:

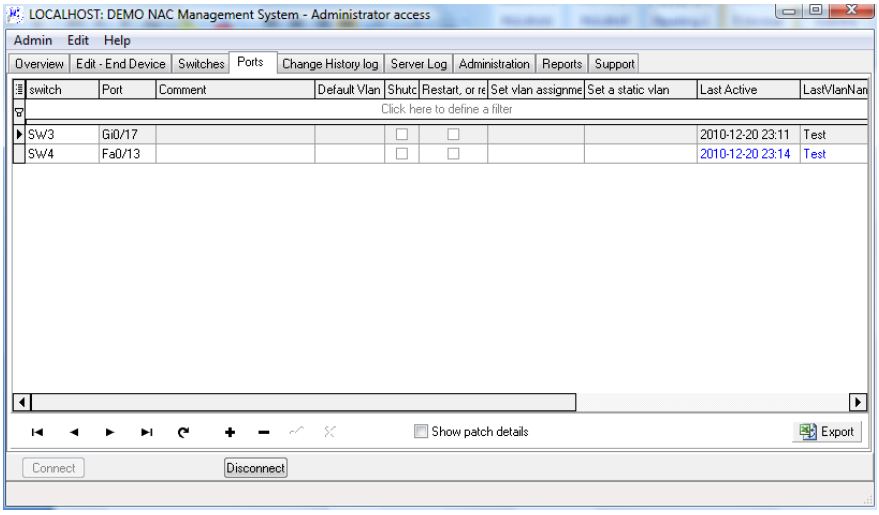


Figura 4.29. Detección de los equipos en diferentes switches

En la interfaz Web se observara lo siguiente:

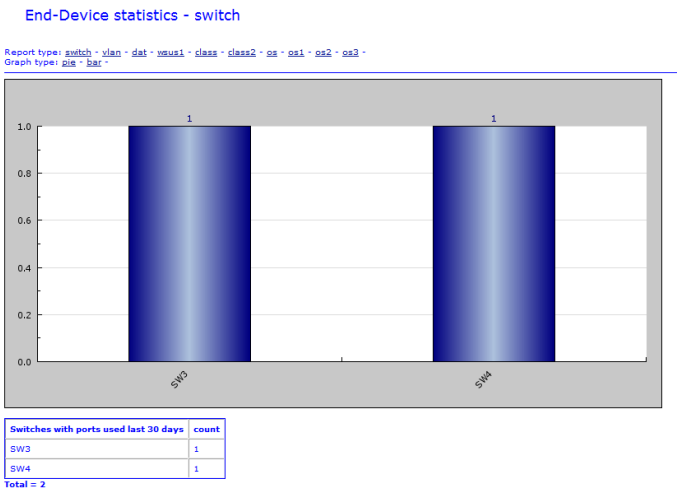


Figura 4.30. Gráfica interfaz Web (Switch – Dispositivos finales)

Y en función de las VLAN's con los dispositivos finales:

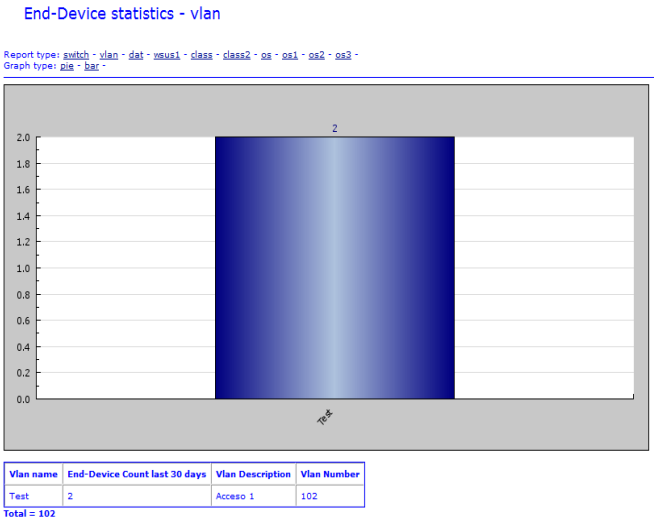


Figura 4.31. Gráfica interfaz Web (VLAN's – Dispositivos finales)

4.2.3.3. VLAN2 – Visitante

Finalmente, se prueba con un equipo que no se encuentre registrado en la red y que haya sido conectado en el otro Switch, en la pestaña **Ports** como se muestra en la gráfica indica el puerto, el Switch y la VLAN que ha sido asignada para el dispositivo final que se ha conectado en el mismo:

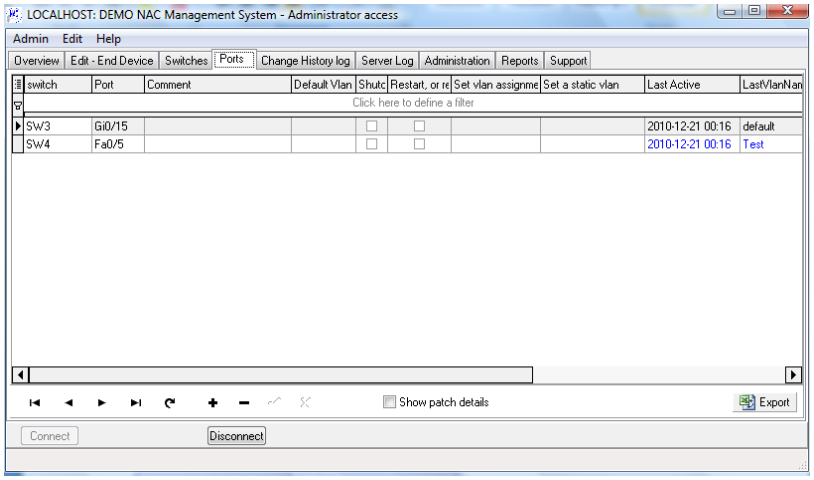


Figura 4.32. Detección de equipo registrado y visitante en Switches diferentes

Así mismo, en la interfaz Web se muestran los resultados en función del Switch así como de la VLAN correspondiente:

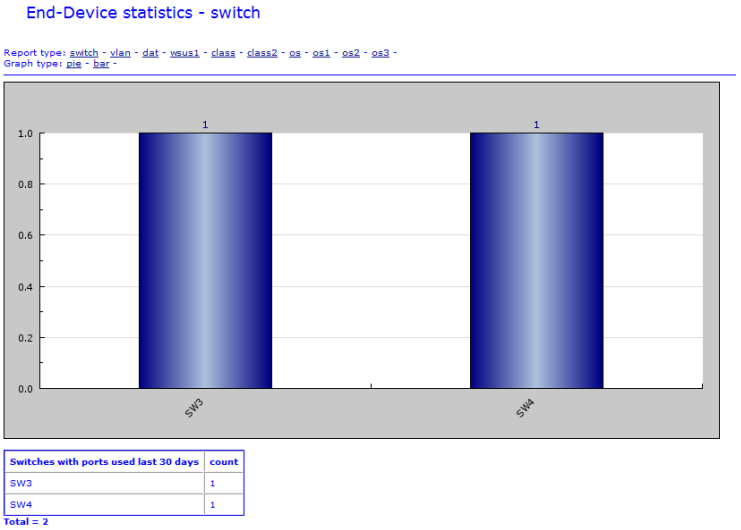


Figura 4.33. Gráfica interfaz Web (Switch – Dispositivos finales)

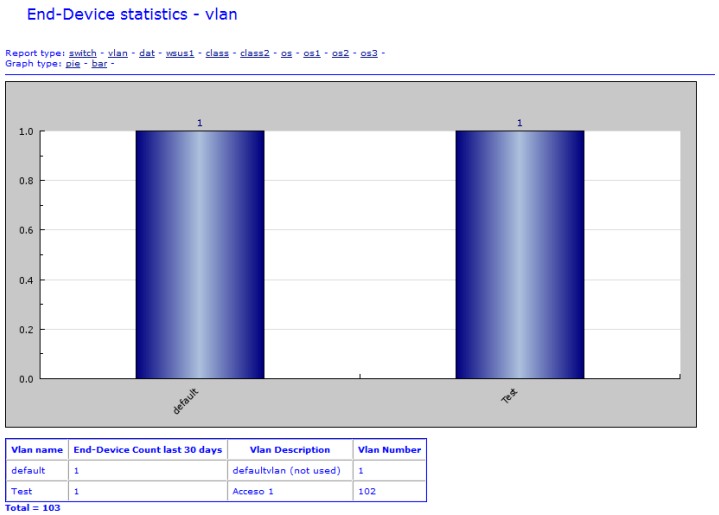


Figura 4.34. Gráfica interfaz Web (VLAN's – Dispositivos finales)

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Se dio un resultado óptimo para el diseño de una red inteligente para la Secretaría Nacional de Telecomunicaciones en los posibles casos presentados, con esto se logró optimizar los recursos de los equipos así como de la seguridad de posibles ataques, además de presentar la ventaja de que este programa es libre costo y no implica la adquisición de nuevos equipos.

De acuerdo al estudio realizado, se cumplió con el objetivo de diseñar una red para cumplir todos los parámetros de seguridad, esto se lo hace con el fin de preservar la información fuera de los peligros de posibles ataques y de optimizar la gestión de administración de la misma de una manera más eficiente que la utilizada actualmente.

El tiempo que tarda el servidor en tomar las decisiones para direccionar a las VLAN's establecidas, no es constante, este dependerá de las características de los equipos y de cómo estos se encuentren configurados, además de que si existen varios usuarios registrados en la tabla de comparación dentro del servidor, este tardara más en entregar el resultado y la respuesta a la solicitud del switch que la envió.

El llevar a cabo la implementación de VLAN's dinámicas demuestra que ya no es necesario dimensionar físicamente la red, esto quiere decir que ya no se debe definir un número predeterminado de puertos en el equipo para cada una de las direcciones sino que FreeNAC se encarga de hacerlo automáticamente de acuerdo a la dirección física del

equipo, sin importar donde se conecte, tomando en cuenta los parámetros que hayan sido configurados previamente dentro del servidor.

De acuerdo al esquema que se planteó en un inicio, se debió tomar en cuenta el tráfico que va a cruzar por cada uno de los puertos, para el caso de los switches únicamente el puerto de administración será troncal ya que va a manejar el tráfico de múltiples VLAN's, mientras que los puertos dinámicos serán de acceso ya que solo manejaran el de la VLAN que le sea asignada. El Core en cambio como es el encargado de recibir todas solicitudes de los switches, todos sus puertos inclusive el que se encuentra conectado al servidor deben ser troncales, ya que a todo momento está enviando el tráfico hacia todos los funcionarios de la Institución.

5.2. Recomendaciones

El momento de llevar este estudio hacia la implementación es aconsejable implementar en lo que refiere al servidor directamente en la plataforma Linux y no a través de una maquina virtual, esto con el fin de que no existan inconvenientes de virus que podrían bajar el rendimiento en lo que respecta a las consultas VMPS, y la interfaz gráfica hacerla desde el ordenador del administrador donde este sea el único que tenga acceso a toda la red.

En la etapa de la configuración de los equipos, para hacerlo de una forma más eficiente se puede recurrir a la utilización de un servidor TFTP, esto servirá para poder guardar la configuración que se realice en un switch y cargarlo en todos los que sean necesarios, como todos los switches van a tener la misma configuración a excepción de su nombre y dirección IP, conlleva a un gran ahorro de tiempo el momento de la implementación.

Para el caso de los equipos que no se encuentren registrados dentro del servidor FreeNAC, se recomienda habilitar un servidor DHCP con un rango considerable de direcciones en el que se deba tomar en cuenta el número de puertos libres en toda la Institución para acceder al servicio de Internet o el que el administrador así lo decida.

Hay que tomar en cuenta también la versión del software FreeNAC con la que se está trabajando, la versión gratuita no cuenta con ciertos parámetros necesarios para conectarse con la interfaz gráfica de usuario, por lo que se debe "migrar" hacia la siguiente versión, esto es descargar el archivo que posee los componentes faltantes para establecer la conexión.

De acuerdo al diseño de la red que se tenga que realizar y tomando en cuenta el número de dispositivos y de equipos de red, FreeNAC está provisto de la posibilidad de implementar servidores VMPS secundarios en el caso de que el servidor principal colapse o presente algún inconveniente inesperado, en el caso de llegarse a dar, FreeNAC automáticamente levanta este servidor para que siga ejecutando las mismas tareas que el servidor primario.

Cada vez que se realicen cambios de acuerdo a los requerimientos que solicite el administrador; ya sea a través de la interfaz gráfica de usuario como en el servidor por línea de comandos se deben reiniciar los demonios (daemons) para que los cambios que se hayan realizado, se actualicen dentro del programa FreeNAC.

Cuando se está trabajando en la etapa de configuración de los equipos de red, y realizando el establecimiento de las VLAN's, hay que tomar en cuenta que existe una VLAN única para la administración de los equipos, es por esta por donde se envían y reciben las solicitudes de asignación, es muy diferente a las VLAN's de cada una de las Direcciones en donde se ubican los equipos de los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

[1] Clasificación de las redes, http://www.slideshare.net/noebiolatto/clasificacin-de-las-redes-presentation

[2] Componentes de una red, http://www.angelfire.com/mi2/Redes/componentes.html

[3] CISCO, Modulo 3, Conmutación y conexión inalámbrica de LAN, Parte 1.1.1. Modelo de Redes Jerárquicas, págs. 2-4

[4] CISCO, Modulo 3, Conmutación y conexión inalámbrica de LAN, Parte 1.1.2. Modelo de Redes Jerárquicas, pág. 7

[5] Redes de Comunicación, http://www.infoab.uclm.es/labelec/Solar/Comunicacion/Redes/index_files/Router.htm

[6] Descripción de la tabla de enrutamiento IP, Microsoft, http://technet.microsoft.com/es-es/library/cc787509(WS.10).aspx

[7] CISCO, Modulo 2, Conceptos y protocolos de enrutamiento, Parte 1.3.1. Introducción de la tabla de enrutamiento, págs. 21-24

[8] Redes de Comunicación, http://www.infoab.uclm.es/labelec/Solar/Comunicacion/Redes/index_files/Switch.htm

[9] CISCO, Modulo 2, Conceptos y protocolos de enrutamiento, Parte 1.2.1. Consideraciones para los switches en redes jerárquicas, págs. 13-17

[10] Alonso, David, 802.3 Ethernet Redes de Área Local Administrador de Sistemas informáticos, http://personal.telefonica.terra.es/web/dmartin/ethnet.pdf, 25/01/2004

[11] Yepes, Isabel, Trama Ethernet, diapositiva 3: Estructura de la dirección MAC Ethernet, http://www.slideshare.net/iyepes/capitulo-93, 10/02/2010

[12] Redes Virtuales VLAN's, http://www.textoscientificos.com/redes/redes-virtuales

[13] Cáceres, Christian, Encriptación de datos, http://www.slideshare.net/christianikolai/encriptación-de-datos-una-vista-general, 28/12/2007

[14] CISCO, Modulo 4, Acceso a la WAN, Capítulo IV: Seguridad de la red, págs. 139-140

[15] Vásquez, Javier, Amenazas y Riesgos de Seguridad en el mundo empresarial, Global Crossing, 23/04/2010

[16] Información proporcionada por la Secretaría Nacional de Telecomunicaciones SENATEL, 25/08/2010

[17] Aguilar, Carlos, Poma, Víctor, Asignación y Administración de VLAN's dinámicas, http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo-tecnico_asignacion-y-administracion-de-vlans-dinamicas.pdf, 20/09/2010

[18] FreeNAC, Características, http://freenacweb.vptt.ch/es/products/features, 2007-2010

[19] FreeNAC, La solución FreeNAC, http://freenacweb.vptt.ch/es/products/features, 2007,2010

[20] FreeNAC, Guía de instalación FreeNAC, http://freenac.net/en/installguide, 2007,2010

ANEXO 1

CONFIGURACION DE LOS EQUIPOS CISCO UTILIZADOS (SWITCHES - ROUTER)

SWITCHES:

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW4
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no ip domain-lookup
!
vmps reconfirm 120
vmps retry 5
vmps server 192.168.56.2 primary
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode trunk
!
interface FastEthernet0/2 - FastEthernet0/44
 switchport access vlan dynamic
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan100
 ip address 192.168.56.5 255.255.255.0
 no ip route-cache
!
```

```
ip http server
!
control-plane
!

line con 0
line vty 0 4
 login
line vty 5 15
 login
!
end
```

Esta configuración se realizo en un Switch 2960, que a diferencia del Switch 2960G, sus puertos son FastEthernet mientras que para el otro son GigabitEthernet, además del número de puertos que posea cada uno.

La primordial diferencia como se explico anteriormente, es en cambiar el nombre del equipo y la dirección que posea dentro de la red, estos parámetros tienen que ser exactamente los mismos con los que fueron registrados a través de la interfaz gráfica de usuario para que pueda enviar y recibir las solicitudes de VMPS.

```
hostname: nombre del switch

interface Vlan100
ip address dirección IP y mascara
```

ROUTER:

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 100
 no ip address
!
interface FastEthernet0/2 - FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
!
interface Vlan1
 no ip address
!
interface Vlan100
 ip address 192.168.56.3 255.255.255.0
!
ip classless
ip http server
!
line con 0
line vty 5 15
!
end
```

En la página de configuración de configuración de FreeNAC, únicamente está disponible la integración del Router desde la interfaz gráfica de usuario, de igual manera que en los switches aquí también se debe crear la VLAN de administración en donde se establecerá la dirección IP del Router y asociarle a uno de los puertos el que será se conectara con el servidor VMPS de FreeNAC.

ANEXO 2

PROBLEMAS DE CONFIGURACION

Cuando el administrador está configurando todas las variables dentro del servidor así como en la interfaz gráfica de usuario, en algún momento puede establecer valores que FreeNAC no interprete como correctos y no permita establecer la comunicación correcta con la interfaz de Windows, durante este estudio se dieron múltiples errores los cuales tuvieron que ir siendo corregidos conforme se fue avanzando en la investigación.

A continuación se muestran los inconvenientes presentados durante la elaboración de la red inteligente para la Secretaría Nacional de Telecomunicaciones:

- Acceso denegado root
- Columna desconocida
- Error del dominio de Windows
- Puertos bloqueados para equipos desconocidos
- Reinicio de demonios

1. Acceso denegado para el usuario 'root'

El momento de estarlo realizando la configuración del servidor mediante la línea de comandos, como se indico anteriormente para poder realizar cualquier tipo de cambio, únicamente se lo hace mediante el administrador de Linux **root.**

Posiblemente, cuando se debe indicar en la interfaz gráfica de usuario, quien está permitido a ingresar y se lo haga para este usuario. Cuando intentamos conectarnos a la base de datos, nos puede presentar el siguiente error:

ERROR 1045: Access denied for user: 'root@localhost' (Using Password: Yes)

Después de haber realizado varias pruebas, se descubrió que FreeNAC como defecto viene configurado únicamente para acceder al usuario **inventwrite** para acceder, por lo que para que no exista este problema en primer lugar a través de la interfaz gráfica de usuario cuando se encripta la contraseña y el usuario se lo debe realizar con este nombre

y de igual manera en el archivo de configuración **config.inc** poner este nombre y contraseña ya que es este el que compara con el que se configuro en la interfaz gráfica de usuario.

2. Columna desconocida en la lista de la base de datos

Si la interfaz gráfica de Windows no detecta ningún problema de restricciones de usuario, puede mostrarnos un problema en la base de datos, que no exista un campo o alguna variable que el GUI necesita para trabajar.

La versión con la que se trabajó para este proyecto de FreeNAC es la 3.0.2 mientras que la interfaz de usuario viene con nuevos parámetros que en esta versión no se han implementado, si todo está correctamente configurado es muy probable que nos salga el siguiente error:

#42S22 Unknown Column 'switch.switch_type' in 'field_list', error code 1054

Si en el servidor dentro de la base de datos se revisa la tabla **switch** para revisar todos los campos, nos encontraremos que esta columna no se encuentra en ella por lo que se debe agregarla.

De acuerdo a los creadores de este programa, indican que próximamente nos ofrecerán la nueva versión de FreeNAC, correspondiente a la 3.0.3 donde no existirá este inconveniente, pero mientras tanto el administrador tendrá que ingresarla manualmente para evitarla para poder trabajar normalmente. Esto se lo puede llevar a cabo directamente mediante línea de comandos SQL en el servidor para añadir una columna mediante el siguiente comando:

```
opennac> ALTER TABLE switch
->ADD switch_type TINYINT (3);
```

Ahora también existe un archivo para "migrar" de la versión 3.0.2 a 3.0.3 que contiene todos los parámetros para trabajar sin ningún problema, es recomendable descargar este archivo y revisar todo lo necesario. A continuación se muestra todo lo que presenta este archivo y puedan realizar la migración:

```
INSERT INTO `config` SET `type`='integer',
`name`='report_old_users_kill_days', `value`='0', `comment`='Kill systems
belonging to users who haven\'t been seen in the directory for longer
than X days';
UPDATE `config` SET `value`='-A -sS -n -P0' WHERE `name`='nmap_flags';

-- New config variable
INSERT INTO `config` SET `type`='boolean', `name`='check_clear_mac',
`value`='false', `comment`='Enable the clear_mac function, for CISCO IOS.
Replaces port_restart no newer IOS versions';

-- Systems table
ALTER TABLE `systems` ADD COLUMN `clear_mac` TINYINT UNSIGNED NOT NULL
DEFAULT '0';
ALTER TABLE `systems` ADD KEY `clear_mac` (`clear_mac`);

-- Switch table
ALTER TABLE `switch` ADD COLUMN `switch_type` TINYINT UNSIGNED NOT NULL
DEFAULT '0';
ALTER TABLE `switch` ADD KEY `switch_type` (`switch_type`);
```

3. Error del dominio de Windows

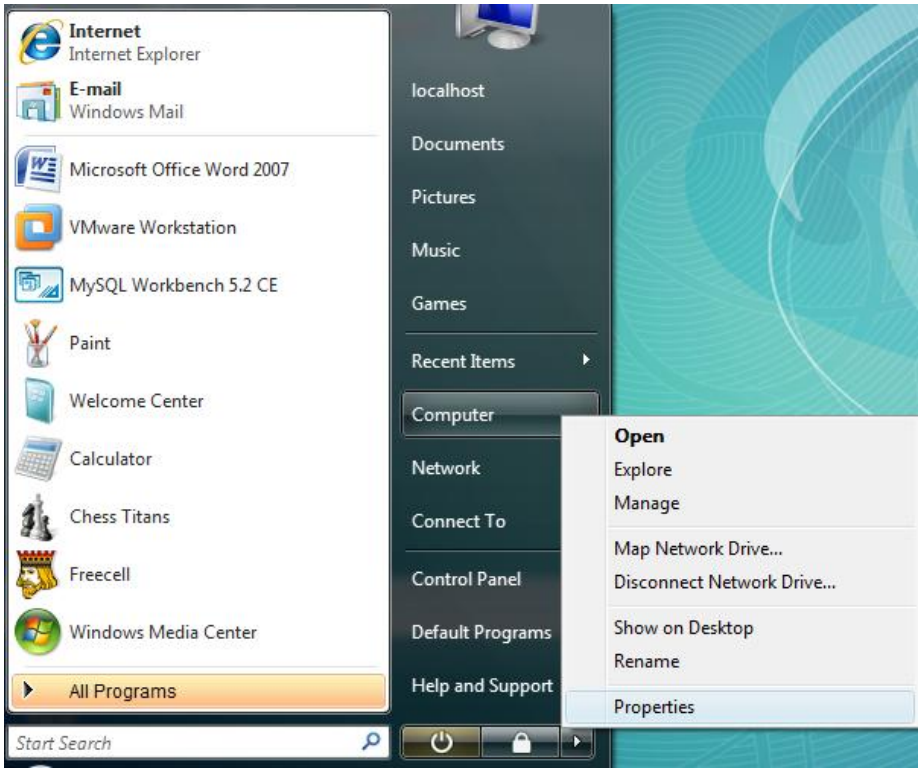
Como se explicó anteriormente, FreeNAC toma el domino del sistema operativo de Windows y del usuario registrado para conectarse, cuando se están dando los permisos de acceso en la base de datos al usuario, se lo hace con el dominio del usuario:

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

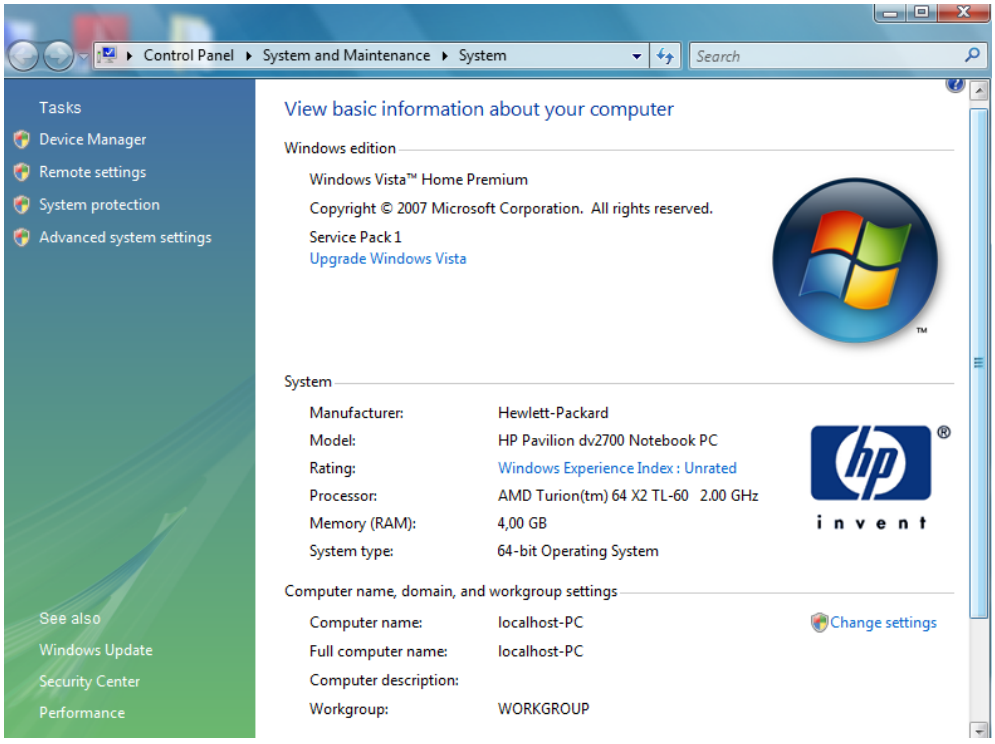
Por lo que el dominio de Windows también tiene que ser el mismo para que el momento de conectarse no nos presente el siguiente error:

"username" on "workstation" is not allowed to use NAC, the Windows domain is "domain" and must be "domain"

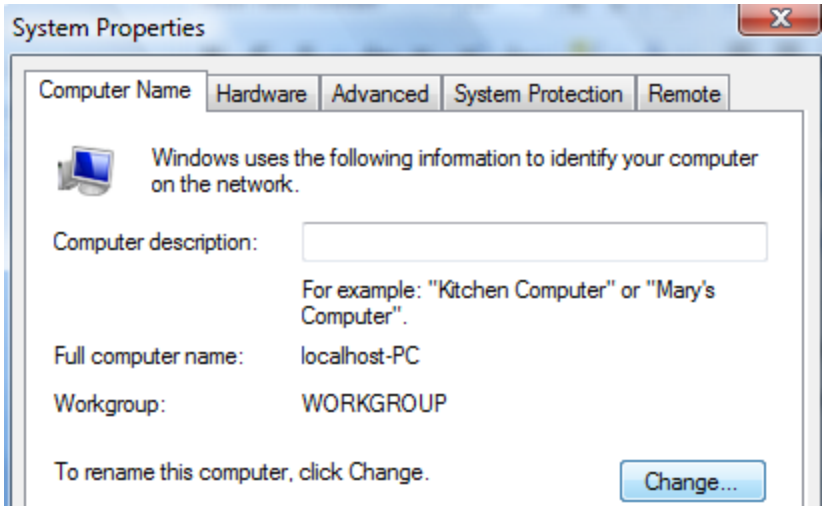
Para cambiar el dominio en Windows se deberá hacer lo siguiente:



Luego aparecerá la siguiente ventana:



Y en donde dice "Change settings" cambiamos el nombre del equipo con el del dominio que se estableció en el servidor:



Con este cambio ahora el servidor tomara el nuevo nombre de dominio y compararlo, si reconoce que ambos tienen el mismo nombre permitirá el acceso a la base de datos sin ningún problema.

4. Puertos bloqueados para equipos desconocidos

FreeNAC por defecto para los equipos desconocidos, bloquea los puertos ya que estos no se encuentran registrados en la base de datos, para ello hay que establecer los parámetros dentro de la interfaz gráfica de usuario y de las políticas de uso dentro del servidor.

FreeNAC posee múltiples políticas de uso de acuerdo a las necesidades que así el administrador lo requiera, y dentro de la GUI ajustar los parámetros para visitantes y desconocidos en el caso de enviarlos a una VLAN temporal o denegar el acceso.

En el capítulo III del presente proyecto se indica la inclusión de la función **clear_mac** la cual elimina la dirección MAC en el switch del equipo no registrado para evitar el bloqueo del puerto. Esta función es agregada el momento que se realiza la migración a la versión 3.0.3 que fue explicada anteriormente.

Otro parámetro importante es el momento de definir en la pestana de administración del GUI en la tabla de configuración a las VLAN's que se van a enviar a los equipos desconocidos, hay que tomar en cuenta que el valor que se ingresa en la variable no es el número de la VLAN, sino el del **índice** que posee, este valor se ajusta automáticamente el momento de la creación de las VLAN's.

5. Reinicio de demonios

Finalmente otro punto para no olvidar es el reiniciar los demonios, esto se lo hace con la finalidad de que cada vez que se realicen cambios en los parámetros de configuración o directamente en el servidor, estos sean actualizados y FreeNAC trabaje como se ha establecido.

Para reiniciar los demonios y en si todo el servidor, se debe ejecutar el siguiente comando:

reboot

Luego de esto se iniciara nuevamente el servidor, con los cambios realizados para trabajar normalmente.

FECHA DE ENTREGA

El presente proyecto de grado fue entregado en la fecha.

Sangolquí, _____ 2011

Realizado por:

_____

Diego Javier Jaramillo C.

_____

Ing. Gonzalo Olmedo

COORDINADOR INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES